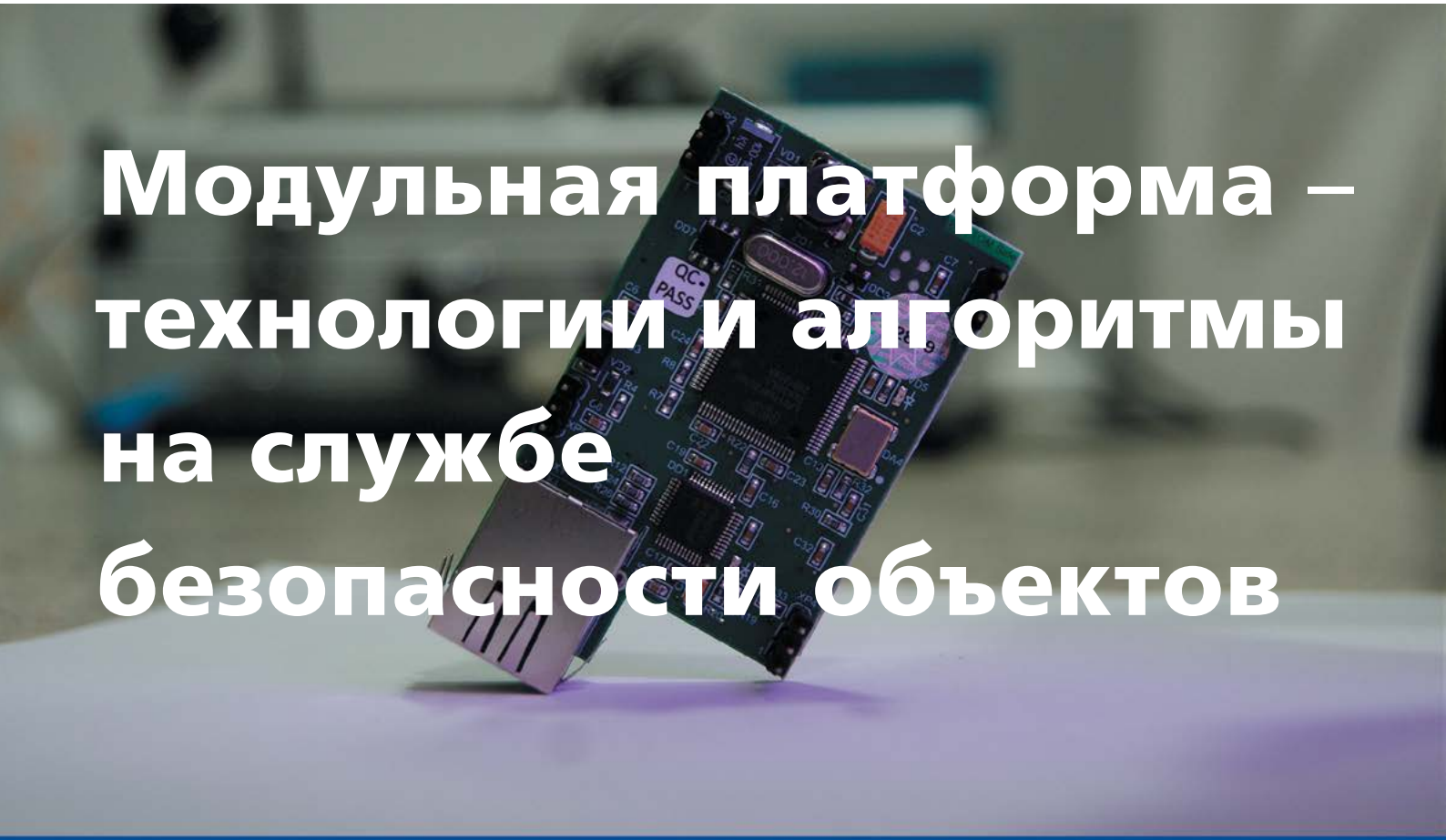
НИКОЛАЙ РЕДИН
Группа компаний Octagram

Модульная платформа – технологии и алгоритмы на службе безопасности объектов



В нашей компании главная задача – создать совершенный продукт, который будет удовлетворять всем требованиям рынка, т. е. качественный, надежный, многофункциональный, универсальный, удобный в работе и недорогой.

Стоит признать, что такой подход приносит свои результаты: к нам приходят пользователи, которые познакомившись с Octagram однажды, продолжают наращивать систему все новыми и новыми функциями и тиражировать ее на новых объектах.

Предлагаем вам самим познакомиться в статье, а потом и на практике с Модульной инженерной платформой Octagram.

Практика – критерий истины и никакие красивые описания не заменят эффективную технику и удобное ПО.

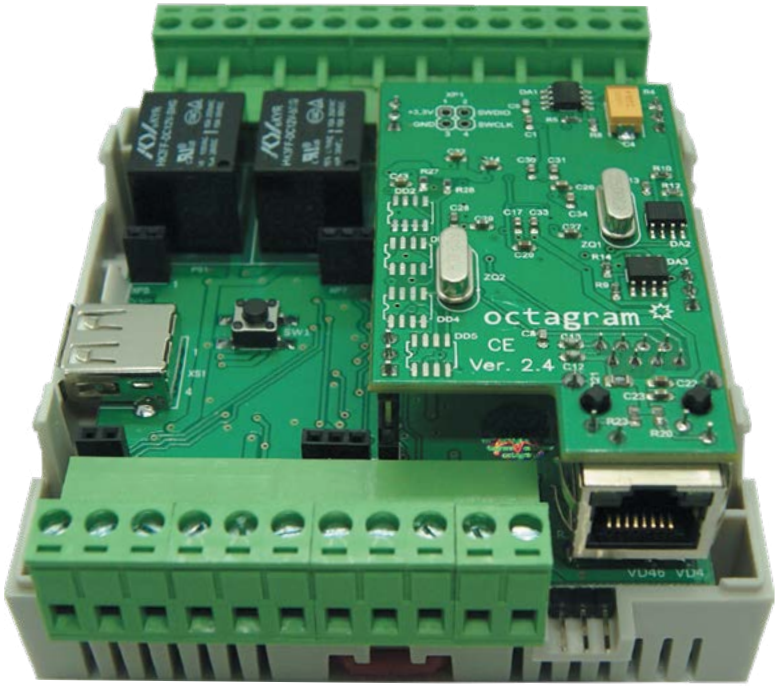
octagram modular systems
Группа компаний Octagram

Москва,
Лефортовский переулок 4, стр. 3
+7 (495) 308-00-64
www.octagram.ru

Совсем немного теории. Как и во всем мире, в России технической основой систем безопасности становятся компьютеры или специализированные контроллеры. Под специализированными контроллерами я подразумеваю приборы с довольно простой структурой, без собственной операционной системы, позволяющие используя минимальное количество кода выполнять функции сбора, обработки информации и управления системами безопасности. Можно спорить о надежности «железа», но теория вероятности показывает, что надежность обратно пропорциональна количеству элементов (в нашем случае количеству кода). Очевидно, что написанный под каждую задачу код требует больше усилий и не гарантирует надежности базовых операций и элементов, не говоря уже о системе в целом. Поэтому так популярны компьютеры в качестве «мозгов» для безопасности. Даже несмотря на увеличение стоимости решений и сложность дальнейшего обслуживания компьютерных систем, заказчики выбирают предсказуемость и тиражируемость решений.

Используя многолетний опыт, наша компания более 9 лет назад предложила рынку базовый контроллер – платформу, совмещающую в себе положительные качества компьютеров и специализированных контроллеров: использование одного «железа» (буквально – одного типа контроллера A1) для всех видов приборов систем безопасности, отсутствие операционной системы, наличие базовых блоков в коде микропрограмм, краткость кода. При использовании платформы A1 предсказуемость и тиражируемость решений стала экономически выгодной.

Все преимущества Модульной инженерной платформы (МИП) были защищены патентами не только в России, но и за рубежом.



Даже если общее количество ключей в контроллере A1Q исчисляется десятками тысяч, можно практически мгновенно менять небольшое количество ключей в его памяти. Благодаря алгоритму обработки данных перезапись всей базы хранящихся, а A1Q ключей не требуется

Рассмотрим на конкретном примере, как преимущества МИП были использованы в СКУД. Базовые алгоритмы работы СКУД остаются теми же, что и 20 лет назад. В связи с этим все чаще встречаются ситуации, когда вся система контроля доступа становится морально устаревшей и не удовлетворяет современным требованиям служб безопасности на объекте.

Так, летом 2018 года при подготовке одного из проектов для РЖД выяснилось, что требуется постоянная перезапись ключей в памяти контроллера при общем количестве ключей в системе более 5000. Серийный характер данного проекта делал невозможной реализацию проекта на высокобюджетном оборудовании, где в качестве контроллеров используются компьютеры. Поэтому проектировщиком был проведен анализ продукции большинства отечественных производителей СКУД. Оказалось, что в отрасли не существует

Считыватель PLR3M для бесконтактных карт, брелоков Mifare Ultralight, Mifare Standard (Classic) 1K и 4K, Mifare ID и смартфонов (в формате NFC). Имеет защиту от копирования ключей

управляющих устройств и программного обеспечения, позволяющего мгновенно добавлять/удалять ключи пользователей в системе, где количество пользователей больше 100. То есть делать это можно, но не мгновенно, а в течении интервала от нескольких минут до нескольких часов в зависимости от общего количества ключей, используемых в системе. Это связано с тем, что изменение одного ключа в памяти контроллера требует перезаписи всей базы ключей.

По отзывам персонала, эксплуатирующего СКУД, во время записи ключей случаются сбои в пропуске пользователей системы. В других реализациях, где запись ключей не велась часто или требования к работе СКУД не настолько критичны, недостатки контроллеров удавалось обойти, используя разные ухищрения. В указанном проекте РЖД применять такие ухищрения было невозможно, так как перезапись ключей должна быть постоянной. Проблема, которая многие годы неявно существовала в СКУД, стала очевидной.

Что же происходит в «стандартной» СКУД? Возьмем любой объект с количеством ежедневных разовых посетителей или принимаемых/увольняемых сотрудников более 50 и общим количеством пропусков более 1000.

Постоянным сотрудникам выдаются «именные» пропуска с уникальным номером в базе СКУД. Вместе с тем в СКУД функционируют «разовые» (номерные) пропуска, которые выдаются в бюро пропусков или на стойке администрации по поступающим от ответственных лиц заявкам на гостей или на вновь принимаемых сотрудников.

«Разовые» пропуска – это ключи в базе данных СКУД и памяти контроллеров, записанные заранее, а не в момент выдачи пропуска (ключа). Гостям/сотрудникам при приеме на работу выдается пропуск № 1, № 2, № 3 и т. д., а не именной пропуск, имеющий уникальные данные в базе СКУД. Номерные пропуска записываются обезличенными в память контроллера в момент запуска системы СКУД на объекте. Права доступа «разовых» пропусков, как правило, одинаковые с правом посещения практически всех помещений общего пользования. В случае необходимости добавить еще несколько подобных ключей, служба безопасности записывает их в нерабочее время, чтобы не «тормозить» работу всей системы.

Почему это необходимо делать в нерабочее время? На запись ключей в память контроллеров требуется значительное время, и во время осуществления записи работа контроллеров может быть не корректной. Именно поэтому сотрудники службы безопасности объекта, в ведении которых находится система контроля доступа, периодически получают претензии пользователей, пытающихся пройти через точку доступа во время перезаписи памяти контроллера. Они вынуждены мириться с нареканиями на качество СКУД и добавлять новые ключи в контроллеры, как правило, в нерабочее время.

Использование контроллеров с Ethernet-подключением частично снимает проблему ускорения обмена данными. Но должного эффекта это не приносит, так как проблема на 90% заключается в особенностях работы памяти контроллера и алгоритмах обработки данных. Удаление утерянных ключей происходит аналогично с добавлением новых. Увеличение емкости памяти дает только половинчатый результат. Обычно утерянные ключи блокируются, оставаясь в памяти контроллера, тем самым засоряя ее.

При использовании таких СКУД данные о посетителе записываются не в системе, а в файл или просто в бумажный журнал. Достоверность занесения этих данных в 99% никто не проверяет, а бумажный архив хранится до тех пор, пока журнал не закончится. Утилизацию этих журналов никто не контролирует и

Снижению стоимости решения способствовала разработка ряда адресных и расширительных модулей

процесс не формализуется руководством. Личные данные посетителей могут оказываться в мусорном ведре, а худшем случае – у третьих лиц.

Таким образом, существующая ситуация опасна для обеих сторон, использующих СКУД. Для администрации она опасна тем, что поиск отчетов о действиях посетителей – злоумышленников затруднен. Представьте, как сложно по информации в «тетрадке» вычислить злоумышленника-гостя. Ведь одной и той же картой в течение дня могут пользоваться несколько человек. Строить отчеты о перемещениях конкретного гостя крайне проблематично. Двойная идентификация (биометрия + карта) в таком случае невозможна в принципе. Для посетителей пользование СКУД опасно тем, что, несмотря на закон о защите персональных данных, их данные очень плохо защищены.

И тем не менее, на сотнях объектов приходится мириться с такой ситуацией, поскольку другого выхода для низкобюджетных проектов нет. Вернее сказать, выхода не было до конца 2018 года.

В декабре 2018 года компания Octagram выпустила в продажу оборудование и ПО, позволяющее исключить ситуацию, описанную выше. На базе выпускаемого более 8 лет контроллера A1 запущена серия Q (турникет, дверь, лифт и др.) путем изменения микропрограмм. В данном случае на практике были использованы преимущества МИП, которая позволяет на базе одного контроллера создавать любые системы безопасности. Благодаря использованию МИП стала возможна реализация вышеупомянутого проекта для РЖД.

При использовании контроллеров A1Q на объектах с высокой «гостевой» нагрузкой алгоритм работы всей системы СКУД выглядит следующим образом: постоянным сотрудникам и гостям выдаются именные пропуска (ключи) с индивидуальными правами и ограничениями по времени и сроку действия. В момент выдачи пропуск записывается в базу контроллера, а в момент прекращения его действия удаляется из нее. Ключ заносится в память контроллера мгновенно, перезапись всей базы данных не требуется.

Достигается 100% идентичность уникального номера ключа и данных пользователя. При необходимости паспортные данные заносятся в базу и привязываются к пользователю автоматически с помощью сканера паспортов. Если требуется двойная идентификация, то биометрический признак также автоматически заносится в базу данных. Естественно, что необходимость в «тетрадках» отпадает. Защита персональных данных пользователей системы выходит на новый, более высокий уровень.

При использовании A1Q доступ пользователю разрешен только в конкретные помещения вне зависимости от того, постоянный он сотрудник или временный посетитель. Несанкционированные перемещения исключены. Блокируется карта автоматически по истечении указанного в правах доступа времени (при этом ключ удаляется из базы контроллера). Информация по данному пользователю остается в базе системы. В случае какого-либо происшествия вычисление злоумышленника происходит в течение нескольких минут, которые потребуются на поиск в базе системы по необходимому параметру.

Приятным бонусом к увеличению безопасности СКУД для сотрудников охраны в случае использования A1Q будет отсутствие необходимости записывать ключи в нерабочее время. А для руководства объекта – возможность более четко спросить с сотрудников охраны выполнения их прямых обязанностей (патрулирование территории и помещений и др.). Пользователи A1Q получат сервисы, аналогичные сервисам высокобюджетных систем.

Существенно упростить работу СКУД и усилить безопасность объекта при использовании A1Q стало возможным благодаря применению более продуктивного алгоритма обработки и записи данных в память контроллера. Каждому пользователю помимо основных параметров, видимых оператору, присваиваются дополнительные скрытые признаки. Это позволяет минимально перезаписывать ключи в памяти контроллера. При добавлении нового пользователя или удалении существующего не важно сколько используется ключей 100

или 100 тыс. Перезапись всей памяти контроллера не требуется и запись единичного ключа или небольшой группы ключей занимает короткий промежуток времени, не влияющий на работу СКУД.

Octagram выпустил ПО и микропрограммы серии Q, позволяющие создавать новую систему и интегрироваться в существующую на объекте. Внедрение в существующую систему позволяет существенно сэкономить за счет использования уже имеющихся периферийных устройств и незначительного обновления центрального программного обеспечения. Контроллер A1 теперь стал более удобным в запуске и эксплуатации. Прямо в свойствах контроллера в ПО «OctagramFlex» можно включить/выключить датчики, сменить режимы индикации на считывателе. А режим блокировки позволяет создавать шлюзы на дверных контроллерах, подключать алкотестеры, металодетекторы и другое нестандартное оборудование. Все эти новшества были выполнены на основе стандартных блоков кода для A1. При этом очень важно, что соблюдаются принципы преемственности и доступности решений.

На основе новых базовых компонент МИП Octagram расширяет функционал и возможности хорошо зарекомендовавших себя решений. В конце 2019 года была существенно доработана микропрограмма разграничения прав пользования лифтом. Сегодня строительная индустрия делает упор на строительство высотных зданий, как жилых, так и коммерческих. В связи с этим существовавшее более 15 лет решение, в котором один контроллер ограничивал доступ в лифт и поездку на этаж до 11 этажей стало слишком дорогим для некоторых клиентов, так как приходилось применять несколько контроллеров на один лифт в высотных зданиях. Теперь один контроллер Octagram A1QL позволяет контролировать до 32-х этажей при вызове с этажа и до 40 этажей, если отправку на этаж необходимо ограничивать только внутри кабины. Снижению стоимости решения для лифта способствовала разработка ряда адресных и расширительных модулей. В решении для лифта в полной мере используются преимущества патентованной МИП. Модули, используемые в решении для лифта, становятся все более универсальными и удобными, сокращается их количество.

В течение 2019 года Octagram, оставаясь в рамках одной платформы A1, существенно обновил линейку модулей и микромодулей. Появились новые модули, такие как, например,

DMT, который максимально упрощает монтаж СКУД двери на основе 32-х дверного контроллера A1DM.

Установив DMT прямо на коробке двери недалеко от замка, монтажник может существенно уменьшить объем работы и сократить время ее выполнения, так как внутри модуля имеется встроенный геркон (и клемма для подключения внешнего геркона). В модуль встроен защитный диод – это застрахует устройство от небрежности или случайной ошибки монтажника при подключении к электромагнитному замку. Внутри корпуса модуля расположена клеммная колодка, к которой подключается, в том числе, кнопка «Выход» и достаточно места для коммутации проводов. Модуль защищен от нежелательного вторжения тампером. Все сигнальные линии DMT защищены от повышенного напряжения и статики. Корпус модуля имеет удобное крепление и сочетает легкость открывания с надежной защитой прибора. Выполнен DMT из ABS-пластика с классом защиты от внешних воздействий IP53.

Другой пример – изменение микромодуля (преобразователя интерфейсов) PIN. Теперь PIN может с успехом использоваться в сторонних системах контроля доступа и безопасности. PIN преобразует интерфейс Wiegand-26 (34, 42) и протокол 8421-BCD (код с клавиатуры) в протокол 1-Wire. Одна из наиболее популярных задач, реализуемых с помощью микромодуля PIN – обновление существующей системы СКУД путем установки новых современных считывателей, в том числе биометрических, без финансовых затрат на замену центрального оборудования.

Более подробную информацию о новинках вы найдете на сайте Octagram: https://octagram.ru.

В 2-м квартале 2020 года в продажу поступит современный считыватель карт формата Mifare. Считыватель PLR3M позволяет работать в формате NFC со смартфонами и шифровать ID используемого ключа. Работа в защищенном режиме передачи ID идентификатора гарантирует защиту от копирования, клонирования и подделки карт на объекте. Возможно неограниченное количество смен секретных кодов. Дизайн считывателя и его привлекательная цена позволяют использовать его на широком спектре объектов.

Как показывает практика 2017-19 годов, вопреки расхожему мнению что «маркетинг это все» все больше специалистов отрасли безопасности обращают внимание на технические детали предлагаемых решений, особенно, если это подкрепляется экономической целесообразностью. ●