

Система контроля доступа

Краткое описание

OnGuard Access это интегрированная система контроля доступа и мониторинга тревог, обеспечивающая максимальную защиту, универсальность, простоту управления и экономичность. OnGuard Access включает в себя самые современные на сегодняшний день технологии, включая объектно-ориентированное программное обеспечение, усовершенствованную клиент/серверную архитектуру базы данных и разработанную Microsoft многозадачную и обеспечивающую многопоточность 32-разрядную операционную систему Windows 2000/XP/2003. Благодаря комбинации надежной технологии и интуитивно-понятного графического интерфейса пользователя OnGuard Access является самой мощной и, одновременно, самой простой в эксплуатации интегрированной системой управления безопасностью на рынке.

Неограниченный масштаб применения

OnGuard Access имеет неограниченные возможности для расширения в рамках единого полностью интегрированного программного решения. Она была разработана с учетом потребностей организации любого размера, от небольшой фирмы, для которой требуется система базового уровня с двумя считывателями, до крупной корпорации с многочисленными зданиями и тысячами считывателей, расположенными по всему миру. OnGuard Access позволяет использовать неограниченное число считывателей, тревожных точек и владельцев карт.

Сегментация

Сегментация является дополнительной функцией, обеспечивающей логический способ группировки компонент базы данных. Системные администраторы делят базу данных на сегменты, затем привязывают каждого пользователя или объект (уровни доступа, форматы карт, типы пропусков и т.д.) к одному или нескольким сегментам. Сегментация полезна в тех случаях, когда каждому владельцу карты не требуется доступ во все зоны объекта. Пользователь видит только те объекты, которые относятся к его сегменту, а также объекты, общие для всей системы. В сегментированной системе в интеллектуальные контроллеры системы и соответствующее периферийное оборудование загружаются только записи, связанные с данным сегментом. Сводя к минимуму число записей, которые должны храниться в заданном устройстве, сегментация позволяет более эффективно использовать ограниченный объем памяти устройств контроля доступа.

Планировщик

Программа планирования заданий OnGuard позволяет системным администраторам координировать и планировать действия системы, которые будут выполняться в будущем. Многие системные операции могут и часто должны происходить в определенные дни и в определенное время.. Чтобы избежать возможных ошибок при выполнении этих функций вручную, администраторы могут устанавливать правила выполнения таких действий, как запуск тура патрулирования, архивирование, загрузка программного обеспечения или баз данных и сценариев обмена данными. Планировщик можно также настроить для повторения определенных действий, таких как таких как постановка/снятие с охраны разделов или маскирование/снятие маскирования определенных тревог. Каждое действие может быть запланировано для выполнения только один раз или для повторения в определенное время каждый день, в конкретные дни недели или по конкретным числам месяца – так часто, как требуется.

Поддержка

- Поддержка следующих типов связи с интеллектуальным системным контроллером
 - Ethernet
 - RS-232
 - Шина (RS-485)
 - Модем
 - Дублирование канала связи
- FIPS 197 – обмен информацией с интеллектуальным системным контроллером с использованием 128-разрядных ключей шифрования AES.
- FIPS 140-2 - сертификат в процессе оформления
- Поддержка большинства стандартных технологий считывателей карт

Возможности

Гибкие возможности программирования

- Разблокировка по первой карте
- Управление лифтами
- (Избирательная) загрузка системной информации
- Программа импорта/экспорта
- Ограничение количества людей в зоне
- Локальный и глобальный запрет повторного прохода

Гибкие возможности мониторинга

- Группы маскирования тревог
- Графические карты и древовидное отображение состояния системы
- Зоны мониторинга
- Распределение и маршрутизация тревог/событий
- Пользовательская настройка речевых инструкций и оповещения

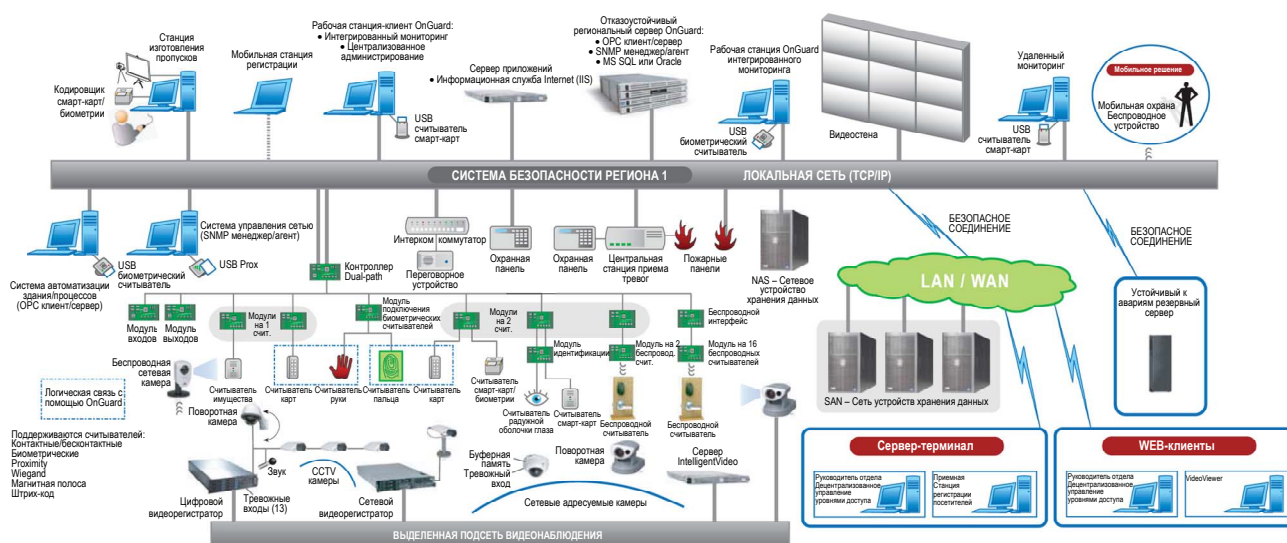
Гибкие режимы работы карт

- Поддержка режима сопровождения
- Ограничение использования карты
- Увеличенное время открытия замка и (по требованию) периода удержания двери.
- Контроль достижения точки назначения (с управлением лифтом)

Гибкие режимы работы считывателей

- Игнорирование временных зон
- Режим кодового замка
- Разные форматы карт
- Счетчик неудачных попыток доступа

Архитектура системы OnGuard



Управление зонами

- **Глобальный жесткий запрет повторного прохода** позволяет администраторам требовать, чтобы владельцы карт предъявляли пропуск, как при входе, так и при выходе из зоны. При этой установке не допускается одновременное использование того же пропуска в другой зоне, и в этом случае передается сигнал тревоги на рабочие станции мониторинга тревог.
- **Глобальный мягкий запрет повторного прохода** позволяет администраторам требовать, чтобы владельцы карт предъявляли пропуск, как при входе, так и при выходе из зоны. При этой установке допускается одновременное использование пропуска в другой зоне, но при этом сигнал тревоги передается на рабочие станции мониторинга тревог.
- **Временный запрет повторного прохода** (между считывателями) позволяет администраторам устанавливать интервал повторного предоставления доступа по одной карте на одном считывателе. Эту установку можно также применить к группе считывателей, что очень удобно в системах с турникетами, где несколько считывателей установлены по соседству друг с другом, и где существует возможность передачи пропуска и его повторного использования другим лицом.
- **Правило 2-х лиц** позволяет администратору задать режим работы, когда необходимо чтобы в зоне с повышенным уровнем защиты находилось не менее двух человек. Чтобы первые два владельца карт могли войти в зону, или последние два владельца карт могли выйти из зоны необходимо предъявить оба пропуска. Между этими проходами возможен индивидуальный доступ в зону, так как соблюдается правило минимального количества людей в зоне.
- **Правило 1-го лица** позволяет администратору задать режим работы, когда необходимо чтобы в зону со специальным уровнем защиты сначала допускалось ответственное лицо. После регистрации в данной зоне ответственного лица туда допускаются другие лица. Ответственное лицо должно покинуть зону последним.
- **Ограничение максимального количества людей в зоне** позволяет администраторам ограничивать количество людей, которые могут одновременно находиться в заданной зоне. После достижения заданного лимита считыватель на входе не позволяет пройти в зону, пока кто-нибудь из владельцев карт не выйдет из зоны, предъявив карту считывателю на выходе. Это полезная функция может использоваться для управления доступом на автостоянку с ограниченным числом мест.

Глобальная связь входов/выходов/событий

OnGuard позволяет администраторам выполнять настройку взаимосвязи, при которой любой из входов/выходов/событий может связываться с любым другим входом/выходом/событием в системе. Такие связи могут осуществляться с любым другим приложением OnGuard и соответствующим оборудованием. Такие события, как неверный уровень доступа, верное считывание карты или сигнал детектора движения могут активировать такие выходные сигналы, как отмена блокировки тревог, разблокировка зоны или активация считывателя карт. С помощью этой функции легко выполнить автоматизацию OnGuard и обеспечить правильное выполнение установок и, в случае необходимости, мгновенное реагирование системы безопасности.