

WHITE PAPER

IDMATIC NET

*Единая модульная платформа управления физическим
доступом
и операционной безопасностью*

Управление людьми, транспортом, активами и оборудованием

от основания и цифрового права до исполнения, присутствия и доказательного аудита

Редакция 2.0 • Июль 2026 года

Публичный коммерческо-технический документ

АО «МТТ Контрол» • Компания на рынке с 1995 года

Содержание

Оглавление обновляется при открытии документа

Структура документа

1. Резюме для руководителя
2. Проблема разрозненного физического доступа
3. Позиционирование IDMATIC NET
4. Продуктовая архитектура
5. Ключевые принципы платформы
6. Объекты управления
7. Цифровое физическое право
8. IDMATIC Rights Governance
9. Жизненный цикл физического права
10. IDMATIC CRM и workflow
11. IDMATIC Visitor
12. IDMATIC Access
13. Идентификация на посту
14. IDMATIC Time & Presence
15. Биометрия
16. IDMATIC Transport
17. Подрядчики и временный персонал
18. Ключи и материальные активы
19. IDMATIC Industrial — допуск к оборудованию
20. Физическая защита информации
21. IDMATIC MOBILE
22. Защищённый цифровой пропуск
23. IDMATIC Edge и offline-first
24. Архитектура и данные
25. Интеграционная и партнёрская программа
26. AI-ассистент
27. Интеграция с экосистемой безопасности
28. Безопасность и защита данных
29. Продуктовая документация и доказательность
30. Варианты развёртывания
31. Аналитика и показатели управления
32. Экономический эффект
33. Порядок внедрения
34. Критерии успешности пилота
35. Основные риски и способы снижения
36. Заключение

1. Резюме для руководителя

IDMATIC NET — единая модульная платформа для управления физическим доступом людей, транспорта, подрядчиков, активов и оборудования. Она объединяет в одной модели основания, заявки, согласования, цифровые права, точки исполнения, присутствие, доказательства и управленческую аналитику.

Платформа предназначена для организаций, которым недостаточно классической СКУД как набора контроллеров, считывателей и пропусков. IDMATIC NET управляет не только фактом открытия двери или шлагбаума, но и всем жизненным циклом физического права:

- почему право возникло;
- кто его согласовал;
- для какого объекта, зоны, маршрута, действия и времени оно выдано;
- какие условия должны соблюдаться;
- где и каким устройством право было исполнено;
- когда и по какой причине оно изменено или отозвано;
- какие доказательства подтверждают решение и фактическое действие.

IDMATIC NET охватывает постоянный доступ сотрудников, посетителей, подрядчиков, транспорт, учёт рабочего времени, ключи и материальные активы, допуск к оборудованию, мобильные и временные КПП, защищённые рабочие зоны и интеграцию с экосистемой безопасности.

Заказчик может начинать с одного законченного процесса — например, автоматизации заявок, модернизации бюро пропусков, мобильного КПП или контроля подрядчиков — и развивать решение без замены центральной модели данных. Поддерживаются локальное, гибридное, распределённое и полностью изолированное развёртывание.

Ключевая бизнес-ценность платформы:

- сокращение ручного ввода и времени согласования;
- автоматическое назначение и отзыв прав по кадровым, договорным и производственным событиям;
- уменьшение избыточных и неподтверждённых полномочий;
- повторное использование действующей инфраструктуры;
- быстрое мобильное расширение без капитального строительства;
- непрерывная работа объекта при потере внешнего канала;
- единый доказательный аудит для эксплуатации, безопасности и расследований;
- переход от набора разрозненных систем к управляемому контуру физических прав.

IDMATIC NET превращает физический доступ из набора отдельных пропусков и устройств в управляемое цифровое право с основанием, условиями, владельцем, исполнением и доказательством.

2. Проблема разрозненного физического доступа

На большинстве объектов процессы физического доступа исторически распределены между несколькими системами и подразделениями. Кадровая система знает, кто работает в организации. Договорная система хранит сведения о подрядчике. Бюро пропусков оформляет заявку. СКУД открывает точку прохода. Видеонаблюдение фиксирует событие. Учёт рабочего времени формирует собственный табель. Ключи, транспорт и оборудование нередко ведутся в отдельных журналах.

В результате организация сталкивается с типовыми проблемами:

- основание права и фактический доступ существуют в разных системах;
- увольнение, окончание договора, смены или квалификации не всегда приводит к своевременному отзыву;
- одинаковые сведения повторно вводятся операторами;
- отсутствует единый владелец физического права;
- постоянные полномочия накапливаются и редко пересматриваются;
- ручные исключения не имеют достаточного обоснования;
- события прохода трудно связать с заявкой, нарядом, автомобилем, активом или видеозаписью;
- удалённые и временные точки зависят от нестабильной связи;
- модернизация требует замены уже установленной инфраструктуры;
- расследование инцидента собирается вручную из нескольких журналов;
- невозможно быстро оценить фактическую загрузку КПП, зон и персонала.

Классическая СКУД отвечает прежде всего на вопрос: «Можно ли сейчас открыть эту точку?».

Современной организации требуется ответ на более широкий набор вопросов:

- на каком основании возникло право;
- соответствует ли оно роли, договору, квалификации и текущему заданию;
- подтверждено ли право владельцем зоны;
- действует ли сопровождение, правило двух лиц или дополнительный фактор;
- не изменились ли исходные атрибуты после выдачи;

- где находится субъект и завершено ли посещение;
- можно ли восстановить решение после автономной работы;
- какое доказательство связано с событием.

IDMATIC NET устраняет этот разрыв и формирует единый сквозной процесс управления физическими правами.

3. Позиционирование IDMATIC NET

IDMATIC NET — не отдельный контроллер, не только бюро пропусков и не замена всех существующих систем заказчика. Это интеллектуальный и операционный уровень, который:

- получает основания и атрибуты из корпоративных систем;
- управляет заявками и согласованиями;
- формирует ограниченные физические права;
- передаёт их стационарным, терминальным, мобильным и объектовым точкам исполнения;
- сохраняет события, причины решений и доказательства;
- автоматически пересматривает и отзывает полномочия;
- интегрируется с действующей СКУД, видео, PSIM, SIEM, HR, ERP, TMS, WMS и документооборотом.

Платформа может работать в трёх ролях:

Роль IDMATIC NET	Назначение
Самостоятельный комплекс	полное управление заявками, правами, идентификаторами, устройствами, событиями и аналитикой
Верхний интеллектуальный уровень	управление правами и процессами над действующей СКУД и корпоративными системами
Отраслевое решение	законченный сценарий для посетителей, транспорта, подрядчиков, активов, оборудования, мероприятий или мобильных КПП

IDMATIC NET сохраняет возможность поэтапного внедрения. Заказчик не обязан сразу менять контроллеры, считыватели и все регламенты. Система подключается к существующей инфраструктуре, принимает на себя выбранный сквозной процесс и расширяется по мере готовности.

4. Продуктовая архитектура

Продуктовая архитектура построена вокруг центральной платформы IDMATIC NET и девяти взаимосвязанных контуров.

Контур	Назначение
IDMATIC Rights Governance	модель физических прав, атрибутные политики, владельцы зон, пересмотр и отзыв
IDMATIC CRM & Workflow	обращения, заявки, согласования, SLA, коммуникации и маршруты обработки
IDMATIC Visitor	предварительная регистрация, визиты, принимающие, бюро пропусков и завершение посещений
IDMATIC Access	классическая СКУД, контроллеры, точки прохода, двери, шлюзы, турникеты и исполнительные устройства
IDMATIC Identification	карты, QR, мобильные идентификаторы, документы, PIN, биометрия и доверенные устройства
IDMATIC Time & Presence	рабочее время, смены, присутствие, отклонения, табели и производственные зоны
IDMATIC Transport	автомобили, водители, маршруты, парковки, КПП, распознавание номеров и логистические задания
IDMATIC Assets	ключи, инструмент, оборудование, внос, вынос, выдача, возврат и цепочка владения
IDMATIC Industrial	квалификация, наряд-допуск, смена, оборудование, второй сотрудник и право на операцию

Мобильный и объектовый уровни IDMATIC MOBILE и IDMATIC Edge являются общими исполнительными контурами для всей продуктовой архитектуры. Физическая защита информации, аудит, безопасность, интеграции и аналитика также проходят через все модули.

Экосистема XVMATIC, XViewsion и NEUROHUB дополняет IDMATIC NET ситуационным управлением, видеодоказательствами и интеллектуальным анализом.

Карта продуктовых контуров IDMATIC NET



Рисунок 1. Карта продуктовых контуров IDMATIC NET

Модули используют общие справочники субъектов, объектов, зон, ролей и идентификаторов, но могут внедряться и лицензироваться поэтапно. Отраслевые приложения получают стабильное ядро и собственные манифесты процессов, интерфейсов и политик.

5. Ключевые принципы платформы

Единое физическое право

Право описывает не только точку прохода, но и субъект, объект, зону, роль, разрешённое действие, время, основание, дополнительные условия и способ подтверждения.

Основание прежде права

Каждое полномочие связано с кадровым событием, договором, заявкой, нарядом, бронированием, билетом, производственной задачей или решением уполномоченного лица.

Атрибутное управление

Права могут автоматически назначаться, изменяться и отзываться при изменении должности, подразделения, договора, квалификации, смены, маршрута, статуса оплаты или другого доверенного атрибута.

Владелец зоны

За каждую значимую зону назначается владелец, который определяет допустимые роли, подтверждает исключения и периодически пересматривает постоянные полномочия.

Минимально необходимые полномочия

Система выдаёт только те зоны, действия и интервалы, которые необходимы субъекту для конкретной роли или задачи.

Offline-first

Критический процесс продолжается на объекте при потере WAN. Локальные узлы и доверенные устройства исполняют актуальную политику, сохраняют события и синхронизируются после восстановления связи.

Integration-first

IDMATIC NET не дублирует без необходимости мастер-данные HR, ERP или договорной системы. Для каждого справочника определяется владелец, а обмен строится через документированные интерфейсы и события.

Privacy by design

Состав данных минимизируется. Сроки хранения, доступ, удаление, обезличивание и доказательства обработки задаются по категориям данных и сценариям.

Доказательность

Решение сохраняется вместе с причиной, версией политики, устройством, временем, оператором и связанным фото-, видео- или документальным подтверждением.

Человек контролирует критические исключения

AI и автоматизация помогают классифицировать, проверять и рекомендовать, но не получают неконтролируемого права самостоятельно разрешать критический физический доступ.

6. Объекты управления

IDMATIC NET использует единую модель объектов.

Тип	Примеры
Субъект	сотрудник, посетитель, подрядчик, водитель, пассажир, клиент, представитель арендатора
Машинный субъект	робот, сервисное устройство, автономная платформа, доверенный терминал
Физический объект	здание, территория, КПП, этаж, помещение, стойка, шкаф, рабочее место
Зона	общая, служебная, производственная, защищённая, временная, транспортная
Точка исполнения	дверь, турникет, шлюз, шлагбаум, лифт, мобильный пост, ключница, станок
Идентификатор	карта, QR, мобильный идентификатор, PIN, документ, номер автомобиля, биометрический шаблон
Основание	трудовые отношения, договор, заявка, наряд, билет, бронирование, заказ, задание
Право	разрешение на вход, проезд, получение актива, открытие шкафа, работу с оборудованием
Доказательство	журнал, фотография, видеозапись, подпись, геопозиция, результат проверки

Один субъект может одновременно выступать в нескольких ролях. Например, сотрудник становится принимающим посетителя, водителем служебного автомобиля, ответственным за ключ и исполнителем наряда. Права рассчитываются по конкретному контексту, а не только по постоянной категории человека.

7. Цифровое физическое право

Центральная сущность IDMATIC NET — цифровое физическое право.

Право включает:

- субъекта или машинный субъект;
- объект, зону, маршрут либо конкретную точку;
- разрешённое действие;
- начало и окончание действия;
- расписание, смену или временное окно;
- основание;
- роль и категорию;
- владельца права и владельца зоны;
- обязательное сопровождение;
- правило двух лиц;

- требуемые идентификаторы и факторы;
- ограничения anti-passback;
- условия автономного исполнения;
- статус пересмотра;
- причину выдачи, изменения, приостановления или отзыва.

Право может разрешать не только проход. Оно также используется для:

- въезда или выезда;
- открытия ключницы;
- получения конкретного ключа или инструмента;
- внесения и вынесения материальной ценности;
- доступа к стойке или защищённому рабочему месту;
- активации оборудования;
- выполнения производственной операции;
- прохода по маршруту;
- присутствия в зоне в пределах задания.

В IDMATIC NET различаются право, идентификатор и способ исполнения. Потеря карты не означает потерю основания, а замена устройства не требует заново создавать бизнес-решение. Одно право может исполняться несколькими разрешёнными идентификаторами, а один идентификатор — содержать несколько ограниченных прав.

8. IDMATIC Rights Governance

IDMATIC Rights Governance управляет постоянными и временными полномочиями на основе ролей, атрибутов и подтверждённых оснований.

Атрибутные политики

Политика может учитывать:

- организацию и подразделение;
- должность и функцию;
- тип занятости;
- объект и рабочее место;
- договор и срок его действия;
- квалификацию и допуск;
- результат инструктажа;
- медицинский статус в допустимом объёме;
- смену и график;
- производственное задание;
- уровень риска зоны;
- необходимость сопровождения;
- статус расследования или ограничения.

Изменение доверенного атрибута запускает автоматический перерасчёт. Например, перевод в другое подразделение прекращает старые права и создаёт проект новых; окончание договора отзывает доступ подрядчика; истечение инструктажа блокирует допуск в производственную зону.

Каталог ролей

Роль описывает типовой набор полномочий и условий. IDMATIC NET поддерживает:

- корпоративные роли;
- объектовые роли;
- отраслевые роли;
- временные роли;
- проектные и сменные роли;
- роли сопровождения;

- конфликтующие роли.

Роль не обязана напрямую содержать список дверей. Она может ссылаться на категорию зон, маршрут, действие и атрибутные условия, что упрощает тиражирование между объектами.

Владелец зоны и пересмотр

Для критических и служебных зон назначается владелец. Система периодически формирует кампанию пересмотра, в которой владелец:

- подтверждает право;
- изменяет условия;
- сокращает срок;
- запрашивает дополнительное основание;
- отзывает полномочие;
- делегирует проверку уполномоченному сотруднику.

Просроченное подтверждение обрабатывается по политике: напоминание, эскалация, временное ограничение или автоматическое прекращение.

Анализ избыточных прав

Платформа выявляет:

- права без действующего основания;
- неиспользуемые разрешения;
- зоны, не соответствующие роли;
- конфликтующие полномочия;
- доступ после окончания договора;
- права с просроченной квалификацией;
- постоянные исключения без пересмотра;
- дублирование ролей и индивидуальных назначений.

Результат передаётся владельцу зоны и службе безопасности для подтверждённого решения.

9. Жизненный цикл физического права

Полный жизненный цикл строится как единый процесс:

Основание → заявка → согласование → регистрация →
выдача → проход → присутствие → завершение → отчёт.



Рисунок 2. Жизненный цикл физического права

1. Основание

Возникает кадровое, договорное, сервисное, производственное или событийное основание.

2. Заявка

Инициатор выбирает субъект, объект, цель, срок и необходимые действия. Часть полей заполняется автоматически из доверенных систем.

3. Согласование

Маршрут учитывает владельца зоны, принимающего, службу безопасности, договорного владельца, производственного руководителя и другие роли.

4. Регистрация

Проверяются сведения, документы, списки контроля, инструктажи, квалификации и согласия, необходимые выбранному сценарию.

5. Выдача

Назначается идентификатор и выпускается ограниченное физическое право: карта, защищённый QR, мобильный идентификатор или другой разрешённый фактор.

6. Исполнение

Стационарная, терминальная, мобильная или объектовая точка проверяет актуальные правила и принимает решение.

7. Присутствие

Система поддерживает состояние нахождения на территории, маршруте, в зоне или у оборудования.

8. Завершение

Визит, смена, наряд или аренда завершаются; временные права прекращаются; пропуск, ключ или актив возвращается.

9. Отчёт и пересмотр

События передаются в аналитику и аудит. Постоянные права периодически подтверждаются владельцем, а изменения оснований автоматически пересчитывают полномочия.

10. IDMATIC CRM и workflow

IDMATIC CRM является процессным интерфейсом платформы для обращений, заявок, согласований и коммуникаций.

Система поддерживает:

- различные типы заявок;
- формы, зависящие от сценария и роли;
- автоматическое заполнение данных;
- проверку обязательных полей;
- маршруты согласования;
- параллельное и последовательное согласование;
- замещение отсутствующего сотрудника;
- делегирование полномочий;
- SLA, уведомления и эскалации;
- возврат на уточнение;
- массовые заявки;
- шаблоны повторяющихся обращений;

- связь с документом, договором, билетом, заказом или нарядом;
- историю коммуникаций;
- регистрацию ручного решения и его причины.

Заявка не является самостоятельным пропуском. После согласования IDMATIC NET формирует ограниченное право, которое может быть автоматически изменено или отозвано при изменении исходных условий.

Пользователь видит только те поля, действия и объекты, которые соответствуют его роли. Интерфейс поддерживает web-, desktop-, мобильные и терминальные сценарии.

11. IDMATIC Visitor

IDMATIC Visitor автоматизирует полный цикл работы с посетителями:

- предварительную регистрацию;
- приглашение и подтверждение;
- согласование визита;
- проверку данных;
- выпуск QR или другого идентификатора;
- прибытие и самостоятельную регистрацию;
- уведомление принимающего;
- выдачу временного пропуска;
- доступ в разрешённые зоны;
- сопровождение;
- контроль присутствия;
- продление по регламенту;
- возврат пропуска;
- завершение визита;
- анализ незавершённых посещений.

Сценарии включают разового посетителя, группу, делегацию, курьера, сервисного инженера, кандидата, клиента, гостя арендатора и представителя подрядчика.

Самообслуживание

Терминал саморегистрации позволяет посетителю:

- выбрать язык;
- найти или подтвердить приглашение;
- ввести минимально необходимые сведения;
- подтвердить согласия;
- уведомить принимающего;
- получить QR или напечатанный пропуск;
- получить инструкции по маршруту.

Для стандартного сценария интерфейс строится без обязательного входа, сложной навигации и прокрутки. Состав действий определяется политикой объекта.

Бюро пропусков

Оператор видит очередь, статус согласования, результаты проверок, уже выданные идентификаторы, присутствие и причину каждого исключения. Ручное разрешение требует выбора основания и сохраняется в аудит.

Завершение посещения

Визит закрывается по выходу, возврату пропуска, истечению допустимого времени либо решению оператора. Незавершённые посещения формируют контролируемый список и уведомления ответственным.

12. IDMATIC Access

IDMATIC Access является классическим исполнительным контуром СКУД и одновременно частью общей модели IDMATIC NET.

Контур поддерживает:

- двери, турникеты, шлюзы, калитки и шлагбаумы;
- лифтовой доступ;
- контроллеры и исполнительные модули;
- карты, QR, PIN, мобильные и биометрические идентификаторы;
- расписания и временные зоны;
- локальный и сетевой anti-passback;
- правило двух лиц;
- режим сопровождения;

- блокирование и разблокирование;
- планы эвакуации и списки присутствующих;
- диагностику оборудования;
- автономную работу контроллеров;
- интеграцию с охранной сигнализацией, BMS, VMS и PSIM.

IDMATIC NET может управлять собственными контроллерами и подключаться к российским и зарубежным СКУД. При интеграции центральная платформа сохраняет владение физическим правом и аудитом, а локальная СКУД исполняет полученную конфигурацию в пределах подтверждённого интерфейса.

Модернизация может выполняться постепенно: сначала подключаются заявки, права и аналитика, затем отдельные точки переводятся на новые контроллеры, Linux-компоненты, Edge Hub или мобильное исполнение.

13. Идентификация на посту

Терминальный или операторский пост объединяет проверку человека, документа, права и контекста.

В зависимости от объекта используются:

- карта или иной физический идентификатор;
- защищённый QR;
- мобильный идентификатор;
- PIN;
- документ;
- фотография;
- биометрическая верификация;
- распознавание номера автомобиля;
- подтверждение принимающим;
- второй оператор или сопровождающий.

Оператор получает понятный результат:

- разрешено;
- отказано;
- требуется дополнительная проверка;

- требуется сопровождение;
- требуется ручное решение;
- право истекло или отозвано;
- зона или действие не соответствуют предъявленному праву.

Интерфейс показывает код применённого правила и только необходимые оператору сведения. Фото- и видеоподтверждение, документ и результат проверки связываются с событием по политике объекта.

14. IDMATIC Time & Presence

IDMATIC Time & Presence связывает события доступа с рабочим графиком, сменой, производственной зоной и фактическим присутствием.

Контур обеспечивает:

- графики и смены;
- вход, выход и перерывы;
- работу на нескольких объектах;
- производственные и служебные зоны;
- командировки и временные назначения;
- опоздания, ранний уход и отсутствие;
- переработку и отклонения;
- подтверждение руководителем;
- формирование табеля;
- экспорт в кадровые и расчётные системы;
- учёт удалённых и мобильных точек;
- контроль фактического времени подрядчиков.

Событие прохода не всегда автоматически признаётся рабочим временем. Политика учитывает назначенный объект, смену, роль, маршрут и подтверждённое производственное основание.

Данные учёта рабочего времени отделяются от задач контроля дисциплины и безопасности, но используют общий проверенный журнал присутствия.

15. Биометрия

Биометрические функции IDMATIC NET применяются как один из факторов подтверждения личности, а не как единственное основание физического права.

Поддерживаются:

- сравнение лица с фотографией оператором;
- верификация «один к одному»;
- проверка живого присутствия;
- подключение внешних биометрических систем;
- локальная обработка в изолированном контуре;
- хранение шаблонов и результатов по установленной политике;
- фиксация основания, согласия или иного допустимого режима обработки;
- разделение биометрического шаблона и общих персональных данных;
- удаление по окончании срока.

Биометрическая проверка отвечает на вопрос, соответствует ли предъявитель зарегистрированному субъекту. Решение о доступе дополнительно учитывает право, зону, время, отзыв, сопровождение и режим объекта.

Для мобильных сценариев может использоваться фотография либо биометрическая сигнатура, связанная с защищённым QR-контейнером. Конкретный режим выбирается по требованиям законодательства, риску зоны и архитектуре заказчика.

16. IDMATIC Transport

IDMATIC Transport управляет доступом транспорта и связывает автомобиль, водителя, пассажиров, груз, маршрут и основание поездки.

Возможности:

- реестр автомобилей и прицепов;
- проверка водителя;
- заявки на въезд и выезд;
- временные и постоянные маршруты;
- парковочные зоны;
- распознавание государственных номеров;
- QR и мобильные идентификаторы;

- контроль пассажиров;
- связь с пропуском на груз или материальную ценность;
- весовые, досмотровые и логистические операции;
- очередь и временные слоты;
- интеграция с TMS, WMS и YMS;
- удалённые КПП;
- водительский мобильный терминал;
- автономная посадка и периодическая синхронизация.

Право автомобиля не заменяет право водителя, а право водителя — право пассажира или груза. IDMATIC NET сопоставляет эти сущности и разрешает только согласованную комбинацию.

Система может использоваться на предприятии, парковке, логистическом объекте, маршруте служебного транспорта или временной площадке.

17. Подрядчики и временный персонал

IDMATIC Contractor & Workforce управляет допуском внешних организаций, временного персонала и исполнителей работ.

Контур связывает:

- подрядную организацию и договор;
- ответственного заказчика;
- конкретного сотрудника подрядчика;
- документы и срок их действия;
- инструктажи и квалификации;
- медицинские и производственные допуски в допустимом объёме;
- смену, объект и территорию;
- наряд, задание или этап работ;
- транспорт, инструмент и материальные ценности;
- фактическое присутствие и завершение работ.

Окончание договора, исключение сотрудника из списка, истечение инструктажа или закрытие наряда автоматически изменяет либо отзывает связанные физические права.

Платформа позволяет контролировать не только вход подрядчика на территорию, но и его право находиться в конкретной зоне, получить ключ или инструмент, использовать оборудование и выполнить предусмотренную операцию.

18. Ключи и материальные активы

IDMATIC Assets управляет физической выдачей, возвратом и перемещением активов.

Контур поддерживает:

- электронные ключницы;
- выдачу и возврат механических ключей;
- радиостанции, приборы и инструменты;
- временную передачу оборудования;
- внос и вынос материальных ценностей;
- связь актива с заявкой, владельцем и зоной;
- контроль просрочки;
- инвентаризацию;
- журнал цепочки владения;
- фото- и видеоподтверждение операции.

Доступ к ячейке и право получить конкретный актив являются разными проверками. Система разрешает открытие ключницы, но отказывает в выдаче выбранного ключа при отсутствии наряда или полномочия.

19. IDMATIC Industrial — допуск к оборудованию

IDMATIC Industrial управляет правом на работу с производственным и инженерным оборудованием.

Решение учитывает:

- профессию и роль;
- квалификацию;
- инструктаж;
- медицинский допуск;
- наряд или задание;
- смену;

- участок;
- конкретный тип оборудования;
- состояние оборудования;
- необходимость присутствия второго сотрудника;
- время и длительность операции.

После проверки платформа передаёт разрешение локальному исполнительному модулю.

Критическая безопасная автоматика оборудования сохраняет собственную независимую логику и не подменяется IDMATIC NET.

Все разрешения, отказы, ручные действия и фактическое время использования связываются с нарядом и субъектом.

20. Физическая защита информации

Физический контур информационной безопасности связывает доступ к помещению, стойке, рабочему месту и информационной сессии.

Платформа обеспечивает:

- допуск к защищённому АРМ только при наличии физического права;
- связь пользователя, рабочего места и зоны;
- блокирование АРМ при прекращении подтверждённого присутствия;
- контроль вскрытия стойки или шкафа;
- правило двух лиц;
- временное разрешение на обслуживание;
- учёт ключей и съёмных носителей;
- сопоставление событий СКУД и информационной системы;
- фиксацию фото- и видеодоказательств;
- передачу коррелированных событий в XVMATIC и SIEM.

Физическая DLP дополняет программные средства защиты информации: она контролирует, кто физически находился у ресурса, на каком основании и в какой момент.

21. IDMATIC MOBILE

IDMATIC MOBILE — мобильный контур IDMATIC NET для точек, где стационарная инфраструктура отсутствует, экономически нецелесообразна, временно недоступна или должна быть быстро расширена.

Смартфон или планшет становится доверенным мобильным постом. Устройство получает правила, ключи, зоны, списки отзыва и профиль автономности, проверяет предъявленное цифровое право и сохраняет доказательный журнал.

Общие возможности:

- запуск временной точки без капитального строительства;
- защищённый QR как переносимое цифровое право;
- мобильный идентификатор;
- работа без WAN;
- локальная проверка зоны, роли и времени;
- сравнение лица с фотографией;
- подключение биометрической проверки;
- ручное решение по регламенту;
- мобильная печать;
- контроль очереди и загрузки;
- фото- и видеодоказательства;
- синхронизация с IDMATIC NET;
- горизонтальное масштабирование добавлением устройств.

Отраслевые решения

Решение	Основной сценарий	Результат
IDMATIC MOBILE Visitor	посетители офиса и предприятия	предварительная регистрация, QR, мобильный пост, завершение визита
IDMATIC MOBILE Event / Guest	деловые и корпоративные мероприятия	приглашения, гостевые категории, зоны и быстрый контроль
IDMATIC MOBILE Conference	конференции и деловые программы	аккредитация, секции, роли, расписание и аналитика посещений
IDMATIC MOBILE Exhibition	выставки	участники, экспоненты, монтаж, сервисный персонал и зоны

Решение	Основной сценарий	Результат
IDMATIC MOBILE Gate	временный или дополнительный КПП	быстрое развёртывание, автономная проверка, мобильный резерв
IDMATIC MOBILE Transport	автобусы, пассажиры и удалённые маршруты	водительский терминал, посадка, списки и периодическая синхронизация
IDMATIC MOBILE Open Air / Festival	массовая открытая площадка	распределённый периметр, временные зоны, antifraud и контроль потоков
IDMATIC MOBILE Sport	спортивные объекты и соревнования	аккредитация, служебные зоны, участники, команды и временные посты
IDMATIC MOBILE ServicePass	сервисные объекты и бронирования	связь услуги, времени, оплаты и физического доступа
IDMATIC MOBILE Contractor & Workforce	подрядчики и временный персонал	договор, инструктаж, смена, территория и фактическая работа
IDMATIC MOBILE Equipment / Asset Pass	инструмент и оборудование	внос, вынос, выдача, возврат и доказательная цепочка
IDMATIC MOBILE Vehicle	транспорт и мобильные КПП	водитель, автомобиль, маршрут, QR и распознавание номера
IDMATIC MOBILE Robot	автономные устройства и роботы	цифровое право устройства на маршрут, шлюз или операцию
IDMATIC MOBILE Data Centre	ЦОД и критические помещения	многофакторный доступ, сопровождение, стойки и сервисные работы
IDMATIC MOBILE Physical Information Security	защищённые рабочие зоны	подтверждение физического присутствия и связь с информационной сессией

Все приложения используют стабильное ядро, общую модель прав и отраслевые манифесты. Это позволяет выпускать и обновлять отраслевые решения независимо, сохраняя совместимость с центральной системой.

22. Защищённый цифровой пропуск

QR в IDMATIC MOBILE является не ссылкой на запись и не открытым номером, а защищённым контейнером ограниченного физического права.

Состав контейнера

Контейнер включает только данные, необходимые выбранному сценарию:

Группа	Содержание
Служебный заголовок	версия формата, издатель, идентификатор ключа, серийный номер

Группа	Содержание
Субъект	внутренний или псевдонимизированный идентификатор, категория, привязка к фотографии или биометрической сигнатуре
Право	объект, зоны, маршрут, роль и разрешённые действия
Условия	начало и окончание, расписание, сопровождение, дополнительные факторы
Antifraud	уникальность, профиль anti-passback, ограничения повторного предъявления
Целостность	цифровая подпись и сведения для проверки доверия

Персональные данные минимизируются. В изолированных или специальных конфигурациях контейнер шифруется, чтобы сведения нельзя было прочесть обычным сканером.

Выпуск и ключи

IDMATIC NET:

- выпускает контейнер;
- подписывает его действующим ключом;
- ведёт версии и сроки ключей;
- выполняет плановую ротацию;
- распространяет доверенные открытые ключи;
- отзывает скомпрометированные ключи и устройства;
- сохраняет связь выпущенного права с основанием и журналом.

Секреты устройства хранятся в защищённом хранилище операционной системы либо в подключённом аппаратном модуле.

Доверенные мобильные устройства

До начала работы смартфон или планшет регистрируется в IDMATIC NET, получает собственный ключ или сертификат, профиль разрешённых объектов и привязку к оператору либо службе.

Система контролирует:

- версию приложения;
- состояние доверия;
- срок ключа;
- последнюю синхронизацию;
- применённую конфигурацию;
- разрешённые объекты и режимы.

Поддерживаются подключение к корпоративному управлению мобильными устройствами, дистанционное прекращение доверия и блокирование утраченного либо скомпрометированного устройства.

Локальная проверка

Мобильный или стационарный пост последовательно проверяет:

1. доверие к устройству и актуальность локальной политики;
2. формат и целостность контейнера;
3. подпись и ключ издателя;
4. срок действия права;
5. объект, зону, роль и разрешённое действие;
6. локальный список досрочного отзыва;
7. состояние anti-passback;
8. необходимость сопровождения или второго фактора;
9. соответствие лица фотографии или биометрической сигнатуре;
10. локальные запреты и режим объекта.

Результат содержит код применённого правила. Поэтому после синхронизации можно восстановить, почему конкретное решение было принято даже без связи с центром.

Досрочный отзыв

Отзыв распространяется несколькими взаимодополняющими способами:

- коротким сроком права;
- синхронизацией списков отзыва;
- немедленной передачей в Edge Hub;
- обновлением мобильных устройств;
- блокированием доверия к устройству или ключу.

Для зон, где требуется практически мгновенный глобальный отзыв, мобильные посты работают через локальный Edge Hub либо доступный канал. Полностью изолированная точка применяет последний полученный список и предел автономности, установленный политикой.

Anti-passback

Локальный anti-passback выполняется самим устройством. Согласованное состояние нескольких точек обеспечивает Edge Hub.

Без связи между независимыми постами глобальное состояние синхронизируется после восстановления обмена; для таких зон заранее выбирается допустимый профиль риска.

Защита от передачи пропуска

В зависимости от объекта применяются:

- фотография;
- сравнение оператором;
- биометрическая верификация;
- проверка живого присутствия;
- PIN;
- подтверждение принимающим;
- привязка к доверенному телефону;
- короткое окно действия;
- контроль повторного предъявления;
- выборочная усиленная проверка.

Эксплуатационные показатели мобильного поста

Платформа измеряет:

- время принятия решения;
- пропускную способность;
- долю повторных сканирований;
- число отказов по причинам;
- объём автономного журнала;
- актуальность правил и списков;
- задержку синхронизации;
- состояние батареи и памяти;
- стабильность приложения;
- попытки предъявления отозванных или поддельных прав.

23. IDMATIC Edge и offline-first

IDMATIC Edge обеспечивает выполнение критического процесса на объекте без зависимости от внешнего канала.

В состав входят:

- Edge Hub или MESH HUB;
- локальный кэш прав и политик;
- событийная шина;
- шлюз периферии;
- локальная аналитика;
- сервис store-and-forward;
- управление конфигурациями;
- Field Edge Mesh для группы мобильных точек.

Распределение ответственности

Центральный IDMATIC NET	IDMATIC Edge
мастер-данные и владельцы	локальные копии необходимых данных
выпуск и отзыв прав	исполнение полученной политики
жизненный цикл ключей	проверка подписи и доверия
единый аудит	защищённый автономный журнал
межобъектовая аналитика	состояние конкретного объекта
корпоративные интеграции	подключение локальной периферии
эталонная конфигурация	работа при потере WAN

Платформа продолжает локальную работу без ограничения по длительности самого режима, однако ни одно право не становится бессрочным. Принимаются только права, срок, ключ и профиль автономности которых остаются действующими.

Синхронизация

Каждое автономное событие получает уникальный идентификатор, время устройства, номер версии права и применённой политики.

После восстановления связи:

- события передаются без дублирования;

- подтверждается доставка;
- обновляются права и списки;
- выявляются конфликты;
- сохраняется исходное локальное решение;
- центральное состояние присутствия пересчитывается;
- отклонения направляются оператору.

Операции интеграции являются повторяемыми и идемпотентными: повторная передача не создаёт второй проход, вторую заявку или повторную выдачу.

24. Архитектура и данные

IDMATIC NET строится как модульная сервисная платформа на Linux и PostgreSQL. Архитектура допускает локальную установку, виртуализацию, частное облако и распределённые объектовые узлы.

Основные компоненты:

- IDMATIC NET Core;
- реестр субъектов, объектов и идентификаторов;
- сервис физических прав;
- механизм политик;
- workflow согласований;
- API Gateway;
- IDMATIC NET Facade для контролируемого доступа к центральной системе;
- событийная шина;
- transactional outbox для надёжной передачи изменений;
- аудит и доказательное хранилище;
- Edge Runtime;
- web-, desktop- и мобильные клиенты;
- аналитический контур.

Логическая архитектура IDMATIC NET



Рисунок 3. Архитектура IDMATIC NET

Модель владения данными определяется для каждого справочника. Например, кадровая система владеет сведениями о занятости, договорная — договором, а IDMATIC NET — физическим правом, его исполнением и аудитом.

Обмен не создаёт несколько конкурирующих эталонных записей.

25. Интеграционная и партнёрская программа

IDMATIC NET включает комплект средств для разработки, тестирования и сертификации интеграций.

Интерфейсы

- документированный REST API;
- спецификации OpenAPI;
- webhooks;
- событийные подписки;
- пакетный обмен;
- SDK для типовых сценариев;
- адаптеры объектовых устройств;
- журнал интеграционных операций;
- версионирование интерфейсов;

- контроль обратной совместимости.

Тестирование

Интеграционному партнёру предоставляются:

- тестовый стенд;
- демонстрационные данные;
- типовые сценарии;
- эмуляторы событий и устройств;
- отрицательные тесты;
- требования к безопасности;
- критерии производительности;
- протокол приёмки;
- проверка восстановления после ошибки.

Сертификация совместимости

Интеграция проходит функциональные, нагрузочные, отказные и безопасностные проверки.

Результат включается в каталог совместимого оборудования и программного обеспечения с указанием версии, поддерживаемых функций и ограничений.

Типовые направления

Платформа подключается к:

- 1С;
- ERP;
- HR и кадровым системам;
- IDM/IAM и каталогам пользователей;
- электронному документообороту;
- TMS, WMS и YMS;
- SIEM;
- VMS, BMS и PSIM;
- парковочным и билетным системам;
- российским и зарубежным СКУД;
- принтерам, терминалам, биометрическим устройствам и контроллерам.

Партнёрская программа позволяет использовать IDMATIC NET как самостоятельный комплекс, отраслевое решение либо интеллектуальный верхний уровень над действующей инфраструктурой.

26. AI-ассистент

AI-ассистент работает с разрешёнными данными IDMATIC NET и помогает:

- классифицировать заявку;
- находить неполные сведения;
- объяснять причину отказа;
- предлагать маршрут согласования;
- выявлять избыточные права;
- контролировать кампании пересмотра;
- анализировать очереди и нагрузку;
- рекомендовать перераспределение мобильных постов;
- диагностировать оборудование;
- подготавливать проекты настроек и регламентов;
- сопровождать расследование инцидента.

AI-ассистент не получает неограниченного права самостоятельно разрешать физический доступ. Решение основывается на утверждённой политике, а критические исключения подтверждаются уполномоченным сотрудником.

В изолированных конфигурациях интеллектуальные функции выполняются локальной языковой моделью без передачи корпоративных документов во внешний контур.

27. Интеграция с экосистемой безопасности

XVMATIC

XVMATIC получает события от IDMATIC NET и других инженерно-технических систем, нормализует их, применяет сценарии и предоставляет оператору инструкции по реагированию.

Примеры:

- отказ в доступе и попытка повторного прохода;
- использование отозванного идентификатора;
- проход лица из списка контроля;

- одновременная тревога СКУД и видеонаблюдения;
- открытие защищённой стойки вне наряда-допуска;
- незавершённое посещение после окончания разрешённого времени.

XViewision

XViewision связывает событие доступа с видео:

- кадром прохода;
- записью действий оператора;
- распознанным номером;
- видео работы с терминалом;
- архивом инцидента.

NEUROHUB

NEUROHUB выполняет интеллектуальный анализ видео и событий:

- обнаружение аномального поведения;
- контроль очередей;
- поиск объекта или человека;
- подтверждение событий доступа;
- выявление присутствия в запрещённой зоне;
- передачу тревоги в XVMATIC.

28. Безопасность и защита данных

IDMATIC NET использует многоуровневую модель безопасности.

Управление доступом операторов

- персональные учётные записи;
- роли и минимально необходимые полномочия;
- разделение функций оператора, администратора и службы безопасности;
- многофакторная аутентификация;
- ограничение рабочих мест;
- управление сессиями;
- регистрация административных действий;
- периодический пересмотр прав операторов.

Защита данных

- шифрование каналов;
- контроль целостности;
- управление ключами;
- резервное копирование;
- горячее резервирование;
- изоляция объектов и арендаторов;
- сроки хранения по категориям;
- удаление или обезличивание;
- активирование уничтожения данных;
- минимизация состава данных в мобильном контуре.

Аудит

Регистрируются:

- создание и изменение заявки;
- согласование, отклонение и возврат;
- автоматическое назначение и пересмотр права;
- выдача и отзыв пропуска;

- изменение ролей и политик;
- вход, выход, въезд и выезд;
- ручные решения;
- изменение настроек;
- ошибки интеграции;
- обращения к персональным данным;
- действия AI-ассистента;
- работа устройств и синхронизация;
- делегирование полномочий;
- результаты проверки списков контроля.

Событие содержит субъект, право, точку, время, устройство, принятое решение, код причины, версию политики и связанное доказательство.

29. Продуктовая документация и доказательность

IDMATIC NET поставляется не только как набор программных модулей, но и как формализованный продуктовый и проектный комплект.

В него входят:

- паспорт каждого продуктового контура;
- сравнительная таблица редакций и лицензий;
- карта модулей и зависимостей;
- матрица совместимого оборудования;
- каталог API, webhooks и событий;
- руководство по защищённому развёртыванию;
- руководство администратора и оператора;
- профили масштабирования и производительности;
- описание резервирования и восстановления;
- модель угроз и рекомендации по защите;
- публичные и предоставляемые по согласованному режиму описания внедрений;
- каталог реализованных сценариев и референсных архитектур;
- программа и методика демонстрации;
- критерии приёмки пилота;

- комплект эксплуатационных регламентов;
- журнал известных ограничений конкретной версии.

Для каждого интегрированного устройства или внешней системы указываются версия, поддерживаемые функции, проверенная конфигурация и ограничения. Это позволяет отличать штатную возможность продукта от индивидуальной проектной доработки.

30. Варианты развёртывания

Вариант	Состав	Рекомендуемое применение
Быстрый старт	CRM, QR-пропуска, мобильные контроллеры, облачный или локальный сервер	небольшой объект, мероприятие, временный КПП
Корпоративный стандарт	IDMATIC NET, CRM, IDMATIC Access, FRACTAL-T, Edge Hub, интеграции и резервирование	офис, предприятие, бизнес-центр, логистический объект
Распределённый комплекс	несколько объектов, единая база, локальные узлы и централизованная аналитика	холдинг, сеть филиалов, крупная промышленная площадка
Отказоустойчивый контур	горячее резервирование, локальное исполнение, XVMATIC, XViewsion и диагностика	объект с повышенными требованиями к непрерывности
Изолированный контур	полностью локальная инфраструктура, локальные ключи, архив и AI	режимный объект, ЦОД, критическая инфраструктура

Масштабирование выполняется по сервисам, объектам и точкам исполнения. Для мобильного контура пропускная способность увеличивается добавлением доверенных устройств и локальных Edge Hub.

31. Аналитика и показатели управления

Операционный уровень

- количество заявок;
- среднее время согласования;
- соблюдение SLA;
- число посетителей на территории;
- загрузка КПП;
- время принятия решения;
- доля отказов;
- причины исключений;

- несданные пропуска, ключи и активы;
- состояние устройств.

Уровень управления правами

- автоматически назначенные и отозванные права;
- права без подтверждённого основания;
- неподтверждённые кампании пересмотра;
- неиспользуемые и избыточные разрешения;
- конфликтующие полномочия;
- просроченные квалификации;
- ручные исключения;
- время от кадрового события до фактического отзыва.

Уровень безопасности

- попытки несанкционированного доступа;
- события по спискам контроля;
- ручные разрешения;
- проходы вне графика;
- нарушения сопровождения;
- несоответствия документов;
- попытки использования отозванного QR;
- инциденты оборудования.

Управленческий уровень

- нагрузка по объектам;
- работа подрядчиков;
- посещаемость;
- использование зон;
- фактическое рабочее время;
- динамика рисков;
- качество согласования заявок;
- стоимость обработки одного обращения.

Эксплуатационный уровень

- доступность узлов;
- состояние серверов и контроллеров;
- задержка синхронизации;
- объём автономных событий;
- ошибки интеграции;
- состояние резервирования;
- актуальность ключей и политик;
- сроки обслуживания.

32. Экономический эффект

IDMATIC NET создаёт эффект за счёт:

- сокращения ручного ввода;
- автоматического назначения и отзыва прав;
- уменьшения времени согласования;
- переноса части регистрации в самообслуживание;
- снижения очередей;
- сокращения числа разрозненных систем;
- повторного использования существующей инфраструктуры;
- мобильного расширения без капитального строительства;
- сокращения времени расследования;
- уменьшения потерь пропусков, ключей и активов;
- автоматизации отчётности и пересмотра прав;
- снижения стоимости подключения новых объектов;
- предотвращения доступа после окончания договора или квалификации.

Экономическая модель рассчитывается по фактическим показателям заказчика:

Эффект = Экономия труда + Снижение потерь + Снижение стоимости инфраструктуры +
Предотвращённые инциденты – Стоимость владения.

В White Paper не используются универсальные проценты экономии, поскольку результат зависит от масштаба, действующей инфраструктуры и стоимости операций конкретного объекта.

33. Порядок внедрения

Этап 1. Обследование

Определяются:

- объекты и зоны;
- категории субъектов;
- виды заявок и пропусков;
- владельцы данных и зон;
- регламенты;
- способы идентификации;
- интеграции;
- режимы отказа;
- требования к доказательствам;
- правила хранения данных;
- перечень прав для автоматического назначения;
- график пересмотра постоянных полномочий.

Этап 2. Модель целевого процесса

Фиксируется сквозной сценарий:

Основание → заявка → согласование → регистрация →
выдача → проход → присутствие → завершение → отчёт.

Одновременно формируются каталог ролей, матрица зон, атрибутные правила, владельцы и допустимые исключения.

Этап 3. Пилот

В пилот включается ограниченный, но законченный процесс. Обязательны:

- успешный доступ;
- отказ;
- ручное решение;
- автоматическое назначение и отзыв права;
- работа без внешней связи;

- восстановление связи;
- синхронизация;
- досрочный отзыв;
- просмотр журнала;
- подтверждение события;
- проверка избыточных и неиспользуемых прав.

Этап 4. Интеграция

Подключаются СКУД, кадровая система, документооборот, транспортные, производственные и видеосистемы.

Этап 5. Тиражирование

После приёмки шаблоны объектов, ролей, политик, коннекторов и эксплуатационных регламентов применяются на следующих площадках.

34. Критерии успешности пилота

Критерий	Способ проверки
Полный жизненный цикл	заявка проходит от основания до завершения посещения
Корректность права	разрешаются только заданные зона, действие и время
Атрибутное управление	изменение исходного атрибута изменяет или отзывает право
Пересмотр прав	владелец зоны подтверждает, изменяет или отзывает полномочия
Управляемый отказ	причина отображается и сохраняется
Автономность	доступ выполняется при отключённом WAN
Проверка QR	подпись, срок, зона, роль и отзыв проверяются локально
Синхронизация	автономные события передаются без дублирования
Досрочный отзыв	отозванное право перестаёт приниматься по выбранному профилю
Аудит	восстанавливается последовательность действий и версия политики
Интеграция	данные корректно передаются между системами
Резервирование	отказ основного узла не останавливает критический процесс
Работа персонала	операторы выполняют сценарии по утверждённым инструкциям
Управление устройствами	утраченное доверенное устройство отзывается

Для каждого критерия до пилота фиксируются исходное значение, целевой показатель, источник измерения и ответственное лицо.

35. Основные риски и способы снижения

Риск	Способ снижения
Неполный регламент	моделирование процесса до настройки
Неопределённый владелец зоны	назначение владельца и кампании пересмотра
Несовпадение справочников	назначение владельцев мастер-данных
Избыточные права	атрибутные политики, анализ использования и подтверждение владельцем
Задержка согласования	SLA, уведомления, замещение и эскалация
Потеря связи	локальное исполнение и Edge Hub
Утрата устройства	доверенные устройства, защищённое хранилище и отзыв ключей
Несанкционированная передача QR	короткий срок, фото, второй фактор и anti-passback
Несвоевременный отзыв в изоляции	короткие права, списки отзыва, предел автономности и Edge Hub
Ошибка оператора	ролевой интерфейс и обязательное указание причины
Проблемы интеграции	контрактные API, идиempотентность, тестовый стенд и журнал ошибок
Чрезмерный сбор данных	минимизация, сроки хранения и удаление
Ошибка AI-рекомендации	подтверждение человеком и работа в рамках политик
Пиковая очередь	мобильный резерв и перераспределение точек
Отказ оборудования	диагностика, резервирование и автономность контроллеров
Неясная совместимость	каталог проверенных версий и сертификация интеграций

36. Заключение

IDMATIC NET объединяет опыт АО «МТТ Контрол», работающего на рынке с 1995 года, в области пропускных систем, СКУД, терминалов, видеонаблюдения и ситуационного управления с современной моделью цифровых физических прав, мобильного контроля и интеллектуальной аналитики.

Платформа позволяет заказчику начинать с одной задачи — автоматизации заявок, управления посетителями, модернизации бюро пропусков, мобильного КПП, транспорта, подрядчиков, учёта рабочего времени или доступа к оборудованию — и последовательно развивать систему без смены центральной модели данных.

Ключевые свойства IDMATIC NET:

- единый жизненный цикл физического права;
- автоматическое предоставление и отзыв по атрибутам;
- периодический пересмотр полномочий владельцем зоны;
- модульная и понятная продуктовая архитектура;
- собственная классическая СКУД;
- совместимость с действующей инфраструктурой;
- стационарные, терминальные и мобильные точки;
- offline-first и IDMATIC Edge;
- защищённые цифровые права;
- доверенные устройства и управляемый отзыв;
- управление людьми, транспортом, активами и оборудованием;
- физическая защита информации;
- доказательный аудит;
- документированные API, SDK и партнёрская сертификация;
- локальное, гибридное и изолированное развёртывание;
- интеллектуальная поддержка операторов без передачи AI неконтролируемого права на физический доступ.

Рекомендуемый следующий шаг — выбрать один сквозной сценарий, определить измеримые критерии и провести демонстрацию либо пилотное внедрение IDMATIC NET на реальном объекте.