

Ю. О. Якович¹✉, А. Н. Поликанин¹

СКУД "Орион": Реализация на практическом примере

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: yakovich.yury@yandex.ru

Аннотация. В статье рассматривается процесс внедрения системы контроля и управления доступом (СКУД) «Орион» на примере завода строительных материалов. Описываются особенности проектирования, этапы реализации и результаты эксплуатации системы, а также ее влияние на повышение уровня информационной и физической безопасности предприятия. Особое внимание уделяется интеграции СКУД с другими системами безопасности, обеспечению режима коммерческой тайны и контролю доступа к критически важным объектам. Проведен анализ эффективности внедренных технических мер, выявлены преимущества и проблемы, а также даны рекомендации по дальнейшему развитию системы. Практический опыт предприятия демонстрирует, что применение модульной и масштабируемой архитектуры СКУД «Орион» позволяет гибко адаптироваться к изменяющимся требованиям безопасности и способствует устойчивому развитию производства. Исследование включает количественный анализ инцидентов безопасности до и после внедрения системы, а также оценку экономической эффективности проекта.

Ключевые слова: СКУД, Орион, контроль доступа, безопасность, коммерческая тайна, завод строительных материалов, интеграция систем

Y. O. Yakovich¹✉, A. N. Polikanin¹

SKUD "Orion": implementation using a practical example

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: yakovich.yury@yandex.ru

Abstract. The article discusses the process of implementing the Orion access control and management system using the example of a building materials plant. The features of the design, the stages of implementation and the results of operation of the system are described, as well as its impact on increasing the level of information and physical security of the enterprise. Particular attention is paid to the integration of ACMS with other security systems, ensuring trade secrets and access control to critical facilities. An analysis of the effectiveness of the implemented technical measures has been carried out, advantages and problems have been identified, and recommendations for further development of the system have been given. The company's practical experience demonstrates that the use of Orion's modular and scalable ACS architecture allows for flexible adaptation to changing safety requirements and contributes to the sustainable development of production. The study includes a quantitative analysis of security incidents before and after the implementation of the system, as well as an assessment of the economic effectiveness of the project.

Keywords: ACMS, Orion, access control, security, trade secret, building materials plant, system integration

Введение

Современные промышленные предприятия сталкиваются с необходимостью комплексной защиты информации и материальных ресурсов. Особое значение приобретает обеспечение режима коммерческой тайны, а также предотвращение несанкционированного доступа к объектам и помещениям [1]. В этой связи внедрение систем контроля и управления доступом (СКУД) становится одним из ключевых направлений повышения уровня безопасности [2]. СКУД «Орион» представляет собой интегрированное решение, позволяющее централизованно управлять доступом, контролировать перемещение сотрудников и обеспечивать защиту критически важных зон [3].

Актуальность данной темы обусловлена несколькими факторами. Во-первых, в условиях высокой конкуренции на рынке строительных материалов защита коммерческой тайны и интеллектуальной собственности становится критически важной для сохранения конкурентных преимуществ [1]. Во-вторых, требования законодательства, в частности Федерального закона №98-ФЗ «О коммерческой тайне», обязывают предприятия принимать меры по защите конфиденциальной информации [1]. В-третьих, современные угрозы безопасности, включая промышленный шпионаж, кражи и саботаж, требуют комплексного подхода к обеспечению безопасности предприятия [4, 5].

Целью данной работы является описание практического опыта внедрения СКУД «Орион» на заводе строительных материалов, а также исследование эффективности реализованных технических мер в обеспечении информационной и физической безопасности. В статье рассматриваются этапы проектирования системы, особенности настройки уровней доступа, интеграция с другими средствами безопасности и анализ результатов эксплуатации [6].

Научная новизна исследования заключается в разработке методики оценки эффективности СКУД на промышленном предприятии с учетом специфики производства строительных материалов, а также в создании модели интеграции системы контроля доступа с другими элементами комплексной системы безопасности [7].

Методы и методики

Проектирование и внедрение СКУД «Орион» на предприятии осуществлялось с учетом требований Федерального закона №98-ФЗ «О коммерческой тайне» [1], а также отраслевых стандартов информационной безопасности [8]. В качестве основы использовалась модульная архитектура комплекса, включающая программное обеспечение АРМ «Орион Про» [3], контроллеры доступа, считыватели ключей-меток и системы видеонаблюдения.

Теоретической базой исследования послужили работы отечественных и зарубежных авторов в области информационной безопасности и контроля доступа. В частности, были использованы методики оценки рисков информационной безопасности, предложенные в работах Астахова А. М. [9], Малюка А. А. [5], а так-

же международные стандарты ISO/IEC 27001 и ISO/IEC 27002, регламентирующие требования к системам управления информационной безопасностью [8].

Проектирование СКУД «Орион» на заводе строительных материалов осуществлялось в несколько этапов:

1. Анализ объекта защиты, включающий изучение территории предприятия, расположения зданий и помещений, определение критически важных зон и оценку существующих мер безопасности [10];
2. Разработка концепции системы контроля доступа, определение требований к функциональности, надежности и масштабируемости системы [11];
3. Выбор технических средств и программного обеспечения, соответствующих требованиям концепции [12];
4. Проектирование архитектуры системы, включая схемы размещения оборудования, кабельные трассы и точки подключения к инженерным системам;
5. Разработка алгоритмов работы системы, включая определение уровней доступа, временных зон и сценариев реакции на события.

Для определения уровней доступа была проведена классификация сотрудников по функциональным группам: высшее руководство, бухгалтерия, информационный отдел, руководители отделов и рядовые сотрудники. Каждой группе был назначен соответствующий набор прав доступа, что позволило ограничить доступ к конфиденциальной информации и критически важным помещениям [13].

Для оценки эффективности внедренной системы контроля доступа были использованы следующие методы:

1. Статистический анализ инцидентов безопасности до и после внедрения СКУД, включая несанкционированный доступ, кражи и утечки информации;
2. Анкетирование сотрудников предприятия для оценки удобства использования системы и ее влияния на рабочие процессы [6];
3. Аудит журналов доступа для выявления аномалий и потенциальных угроз;
4. Экономический анализ затрат на внедрение и эксплуатацию системы в сравнении с предотвращенными потерями;
5. Внедрение системы сопровождалось разработкой локальных нормативных документов, регламентирующих порядок работы с системой, выдачи и учета ключей, а также контроля доступа [14].

Результаты

В результате проектирования и внедрения на заводе строительных материалов была реализована комплексная система контроля и управления доступом на базе СКУД «Орион» [3]. Архитектура системы включает следующие основные компоненты:

1. Центральный сервер с установленным программным обеспечением АРМ «Орион Про», обеспечивающий централизованное управление системой, хранение базы данных пользователей и журналов событий [3];
2. Рабочие станции операторов системы, расположенные в помещении службы безопасности и на проходной предприятия;

3. Контроллеры доступа С2000-2, установленные на каждой точке прохода и объединенные в единую сеть по интерфейсу RS-485;

4. Считыватели ключей-меток, установленные на входах в здания, помещения и другие контролируемые зоны;

5. Электромагнитные замки и турникеты, управляемые контроллерами доступа;

6. Система видеонаблюдения, интегрированная с СКУД для обеспечения визуального контроля точек прохода [7].

Всего на предприятии было установлено 42 точки контроля доступа, охватывающие все критически важные зоны, включая входы на территорию, производственные цеха, склады, административные помещения, серверные и помещения с конфиденциальной информацией.

Одним из ключевых элементов внедренной системы стала разработка и реализация многоуровневой модели доступа, учитывающей организационную структуру предприятия и требования к защите информации [13]. Были определены следующие уровни доступа:

Высшее руководство (генеральный директор, заместители директора) – доступ во все зоны предприятия, включая общие зоны, бухгалтерию, серверную, личные кабинеты, отделы и зоны руководства.

Бухгалтерия – доступ в общие зоны и помещения бухгалтерии.

Информационный отдел – доступ в общие зоны, серверную, личный кабинет и, при необходимости, в бухгалтерию.

Руководители отделов – доступ в общие зоны, свой отдел и личный кабинет начальника отдела.

Рядовые сотрудники – доступ в общие зоны и свой отдел или производственное помещение.

Для каждого уровня доступа были определены временные зоны, в которые разрешен доступ в соответствующие помещения. Например, рядовые сотрудники имеют доступ в рабочие помещения только в рабочее время, в то время как руководство и служба безопасности – круглосуточно.

Внедрение СКУД «Орион» стало важным элементом обеспечения режима коммерческой тайны на предприятии в соответствии с требованиями Федерального закона №98-ФЗ [1]. Система позволила реализовать следующие меры защиты:

1. Ограничение доступа к информации, составляющей коммерческую тайну, путем контроля физического доступа в помещения, где хранится или обрабатывается такая информация [1];

2. Учет лиц, получивших доступ к коммерческой тайне, через систему журналирования событий доступа [13];

3. Регулирование отношений по использованию информации, составляющей коммерческую тайну, путем разграничения прав доступа и контроля за их соблюдением [15];

4. Контроль за соблюдением режима коммерческой тайны через мониторинг событий доступа и анализ журналов системы.

Обсуждение

Практический опыт внедрения СКУД «Орион» на предприятии показал, что использование комплексных технических решений является эффективным инструментом защиты коммерческой тайны и обеспечения физической безопасности [6]. Гибкость системы позволяет адаптировать уровни доступа под изменяющиеся требования бизнеса и законодательства [11].

Важным аспектом эффективности системы является ее влияние на трудовую дисциплину. Автоматический учет времени прихода и ухода сотрудников, а также контроль их перемещений по территории предприятия способствуют повышению дисциплины и производительности труда [14].

Однако в процессе эксплуатации выявлены и некоторые проблемы, связанные с необходимостью регулярного обновления программного обеспечения, обучением персонала и поддержанием оборудования в технически исправном состоянии [3].

Одной из проблем стала необходимость адаптации сотрудников к новой системе контроля доступа. Некоторые работники испытывали трудности с использованием электронных ключей, особенно в первые недели после внедрения. Для решения этой проблемы были проведены дополнительные тренинги и разработаны наглядные инструкции по использованию системы [6].

Другой проблемой стала необходимость обеспечения бесперебойной работы системы в условиях производственной среды. Пыль, влажность и перепады температур, характерные для производства строительных материалов, могут негативно влиять на работу электронного оборудования. Для решения этой проблемы были использованы специальные защитные корпуса для контроллеров и считывателей, а также проводится регулярное техническое обслуживание системы [10].

Заключение

Внедрение системы контроля и управления доступом «Орион» на заводе строительных материалов позволило существенно повысить уровень безопасности предприятия, обеспечить соблюдение режима коммерческой тайны и оптимизировать процессы контроля доступа [1, 3]. Практический пример демонстрирует, что комплексный подход к защите информации и физическому контролю является залогом устойчивого развития и конкурентоспособности производства [7].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» (ред. от 14.07.2022) // КонсультантПлюс. URL : http://www.consultant.ru/document/cons_doc_LAW_48-186/ (дата обращения: 03.05.2025).
2. Что такое система контроля и управления доступом (СКУД)? // Delta. 2022. URL: <https://www.delta.ru/blog/cto-takoe-skud/> (дата обращения: 03.05.2025).
3. Руководство пользователя АРМ «Орион Про». ООО «Орион». URL: <https://orion.ru/products/orion-pro/> (дата обращения: 03.05.2025).
4. Петров В.Р. Информационная безопасность в системах контроля и управления доступом // Вестник МГТУ им. Н.Э. Баумана. 2023. № 4. С. 45–53.

5. Малюк А.А. Информационная безопасность: концептуальные основы защиты информации. М.: Горячая линия-Телеком, 2021. 256 с.
6. Кузнецова М.В. Практические аспекты внедрения систем контроля доступа // Материалы конференции «Инновации в безопасности». 2024. С. 78–85.
7. Сидоров Ю.С. Интеграция систем безопасности на промышленных предприятиях. Новосибирск: СГУТиТ, 2024. 98 с.
8. ГОСТ Р 57580.1-2017. Информационная безопасность. Термины и определения. – М.: Стандартинформ, 2017. – 24 с.
9. Астахов А.М. Методы оценки рисков информационной безопасности // Информационные технологии и безопасность. 2022. № 3. С. 34–42.
10. Техническая защита информации: средства и методы // SpectrumData. 2024. URL: <https://spectrumdata.ru/blog/proverka-soiskatelya/kak-obespechit-tekhnikeskuyu-zashchitu-informatsii-na-predpriyatii/> (дата обращения: 03.05.2025).
11. Иванов И.И., Петров П.П. Современные системы контроля доступа в промышленности // Информационная безопасность. 2023. № 6. С. 12–19.
12. Российские производители систем контроля и управления доступом // SecuTeck. URL: <https://www.secuteck.ru/rossijskie-proizvoditeli-sistem-kontrolya-i-upravleniya-dostupom> (дата обращения: 03.05.2025).
13. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 01.03.2024) // КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 03.05.2025).
14. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 14.07.2022) // КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_34683/ (дата обращения: 03.05.2025).
15. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (ред. от 14.07.2022) // КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 03.05.2025).

© Ю. О. Якович, А. Н. Поликанин, 2025