

РАЗРАБОТКА АВТОМАТИЧЕСКОЙ СКУД ПОВЫШЕННОЙ БЕЗОПАСНОСТИ НА БАЗЕ ТИПОВОГО РЕШЕНИЯ СКУД BIOSMART С ИСПОЛЬЗОВАНИЕМ АВТОМАТНОГО ПОДХОДА

Максимов Р.Л.¹, Рафиков А.Г.²

Анализ текущего состояния систем безопасности доступа к промышленным объектам демонстрирует наличие ряда критичных проблем в данной области. Проведённые исследования указывают на рост уязвимостей в системах контроля доступа, наряду с увеличением функционала растёт сложность, стоимость внедрения и стоимость владения такими системами. Следовательно, значимость и удельный вес вопросов безопасности с учётом последствий различного рода атак на системы непрерывно повышается. В статье предложен оригинальный подход к разработке СКУД, которым целесообразно руководствоваться при выборе и разработке средств контроля и управления доступом на промышленном объекте, с целью снижения затрат на разработку, повышения информационной безопасности, функциональных возможностей и, как следствие, обеспечения надёжной физической защиты промышленного предприятия (объекта). Предложенный подход к модернизации системы «BioSmart» был реализован в рамках хозяйственных отношений при построении шлюзовой СКУД повышенной защищённости на действующем предприятии.

Ключевые слова: система контроля и управления доступом, автоматизированная система управления, технологический процесс, информационная безопасность, система диспетчерского контроля и управления доступом на объект, система сбора данных

1. Введение

В настоящее время биометрическая аутентификация не только является неотъемлемой процедурой для допуска к объектам повышенной секретности, но и входит в нашу повседневную жизнь, широко применяется в системах контроля доступа и учёта рабочего времени. Огромный интерес к биометрии обусловлен рядом объективных причин. В классических парольных системах, а также системах на основе карт доступа подглядывание или угадывание пароля, кража или изготовление дубликата карты приводит к компрометации всей системы. Более того, законный пользователь, потеряв или испортив карту, теряет возможность доступа к системе. Системы на основе биометрии имеют идентификатор (аутентификатор), неразрывно связанный с самим пользователем, поэтому потеря или изменение идентификатора возможны только в чрезвычайных ситуациях, кроме того, современные сканеры биометрических данных позволяют без труда обнаруживать попытки использования муляжей.

Такие системы могут осуществлять контроль перемещения людей и транспорта по территории охраняемого объекта, обеспечивать безопас-

ность персонала и посетителей, а также сохранность материальных и информационных ресурсов предприятия. Системы контроля и управления доступом используются на промышленных предприятиях, в офисах, магазинах, на автостоянках и автосервисах, в жилых помещениях.

Интерес к системам контроля и управления доступом растёт ещё и потому, что наличие такой системы важно для эффективной работы предприятия.

Существующий ГОСТ Р 51241-2008 «Средства и системы контроля и управления доступом» [1], устанавливает классификацию, общие технические требования и методы испытаний, подразделяет СКУД по:

- способу управления;
- числу контролируемых точек доступа;
- функциональным характеристикам;
- виду объектов контроля;
- уровню защищённости системы от несанкционированного доступа.

В соответствии с документом Р 78.36.005-99 «Выбор и применение систем контроля и управления доступом» все СКУД делятся на четыре класса [2].

1 Максимов Роман Леонидович, МГТУ им. Н.Э. Баумана, Москва, iu8asvt@gmail.com

2 Рафиков Андрей Гяззович, МГТУ им. Н.Э. Баумана, Москва, r.l.maksimov@gmail.com

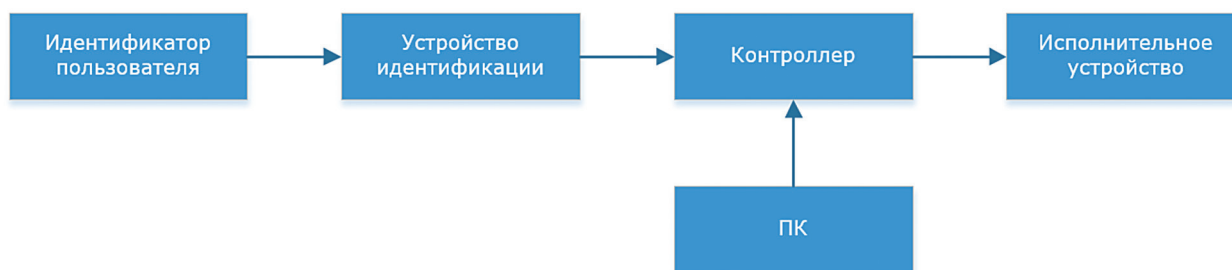


Рис.1. Обобщённая схема СКУД

2. Описание обобщённой схемы СКУД и её параметров

На сегодняшний день существует множество разновидностей СКУД и её компонентов от различных производителей. Несмотря на уникальность каждой конкретной системы контроля доступа, она содержит 4 основных элемента: идентификатор пользователя (карта-пропуск, ключ, биометрический признак), устройство идентификации, управляющий контроллер и исполнительные устройства. Обобщённая схема СКУД показана на рис.1 [3].

Одна из самых распространённых биометрических СКУД отечественного производства – **СКУД BioSmart**, производитель ПРОСОФТ БИОМЕТРИКС, город Екатеринбург [4, 5].

Система контроля и управления доступом (СКУД) BioSmart позволяет предприятиям организовать эффективную систему контроля и управления доступом, предотвратить несанкционированный доступ на территорию предприятия. СКУД BioSmart отвечает всем современным требованиям, предъявляемым к таким системам, включающим высокий уровень безопасности, обеспечение контроля посещаемости и трудовой дисциплины, интеграцию с системами сторонних производителей. Принцип работы СКУД BioSmart основывается на технологии идентификации личности путем сканирования отпечатка пальца или бесконтактной пластиковой карты. Использование последних технических разработок обеспечивают высокую надежность системы при достаточной простоте и удобстве её эксплуатации.

СКУД BioSmart имеет ряд преимуществ перед традиционными системами контроля доступа: адаптированность к российским условиям (температурный диапазон работы от -40°C до +50°C); алгоритмы обработки шаблонов отпечатков пальцев соответствуют ГОСТ-Р ИСО/МЭК 19794/2 2005; возможность идентификации до 30 тыс. отпечатков пальцев в серверном режиме; запатентованная аппаратная защита от муляжей.

3. Пример СКУД на базе оборудования BioSmart

3.1. Описание системы

Однако, все преимущества системы могут быть сведены на нет, если потребуется изменить набор функций СКУД BioSmart.

В качестве примера, рассмотрим создание СКУД на базе оборудования BioSmart.

Рассматриваемый объект: центральный офис некоторого банка.

Поставлена задача: строгое ограничение входа в служебную зону.

Одно из очевидных решений – использование шлюза: шлюзовой кабины или тамбур-шлюза [6]. В качестве элементов системы контроля и управления доступом, а также в качестве элементов технической укреплённости банков применяют шлюзовые кабины (тамбур-шлюзы) с автоматическими раздвижными дверями (рис. 2) таких производителей, как Circle, Evolution Light, Evolution Star, TITANIC.



Рис.2. Шлюзовая кабина

Интегрированные автоматические шлюзовые кабины предназначены для защиты доступа на объект или в его особую зону от несанкционированного проникновения, с целью обнаружения оружия, разделения людских потоков, предупреждения захвата заложников, противодействия терроризму.

Представляют собой металлические остеклённые бронированные кабины с автоматическими системами сдвижных дверей из пулеустойчивого стекла.

Шлюзы хорошо решают многие задачи контроля доступа. Однако стоимость таких шлюзов высокая, даже для коммерческих банков.

Поэтому наиболее оптимальным, в этом случае, будет решение, с использованием *взаимосвязанных дверей тамбура с логикой шлюза*.

Для решение этой задачи, также, может быть использована СКУД BioSmart.

3.2. Структурная схема СКУД BioSmart

СКУД BioSmart (рис. 3) может быть организована как сетевая, распределённая система, с разграничением прав доступа пользователей, которая, при необходимости, может быть наращиваемой и открытой для интеграции с оборудованием других производителей.

Таким образом, СКУД BioSmart сможет реализовать хорошее решение с точки зрения безопасности и цены – шлюз на базе двух дверей, которое позволяет организовать вход и выход из помещения по шлюзовому алгоритму, используя две стандартные двери с электромагнитными замками.

Объект: здание главного управления коммерческого банка, оснащённое системой контроля доступа СКУД BioSmart.

Цели: обеспечение усиленного контроля доступа при входе и выходе. Защита жизни и здо-

ровья сотрудников банка, повышение доверия клиентов и посетителей. Защита материальных и информационных ценностей, находящихся в здании банка.

Задачи:

1. Создание двух взаимозависимых точек прохода на базе стандартных дверей, работающих по шлюзовому алгоритму.
2. Обеспечение входа и выхода постоянного персонала в автоматическом режиме с минимальной задержкой.
3. Проход по временным и разовым пропускам только после получения подтверждения от оператора (охранника).
4. Обеспечение возможности блокировки человека в шлюзе.
5. Наличие режима полной разблокировки дверей шлюза.
6. Регистрация в архиве системы всех событий, включая действия оператора по управлению работой шлюза.

Решение, представленное на рис. 4, включает в себя:

1) *Двери шлюза.* Каждая дверь в помещении шлюза оснащается электромагнитным замком, двумя считывателями, доводчиком, датчиком прохода (СМК), световыми индикаторами состояния двери. Вход в шлюз выполняется автоматически по предъявлению карты любого типа. Выход из шлюза через вторую дверь возможен только после закрытия первой двери, при этом для постоянных карт выход выполняется автоматически (по считывателю), а для временных и разовых – только после нажатия кнопки подтверждения на пульте охранника.

2) *Считыватель карт доступа.* Считыватели установлены по обе стороны дверей шлюза. Если

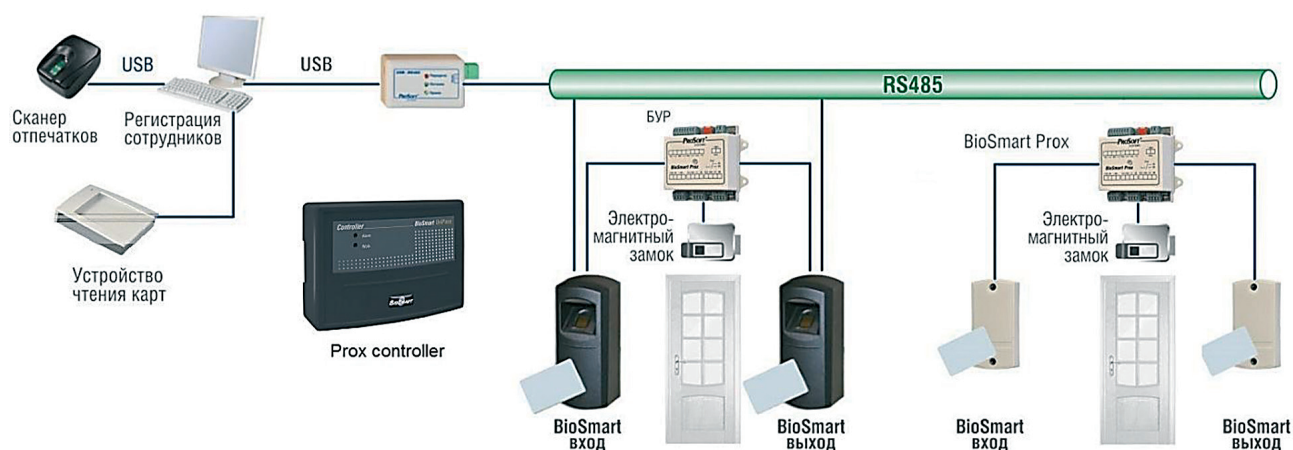


Рис. 3. Структурная схема СКУД BioSmart



Рис. 4. Тамбур-шлюз

человек находится внутри, внешние считыватели обеих дверей временно блокируются, пока шлюз не освободится.

3) *Индикатор состояния двери.* Индикатор состояния двери выполнен на светодиодах красного и зеленого цвета и показывает текущее состояние замка. Если проход через дверь разрешён, загорается зеленый индикатор, запрету прохода через дверь соответствует красный сигнал индикатора.

4) *Электромагнитный замок.* Двери шлюза оснащены электромагнитными (электрохимическими) замками. После выполнения прохода, дверь закрывается автоматическим доводчиком. По срабатыванию СМК дверного датчика, замок включается и блокирует дверь.

5) *Датчик прохода.* Магнитоконтактный датчик положения на каждой двери решает две задачи – контролирует незаконное проникновение в помещение шлюза без предоставления доступа, а также регистрирует проход через дверь в штатном режиме работы СКУД.

6) *Контроллер СКУД (Prox).* Контроллер СКУД Prox – центральный элемент управления работой шлюза. В приведённой конфигурации используется контроллер Prox (рис. 3, связи не показаны), позволяющий выполнить подключение четырёх считывателей.

7) *Пульт ручного управления шлюзом.* Пульт ручного управления находится на рабочем столе охранника и предназначен для подачи мини-

мального набора команд управления шлюзом вручную: открыть внешнюю дверь, открыть внутреннюю дверь. Все факты нажатия кнопок пульта ручного управления шлюзом фиксируются в протоколе СКУД.

8) *АРМ оператора.* Рабочее место оператора организовано на основе компьютера, работающего под управлением СКУД BioSmart. На мониторе отображается текущее состояние дверей шлюза, направление прохода, личные данные предъявителя карты, включая фотографию. Охранник по фотографии пользователя на мониторе и дополнительной информации в окне событий (на экране видеокamеры) принимает решение о предоставлении доступа или отказе в доступе.

9) *Датчик присутствия (ДП).* Регистрирует присутствие человека внутри тамбур-шлюза в штатном режиме работы СКУД. Количество человек, присутствующих в шлюзе, при этом, не распознается.

3.3 Адаптация СКУД под дополнительные требования

Анализ состава оборудования и набора функций системы показывает, что все перечисленные требования легко реализуются с использованием СКУД BioSmart, но ситуация совершенно меняется, если накладываются *дополнительные требования*: меняется режим и объект охраны, изменяется состав и конфигурация оборудования тамбура-шлюза.

Например, требуется обеспечить контролируемый автоматический проход с использованием многофакторной аутентификацией на режимное предприятие (банк, офис компании) сотрудников с одновременным учётом рабочего времени. Используется «глухой» тамбур, охранник отсутствует, контроль прохода полностью автоматический, нештатные ситуации вместо охранника периодически разрешает дежурный из числа постоянных сотрудников. Вход в шлюз выполняется по одному человеку, что, также, должна контролировать СКУД. Занятость шлюза должна сопровождаться дополнительной индикацией и блокировкой дверей шлюза.

Приведённый набор требований оказывается не под силу даже такой мощной СКУД как BioSmart. Для решения задачи предлагается реализовать синтез блока управления, используя автоматное представление СКУД для формирования оптимального набора необходимых дополнительных функций и управляющих воздействий, возникающих в изменённых условиях функционирования СКУД BioSmart. При этом, существующий набор функций СКУД BioSmart будет частично задействован при построении новой, более совершенной автоматической шлюзовой СКУД повышенной защищённости.

Для этого производим декомпозицию исходной системы, используя автоматное представление системы. Выделим в структуре исходной системы СКУД BioSmart (рис. 5) управляющий (УА) и операционные автоматы (ОА1, ОА2) и наборы управляющих и входных сигналов (флагов).

Полученная декомпозиция наиболее точно соответствует описанию автомата Мили. Математическая модель автомата Мили и схема рекуррентных соотношений ничем не отличаются от математической модели и схемы рекуррентных соотношений абстрактного автомата [7, 8]. Законы функционирования такого автомата имеют вид:

$$a(t+1) = \delta[a(t), x(t)],$$

$$y(t) = \lambda[a(t), x(t)].$$

Алгоритм функционирования (А0) можно представить в виде суперпозиции уравнений, которая описывается приведёнными зависимостями и может быть изображена как диаграмма состояний или БСА. Новый набор дополнительных функций представим аналогично, в виде алгоритма и обозначим А1.

Структура УА и ОА, реализующая алгоритм А0 это управляющий автомат УА0 и операционный автомат ОА0. Структура УА и ОА, реализующая алго-

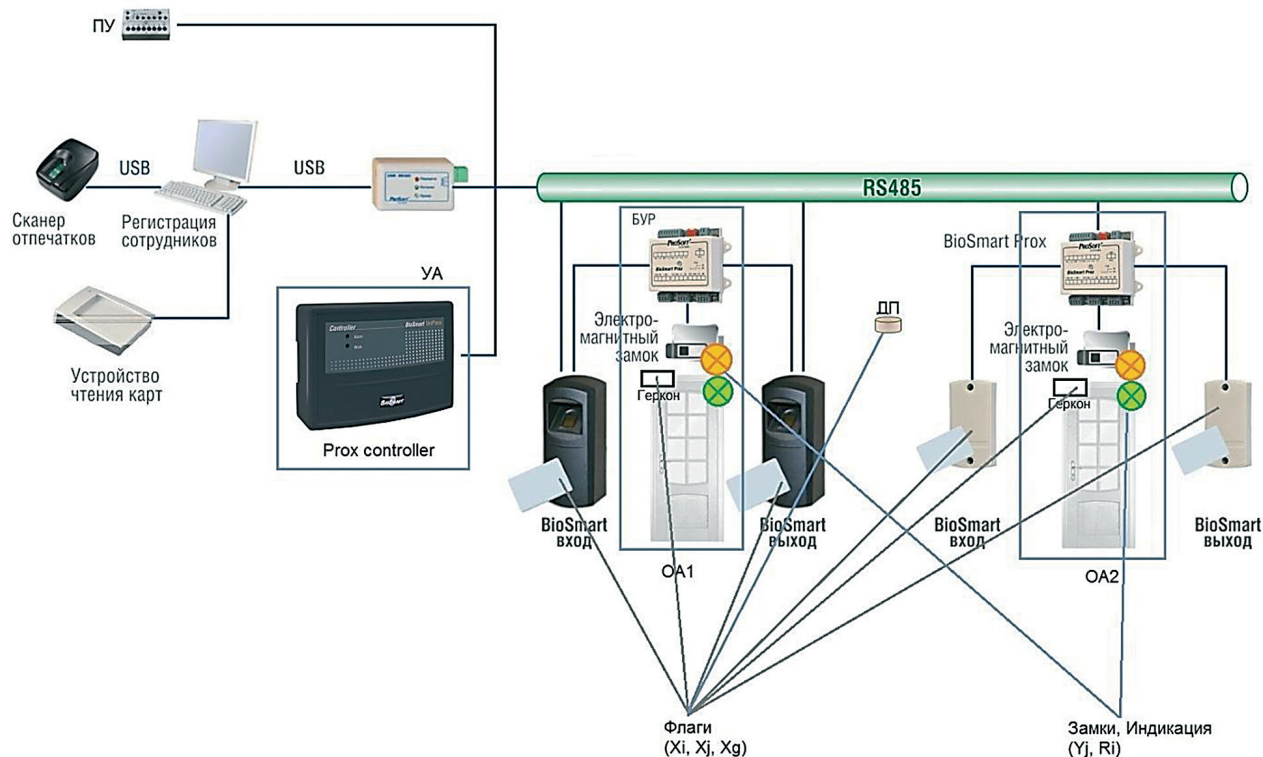


Рис.5. Система управления шлюзом (базовый вариант)

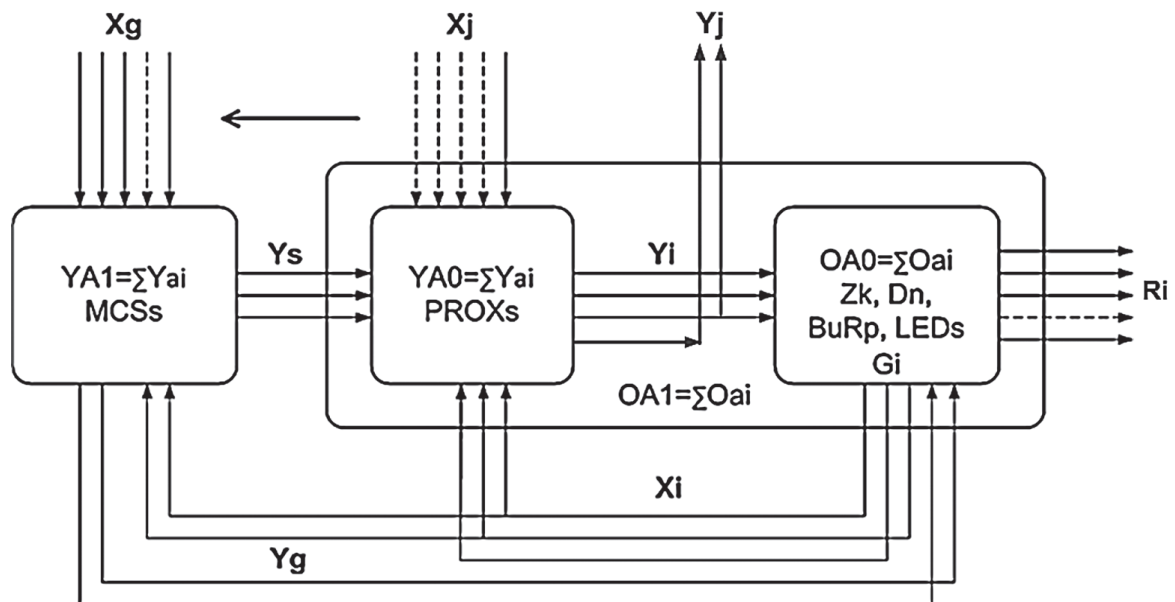


Рис.6. Блок управления шлюзом

ритм $A0+A1$, - это управляющий автомат YA1 и операционный автомат OA1, изображённые на рис.6.

Разработка ПО для YA1 возможна без наличия OA1, причём набор входных сигналов X_i имитируется простыми переключателями, а для эмуляции управляющих сигналов $Y_j \setminus R_i$ используются светодиоды, подключённые к шине питания через резисторы номинала 100 Ом.

Модель для отладки ПО автомата YA1 контроллера шлюза (КШ) реализована в системе моделирования Proteus 7.10 и изображена на рис.7.

Управляющий автомат YA1, который участвует в управлении шлюзом, представляет собой электронный блок, состоящий из микроконтроллера семейства PIC18Fх5xx, интерфейсных ИС и дискретной логики, и предназначен для контроля и

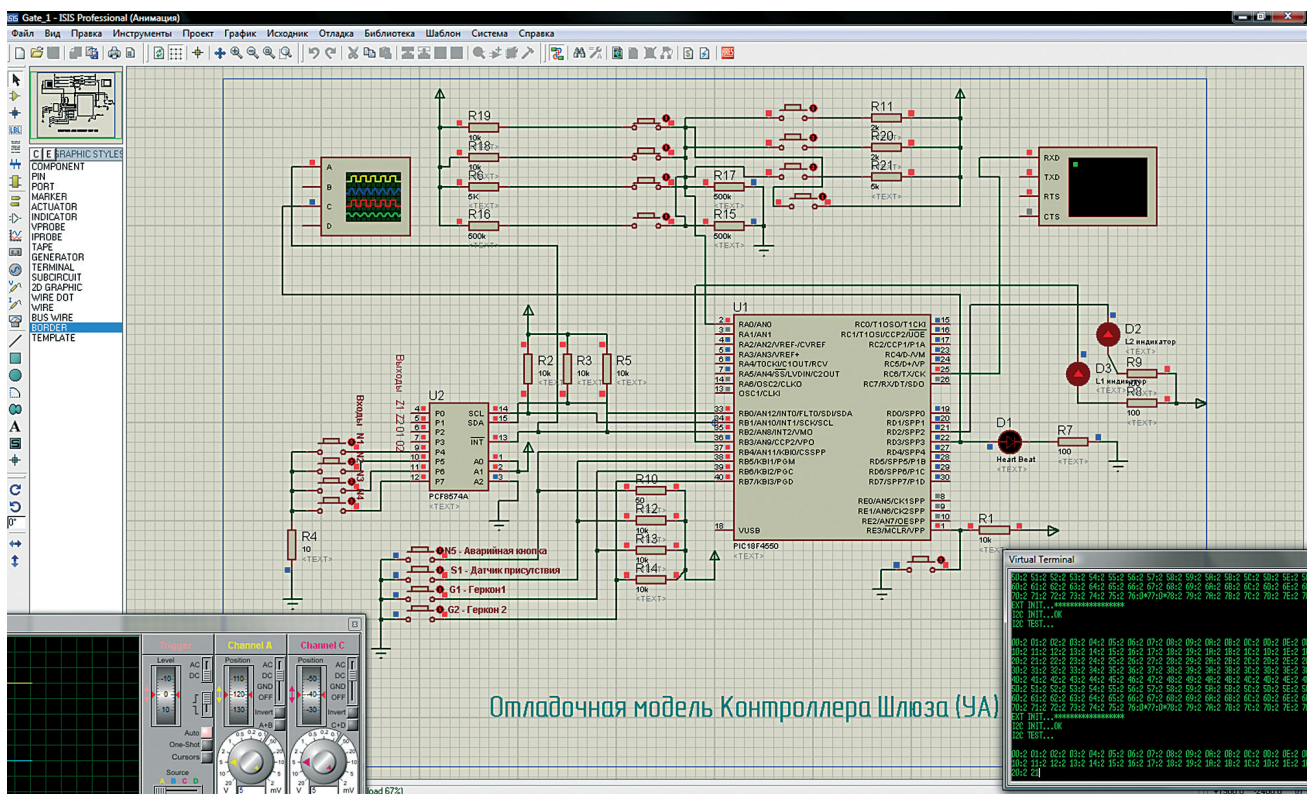


Рис.7. Модель для отладки ПО автомата YA1 (контроллера шлюза)

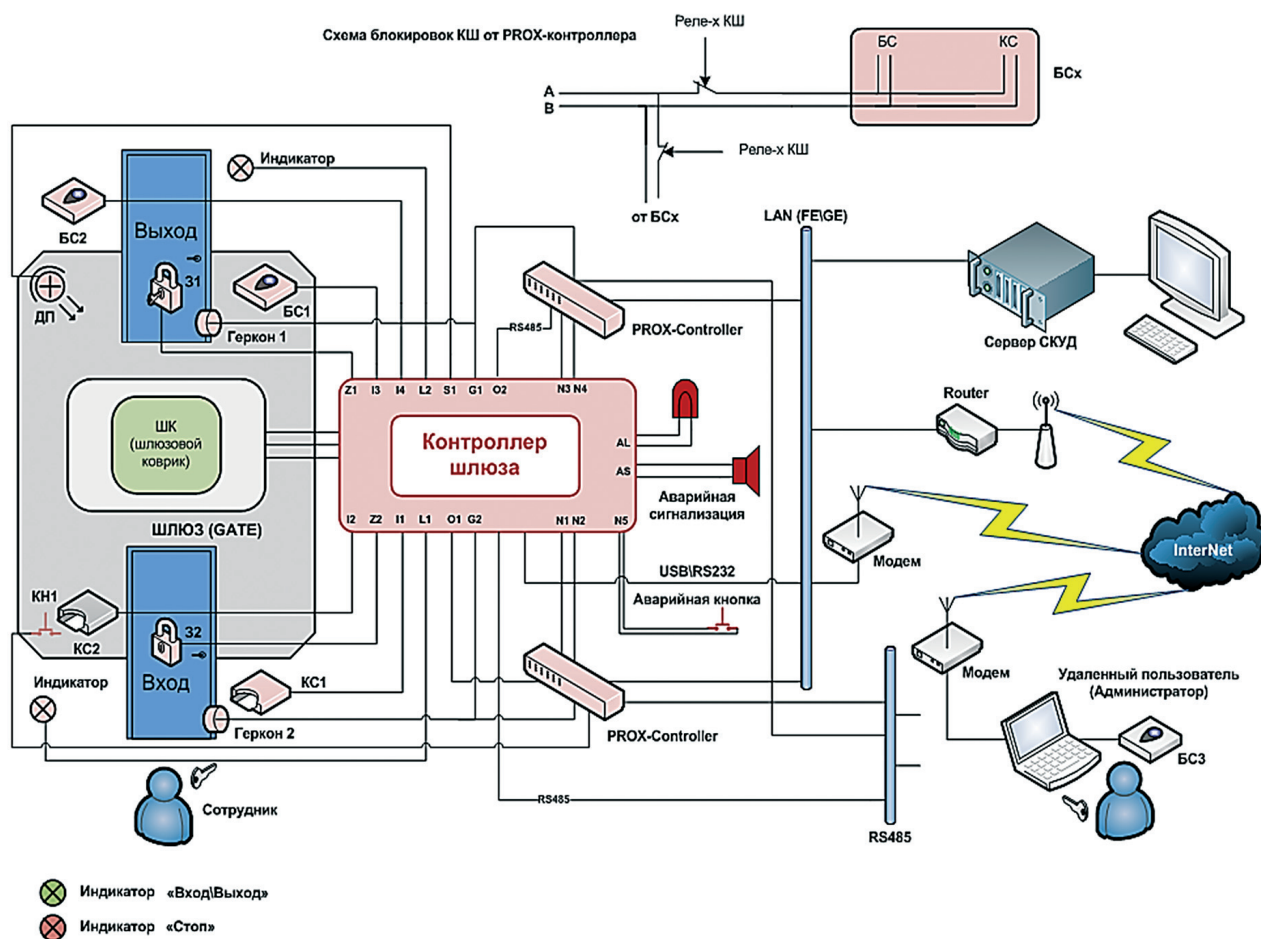


Рис.8. Схема автоматического шлюза на базе КШ (УА1)

управления квази-операционным автоматом ОА1, реализующим базовые функции СКУД BioSmart.

Изложенный подход позволяет на основе существующей функционально ограниченной системы построить автоматическую полнофункциональную СКУД повышенной защищенности.

Итоговая схема управления шлюзом с полным набором функций, соответствующая поставленной задаче, приведена на рис. 8 и содержит УА1 (контроллер шлюза) и квази-операционный автомат ОА1, состоящий из управляющего и операционного автоматов УА0 и ОА0 из состава базовой СКУД BioSmart.

4. Заключение

В статье предложен эффективный подход к процедуре синтеза блока управления шлюзами СКУД повышенной защищенности. Блок управления представляется в виде конечного автомата,

что позволяет использовать методологию теории конечных автоматов, существенно расширить функциональные возможности базовых, серийно выпускаемых СКУД, автоматизированных-информационных систем. Предложен подход, который, в зависимости от требуемого функционала СКУД и ИС, позволяет реализовать алгоритмы любой сложности минимальными средствами и обеспечить непрерывный пошаговый контроль за синтезом узлов СКУД с целью минимизации аппаратных затрат на реализацию, заданного набора функций блоков управления СКУД или других систем информационной и физической безопасности. Предложенный подход к модернизации системы «BioSmart» был реализован в рамках хозяйственных отношений при построении шлюзовой СКУД повышенной защищенности компанией ЗАО ГК «ИСКАНДЕР» для НП СРО «ПРОЕКТ».

Рецензент: кандидат технических наук, доцент Медведев Николай Викторович, medvedevnick54@yandex.ru

Литература:

1. ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. М.: Стандартинформ, 2009. 31 с.
2. Р 78.36.005-99. Выбор и применение систем контроля и управления доступом. М.: НИЦ «Охрана», 1999. (послед. ред. - 21.05.2015).
3. Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. М.: Изд-во Горячая Линия-Телеком, 2010. 272 с.
4. Биометрическая система контроля доступа Biosmart, руководство по эксплуатации контроллера биометрического Biosmart, ПАДФ.425723.002 РЭ. Екатеринбург: ООО Прософт-системы, 2011. 36 с.
5. Биометрическая система контроля доступа Biosmart, руководство по эксплуатации считывателя Biosmart mini, ПАДФ.425723.032 РЭ. Екатеринбург: ProSoft Biometrics, 2011. 18 с.
6. Пособие к МГСН 4.10-97, здания банковских учреждений. М.: 1999. URL: <http://www.gosthelp.ru/text/PosobieMGSN41097Zdaniyab.html> (дата обращения: 09.12.2015).
7. Карпов Ю.Г. Теория автоматов. СПб.: Питер, 2002. 208 с.
8. Богаченко Н.Ф., Файзуллин Р.Т. Синтез дискретных автоматов. Омск: Изд-во Наследие. Диалог-Сибирь, 2006. 107 с.

DEVELOPMENT OF THE AUTOMATIC ENHANCED SECURITY ACCESS CONTROL SYSTEM BASED ON THE TYPICAL SOLUTION OF THE ACS BIOSMART USING AUTOMATA-BASED APPROACH

Maksimov R.L.³, Rafikov A.G.⁴

Analysis of the current state of the access control systems of the industrial facilities demonstrates the existence of a number of critical issues in this area. The carried out researches show the increasing vulnerabilities in the access control systems. The complexity, the implementation cost and the cost of ownership are growing along with increasing functionality of these systems. Therefore, taking into account the effects of various types of attacks on the systems the importance of security issues continuously increased. This paper proposes a novel approach to the development of ACS, which should be guided when choosing and developing of access and control tools at an industrial facility, in order to reduce development costs, improving information security, functionality and providing reliable physical protection of industrial enterprises. The proposed approach to the modernization of the system «BioSmart» was implemented under terms of the agreement when constructing a gateway ACS with enhanced security at the real facility.

Keywords: access control system, automated control system, industrial process, technological process, information security, supervisory control and data acquisition

References:

1. GOST R 51241-2008. Sredstva i sistemy kontrolya i upravleniya dostupom. Klassifikatsiya. Obshchie tekhnicheskie trebovaniya. Metody ispytaniy. M.: Standartinform, 2009. 31 P.
2. R 78.36.005-99. Vybora i primeneniya sistem kontrolya i upravleniya dostupom. Moscow: NITs «Okhrana», 1999. (posled. red. - 21.05.2015).
3. Vorona V.A., Tikhonov V.A. Sistemy kontrolya i upravleniya dostupom. Moscow: Izd-vo Goryachaya Liniya-Telekom, 2010. 272 P.
4. Biometricheskaya sistema kontrolya dostupa Biosmart, rukovodstvo po ekspluatatsii kontrollera biometricheskogo Biosmart, PADF.425723.002 RE. Ekaterinburg: OOO Prosoft-sistemy, 2011. 36 P.
5. Biometricheskaya sistema kontrolya dostupa Biosmart, rukovodstvo po ekspluatatsii schityvatelya Biosmart mini, PADF.425723.032 RE. Ekaterinburg: ProSoft Biometrics, 2011. 18 P.
6. Posobie k MGSN 4.10-97, zdaniya bankovskikh uchrezhdeniy. Moscow: 1999. URL: <http://www.gosthelp.ru/text/PosobieMGSN41097Zdaniyab.html> (data obrashcheniya: 09.12.2015).
7. Karpov Yu.G. Teoriya avtomatov. SPb.: Piter, 2002. 208 P.
8. Bogachenko N.F., Fayzullin R.T. Sintez diskretnykh avtomatov. Omsk: Izd-vo Nasledie. Dialog-Sibir', 2006. 107 P.

3 Roman Maksimov, Bauman Moscow State Technical University, Moscow, iu8asvt@gmail.com

4 Andrey Rafikov, Bauman Moscow State Technical University, Moscow, r.l.maksimov@gmail.com