**СОВРЕМЕННЫЕ МЕТОДЫ В ОБЛАСТИ**

**СИСТЕМ КОНТРОЛЯ УПРАВЛЕНИЯ ДОСТУПОМ**

преп. Гиш Т.А. , студ. Новиков К.И.

Северо-Кавказский Федеральный Университет

В современном мире, где информационные технологии играют ключевую роль в образовательном процессе, обеспечение информационной безопасности в образовательных учреждениях становится неотъемлемой частью образовательной политики. Эта статья рассматривает ключевые аспекты и методы обеспечения информационной безопасности предприятий путем использования систем контроля управления доступом.

**Введение**

Системы контроля и управления доступом (СКУД) представляют собой комплекс программных и технических средств, предназначенных для автоматизации контроля пропускного режима объектов (людей, машин) и учета рабочего времени на охраняемой территории. Они играют ключевую роль в обеспечении безопасности и контроля доступа к информации, активам и материальным ценностям организаций различных типов, включая промышленные предприятия, офисы, торговые центры и жилые здания.

СКУД могут включать в себя различные устройства и оборудование, такие как шлагбаумы, турникеты, видеодомофоны, вызывные панели, контроллеры, считыватели карт и другие средства. Основные задачи СКУД включают:

* Предотвращение криминального проникновения и контроль доступа к охраняемой территории.
* Ограничение доступа на охраняемую территорию определенным категориям лиц.
* Учет рабочего времени персонала и фиксация опозданий, досрочных уходов с работы, прогулов, переработок.
* Ведение базы данных персонала и посетителей объекта.
* Расчет заработной платы сотрудников при интеграции СКУД с системами бухгалтерского учета.
* Обеспечение безопасности охраняемого объекта.

Существуют разные виды СКУД, которые отличаются по автономности, комплектации и принципу работы:

* Автономные СКУД обычно устанавливаются в коммерческих помещениях и выполняют функцию дверных замков. Доступ разрешается при наличии карты с кодом, внесенным в программу управления доступом.
* Сетевые комплексы имеют большую функциональность и подключены к ПК для дистанционного управления. Они позволяют настраивать доступ на объект по временному графику, учет рабочего времени сотрудников, интеграцию с другими системами безопасности.
* Биометрические СКУД работают с уникальными особенностями сотрудников, такими как отпечаток пальца или рисунок радужной оболочки глаза, обеспечивая высокий уровень безопасности и уменьшение вероятности ошибок.

Выбор конкретной системы контроля и управления доступом зависит от масштабов организации, требований к безопасности и специфики использования. В крупных компаниях и офисах часто применяются биометрические системы, в то время как в бизнес-центрах и малых офисах могут быть предпочтительны автономные системы.

Системы контроля и управления доступом (СКУД) играют ключевую роль в современном мире, обеспечивая защиту информации, сохранность активов и контроль над проникновением на охраняемую территорию. Они широко применяются в различных сферах жизни, начиная от промышленных предприятий и заканчивая офисами компаний, отелями и гипермаркетами. Рассмотрим подробнее значение СКУД в современном мире.

Одним из основных назначений СКУД является защита информации, составляющей государственную или коммерческую тайну. Системы контроля доступа помогают предотвратить несанкционированный доступ к чувствительным данным и обеспечивают сохранность активов и материальных ценностей организации. Это достигается за счет ограничения доступа на охраняемый объект и контроля за действиями посетителей и сотрудников.

СКУД позволяет контролировать проникновение на охраняемую территорию лиц, чья цель может быть нарушение нормальной работы организации через саботаж или промышленный шпионаж. Это обеспечивает дополнительный уровень безопасности, защищая от нежелательных посетителей и предотвращая попытки несанкционированного доступа.

Системы контроля доступа также используются для отслеживания количества людей, одновременно находящихся в помещении, учета рабочего времени персонала и фиксации опозданий, досрочных уходов с работы, прогулов, переработок. Это позволяет организациям лучше управлять ресурсами и оптимизировать процессы.

СКУД способствует организации пропускного режима, запрещая доступ на охраняемую территорию посторонним лицам. Это обеспечивает дополнительный уровень безопасности и контроль за движением людей внутри организации.

В некоторых случаях СКУД также используется для учета транспортных средств, которые въезжают на территорию объекта и выезжают с нее. Это позволяет контролировать движение транспорта и обеспечивать безопасность на парковках и других охраняемых территориях.

Таким образом, СКУД играет важную роль в обеспечении безопасности и эффективности работы организаций всех типов. Они помогают защитить ценные активы, контролировать доступ к информации и обеспечивают безопасность на охраняемых территориях. В современном мире, где информационная безопасность и контроль доступа становятся все более актуальными вопросами, СКУД остаются неотъемлемым элементом защиты от угроз и рисков.

**Основные методы контроля доступа**

Идентифика

* Идентификация представляет собой процесс установления личности пользователя или устройства, которое хочет получить доступ к ресурсу. Это может быть выполнено путем предоставления имени пользователя или другого уникального идентификатора.
* Аутентификация следует после идентификации и подтверждает, что пользователь действительно является тем, за кого себя выдает. Это может быть достигнуто с помощью пароля, биометрических данных, цифровых сертификатов или других методов проверки подлинности.

Авторизация

После успешной аутентификации следующим шагом является авторизация, которая определяет, какие ресурсы и операции доступны пользователю. Это может включать в себя проверку прав доступа, установленных в системе, и соответствие между этими правами и требованиями пользователя.

Избирательное Управление Доступом

Этот метод позволяет администраторам системы точно контролировать доступ к ресурсам, предоставляя или запрещая доступ на основе конкретных условий или правил. Это может включать в себя управление доступом на основе времени, географического местоположения, типа устройства и других параметров.

Мандатное Управление Доступом

Мандатное управление доступом использует политики безопасности, которые определяют, кто может делать что с ресурсами. Эти политики могут быть автоматически применены к пользователям или группам пользователей, основываясь на их роли в организации или других атрибутах.

Управление Доступом На Основа Ролей

Этот метод основан на назначении ролей пользователям, каждая из которых имеет набор привилегий и прав доступа. Управление доступом на основе ролей позволяет легко управлять доступом к ресурсам, изменяя или добавляя роли без необходимости изменения прав каждого отдельного пользователя.

Административная Политика и Процедуры

Важным аспектом контроля доступа является разработка и следование административной политике и процедур, которые определяют, как и когда доступ к ресурсам может быть предоставлен. Эти политики и процедуры должны быть четко документированы и регулярно пересматриваемы для обеспечения актуальности и эффективности.

Каждый из этих методов может быть использован самостоятельно или в сочетании друг с другом в зависимости от требований к безопасности и специфики применения. Важно отметить, что эффективность системы контроля доступа зависит не только от выбора методов, но и от правильного их применения и поддержки в соответствии с текущими требованиями и угрозами безопасности.

**Методы мониторинга и аналитики**

Использование видеонаблюдения в системах контроля доступа (СКУД) позволяет улучшить безопасность и контроль над объектами. Видеонаблюдение может быть интегрировано с СКУД для обеспечения дополнительного уровня защиты, включая мониторинг входов и выходов, обнаружение нарушений и анализ поведения персонала. Вот основные аспекты интеграции видеонаблюдения в СКУД:

Виды видеокамер для СКУД

* Корпусные камеры часто используются в открытых пространствах, таких как парковки или фасады зданий.
* Купольные камеры монтируются внутри зданий и могут быть поворотными или скоростными.
* IP-камеры обрабатывают изображения и передают их по сетям, что делает их идеальными для удаленного мониторинга.
* Установки с подогревом обеспечивают надежную работу в различных погодных условиях.
* Видеоглазки похожи на обычные дверные глазки и могут использоваться для наблюдения за внутренними проходами.

Интеграция с СКУД

* Системы видеонаблюдения могут быть интегрированы с СКУД через специальные модули, позволяющие передавать данные о событиях между системами. Например, при обнаружении несанкционированного доступа, система видеонаблюдения может автоматически начать запись или повернуть камеру на интересующую область.
* Возможность создания индивидуальных видов наблюдения, добавления элементов и их расположения на экран мониторинга для удобства оператора.
* Подключение IP-камер к СКУД позволяет использовать функции, такие как показ кадра при клике на событие в архиве СКУД, сохранение кадров в базу данных с настройками временного отрезка, количества кадров в секунду и размера изображения.

Преимущества интеграции

* Улучшение безопасности объекта за счет дополнительного уровня контроля и мониторинга.
* Снижение риска несанкционированных действий и утечки конфиденциальной информации.
* Оптимизация работы персонала за счет сокращения числа ненужных отлучек и преждевременных уходов.

Интеграция видеонаблюдения с СКУД требует тщательного планирования и установки соответствующего оборудования и программного обеспечения. Выбор конкретных компонентов зависит от потребностей объекта и бюджета на проект.

Анализ данных для оптимизации системы контроля доступа (СКУД) включает в себя детальное изучение поведения сотрудников и посетителей, что позволяет улучшить управление доступом и повысить уровень безопасности. Основываясь на предоставленных источниках, вот ключевые аспекты анализа данных для СКУД:

Детализация

* Отчеты позволяют отслеживать присутствие сотрудников в офисе, включая время прибытия и ухода, количество перерывов на курение и обед, а также общее количество отработанных часов за день.
* Эта детализация помогает управлять рабочим временем и дисциплиной сотрудников, а также определять, кто регулярно отсутствует или работает вне офиса.

Данные в динамике

* Анализ посещаемости и дисциплины сотрудников по дням позволяет выявлять системные нарушения дисциплины и определить, как часто сотрудники, работающие на частично удаленной основе, приходят в офис.
* Это помогает адаптировать политики доступа и график работы, учитывая изменения в работе сотрудников.

Простая обработка большого объема данных

* Использование интерактивных диаграмм и фильтрации по параметрам упрощает анализ данных.
* Отчеты могут формироваться как по группе сотрудников или объектов, так и по конкретному человеку, что позволяет гибко адаптировать анализ под различные задачи.

Визуализация и доступность данных

* Визуализация данных через диаграммы и таблицы облегчает понимание тенденций и паттернов, связанных с доступом и поведением сотрудников.
* Использование NQGS (природных генераторов запросов) упрощает доступ к данным, позволяя пользователям извлекать значимую информацию без необходимости владения сложными языками запросов.

Применение аналитики для оптимизации

* Регулярный анализ данных помогает выявлять области для улучшения в управлении доступом и безопасности.
* Постоянная оценка и уточнение целей анализа данных позволяет принимать обоснованные решения для оптимизации работы СКУД.

Таким образом, анализ данных для оптимизации СКУД включает в себя детальный отслеживание поведения сотрудников и посетителей, использование современных инструментов аналитики для визуализации и обработки данных, а также применение полученных выводов для улучшения управления доступом и повышения безопасности объекта.

**Будущее развитие технологий**

Будущее развития технологий систем контроля доступа (СКУД) ожидается как продолжение текущих тенденций, так и внедрение новых технологий и методов идентификации. Вот ключевые моменты, которые следует отметить:

Беспроводные технологии

* В ближайшее время ожидается увеличение использования беспроводных технологий для обмена данными между устройствами СКУД и серверами. Однако, из-за высокой уязвимости радиоканалов, полное переход на беспроводные технологии в критически важных областях безопасности может произойти медленно. Более вероятно, что беспроводные технологии будут активно использоваться в системах управления предприятиями, где преимущества беспроводности очевидны [**1**](https://www.parsec.ru/articles/budushchie-tekhnologii-skud/).

Интеграция и универсальность

* СКУД будет стремиться к интеграции с другими системами управления и контроля, такими как системы обеспечения жизнедеятельности здания, управления предприятием и другие компоненты. Это приведет к тому, что СКУД перестанет быть обособленной системой и станет частью более широкой интегрированной системы [**1**](https://www.parsec.ru/articles/budushchie-tekhnologii-skud/).
* Интеграция будет развиваться в сторону использования более универсальных платформ и технологий, что позволит легче интегрировать СКУД с различными системами и приложениями [**1**](https://www.parsec.ru/articles/budushchie-tekhnologii-skud/).

Технологии идентификации

* В области технологий идентификации ожидается продолжение использования традиционных методов, таких как proximity карточки, а также рост доли комбинированных считывателей, дополненных биометрическими технологиями. Биометрические технологии, такие как сканирование пальцев, будут продолжать развиваться, но не предполагаются радикальные изменения в ближайшие 5-10 лет [**1**](https://www.parsec.ru/articles/budushchie-tekhnologii-skud/).
* Также ожидается развитие "фенечков" — функций, которые позволяют пользователю получать информацию непосредственно на мобильные устройства, например, видеоотчеты о событиях в офисе или информацию о срабатывании охранной сигнализации [**1**](https://www.parsec.ru/articles/budushchie-tekhnologii-skud/).

**Заключение**

В целом, будущее СКУД ожидается как продолжение текущих тенденций к интеграции и универсализации, с постепенным внедрением новых технологий идентификации. Однако, полное переход на новые технологии, такие как беспроводные системы и биометрия, будет происходить постепенно, учитывая требования к безопасности и надежности.

**Литература**

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»  
2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».  
3. Куприянов А.И., Сахаров А.В., Шевцов В.А. «Основы защиты информации».