

# ГОТОВА ЛИ ВАША СИСТЕМА УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ К КРИЗИСНОЙ СИТУАЦИИ НА ОБЪЕКТЕ?

**К**огда речь заходит о тенденциях в области технологии контроля доступа, внедрение предопределенных сценариев реагирования на локальные кризисные ситуации, таких как опция управления уровнями безопасности (Security Level Management) от компании Nedap, является ключевым моментом в возможностях систем контроля доступа для адаптации к чрезвычайным ситуациям. В частности, с точки зрения времени реакции и с точки зрения возможного реагирования пропорционально серьезности инцидента.

В сегодняшнем постоянно меняющемся мире обычный контроль доступа может оказаться недостаточным для обеспечения безопасности всей структуры зданий компании - клиента. Все большее число заказчиков требуют системы контроля доступа, способные реагировать на различные тревожные ситуации и возможные угрозы без остановки общего контроля.

## ОСНОВНЫЕ ПРЕИМУЩЕСТВА

С точки зрения безопасности и возможных рисков мы считаем, что переход к более интеллектуальным системам контроля доступа с предопределенными сценариями реагирования на кризисные ситуации дает заказчику целый ряд весомых преимуществ. В частности, такой подход позволяет выбрать оптимальную реакцию в соответствии с политикой безопасности в конкретной кризисной ситуации.

Электронные системы контроля доступа были разработаны в качестве инструментария для работников служб безопасности при предоставлении посетителям доступа, основанного на таких параметрах, как идентификационный номер, время, день и место. В случае возникновения чрезвычайной ситуации вы можете переопределить эти параметры вручную, изменив настройки системы. Для небольшой организации с ограни-

ченным числом точек доступа и небольшим людским потоком такой вариант может работать без каких-либо проблем. В случае более крупных организаций, с большим штатом сотрудников, потоком посетителей и множеством точек доступа, задача вручную оперативно изменить настройки авторизации, особенно если оператор системы находится под психологическим давлением, становится очень серьезной проблемой. Управление уровнями безопасности позволяет менеджерам по безопасности заранее создавать чрезвычайные сценарии реагирования и активировать их в системе одним кликом мыши. Безусловно, это значительно облегчает адекватную и быструю реакцию на ситуацию.

Кроме того, ручная перенастройка параметров системы, закрывание или открывание ряда физических входов или аннулирование прав доступа определенным лицам в режиме «все или ничего» – является рискованным решением, которое может быть очень несоизмеримым действием для данного инцидента. В конечном счете, это может привести к ненужным нарушениям правил безопасности на объекте и затруднить последующее функционирование системы контроля доступа в нормальном режиме. Функция управления уровнями безопасности позволяет менеджерам по безопасности возвращать и забирать авторизацию для конкретных лиц и транспортных средств посредством моментального переключения на другой уровень безопасности.

## ПРАВИЛЬНАЯ АРХИТЕКТУРА КАК РЕШАЮЩИЙ АРГУМЕНТ

Кроме прогнозирования определенных угроз и предопределения желаемой реакции системы контроля доступа, очень важно иметь возможность заставить систему повести себя соответствующим образом в доли секунды.

В чрезвычайных ситуациях вы, безусловно, не захотите зависеть от скорости сети для отработки необходимого сценария - реакции на тревогу. Время имеет решающее значение. Поэтому требуемый сценарий ответа на внешнее вторжение должен храниться непосредственно на локальных контроллерах.

Создавая определенные комбинации для групп посетителей и входных групп (точек прохода) и сохраняя их затем на локальном уровне, вы можете создать адекватную реакцию системы на любые предсказуемые происшествия.

## ПРИМЕРЫ КРИЗИСНЫХ СЦЕНАРИЕВ

Примером предопределенной модели реакции может быть сценарий реагирования на панику. Как правило, все внешние входы по периметру определенного департамента или отдела (например финансового), находятся под контролем. Если что-то происходит, данный отдел подлежит эвакуации. Работники должны быстро выйти, но им не должно быть разрешено зайти обратно или заходить в особо охраняемые помещения. С помощью функции управления уровнями безопасности данный сценарий можно включить моментально после поступления сигнала о панике. Таким образом, немедленная смена уровня доступа позволяет организовать эвакуацию сотрудников так, что всем дается право на выход, но никому не разрешается войти обратно.

## БЫТЬ ПОД КОНТРОЛЕМ ПРИ ЛЮБЫХ ОБСТОЯТЕЛЬСТВАХ

В заключение можно сказать, что появление таких опций, как управление уровнями безопасности в системе AEOS, вне всяких сомнений, открывает широчайшие возможности для служб безопасности, позволяя им сохранять полноценный контроль доступа к своим помещениям даже во время кризисных ситуаций. При этом сотрудники служб безопасности могут быстро и точно реагировать на ожидаемые инциденты без причинения какого-либо ущерба всей организации безопасности на объекте.



nedap  
aeos

109129, Москва, а/я 10,

+7 (495) 662-89-84,

+7 (916) 675-10-55

E-mail: info-ru@nedap.com

[www.nedap-securitymanagement.com](http://www.nedap-securitymanagement.com)