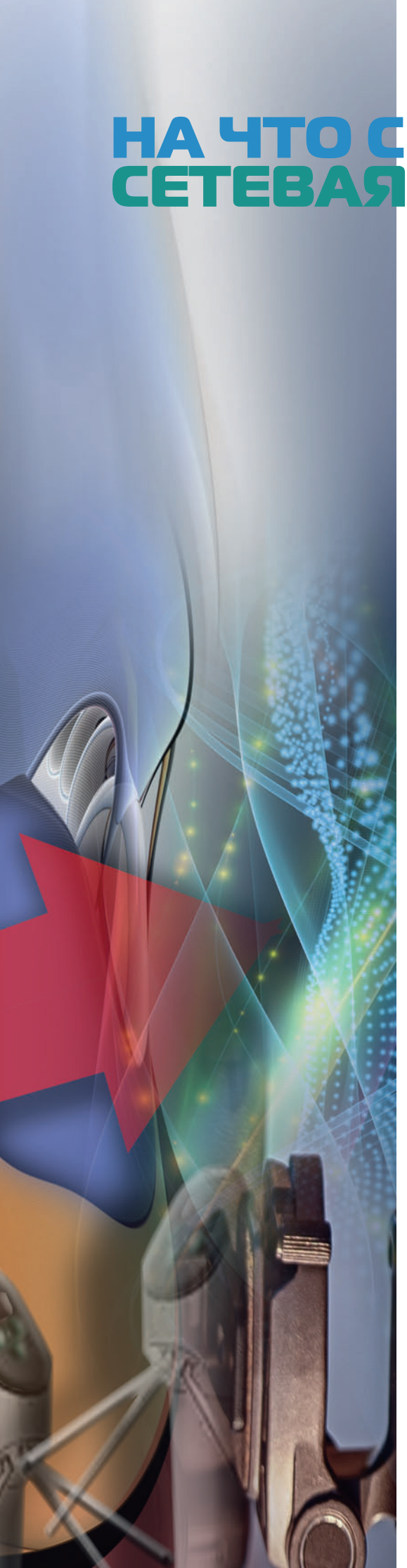


НА ЧТО СПОСОБНА СЕТЕВАЯ СКУД

О. Батманов
начальник отдела разработок ООО «ЕС-пром»,
Ю. Суконщиков
начальник отдела продвижения продукции ООО «ЕС-пром»

Удивительно, но факт: большинство эксплуатирующихся систем контроля и управления доступом (СКУД) решают единственную задачу, заключающуюся в автоматическом различении «своих» от «чужих». Домофоны и подобные им устройства успешно распознают «своих», обеспечивая чистоту в подъездах и отсутствие незваных «чужих» на парковках. Отсутствие централизованного управления – очевидного преимущества сетевой СКУД – автономных системах зачастую компенсируется невысокой ценой создания и владения. Все пользователи простейшей автономной СКУД имеют равные права доступа, в любое время им доступны заданные точки прохода… Такое равенство вряд ли удовлетворит требованиям безопасности мало-мальски серьезного предприятия, где важно разграничить персонал в координатах «кому, когда и куда можно ходить?».

В решении этой задачи на первый план выходит другое достоинство сетевых СКУД – гибкая (в зависимости от выбора системы) настройка уровней доступа.

УРОВЕНЬ ДОСТУПА

«Уровень доступа» (Access Level) – наиболее известное понятие, используемое в СКУД. Уровень доступа (УД) определяет требования по разграничению доступа в помещения или области контроля на объекте и включает в себя множество точек контроля доступа, временные блоки и интервалы и дни недели (календарные числа месяца), в которые разрешен проход *(рис. 1)*.

ФОРМИРОВАНИЕ СПИСКА ТОЧЕК КОНТРОЛЯ ДОСТУПА (КУДА МОЖНО ХОДИТЬ?)

Список точек контроля доступа может формироваться двояко:

- без учета направления прохода (права на вход и выход идентичны);
- учитывая направление прохода (права на вход и выход задаются раздельно).

Первый вариант – проще в реализации, поддерживается всеми сетевыми СКУД. Второй вариант, позволяющий формировать различные правила пропуска на вход и выход для каждой точки доступа, распространен не столь широко, однако только такой подход позволяет решить ряд распространенных задач. Например, организовать разделение зон входа и выхода для отдельных категорий персонала или посетителей на уровне технических средств СКУД, не полагаясь на организационные мероприятия.

РАЗРЕШЕНИЕ ДОСТУПА В ЗАВИСИМОСТИ ОТ ВРЕМЕНИ ПРОХОДА (В КАКИЕ ДНИ, В КАКОЕ ВРЕМЯ?)

Временные блоки и интервалы (Time Zone) – элемент уровня доступа, обеспечивающий возможность запрета/разрешения прохода в определенные промежутки времени. В состав временных блоков включают временные интервалы (в рамках суток), дни недели или календарные дни, в течение которых временные блоки действительны. В простейшем случае может использоваться один интервал времени для всех или выбранных дней недели *(рис. 2)*.

Для предприятий со сменным режимом работы может представлять интерес функция СКУД, обеспечивающая организацию скользящего графика, – автоматическое изменение разрешенных для прохода календарных дней в соответствии с установленным графиком работы.

Сформированные временные блоки должны быть сопоставлены со списком точек доступа. Возможность формирования этого списка с разделением прав

на вход и выход для каждой точки доступа *(рис. 3)* делает реальной реализацию таких режимов прохода, как:

- вход через проходную возможен исключительно в течение 15-30 минут до начала рабочего дня, выход – в течение 30-60 минут после его окончания;
- ограничение доступа посетителей на время проведения периодических работ по причине повышенных требований к безопасности (обслуживание банкоматов инкассаторами – для банковской сферы, ответственные технологические операции – для промышленности).

ФОРМИРОВАНИЕ СОВОКУПНЫХ ПРАВИЛ ПРОХОДА (КОМУ? КУДА? КОГДА?)

В зависимости от функциональных возможностей сетевой СКУД, метод формирования полномочий для каждого пропуска или группы пропусков может отличаться. Можно выделить два основных способа:

1. прямой выбор разрешенных для прохода точек доступа и индивидуальное назначение временных интервалов при добавлении нового пропуска или редактировании его свойств;
2. предварительное формирование списков УД, каждый из которых содержит необходимый набор правил для определенной группы лиц.

На крупных объектах, при большом количестве элементов СКУД, прямой выбор точек доступа и присвоение временных интервалов – задача крайне трудоемкая. Упростить настройку и последующее назначения уровня полномочий можно путем предварительного формирования списков УД, каждый из которых содержит необходимый набор правил доступа для определенной группы лиц *(рис. 4)*, обладающих равными полномочиями: сотрудников одного отдела, руководителей структурных подразделений, персонала охраны, обслуживающего персонала и т.п.

При выдаче пропуска производится сопоставление пропуска с выбранным УД и автоматическое назначение соответствующих прав владельцу идентификатора. Количество уровней доступа, которое может храниться в оборудовании СКУД и/или в базе данных программного обеспечения, может достигать нескольких тысяч, обеспечивая достаточную гибкость формирования полномочий даже на крупных объектах.

ФОРМИРОВАНИЕ ДОПУСТИМЫХ МАРШРУТОВ ПЕРЕМЕЩЕНИЯ (...И ПО КАКОМУ МАРШРУТУ?)

Одним из ключевых достоинств сетевой СКУД является отслеживание последовательности прохода для каждого владельца пропуска, наиболее часто встречающийся вариант которой – функция «запрет повторного прохода» (antipassback).

Основное назначение функции antipassback заключается в защите от несанкционированного прохода нескольких человек в одном направлении по одному пропуску, предотвращении или фиксации нештатных перемещений (например, проникновение на территорию

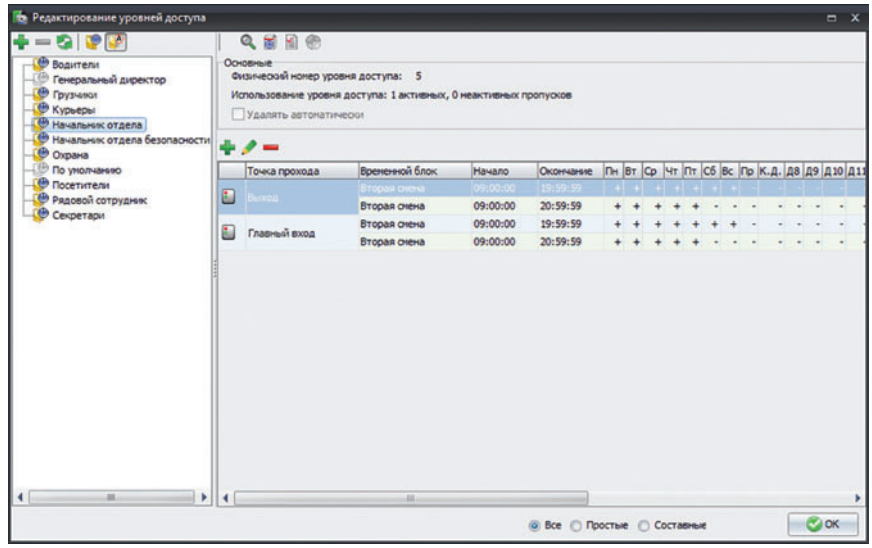


Рис. 1. Редактирование уровня доступа

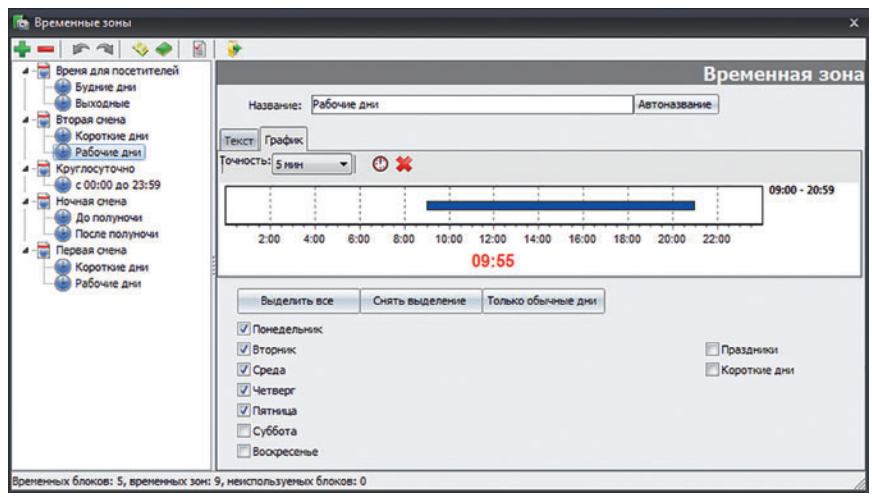
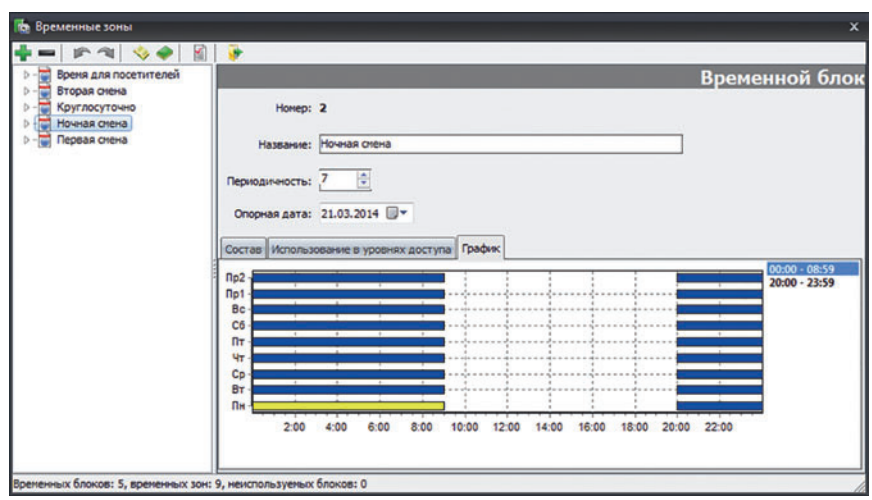


Рис. 2. Один временной интервал для пятидневной рабочей недели (понедельник-пятница)

Рис. 3. Задание временного блока для организации доступа в ночную смену



через ограждение) сотрудников, минуя точки доступа. В более общем случае применения функции контроля последовательности прохода, персоналу предприятия определяются штатные маршруты перемещения, нарушение которых либо препятствует дальнейшему доступу в определенные области контроля, либо обеспечивает фиксацию фактов нарушений с уведомлением персонала охраны и сохранением соответствующих записей в протоколе событий системы. Дополнительный эффект от возможности СКУД поддерживать такую функцию – автоматическое определение зоны нахождения сотрудников, автоматический подсчет числа сотрудников в зонах (что важно при организации экстренной эвакуации) и др.

Для работы этой функции обязательным условием является оборудование всех входов/выходов раздельными считывателями на вход и на выход («двухсторонние точки доступа»).

На практике используются два типа контроля последовательности прохода – локальный и глобальный. Локальный контроль осуществляется в пределах одного контроллера доступа или, чаще всего, в пределах одной точки доступа. Фактически этот тип контроля применим только для замкнутых областей, имеющих один вход, так как при наличии двух и более входов возможен повторный проход через разные точки доступа.

Глобальный контроль последовательности прохода осуществляется на уровне системы в целом и может применяться для областей контроля с большим количеством точек доступа, например, на проходных крупных предприятий, оснащенных турникетами, в зданиях с несколькими входами и т.д. Реализация контроля на уровне системы дает возможность создания сложных маршрутов перемещения.

Большинство систем позволяет отключать функции контроля последовательности прохода для отдельных категорий персонала и руководства в целях обеспечения выполнения ими служебных обязанностей.

БОЛЬШЕ БЕЗОПАСНОСТИ, БОЛЬШЕ УДОБСТВА

Там, где критична безопасность, может быть востребована возможность сетевой СКУД контролировать дополнительные признаки при разрешении прохода:

- «правило нескольких карт» (доступ в помещение, в котором по правилам режима, охраны труда или технологии должно находиться не менее двух (трех) человек);
- подтверждение прохода сопровождающим лицом, сотрудником охраны;
- дополнительная биометрическая идентификация личности;
- предъявление основного идентификатора и ввод пин-кода (с возможностью ввода специально модифицированного личного кода для формирования события «проход под принуждением»).

Следует учесть, что перечисленные выше режимы доступа требуют больше времени на процесс идентификации, потому их использование оправдано для ограниченного количества особо ответственных точек доступа при невысокой интенсивности проходов.

В ситуациях, когда безопасность должна сочетаться с удобством применения, можно обратить внимание на такие режимы доступа, как:

- временный запрет прохода персонала без соответствующих привилегий;
- запрет на вход в зону контроля, обусловленный отсутствием в зоне ответственного за нее лица.

Первый режим может активироваться на время проведения совещаний для запрета входа в кабинет рядовых сотрудников и сохранения возможности входа их руководителей, типичным применением второго режима является необходимость ограничения доступа в кабинет руководителя на время его кратковременных отлучек с рабочего места.

АППАРАТНЫЕ ОСОБЕННОСТИ РЕАЛИЗАЦИИ КОНТРОЛЯ ПОЛНОМОЧИЙ

Важным фактором, определяющим надежность СКУД и ее возможность сохранять работоспособность в условиях значительных потоков событий, является способ реализации контроля полномочий с учетом аппаратных особенностей СКУД. Как правило, основные параметры УД формируются средствами программного обеспечения и через сервер системы заносятся в память контроллеров СКУД. Однако функция контроля последовательности прохода требует изменения правил работы всех контроллеров системы после любого события в одном из них. При программной реализации таких изменений контроллеры необходимо перезагружать по каждому событию в системе, что при большом потоке событий приводит к перегрузкам и полному блокированию СКУД. Кроме того, выполнение функции полностью зависит от работоспособности сервера.

В силу этих причин в профессиональных СКУД предусматривают межконтроллерный обмен информацией и необходимое частичное изменение правил работы для обеспечения функции контроля последовательности прохода. Кроме того, в контроллерах профессиональных СКУД используются встроенные механизмы автоматического упорядочивания базы данных пропусков и оперативного добавления кодов идентификаторов (и уровней доступа) в момент выдачи или изъятия пропуска. Это обеспечивает возможность длительной работы системы без проведения полной инициализации контроллеров, ускорение операций по активации новых пропусков, уменьшение количества информации, передаваемой по сети СКУД, и исключение периодов простоя отдельных точек доступа, вызванных процессом инициализации.

Рис. 4. Назначение уровня доступа из предварительно сформированного списка