Петропавлов Д.М. Повышение безопасности и эффективности: комплексный обзор корпоративных систем контроля и управления доступом // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 6(44) с. 80–87

Международный журнал информационных технологий и энергоэффективности

Сайт журнала: http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.09

ПОВЫШЕНИЕ БЕЗОПАСНОСТИ И ЭФФЕКТИВНОСТИ: КОМПЛЕКСНЫЙ ОБЗОР КОРПОРАТИВНЫХ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Петропавлов Д.М.
ФГБОУ ВО "МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Н.Э. БАУМАНА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)", Москва, Россия, (105005, город Москва, 2-Я Бауманская ул, д. 5 стр. 1), e-mail: petropavlov.deniz@yandex.ru

В статье исследуется пересечение корпоративных систем контроля и управления доступом (СКУД) и систем учета рабочего времени (СУРВ) в современных организациях. Начиная с подробного введения, рассматриваются приложения, состав и требования СКУД, подчеркивая ее роль в защите цифровых активов и регулировании доступа, дополнительно разъясняются сложные технологические аспекты и преимущества интеграции СУРВ, обеспечивая детальное понимание того, как эти системы взаимодействуют друг с другом для оптимизации управления персоналом и усиления мер безопасности. Подчеркивается динамичный характер этой интеграции, учитывая будущие соображения, и поощряет организации оставаться адаптивными в постоянно меняющемся технологическом ландшафте. Эта статья послужит руководством, предлагающим информацию для предприятий, стремящихся повысить уровень безопасности, оптимизировать управление персоналом и использовать перспективный подход к цифровой инфраструктуре.

Ключевые слова: Контроль доступа предприятия, системы управления, учет рабочего времени, аудит пользователей, биометрическая аутентификация, облачные решения, уровень безопасности, управление персоналом.

IMPROVING SECURITY AND EFFICIENCY: A COMPREHENSIVE REVIEW OF CORPORATE ACCESS CONTROL AND MANAGEMENT SYSTEMS

Petropavlov D.M.
BAUMAN MOSCOW STATE TECHNICAL UNIVERSITY (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (105005, Moscow, 2nd Baumanskaya str., 5, bldg. 1), e-mail: petropavlov.deniz@yandex.ru

This article explores the intersection of Enterprise Access Control and Management Systems (EACMS) and Time Tracking Systems (TTS) within the modern organizations. Beginning with an insightful introduction, the article navigates through the applications, composition, and requirements of EACMS, emphasizing its role in securing digital assets and regulating access, it further elucidates on the intricate technological aspects and benefits of integrating a TTS, providing a nuanced understanding of how these systems synergize to streamline workforce management and bolster security measures. It emphasizes the dynamic nature of this integration, addressing future considerations and encouraging organizations to remain adaptive in the ever-evolving technological landscape. This article serves as a guide, offering valuable insights for organizations seeking to fortify their security postures, streamline workforce management, and embrace a future-ready approach to digital infrastructure.

Keywords: Enterprise access control, management systems, time tracking, user auditing, biometric authentication, cloud-based solutions, security posture, workforce management.

Введение

В динамичной и цифровой среде современных предприятий первостепенную важность защиты конфиденциальной информации и управления доступом невозможно переоценить. По мере того, как организации преодолевают сложности взаимосвязанного мира, необходимость в надежном и комплексном решении для контроля и управления доступом становится насущной.

Наступление цифровой эпохи привело к беспрецедентному удобству и эффективности, но одновременно подвергло бизнес множеству киберугроз и проблем безопасности. Растущая зависимость от цифровых платформ для хранения данных, связи и совместной работы требует стратегического и комплексного подхода к контролю доступа. СКУД выступает в качестве стержня этой стратегии, являясь привратником в цифровую сферу организации, одновременно обеспечивая плавное и безопасное взаимодействие.[9]

Цель данной работы — предоставить дорожную карту для организаций, стремящихся улучшить свои меры безопасности и оптимизировать операционную эффективность за счет синергетического объединения систем управления персоналом.

1. Применение и структура системы контроля управления доступом

В сложной системе современного предприятия применение и структура корпоративных систем контроля и управления доступом образуют основу, на которой строится безопасная и эффективная организационная структура. Углубимся в многогранное применение СКУД, выходящее за традиционные границы контроля доступа, и раскроем сложную структуру, определяющую ее функциональность в корпоративной экосистеме.

1.1. Применение

Роль СКУД выходит далеко за рамки простого регулирования физического доступа к зданиям или цифровым системам. В современной динамичной бизнес-среде СКУД служит комплексным решением для управления идентификацией, обеспечивает детальный подход к безопасности: от управления доступом сотрудников к цифровым платформам, базам данных и конфиденциальным файлам до регулирования доступа в безопасные физические места.

Более того, СКУД облегчает управление механизмами аутентификации пользователей, включая биометрические идентификаторы, смарт-карты и многофакторную аутентификацию для укрепления системы безопасности. Это не только предотвращает несанкционированный доступ, но и защищает организацию от кражи личных данных и мошеннических действий.

В сфере контроля цифрового доступа СКУД играет ключевую роль в регулировании разрешений и авторизаций, что позволяет организациям определять детализированную политику доступа. Это не только защищает важную информацию, но и оптимизирует рабочие процессы, обеспечивая доступ к необходимым ресурсам.[2]

Кроме того, СКУД находит применение в управлении посетителями. Предприятия могут улучшить протоколы безопасности, гарантируя, что временный доступ предоставляется только определенным областям и персоналу.

1.2. Структура

Эффективность СКУД заключается в ее сложной структуре, состоящей из нескольких фундаментальных компонентов, которые работают согласованно, укрепляя инфраструктуру безопасности организации:

- *Политики контроля доступа*: определяют правила и положения, регулирующие доступ пользователей. Эти политики адаптированы к конкретным потребностям организации и определяют, кто, к каким ресурсам и при каких условиях может получить доступ.
- *Механизмы аутентификации*: процесс проверки системой личности пользователя, запрашивающего доступ. Могут быть нескольких видов: от комбинаций имен пользователя и пароля, заканчивая усовершенствованными биометрическими идентификаторами. Многофакторная аутентификация добавляет уровень безопасности за счет объединения двух или более механизмов, укрепляя структуру контроля доступа.
- *Протоколы авторизации*: определят уровень доступа, предоставленный аутентифицированным пользователям. Управление доступом на основе ролей (RBAC) назначает разрешения на основе предопределенной роли, в то время как управление доступом на основе атрибутов (ABAC) учитывает характеристики пользователей, время и местоположение, для определения уровней доступа.
- *Мониторинг и аудит*: предоставляют организациям информацию в режиме реального времени о действиях пользователей и потенциальных угрозах безопасности. Регистрация попыток доступа, изменения в разрешениях и аномальное поведение позволят заранее выявить и снизить риски безопасности.

По сути, СКУД представляет собой сложное сочетание политик, технологий и протоколов, сложно переплетенных вместе для создания надежной и адаптируемой структуры контроля доступа внутри предприятия.

2. Требования к системе контроля и управления доступом на предприятие

Развертывание корпоративной системы контроля и управления доступом (СКУД) — это стратегическое мероприятие, требующее тщательного рассмотрения множества требований. Поскольку организации стремятся укрепить свою безопасность и оптимизировать операционную эффективность, понимание и выполнение этих требований становится ключевым. Рассмотрим их:

- *Масштабируемость*: по мере развития и роста организаций инфраструктура контроля доступа должна плавно расширяться. Масштабируемость гарантирует, что СКУД может умело адаптироваться к динамичному характеру предприятий, предотвращая узкие места и неэффективность, которые могут возникнуть в жесткой и нерасширяемой системе. Независимо от того, происходит ли органический рост или стратегическое расширение, масштабируемая СКУД гарантирует, что система контроля доступа остается гибкой и реагирует на меняющиеся требования.[3]
- *Возможности интеграции*: фундаментальным требованием СКУД является его способность интегрироваться с существующей инфраструктурой, приложениями и базами данных, что устраняет разрозненность и повышает общую эффективность системы контроля доступа. Совместимость с протоколами отраслевых стандартов обеспечивает процесс внедрения.
- *Соответствие отраслевым стандартам*: Соблюдение отраслевых стандартов и нормативной базы не подлежит обсуждению для СКУД. Организации действуют в

рамках сложной сети законодательных и нормативных требований, требующих защиты конфиденциальной информации и обеспечения безопасного доступа. Будь то здравоохранение, финансы или любая другая отрасль, СКУД должна соответствовать таким стандартам, как ISO 27001[6], HIPAA или GDPR. Соблюдение требований не только обеспечивает соблюдение правовых норм, но и создает основу для надежных методов обеспечения безопасности. СКУД, соответствующая отраслевым стандартам, предоставляет организациям основу, признанную и уважаемую в глобальном масштабе, укрепляя доверие между заинтересованными сторонами и регулирующими органами.

- *Удобный интерфейс*: удобный интерфейс является обязательным условием, поскольку от него напрямую зависит эффективность взаимодействия сотрудников с системой контроля доступа. Дизайн должен быть интуитивно понятным, сводить к минимуму время обучения для пользователей и обеспечивать удобство работы. С точки зрения администраторов, управляющих разрешениями доступа для конечных пользователей, осуществляющих процессы аутентификации, интерфейс должен быть эргономичным, обеспечивающим положительный опыт без ущерба для безопасности.
- *Адаптация к новым технологиям*: эффективная СКУД должна демонстрировать способность адаптироваться к новым технологиям, гарантируя, что она останется в авангарде достижений в области безопасности. Будь то интеграция методов биометрической аутентификации, внедрение искусственного интеллекта для обнаружения угроз или внедрение блокчейна для повышения целостности данных, адаптируемая СКУД защищает организацию от развивающихся проблем безопасности.
- *Непрерывный мониторинг*: надежная СКУД должна осуществлять бдительный контроль за действиями пользователей. Функции непрерывного мониторинга предоставляют в режиме реального времени информацию о поведении пользователей и потенциальных угрозах безопасности. Регистрация попыток доступа, изменений в разрешениях и аномальных действий позволяет организациям активно выявлять и снижать риски.[8]
- *Мобильный доступ и вопросы удаленной работы*: система должна обеспечивать безопасный доступ с различных устройств, гарантируя, что сотрудники смогут беспрепятственно работать из разных мест без ущерба для безопасности. Это включает в себя внедрение безопасных методов мобильной аутентификации, протоколов шифрования и безопасных соединений для обеспечения гибкости, необходимой современной рабочей силе.

3. Система учета рабочего времени на предприятии

По мере развития современного корпоративного ландшафта интеграция системы учета рабочего времени (СУРВ) с более широкой системой контроля и управления доступом предприятия (СКУД) становится все более необходимой. Комплексные функциональные возможности СУРВ выходят за рамки простого включения и выключения синхронизации; они воплощают в себе сложный подход к управлению персоналом, мониторингу посещаемости и

повышению производительности. В этом разделе рассматриваются тонкости интеграции СУРВ в рамках предприятия, изучаются технологические аспекты, преимущества и соображения, которые делают его синергетическим дополнением к СКУД.

3.1. Технологические аспекты систем учета рабочего времени

Биометрическая аутентификация: современные СУРВ часто используют передовые методы биометрической аутентификации для обеспечения точного и безопасного отслеживания времени. Биометрические идентификаторы[5], такие как отпечатки пальцев, распознавание лиц или сканирование сетчатки глаза, добавляют дополнительный уровень проверки личности, исключая возможность мошенничества со временем.[4]

Мобильные приложения: в эпоху растущей мобильности СУРВ включает в себя мобильные приложения, которые позволяют сотрудникам отслеживать свое время независимо от их физического местонахождения. Мобильные приложения обеспечивают удаленный доступ к функциям учета рабочего времени, обеспечивая гибкую рабочую среду и отвечая потребностям современной рабочей силы.

Облачные решения: облачная СУРВ обеспечивает масштабируемость, доступность и синхронизацию данных в режиме реального времени. При интеграции с СКУД облачные решения обеспечивают беспрепятственный обмен информацией и аналитическими данными между системами контроля доступа и учета рабочего времени.[7]

3.2. Управление посещаемостью и мониторинг производительности

Оптимизация управления посещаемостью: СУРВ при интеграции с СКУД упрощает управление посещаемостью за счет автоматизации процесса регистрации посещаемости сотрудников. СУРВ обеспечивает точное отслеживание данных о посещаемости в режиме реального времени. Эти данные затем легко интегрируются с СКУД, что способствует представлению о деятельности сотрудников и соблюдению политик контроля доступа.

Улучшение мониторинга производительности: СУРВ способствует мониторингу производительности, предоставляя информацию о том, как сотрудники распределяют свое рабочее время. Классифицируя задачи, отслеживая сроки реализации проекта, организации получают данные для оптимизации распределения ресурсов, улучшая управление проектами. Интеграция с СКУД гарантирует, что данные о производительности совпадают с данными контроля доступа, обеспечивая полное понимание вовлеченности сотрудников.[1]

3.3. Синергетическая интеграция с СКУД

Единые профили пользователей: интеграция между СУРВ и СКУД приводит к созданию унифицированных профилей пользователей и созданию централизованного хранилища данных о сотрудниках. Этот подход обеспечивает согласованность аутентификации пользователей, политик контроля доступа и действий, связанных со временем. Полная интеграция гарантирует, что любые изменения в ролях пользователей, разрешениях или уровнях доступа единообразно отражаются в обеих системах, что снижает административные издержки и повышает точность.

Политика скоординированного контроля доступа и учета рабочего времени: сплоченная интеграция СКУД и СУРВ позволяет организациям координировать политику контроля доступа и учета рабочего времени, при которой права доступа динамически корректируются на основе показателей, связанных со временем, что способствует как безопасности, так и эффективности. Например, определенные права доступа могут зависеть

от определенных критериев, связанных со временем, таких как регулярное посещение или выполнение назначенных задач.

Отчетность и аналитика: интеграция облегчает создание комплексных отчетов и аналитики. Эти данные позволяют организациям оценивать производительность сотрудников, выявлять тенденции и принимать обоснованные решения относительно распределения ресурсов, сроков реализации проекта и протоколов безопасности.

3.4. Соображения и преимущества

Соответствие требованиям и точность расчета заработной платы: интеграция СУРВ и СКУД обеспечивает соблюдение трудового законодательства путем предоставления точного и поддающегося проверке учета рабочего времени. Это не только защищает организацию от юридических проблем, но и повышает точность расчета заработной платы, поскольку данные, связанные со временем, легко интегрируются с профилями сотрудников и записями контроля доступа.

Расширение возможностей и вовлеченность сотрудников: СУРВ способствует расширению прав и возможностей сотрудников, предоставляя им возможность просмотра своих данных, связанных со временем. Сотрудники могут активно участвовать в управлении своим рабочим временем, задачами и производительностью. Это расширение прав и возможностей способствует развитию вовлеченности, что соответствует современным тенденциям на рабочем месте, которые ставят во главу угла благополучие и удовлетворенность сотрудников.

Вывод

В быстро развивающемся ландшафте современных предприятий интеграция надежных корпоративных систем контроля и управления доступом (СКУД) и систем учета рабочего времени (СУРВ) становится стратегическим императивом. Это исследование позволило углубиться в сложные области применения, состав, требования и синергетическую интеграцию этих систем, подчеркнув их симбиотическую роль в укреплении безопасности и оптимизации операционной эффективности.

Взаимосвязанное значение СКУД и СУРВ: СКУД с ее приложениями для контроля доступа, управления идентификацией и авторизации обеспечивает базовый уровень защиты цифровых активов. В то же время интеграция СУРВ привносит динамичный элемент за счет оптимизации управления посещаемостью, улучшения мониторинга производительности и развития культуры подотчетности. Объединение систем приводит к созданию единой цифровой экосистемы, в которой органично сочетаются контроль доступа, учет рабочего времени и управление пользователями.

Повышение безопасности и операционной эффективности: меры контроля доступа подкреплены методами биометрической аутентификации СУРВ, которые предотвращают мошенничество и обеспечивают точность личности пользователя. Операционная эффективность оптимизируется за счет оптимизации управления посещаемостью и аналитики, полученной с помощью СУРВ. Организации получают представление о вовлеченности сотрудников, сроках реализации проекта и распределении ресурсов, что позволяет принимать обоснованные решения.

Расширение прав и возможностей пользователей и соблюдение требований: интегрированный подход расширяет возможности сотрудников, предоставляя им видимость и

контроль над их данными. Преимущества соблюдения требований, получаемые за счет точного учета рабочего времени и контроля доступа, способствуют укреплению правовой и нормативной базы, снижая риски, связанные с несоблюдением требований.

Будущие соображения: поскольку технологии продолжают развиваться, будущие соображения по интеграции СКУД и СУРВ могут включать в себя интеграцию искусственного интеллекта для прогнозной аналитики, усовершенствованные методы биометрической аутентификации и исследование технологии блокчейн для обеспечения большей целостности данных. Постоянное развитие технологий кибербезопасности и управления персоналом, несомненно, будет определять траекторию развития этих систем, требуя от организаций сохранять бдительность и адаптивность.

Список литературы

1. Шварц М. и Мачулак М. (2018). «Защита периметра: развертывание управления идентификацией и доступом с помощью бесплатного программного обеспечения с открытым исходным кодом».
2. Рави С. Сандху. (2008). «Управление доступом на основе ролей».
3. Ангелос Д. Керомит, Джонатан М. Смит (2007). «Требования к масштабируемым архитектурам контроля доступа и управления безопасностью».
4. Крахмалев А. Нормативная база для СКУД // Алгоритм безопасности. № 4. (2008).
5. Лиакат Али, Джон В. Монако, Чарльз К. Тапперт, Мэйкан Цю (2016). «Биометрические системы для аутентификации пользовалей».
6. Международная организация по стандартизации. (ISO/IEC 27001:2022). «Системы менеджмента информационной безопасности – Требования».
7. Цзяньтин Нин, Синьи Хуан, Вилли Сусило, Кайтай Лян, Симэн Лю, Инхуэй Чжан (2020). «Двойной контроль доступа для облачного хранения данных и их совместного использования».
8. РД 78.36.003-2002 Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств / НИЦ «Охрана» ГУВО МВД России; сост. Н.Н. Котов, Л.И. Савчук, Е.П. Тюрин. (2002).
9. Бадиков А.В., Бондарев П.В. Системы контроля и управления доступом. Лабораторный практикум. М.: НИЯУ МИФИ. (2010).
10. Рекомендации Р 78.36.005-99 / НИЦ «Охрана» ГУВО МВД России; сост. Н.Н. Котов, Л.И. Савчук, Е.П. Тюрин, В.Г. Синилов. (1998).

References

1. Schwartz M. and Machulak M. (2018). "Perimeter Protection: Deploying identity and access management using free and open source software."
2. Ravi S. Sandhu. (2008). "Role-based access control".
3. Angelos D. Keromit, Jonathan M. Smith (2007). "Requirements for scalable access control and security management architectures."
4. Krakhmalev A. Regulatory framework for ACS // Security algorithm. № 4. (2008).
5. Liaqat Ali, John V. Monaco, Charles K. Tappert, Meikan Qiu (2016). "Biometric systems for user authentication".

6. International Organization for Standardization. (ISO/IEC 27001:2022). "Information Security Management Systems – Requirements".
7. Jiantin Ning, Xinyi Huang, Willy Susilo, Kaitai Liang, Ximeng Liu, Yinhui Zhang (2020). "Dual access control for cloud storage and data sharing."
8. RD 78.36.003-2002 Engineering and technical fortification. Technical means of protection. Requirements and design standards for the protection of objects from criminal encroachments / SIC "Protection" GUVO of the Ministry of Internal Affairs of Russia; comp. N.N. Kotov, L.I. Savchuk, E.P. Tyurin. (2002).
9. Badikov A.V., Bondarev P.V. Access control and management systems. Laboratory workshop. Moscow: NRU MEPhI. (2010).
10. Recommendations P 78.36.005-99 / SIC "Protection" GUVO of the Ministry of Internal Affairs of Russia; comp. N.N. Kotov, L.I. Savchuk, E.P. Tyurin, V.G. Sinilov. (1998).