*Ахметгалеев Роберт Ильсурович*

*г. Казань, КНИТУ*

**Внедрение системы контроля и управления доступом на предприятии**

Системы контроля и управления доступом (СКУД) прочно вошли в нашу повседневную жизнь. Современные предприятия подвергаются массе внешних и внутренних угроз. Еще не так давно, проблема решалась установкой стандартной охранной сигнализации, но в настоящее время такой меры оказывается явно недостаточно. Внедрение СКУД на предприятии – это действенный инструмент управления бизнесом, а также эффективное средство обеспечения безопасности персонала и материальных ценностей. СКУД – это целостная система, которая состоит из программных и технических средств, осуществляющих контроль и управление доступом в отдельные помещения, на обозначенные зоны и территории, контроль передвижения транспорта и персонала, а также контроль времени их присутствия на территории охраняемого объекта. В системах управления доступом применяются такие принципы кибербезопасности как проверка подлинности и авторизация. При монтаже СКУД на предприятии нужно понимать какие цели и задачи должна будет выполнять будущая система контроля доступа. При разработке проекта СКУД необходимо учесть следующие параметры:

* особенности здания – конфигурация, количество помещений, наличие уязвимых зон
* расположение секретных цехов, опасного производства и других режимных помещений
* наличие сотрудника службы охраны на проходной
* требование к уровню безопасности

СКУД подразделяются на сетевые, автономные и комбинированные. Сетевые используются на больших объектах, они довольно дорогие при внедрении и в эксплуатации. Их функционал позволяет не только организовать контроль доступа, но и вести учет рабочего времени, следить за состоянием дверей. Сетевые СКУД легко интегрировать с системой видеонаблюдения, пожарной сигнализации. Автономные СКУД дешевле, но имеют свои недостатки: максимальное количество пользователей ограничено. Поэтому на практике обычно используют комбинированные системы, которые имеют функции как автономных, так и сетевых СКУД. Комплексная система контроля и управления доступом состоит из следующих компонентов:

**1. Аутентификация**

Аутентификация — это процесс проверки личности пользователей, гарантирующий, что они являются теми, за кого себя выдают. Этого можно добиться различными методами, в том числе:

* Имя пользователя и пароль
* Биометрическая аутентификация (например, отпечаток пальца, распознавание лица)
* Смарт-карты
* Одноразовые пароли (OTP)

**2. Авторизация**

Авторизация определяет уровень доступа пользователя к определенным ресурсам, данным или системам. Обычно это зависит от роли пользователя, должностных функций или уровня допуска.

**3. Контроль доступа**

Контроль доступа предполагает физическое или логическое ограничение доступа к ресурсам, данным или системам. Этого можно достичь посредством:

* Физические барьеры (например, двери, ворота)
* Электронные системы контроля доступа (например, считыватели карт, биометрические сканеры)
* Системы контроля доступа к сети (например, межсетевые экраны, VPN)

**4. Управление**

Компонент управления включает в себя администрирование и мониторинг системы контроля и управления доступом. Это включает в себя:

* Управление пользователями (например, создание, изменение, удаление пользователей)
* Управление уровнями доступа (например, управление доступом на основе ролей)
* Аудит и регистрация (например, отслеживание активности пользователей, системных событий)

Требования к внедрению СКУД содержатся в ряде документов: Государственных стандартах (ГОСТ), Сводах правил (СП), Строительных нормах и правилах (СНиП), Правилах устройства электроустановок (ПУЭ), и т. д. Также учитываются и индивидуальные стандарты организации.

Внедрение системы контроля и управления доступом на предприятии дает множество преимуществ, в том числе:

1. **Улучшенная безопасность**

Система контроля и управления доступом помогает предотвратить несанкционированный доступ к конфиденциальным областям, данным и системам, снижая риск нарушений безопасности и кражи данных.

1. **Повышенная эффективность**

Автоматизированные системы контроля и управления доступом упрощают процесс предоставления и отзыва доступа, сокращая административную нагрузку и повышая производительность.

1. **Повышенное соответствие**

Система контроля и управления доступом помогает предприятиям соблюдать нормативные требования и отраслевые стандарты.

1. **Лучшее принятие решений**

Система предоставляет ценную информацию и аналитику, позволяя принимать обоснованные решения и стратегическое планирование.

Успешное внедрение системы контроля и управления доступом в сочетании с ее плавной интеграцией в единую базу данных учета рабочего времени является ключевым шагом в обеспечении целостности организации. Такое стратегическое объединение позволяет предприятиям:

* Защитить организационную стабильность

Внедряя надежную систему контроля доступа, компании могут обеспечить надежность и устойчивость своих внутренних отношений, а также разработать быстрый и эффективный механизм реагирования для противодействия негативным тенденциям. Такой упреждающий подход позволяет организациям выявлять и смягчать потенциальные угрозы безопасности, тем самым поддерживая стабильную и безопасную рабочую среду.

* Защита законных интересов

Интеграция систем контроля доступа и учета рабочего времени также позволяет предприятиям защитить свои законные интересы от потенциальных угроз. Это достигается за счет стратегического развертывания комплекса мер, в том числе правовых, экономических, организационных, социально-психологических, технических и других средств. Используя эти разнообразные инструменты, организации могут обнаруживать и нейтрализовать источники угроз безопасности, обеспечивая защиту конфиденциальной информации и ресурсов.

Приняв единый подход к контролю доступа и управлению временем, предприятия могут создать надежную защиту от потенциальных нарушений безопасности, гарантируя конфиденциальность, целостность и доступность своих активов. Это интегрированное решение обеспечивает надежную основу для корпоративной безопасности, позволяя организациям уверенно работать во все более сложной и динамичной бизнес-среде.

Внедрение СКУД – это многоэтапный процесс, им следует заниматься комплексно. Сотрудники службы обеспечения информационной безопасности и режима предприятия, которые будут взаимодействовать со СКУД должны быть обучены правильному управлению системой, иметь представление о технических нюансах и понимать распределение ответственности сотрудников в пределах работы со СКУД. СКУД – превосходное решение для организации контрольно-пропускных пунктов, регулирующих посещение закрытой территории людьми или транспортом. Подойдет для фирмы любого масштаба и направленности, но необходимо правильно подобрать оборудование, в противном случае возможна ненужная переплата или наоборот, СКУД окажется недостаточно функциональной.

**Список литературы**

1. Раков И. Системы контроля и управления доступом: куда идем? // Алгоритм безопасности. 2011. № 4.
2. Александровская, JI. H. Современные методы обеспечения безотказности сложных технических систем / Л. Н. Александровская, А. П. Афанасьев А. П., A. А. Лисов. – М.: Логос,2001. 234 с.
3. Ворона В. А. Системы контроля и управления доступом / В. А. Ворона, В. А. Тихонов. – Горячая линия – Телеком, 2010. – 272с.
4. Бадиков А.В., Бондарев П.В. Системы контроля и управления доступом. Лабораторный практикум. М.: НИЯУ МИФИ, 2010. 128 с.
5. Крахмалев А. Нормативная база для СКУД // Алгоритм безопасности. 2008. № 4.