

BIS — Access Engine (ACE) 5.0



Управление доступом на сегодняшний день является одной из важнейших технологий, способствующих повышению безопасности людей, имущества и ресурсов. BIS модуль Access Engine и самые современные контроллеры обеспечивают широкий функционал системы контроля и управления доступом.

При объединении базового пакета Access Engine и дополнительных функций можно построить систему управления доступом, отвечающую именно вашим требованиям. После этого нужно лишь воспользоваться программным обеспечением Building Integration System для объединения модуля Access Engine с системой видеонаблюдения и охранной системой.

Обзор системы

Программное обеспечение Access Engine (ACE) в сочетании с оборудованием управления доступом Bosch составляют комплексную систему управления доступом на платформе Building Integration System (BIS). Эта система имеет все основные функции любой автономной системы управления доступом, а также целый ряд дополнительных функций.

Как и другие модули BIS, ACE пользуется всеми преимуществами, предоставляемыми системой BIS, например интерактивными планами объектов и

- ▶ Распределенная система управления доступом с графическим управлением тревогами
- ▶ Идеальная интеграция и взаимодействие с системой видеонаблюдения, охранной системой, системой пожарной сигнализации и системой речевого и аварийного оповещения через общую платформу BIS.
- ▶ Высокая устойчивость благодаря 4-уровневой архитектуре системы и резервному развертыванию ключевых компонентов
- ▶ Интеграция продуктов сторонних производителей с помощью защищенных протоколов и комплекта SDK
- ▶ Быстрая, эффективная и безопасная процедура регистрации

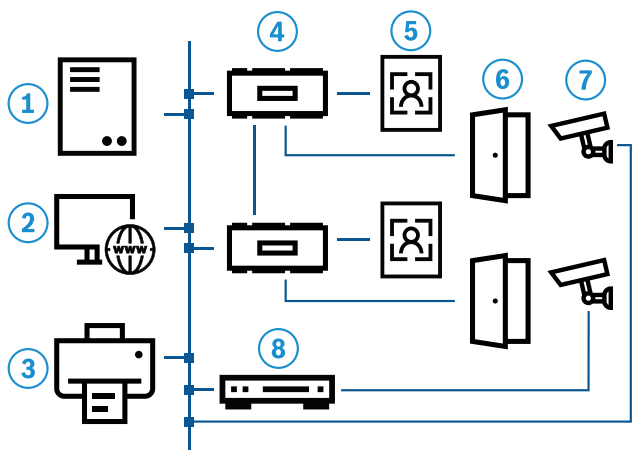
планами действий, обеспечивающими комплексное и эффективное управление тревогами. Тревожные сообщения и события управления доступом могут отображаться вместе с графической информацией и инструкциями в потоке заданий.

ACE использует стандартные пользовательские интерфейсы BIS, допускающие настройку с учетом индивидуальных требований. Кроме того, ACE обеспечивает специфические интерфейсы управления доступом для владельцев карт, аппаратного оборудования и правил доступа.

Основное преимущество системы Building Integration System заключается в интеграции различных систем защиты и безопасности в одном учреждении. Благодаря объединению ACE с другими модулями BIS (например, Automation и Video) можно создавать интеллектуальные системы безопасности, в точности соответствующие требованиям заказчика.

Модуль Access Engine может работать на одной рабочей станции в клиент-серверной системе или в распределенной среде с центральным сервером и локальными или региональными серверами. В распределенной многосерверной среде всеми устройствами, держателями карт и разрешениями можно управлять с сервера верхнего уровня.

Чтобы обеспечить повышенную безопасность и целостность данных, BIS ACE может управлять контроллерами RS485 с высокой степенью защиты с помощью протокола OSDP v2 для аутентифицированного зашифрованного обмена данными и контроля считывателей.



№	Описание (односерверная система)
1	Центральный сервер BIS с ПО Access Engine и Video Engine
2	Несколько рабочих станций для управления тревогами или регистрации
3	Устройства регистрации, такие как принтер карт, сканер подписей, регистрационное считывающее устройство, камера для идентификационных фотографий
4	Контроллеры доступа
5	Считыватели доступа
6	Дверные замки
7	IP-камера
8	Цифровой видеорегистратор, например DIVAR, для записи тревог

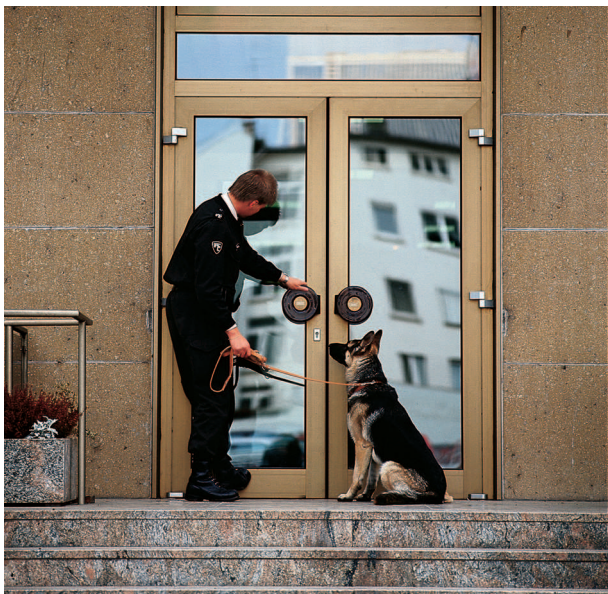
Функции

В базовый пакет Access Engine (в сочетании с контроллерами доступа АМС) входят следующие функции:

- Широкий диапазон понятных шаблонных моделей дверей, обеспечивающих быструю и удобную настройку оборудования (например, стандартная дверь, турникет, лифт со считывателями, учет времени и присутствия и т. д.).
- В диалоговом окне настройки моделей дверей генерируется план проводки для установщика оборудования.

- Отлаженный процесс регистрации, включая регистрацию карт и биометрических данных.
- Настраиваемые диалоговые окна для сбора только необходимых личных сведений.
- Временные модели для контроля доступа по времени, включая определение особых дней, ежегодных государственных праздников и т. д.
- Временные модели для автоматической активации/деактивации учетных данных владельца карты, PIN-кодов и т. д.
- Временные модели для автоматической активации/деактивации системных параметров (например, установка разблокированного состояния двери офиса в период с 9:00 до 17:00).
- Дополнительный PIN-код для активации/деактивации тревоги охранной системы.
- Временное блокирование/разблокирование владельцев карт (вручную или по времени).
- Занесение карт в черный список.
- Запрет двойного прохода.
- Балансировка области доступа, включая проверку последовательности доступа, обеспечивает средства ограничения количества людей в определенной области, автоматическую активацию/деактивацию тревоги охранной системы, если область пуста/не пуста и создание списков опроса.
- Авторизация доступа для N человек обеспечивает доступ к двери только в том случае, если определенное количество (N) авторизованных владельцев карт предоставляют свои бэйджи в соответствующим образом настроенный считыватель. Этот параметр может быть установлен для каждого считывателя отдельно и для количества людей от 2 до N (без ограничений).
- Функция шлюза для управления двумя взаимодействующими дверьми с двумя парами считывателей; рекомендуется для зон с высокой степенью защиты, например для входа в серверные или исследовательские отделы.
- Маршрут патрулирования: современная система отслеживания патрулирования, использующая считыватели системы управления доступом, последовательности доступа и проверку времени доступа. Любые нарушения последовательности или времени доступа вызывают сигнал тревоги, если они отслеживаются современными

функциями управления тревог BIS. Отчеты о патрулировании могут создаваться на основании журнала регистрации событий BIS.



- Функция случайного досмотра: владельцы карт, входящие на участок или покидающие его, могут быть остановлены случайным образом и направлены к персоналу службы безопасности для более тщательного досмотра. Карты, принадлежащие указанным VIP-персонам, могут быть исключены из процедуры случайного досмотра.
- Управление посетителями: карты могут отслеживаться и обрабатываться отдельно в соответствии со сроком действия и возможной необходимостью в сопровождении.
- Интерфейс для постановки на охрану/снятия с охраны системы охранной сигнализации, включая обработку операций авторизации и назначение карт.
- С помощью веб-интерфейса можно импортировать и экспортировать данные о владельцах карт, хранящиеся в сторонних системах или на сервере каталогов, например на сервере Microsoft Active Directory или Apache Directory.
- Все персональные данные (включая фотографии и подписи) хранятся в защищенной базе данных SQL.
- С помощью функций управления уровнями угроз можно предварительно настроить до 15 сценариев, включая экстренную блокировку дверей и эвакуацию.
- Интерфейс лифта для контроля до 64 этажей с помощью встроенного в лифт считывателя карт, а также для назначения владельцам карт прав доступа на определенные этажи.
- Интерфейс для взаимодействия с системами управления лифтами позволяет контролировать доступ до 255 этажей в лифтовой системе с передней и задней дверями.
- Интерфейс для импорта данных о персонале из системы управления персоналом или для экспорта этих данных из ACE в такую систему.
- Улучшенная персонализация карт для импорта изображений владельцев карт и создания корпоративных бейджей, которые можно распечатать на стандартном принтере для печати карт.
- Функция дистанционного открывания дверей, например посредством щелчка мышью по значку на интерактивном плане объекта BIS.
- Создание логических областей, например отдельных помещений, групп помещений, этажей или автостоянок, которым назначаются специализированные точки управления доступом.
- Гибкое управление тревожными сигналами для целого ряда тревожных ситуаций (например, отказ в доступе, несанкционированный доступ, бейдж из черного списка, сигнал действия по принуждению и т. д.) в сочетании с такими функциями BIS, как интерактивные планы объектов и планы действий.
- Использование контролируемых цифровых систем ввода-вывода контроллеров Bosch для дополнительного контроля и мониторинга, включая обнаружение попыток вторжения и несанкционированного доступа.
- Связь между локальными контроллерами доступа и считывателями обеспечивается OSDP v2 (безопасный канал OSDP).
- Связь между основной системой управления доступом и локальными контроллерами доступа выполняется по протоколу DTLS (с шифрованием AES-256).

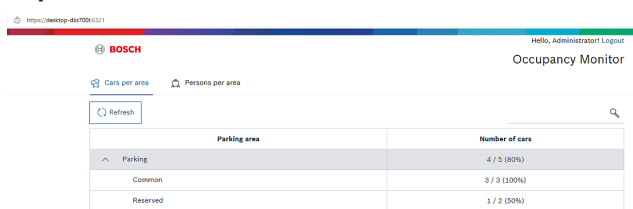


- Подробная регистрация в журнале всех событий доступа и тревог для обеспечения соответствия законам и анализа событий.
 - Отслеживание изменений в главных записях и авторизациях, включая создание, модификацию и удаление записей.
 - Создание комплексных отчетов с возможностью фильтрации.
- Одновременная поддержка до восьми различных форматов карт.
- Массовое редактирование данных авторизаций и других данных.

Видеоподтверждение

Функция видеоподтверждения повышает уровень надежности системы управления доступом благодаря использованию видеотехнологий. Когда считыватель находится в режиме видеоподтверждения, владельцу карты не предоставляется непосредственный доступ. Считыватель выполняет запрос на вход, который отображается как сообщение на экране оператора. План действий (см. дополнительные аксессуары BIS) показывает оператору изображение владельца карты, сохраненное в базе данных ACE, рядом с изображением с камеры, расположенной у входа/считывателя, с которого поступил запрос. Оператор сравнивает изображения и принимает решение об открытии дверей.

Управление автостоянкой



Эта функция позволяет определить и использовать модель дверей «автостоянка», в которой содержатся два ограждения на выход и на вход, а также световор, препятствующий доступу, когда на автостоянке больше нет свободных мест.

Доступ к парковкам может осуществляться с помощью считывателей дальнего действия и идентификационных карт, или посредством камеры и номерных знаков.

Каждую автостоянку можно разделить на логические области и определить для каждой из них максимальное количество автомобилей.

Авторизация для прохождения ограждения и парковки в логической области может быть определена для владельцев карт в стандартном диалоговом окне. Возможно также динамическое распределение нагрузки на автостоянке при отображении на экране оператора текущей информации о свободных местах. Распределение нагрузки по автомобилям (парковки) и людям (зоны доступа) осуществляется отдельно, поэтому можно одновременно отследить местоположение владельца карты и автомобиля.

Управление посетителями

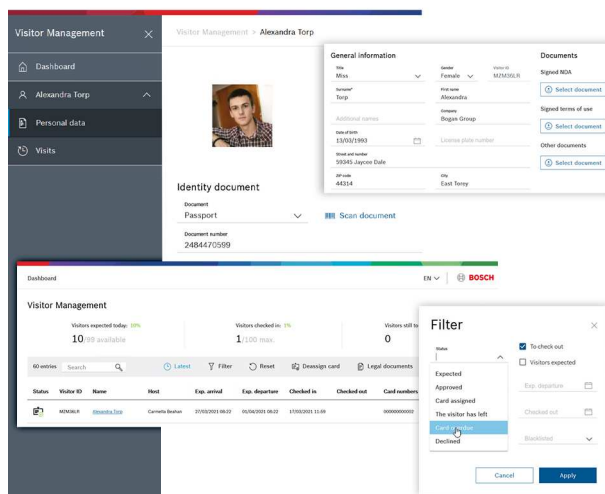
- Осуществляйте предварительную регистрацию встреч в системе для сокращения времени обработки.
- Предоставьте возможность посетителям создавать собственные профили в режиме kiosка, чтобы избежать очередей на ресепшене.
- Используйте панель мониторинга для отслеживания ожидаемых посещений дня, текущего количества посетителей на территории

объекта, используемых в данный момент ID карт, а также ID карт, запланированных к использованию.

- Настройте даты истечения срока действия профилей посетителей и их вложений, чтобы обеспечить соблюдение национальных нормативных требований в отношении конфиденциальности данных, например Общего регламента защиты данных (GDPR) Евросоюза.

Welcome

Please enter your visitor ID.



Интеграция охранных панелей

Разрешения на работу с охранными панелями Bosch V/G series могут быть назначены картодержателям централизованно, что позволяет им ставить на охрану и снимать с охраны разделы охранной сигнализации.

При наличии соответствующих прав доступа картодержатель может снять область с охраны и разблокировать дверь с помощью считывания одной карты простым считывателем.

Управление доступом для контроля заболеваний

- Новые бесконтактные считыватели и считыватели с распознаванием лиц позволяют избавиться от опасного источника заражения. В целях повышения безопасности система может дополнительно требовать для проверки подлинности бесконтактную карту или дополнительные биометрические учетные данные.
- Управление последовательностью доступа помогает обеспечить движение людей в одном направлении, что снижает риск заражения и избавляет от встречи лицом к лицу.
- Управление уровнями угроз ACE позволяет мгновенно переключаться с одной схемы движения людей на другую в чрезвычайной ситуации.

- Области управления доступом ACE идеально подходят для быстрой реализации гигиенических ограничений на количество лиц в заданном пространстве.
- Бесконтактные считыватели избавляют от необходимости использования физических кнопок лифта.
- Бесконтактная постанковка на охрану и снятие с охраны охранных разделов дополнительно сокращает количество источников заражения.
- Использование мобильных телефонов для доступа повышает уровень гигиены за счет уменьшения количества совместно используемых физических идентификаторов. Это решение разработано совместно с нашими партнерами **NiD** и **STiD**.
- Системы распознавания номерных знаков снижают необходимость использования кабин с операторами, клавиатур и кнопок, а также необходимость выхода из автомобиля для использования физических идентификаторов.

Аксессуары для BIS Access Engine

Расширенное управление парковкой

Обеспечивает управление гостевой парковкой, включая создание парковочных талонов и уведомлений о посетителях, которые остаются на парковке дольше, чем запланированная встреча.

Интерфейс прикладного программирования

Пакет разработки программ (SDK) для интеграции Access Engine со сторонними приложениями, такими как системы управления идентификациями, системы данных о времени и присутствии и расширенные системы управления посетителями.

Интеграция ключниц

Интеграция ключниц **Deister** и **Kemas** для обеспечения безопасности физических ключей и мониторинга их использования. Доступно только в определенных странах.

Интеграция беспроводных сетевых замков

Интеграция беспроводных сетевых замков **SimonsVoss SmartIntego** (цилиндры, ручки дверей и замки) для дверей, которым требуется средний уровень безопасности, например дверей офисов и аудиторий. Доступно только в определенных странах.

Интеграция удаленных автономных замков

Интеграция **совместимых с OSS-SO автономных замков** или автономных замков **Normbau (Pegasys)** для удаленных дверей, которые невозможно подключить кабелем из-за большого расстояния, условий в здании или стоимости. Автономная система блокировки состоит из программного обеспечения, аппаратной части и аксессуаров. Аппаратное обеспечение доступно на рынке и предоставляется партнерами Bosch. Лицензия

программного обеспечения поддерживает несколько диалогов в BIS и ACE. Доступно только в определенных странах.

Увеличение ресурсов управления доступом

ACE обеспечивает удобное масштабирование в соответствии с растущими потребностями ваших объектов. Дополнительные лицензии MAC (Main Access Controller) позволяют увеличить географическое покрытие или производительность. Добавляя лицензии владельцев карт, можно работать с увеличивающимся числом сотрудников или посетителей.

Лицензии на дополнительные входы приобретаются в количестве, кратном 32, 128 или 512. В этом смысле вход соответствует модели двери ACE, что облегчает расчет требований.

Пример. На участке находятся 2 главных входа, каждый из которых оснащен считывателями на вход и на выход, 26 офисных дверей со считывателем на входе и 1 шлюз для серверной. Общее количество моделей дверей/входов составляет 29 независимо от количества задействованных считывателей. Общее количество (32 входов) уже охватывается лицензией на базовый пакет ACE.

Замечания по установке и настройке

Access Engine в цифрах

Приведенные максимальные значения относятся к эталонной системе, описанной ниже.

Макс. кол-во активных карт на систему	400,000
Макс. кол-во считывателей на сервер	10,000
Макс. кол-во главных контроллеров доступа (MAC) на сервер	40
Макс. кол-во авторизаций доступа на MAC	1,000
Макс. число контроллеров АМС на один контроллер MAC	125 Для высокопроизводительных систем: 60
Макс. кол-во авторизаций доступа на ACE	40,000
Макс. количество подразделений на систему ACE	400
Макс. количество маршрутов патрулирования на систему ACE	200
Макс. количество одновременных маршрутов патрулирования	8
Макс. число охранных панелей В/Г для синхронизации держателей карт с ACE	500

Эталонные системы для сервера и клиента

	Серверная система (без клиента)	Клиентская система
ЦП	Intel Xeon E-2144G @ 3,6 ГГц (4 ядра, 8 логических)	Intel Core i7-8700 @ 3,2 ГГц (6 ядер, 12 логических)
ОЗУ	32 ГБ (2667 МГц)	8 ГБ (2667 МГц)
Видеокарта	Графический процессор, встроенный в ЦП	Intel UHD Graphics 630 (4 ГБ графической памяти)
Системный диск	NVMe Скорость записи: 1440 скорость считывания МБ/с: 2250МБ/с Среднее время отклика 10мс	Твердотельный диск
Диск, на котором установлено AMS	Твердотельный диск Скорость записи: 1000 скорость считывания МБ/с: 1100МБ/с Среднее время отклика 10мс	
Операционная система	Microsoft Server 2019 Standard	Microsoft 10 Pro

Версии браузера для веб-надстроек

Браузер	Версия
Google Chrome	112 или выше
Microsoft Edge	111 или выше
Mozilla Firefox	102 или выше

Технические характеристики

См. спецификации для соответствующей версии базового пакета BIS.

Информация для заказа**BIS-FACE-API50 Лицензия на API**

Лицензия на BIS Access Engine для API
Номер заказа **BIS-FACE-API50 | F.01U.415.274**

BIS-FACE-BPA50 Базовая лицензия

Базовая лицензия на BIS Access Engine
Номер заказа **BIS-FACE-BPA50 | F.01U.415.273**

BIS-FACE-OFFL50 Лицензия на автономный базовый пакет

Лицензия на автономный базовый пакет (ACE)
Номер заказа **BIS-FACE-OFFL50 | F.01U.415.275**

BIS-FACE-PRK50 Лицензия на управление парковкой

Лицензия на управление парковкой (ACE)
Номер заказа **BIS-FACE-PRK50 | F.01U.415.277**

BIS-FACE-VISWEB50 Лицензия на управление посетителями

Лицензия на управление посетителями (ACE)
Номер заказа **BIS-FACE-VISWEB50 | F.01U.415.276**

BIS-XACE-100C50 Лицензия на 100 идентификационных карт

Лицензия на 100 идент. карт (ACE)
Номер заказа **BIS-XACE-100C50 | F.01U.415.290**

BIS-XACE-10KC50 Лицензия на 10 000 идентификационных карт

Лицензия на 10 000 идент. карт (ACE)
Номер заказа **BIS-XACE-10KC50 | F.01U.415.292**

BIS-XACE-10MC50 Лицензия на 10 контроллеров MAC

Лицензия на 10 контроллеров MAC (ACE)
Номер заказа **BIS-XACE-10MC50 | F.01U.415.285**

BIS-XACE-128D50 Лицензия на 128 дверей

Лицензия на 128 дверей (ACE)
Номер заказа **BIS-XACE-128D50 | F.01U.415.288**

BIS-XACE-1KC50 Лицензия на 1000 идентификационных карт

Лицензия на 1000 идент. карт
Номер заказа **BIS-XACE-1KC50 | F.01U.415.291**

BIS-XACE-1KEY50 Лицензия на 1 ящик с ключами

Лицензия на 1 ящик с ключами
Номер заказа **BIS-XACE-1KEY50 | F.01U.415.295**

BIS-XACE-1MAC50 Лицензия на 1 контроллер MAC

Лицензия на 1 контроллер MAC
Номер заказа **BIS-XACE-1MAC50 | F.01U.415.284**

BIS-XACE-25OF50 Лицензия на 25 автономных дверей

Лицензия на 25 автономных дверей
Номер заказа **BIS-XACE-25OF50 | F.01U.415.286**

BIS-XACE-25ON50 Лицензия на 25 беспроводных подключенных к сети дверей

Лицензия на 25 беспроводных подключенных к сети дверей
Номер заказа **BIS-XACE-25ON50 | F.01U.415.294**

BIS-XACE-32DR50 Лицензия на 32 двери

Лицензия на 32 двери
Номер заказа **BIS-XACE-32DR50 | F.01U.415.287**

BIS-XACE-50KC50 Лицензия на 50 000 идентификационных карт

Лицензия на 50 000 идент. карт
Номер заказа **BIS-XACE-50KC50 | F.01U.415.293**

BIS-XACE-512D50 Лицензия на 512 дверей

Лицензия на 512 дверей
Номер заказа **BIS-XACE-512D50 | F.01U.415.289**

BIS-XACE-25OS50 Лицензия на 25 автономных дверей OSS-SO

Лицензия на 25 автономных дверей OSS-SO
Номер заказа **BIS-XACE-25OS50 | F.01U.415.309**

Представительство:

Europe, Middle East, Africa:

Bosch Security Systems B.V.
P.O. Box 80002
5600 JB Eindhoven, The Netherlands
Phone: + 31 40 2577 284
www.boschsecurity.com/xc/en/contact/
www.boschsecurity.com

Germany:

Bosch Sicherheitssysteme GmbH
Robert-Bosch-Ring 5
85630 Grasbrunn
Tel.: +49 (0)89 6290 0
Fax: +49 (0)89 6290 1020
de.securitysystems@bosch.com
www.boschsecurity.com