Министерство образования и науки Российской Федерации

Федеральное агентство по образованию

"МАТИ" – Российский государственный технологический университет им. К.Э.Циолковского

Автоматизированная система комплексной безопасности, интегрируемая в единую систему управления вузом

Введение

Анализ статистики в области безопасности образовательных учреждений показывает, что в последние годы наблюдается устойчивая тенденция роста чрезвычайных ситуаций. Последствия террористических актов и пожаров в зданиях высших и средних учебных заведений, произошедших за последнее время, заявляют об актуальности предупреждения чрезвычайных ситуаций в сфере образования. Минобразования России была разработана и принята программа на 2004–2007 годы “Безопасность образовательного учреждения”.

Основным направлением деятельности, определяемым вышеуказанным документом, обозначено обеспечение безопасности обучающихся, воспитанников и работников образовательных учреждений всех типов и видов на основе использования современных достижений науки и техники в этой области.

Приказом Федерального агентства по образованию от 06.04.2005 № 241 “Об итогах выполнения отраслевой программы “Безопасность образовательного учреждения” в 2004 году” приоритетным направлением определены обеспечение комплексной безопасности (пожарной, электрической, технической, экологической, антитеррористической и антикриминальной) объектов образования, разработка отраслевой программы “Комплексная безопасность образовательного учреждения” на 2006–2010 годы.

Исходя из вышеизложенного, обеспечение безопасности университета является приоритетной задачей, поэтому в рамках ее решения в 2001 году была принята и реализуется программа комплексной безопасности “МАТИ”. Отсутствие на рынке

технологических решений, обеспечивающих комплексную безопасность образовательных учреждений, определило направление развития научных и исследовательских проектов по созданию единой системы комплексной безопасности (СКБ) вуза.

Основной частью системы является многофункциональный программируемый контроллер МАТИ МПК-3, разработанный в вузе. Уникальность данного изделия заключается в том, что в контроллер можно подгрузить десятки различных программ, определяющих логику работы любых устройств управления инженерных систем и СКБ. Модели систем разработанные на базе МАТИ МПК-3, демонстрировались на различных конференциях, выставках, профильных семинарах-совещаниях, проводимых Минобрнауки и Рособразованием. Признание СКБ на базе МАТИ МПК-3 отмечено дипломами Рособразования и ВВЦ.

Развитие СКБ в МАТИ ведется в рамках единой информационной системы. Это обусловлено двумя причинами:

1) все современные технические системы обеспечения безопасности функционируют на базе программно-аппаратных комплексов (ПАК) и требуют информационной поддержки

2) система обеспечения контроля доступа на территорию и экстренной эвакуации не может эффективно функционировать без актуальной информации о персонах, имеющих право посещения территории университета. Большая численность и многообразие групп контингента посетителей делают невозможным решение задачи его оперативного учета службой безопасности. Поэтому целесообразно получать эту информацию из единой информационной системы, где этот перечень может быть оперативно сформирован несколькими подразделениями, отвечающими за поддержку информации о своей группе контингента.

Поскольку СКБ единой информационной системы является компонентом системы управления, то ее приложение может быть использовано во всех направлениях автоматизации предприятия. Функции удаленного мониторинга, диагностики управления техническими системами, а также авторизация персон при

помощи электронного ключа позволяют обеспечить новые возможности системы управления вузом. Особенным применением компонента СКБ единой информационной системы является автоматизация задач инженерного обеспечения зданий и сооружений, что позволяет интегрировать систему контроля доступом, охранную, противопожарную системы и системы управления освещением, вентиляцией, дымоудаления в единый комплекс средств технического управления вузом.

Программная и аппаратная части системы образуют ПАК и имеют модульный принцип организации, что позволяет легко их наращивать, расширять территорию функционирования и круг решаемых задач.

1. Назначение системы

Поскольку ПАК является компонентом системы управления, то его приложение может быть использовано во всех направлениях автоматизации предприятия. Функции удаленного мониторинга, диагностики управления техническими системами, а также авторизация персон при помощи электронного ключа позволяют обеспечить новые возможности системы управления вузом. Особенным применением ПАК является автоматизация задач инженерного обеспечения зданий и сооружений, что позволяет интегрировать систему контроля доступом, охранную, противопожарную системы и системы управления освещением, вентиляцией, дымоудаления в единый комплекс средств технического управления вузом.

Новые технические возможности влекут за собой и новый подход в административном управлении и организации обеспечения комплексной безопасности учебного заведения путем формирования современных организационных, информационных и технических решений, интегрированных в систему управления вузом, с одной стороны, и увязанных с инженерными системами жизнеобеспечения, с другой. Только единая система автоматизации с единым пространством данных всех ее подсистем может обеспечить эффективное управление, готовность к чрезвычайным и криминальным ситуациям, порядок и

прогнозируемость деятельности как всего предприятия, так и каждого подразделения в его составе.

Разработанный нами комплекс изначально проектировался как единая система автоматизации. С возможностью взаимодействия с системами других производителей в большинстве случаев может быть использован частично, совместно с имеющимися системами. Это достижимо благодаря использованию открытой технологии Java (спецификации J2EE, J2SE) и общепринятых стандартов: SQL92, CORBA, SSL, TCP/IP и др.

2. Структура системы

Программная и аппаратная части системы имеют модульный принцип организации, что позволяет легко их наращивать, расширять территорию функционирования и круг решаемых задач.

Схема технологического функционирования ПАК СКОБО (система комплексного обеспечения безопасности объекта) вуза представлена на рис. 1.

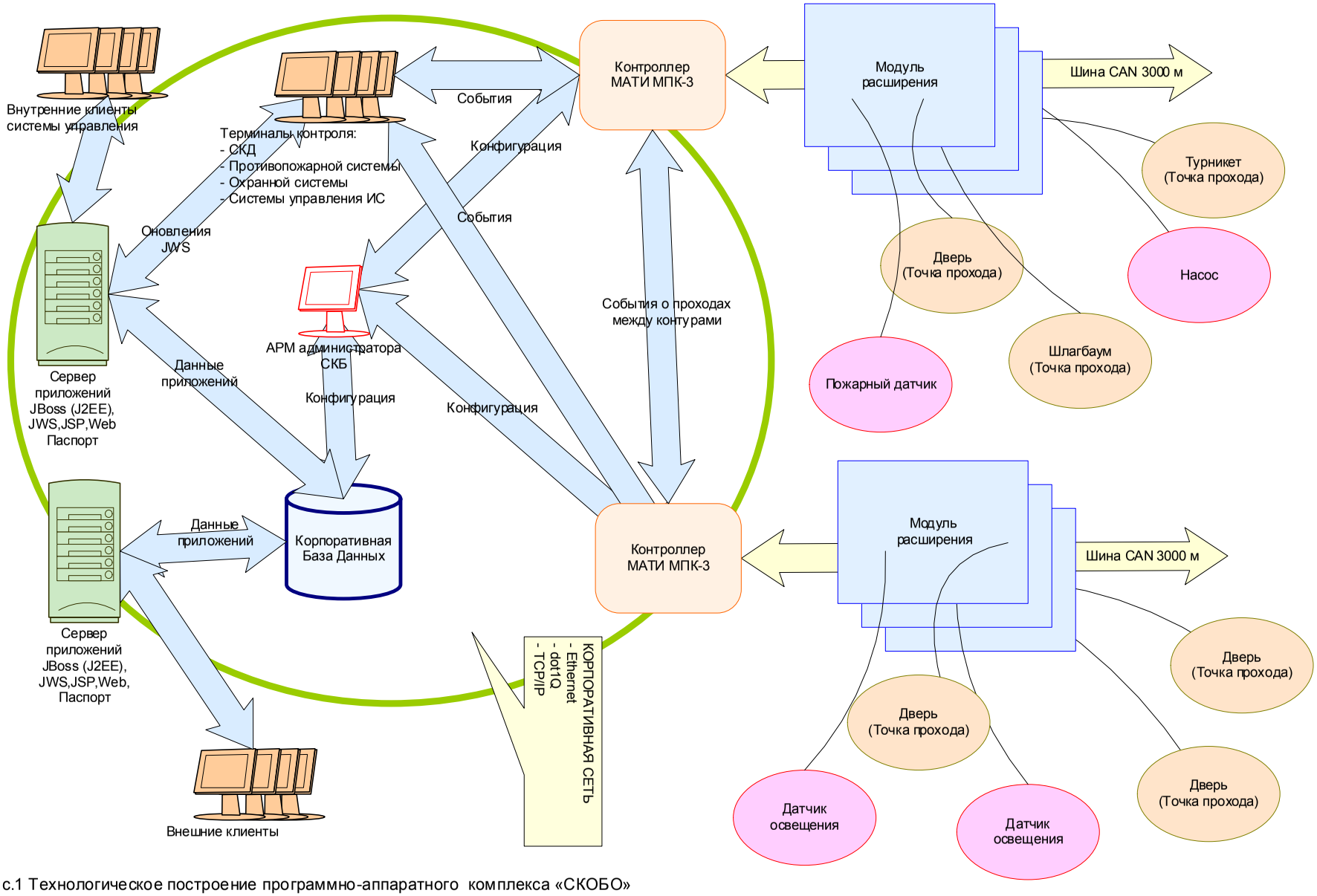

Рис.1 Технологическое построение программно-аппаратного комплекса «СКОБО»

Основной частью системы является многофункциональный программируемый контроллер МАТИ МПК-3, построенный на базе ОС Linux со специализированным мультикомпонентным программным обеспечением, основанным на технологии J2SE. Суть мультикомпонентного подхода заключается в том, что в контроллер можно подгрузить десятки различных компонентов, определяющих логику работы устройства. Таким образом, возможно параллельное решение различных задач — от системы контроля доступа (СКД) до управления инженерными сооружениями на одном контроллере. Компоненты работают в специализированной среде MPCInstance, которая обеспечивает взаимодействие компонентов в рамках модели связывания. Именно при помощи модели связывания определяются круг задач и логика работы каждого контроллера и его взаимодействия с другими подсистемами.

В зависимости от конфигурации МАТИ МПК-3 может хранить данные о 100 000 пользователей (с фотографиями и прочей персональной информацией) и о более чем 1 000 000 последних событий. Хранение в контроллере не только кода карты доступа, но и другой информации о персоне позволяет исключить промежуточные узлы (например, базу данных или сервер приложений) между контроллерами и терминалами СКД/охраны, что в значительной степени повышает надежность системы во время чрезвычайных ситуаций, увеличивает производительность, упрощает обслуживание и делает поддержку более дешевой.

Контроллеры включаются в корпоративную сеть при помощи интерфейса Ethernet100BaseT и протокола TCP/IP. Все соединения, как между контроллерами, так и с управляющими терминалами, защищены при помощи протокола SSL. Управление периферийными устройствами (двери, шлагбаумы, турникеты, охранные/пожарные датчики и др.) осуществляется при помощи модулей расширения, которые включены на дифференциальной шине CAN. CAN-протокол поддерживает методику арбитража для разделения коллизий, что позволяет получать информацию от сотен элементарных устройств (например, от датчиков) без потери производительности в отличие от большинства систем на базе RS485, где устройства постоянно опрашиваются головным модулем и каждое новое устройство на шине увеличивает

время реакции системы на событие. Общая длина шины CAN может достигать 3000 м против заявленных 1000 м у шины RS485.

Для обеспечения бесперебойной работы корпоративных приложений используется трехуровневая архитектура по технологии J2EE, включающая в себя корпоративный сервер баз данных (Oracle9i), серверы приложений под управлением J2EE-сервера JBoss и клиентские рабочие места с прикладным программным обеспечением (рис. 2).

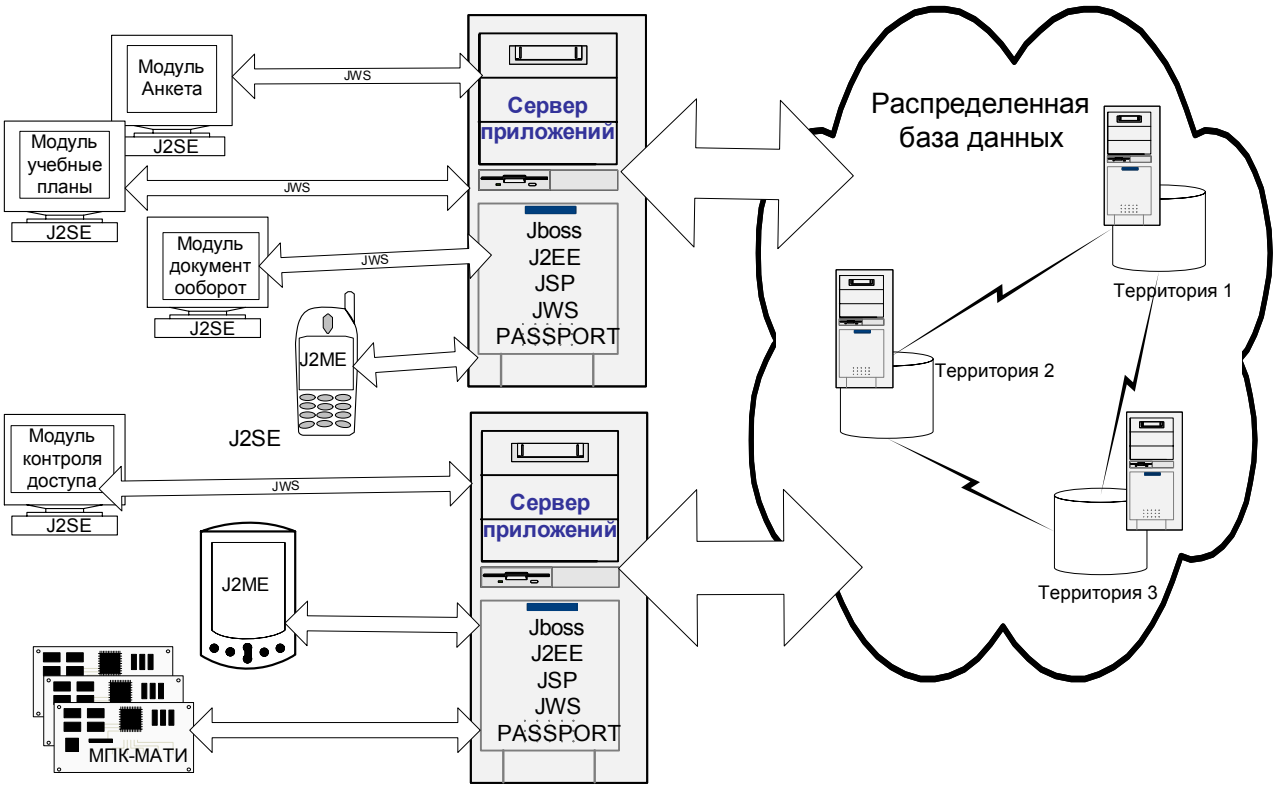

Рис. 2 Программно-аппаратная архитектура Единой информационной системы

Обновление клиентских приложений и их конфигураций осуществляется при помощи средств Java Web Start, что значительно позволяет снизить затраты на обслуживание конечных пользователей и сделать их такими же, как при использовании веб-терминалов. Только в отличие от веб-доступа конечный

пользователь получает полноценный пользовательский интерфейс, что положительно сказывается на темпах внедрения и запуска системы.

Для разделения доступа к ресурсам базы данных (БД) аудита и исторического хранения данных используется специализированный J2EE-компонент “Паспорт”. Разработка и внедрение “Паспорта” дали возможность не зависеть на прикладном уровне от реализации сервера БД и позволяют без проблем портировать с сервера Oracle все прикладные приложения на другие платформы, такие, как MS SQL Server, Postgress, Interbase, IBM DB2 и др. “Паспорт” позволяет разделить доступ к записям БД между различными пользователями, что особенно удобно в структурах с разветвленной иерархией, например в вузе, где связка ректорат — факультеты — кафедры может достигать десятки, а то и сотни конечных элементов идентификации с персональными правами доступа к записям БД.

Благодаря возможностям “Паспорта” и прозрачности JAVA-архитектуры автоматизированы многие процессы управления в вузе. В первую очередь, это автоматизация учета контингента при помощи соответствующих серверных компонентов и автоматизированного рабочего места (АРМ) “Анкета”. Вся система позволяет не только манипулировать контингентом на уровне групп и персон, но и прозрачно портировать постоянно меняющиеся списки необходимых групп контингента в две не связанные между собой конфигурации “1С-бухгалтерия” и в автоматизированную библиотечную систему MARC-SQL. Таким образом, электронный ключ системы контроля доступа используется для авторизации не только на турникетах и дверях комплекса зданий, но и в библиотечной системе и терминалах общего доступа. Помимо АРМ “Анкета” разработаны другие системы автоматизации: “Приемная комиссия”, “Приказы”, “Система тестирования обучающихся”, “Учебные планы и расписание”, “Электронный кондуит”, “Система отчетов вуза” (рис. 3).

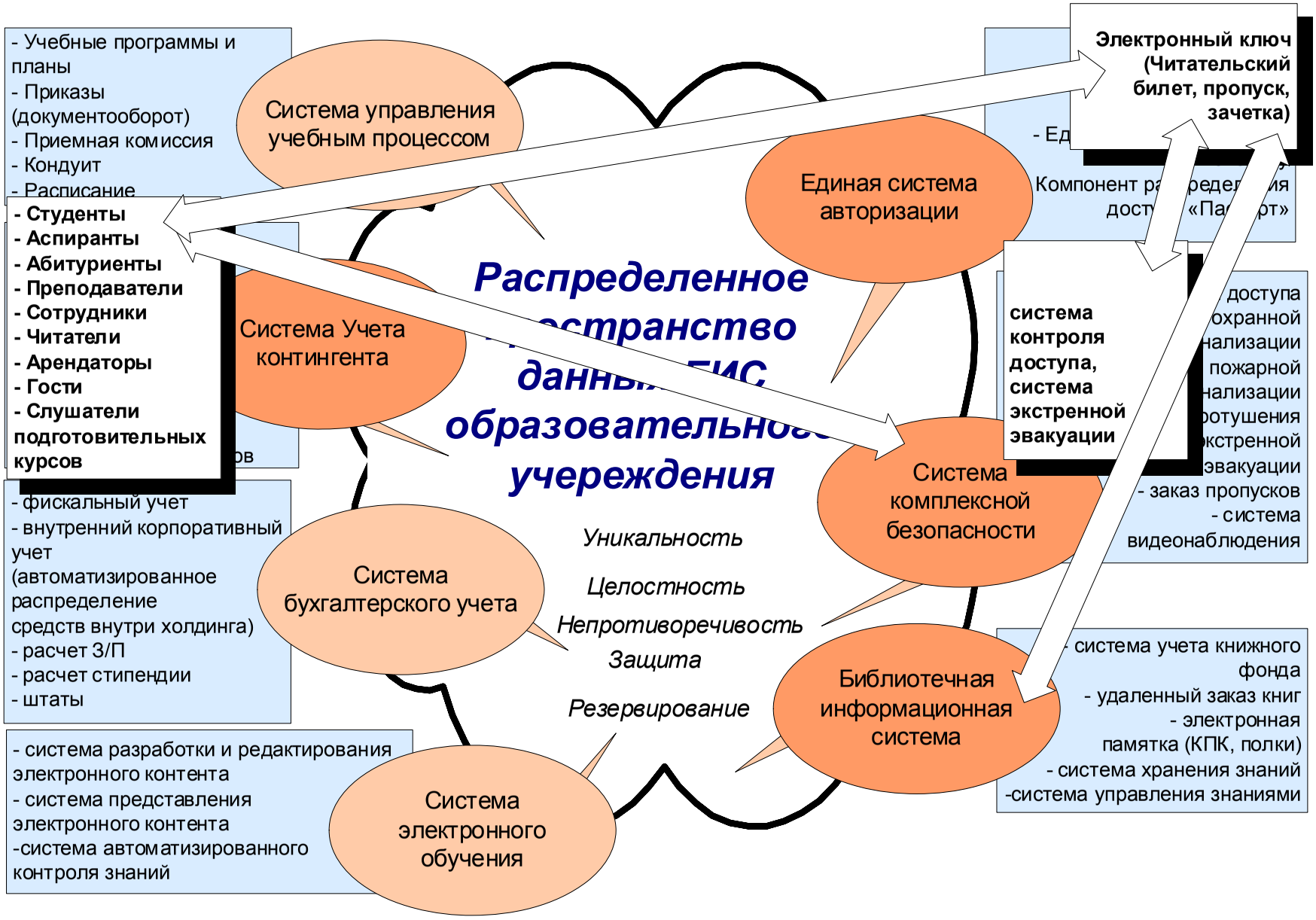

Рис.3 Информационные потоки данных о контингенте для системы комплексной безопасности

Из всех приложений пользователь использует единый логин/пароль доступа к данным.

3. Функциональные возможности СКОБО

Область применения комплекса благодаря многофункциональности и универсализации реализованных решений обширна. На базе интегрированных элементов СКОБО могут быть спроектированы и инсталлированы системы инженерного обеспечения зданий, СКБ предприятия, компоненты обеспечения производственного, управленческого процессов, прикладные модули сервисных функций. Примененные стандартные интерфейсы и широкие возможности оперативного модифицирования снимают ограничения на выбор конечного оборудования и обеспечивают интеграцию практически с любыми известными на сегодня системами.

3.1. Аппаратно-программные компоненты системы

Все функциональные решения формируются на базе модулей выполняющих конкретный унитарный процесс.

3.2. Автоматизированная система контроля и управления доступом (СКУД) СКОБО

Согласно классификации, определяемой ГОСТ Р 51241–98 “Средства и системы контроля и управления доступом”, СКУД СКОБО можно определить как универсальную, сетевую со смешанной архитектурой управления систему.

СКУД СКОБО предназначена для управления доступом на территорию и в служебные помещения университета. Каждый учащийся, преподаватель, сотрудник учебного заведения получает идентификатор (электронный ключ) — пластиковую карточку с содержащимся в ней индивидуальным кодом. Электронные ключи выдаются в результате регистрации перечисленных лиц с помощью средств подсистемы “Бюро пропусков”. Паспортные данные, фото (видеоизображение) и другие сведения о владельце электронного ключа заносятся в персональную электронную карточку. Персональная электронная карточка владельца и код его

электронного ключа связываются друг с другом и заносятся в специально организованную БД.

Система способна переходить в режим автономной работы при возникновении отказов управляющих компьютеров, сетевого оборудования или обрыве связи. СКОБО относится к классу крупных систем: максимальное количество управляемых и сенсорных устройств не ограничено.

СКУД СКОБО организуется за счет элементов следующих подсистем:

— автоматизированная проходная

— подсистема контроля въезда/выезда с территории

— подсистема контроля въезда/выезда с парковочной площадки

— подсистемы контроля доступа в служебные помещения

— подсистемы контроля доступа через эвакуационные выходы

— подсистемы контроля доступа в специализированные аудитории общего пользования

— подсистема бюро пропусков.

3.2.1. Автоматизированная проходная

У входа в здание или на проходной устанавливаются устройства, считывающие с карточек их код и информацию о правах доступа владельца карты и передающие эту информацию в контроллер системы.

В системе каждому коду поставлена в соответствие информация о правах владельца карточки. На основе сопоставления этой информации и ситуации, при которой была предъявлена карточка, система принимает решение: контроллер открывает или блокирует турникеты (рис. 4).

Все факты предъявления карточек и связанные с ними действия (проходы, тревоги и т.д.) фиксируются в контроллере и сохраняются в компьютере. Информация о событиях, вызванных предъявлением карточек, может быть использована в дальнейшем для получения отчетов по учету рабочего времени, нарушениям трудовой дисциплины и др. Как дополнительная мера защиты от несанкционированного прохода в СКУД СКОБО применяется фотоидентификация (вывод на экран монитора фотографии владельца идентификатора (рис. 5).

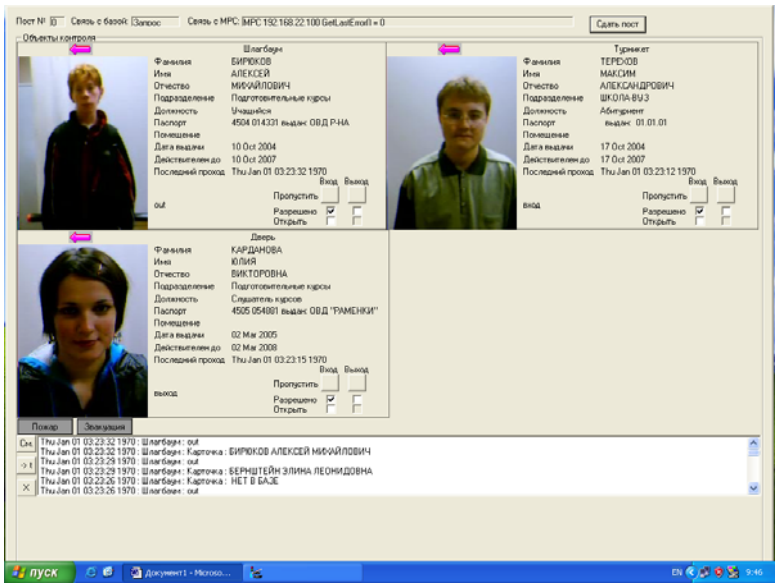

Рис. 5. Окно АРМ автоматизированной проходной СКОБО

При наличии очень большого количества людей, проходящих через проходную, актуально разделять потоки идущих “на вход” и “на выход”. В контексте данной задачи рассматриваются проходные, состоящие из двух, трех и четырех турникетов. В первом случае один турникет устанавливается “на вход”, а другой — “на выход”. Второй случай добавляет третий (средний) турникет, которой работает в обе стороны. Третий случай подразумевает работу одной пары турникетов “на вход”, другой пары — “на выход”. В случае чрезвычайных ситуаций, все турникеты автоматически открываются в одну (например, “на выход”) или в обе стороны.

За работой турникетов следят сотрудники службы безопасности. Для этого в помещении проходной установлено АРМ “Контроль проходов”, при помощи которого охранник может видеть как изображение проходящего, взятого с usb-камеры, установленной на турникете, так и изображение из БД контроллера с информацией о персоне (Ф.И.О., паспортные данные, статус). Таким образом, можно организовать полноценный контроль прохода персон через проходную.

3.2.2. Подсистема контроля въезда/выезда с территории

Если двор в вуз огорожен и въезд на него ограничен, то средством этого ограничения обычно служат автоматические ворота. Ворота открываются по специальным разрешениям сотрудником службы безопасности или автоматически при поднесении электронного ключа к считывателю. Для контроля прохода персон во двор рядом с воротами может располагаться калитка (рис. 6) или уличный полноростовый турникет, оборудованный считывателями электронных ключей “на вход” и(или) “на выход”. Наблюдение за проходами через калитку (турникет) может осуществляться при помощи АРМ “Контроль въезда”. Калитка (турникет) и ворота автоматически открываются по сигналу общей эвакуации.

Рис. 6. Калитка и автоматические ворота

3.2.3. Подсистема контроля въезда/выезда с парковочной площадки

СКОБО поддерживает автоматизацию регулирования въезда на парковочную площадку вуза, которая может располагаться на прилегающей территории или внутри основной. Автоматизация регулирования въезда осуществляется посредством шлагбаумов и считывателей электронных ключей (рис. 7). При поднесении электронного ключа к считывателю шлагбаум открывается, после проезда транспортного средства закрывается. Все факты предъявления карточек на въезде и непосредственно въезды на территорию фиксируются в контроллере и сохраняются в компьютере.

Рис. 7.

При большом количестве транспортных средств, размещаемых на стоянке, имеет смысл разделить потоки и установить один шлагбаум “на въезд”, а другой — “на выезд”. При небольших размерах стоянки можно обойтись одним шлагбаумом, осуществляющим контроль проезда в обе стороны. В случае чрезвычайных ситуаций шлагбаум открывается. В случае с двумя шлагбаумами возможен режим, когда оба или один из двух работает в обе стороны.

За работой шлагбаумов следят сотрудники службы безопасности. Как и на проходной, при попытке въезда или выезда на АРМ “Контроль въезда” появляется

полная информация о проезжающей персоне с номером, зарегистрированного на нее транспортного средства.

3.2.4. Подсистемы контроля доступа в служебные помещения и через эвакуационные выходы

Дверь оборудуется двумя считывателями карт доступа, автоматическим замком, датчиком положения (открыто/закрыто) и доводчиком. Такие двери необходимы для контроля доступа в специализированные помещения, например на лестничные пролеты, в малоиспользуемые коридоры, куда имеет доступ ограниченный контингент. При необходимости наблюдения за проходами дверь может контролироваться при помощи АРМ “Контроль проходов”. На время чрезвычайных ситуаций, в зависимости от плана эвакуации, все или некоторое количество дверей разблокируется, освобождая дополнительные пути для выхода из здания.

3.2.5. Подсистемы контроля доступа в специализированные аудитории общего пользования

Для вузов нередка ситуация, когда одна и та же аудитория используется для занятий преподавателями разных кафедр и факультетов. При этом ответственность за сохранность мебели, оборудования, реквизита аудитории распределяется между несколькими персонами. По тем или иным причинам использование обычных ключей может привести к ситуации, когда ответственного за воровство или порчу имущества не удается выявить. Во избежание подобных ситуаций вход в аудиторию может быть оснащен средствами контроля разрешения доступа в аудиторию. Рассмотрим следующий пример. Преподаватель при помощи своей карты доступа разблокирует дверь, и система с этого момента считает его ответственным за сохранность имущества, так как дверь во время занятий должна быть разблокирована. После окончания занятий дверь блокируется преподавателем при помощи той же карты доступа, а контроль за ней переходит к службе безопасности до начала следующих занятий.

Круг лиц, имеющих право на блокировку, ограничен временем расписания занятий и правом ведения занятий конкретным преподавателем в конкретной

аудитории. Для предотвращения нештатных ситуаций система оснащена кнопкой внутри помещения, сигнализация с которой выведена на пост охраны, чтобы сотрудник службы безопасности смог освободить случайно забытого посетителя. Такой способ охраны может использоваться и для других помещений.

3.2.6. Подсистема бюро пропусков

Данная подсистема выполняет следующие функции:

— поиск персоны в БД

— определение типа пропуска, предназначенного для данной персоны (временный, социальная карта, штатный пропуск)

— считывание уникального кода электронного ключа с последующим сохранением в БД

— определение зон доступа согласно статусу персоны (определяются заранее в БД в момент занесения персоны в БД структурой, ответственной за персону)

— фотографирование персоны с последующим сохранением фото в БД

— фиксация должности и подразделения, к которому относится персона пропуска (определяются заранее в БД в момент занесения персоны в БД структурой, ответственной за персону)

— фиксация срока начала и окончания действия (определяется заранее в БД в момент занесения персоны в БД структурой, ответственной за персону)

— печать на носителе электронного ключа фотографии и персональных данных

— сохранение данных о карте и персоне в контроллерах доступа и управления.

3.2.7. Система охранной сигнализации

Предназначена для автоматизации охраны помещений службой безопасности путем отображения состояния охранного шлейфа помещения на мониторе сотрудника безопасности, постановки и снятия помещений с охраны.

3.2.8. Охрана помещения при помощи охранного шлейфа

Это самый простой способ охраны помещения. Комната оборудуется датчиком открытия дверей, окон и в некоторых случаях датчиком объема, подключенными к одному из шлейфов охранной сигнализации. После окончания рабочего дня

помещение закрывается и ставится на охрану при помощи АРМ “Пост охраны”. В случае срабатывания одного из датчиков в помещении АРМ сигнализирует сотруднику службы безопасности о тревожности шлейфа. В начале следующего рабочего дня помещение снимается с охраны. Возможна так же адресная постановка на охрану. Для этого перед помещением монтируется считыватель электронного ключа и постановка/снятие с охраны выполняются при помощи электронного ключа лицами, имеющими на это санкцию, а событие постановки/снятия с охраны автоматически фиксируется в электронном журнале СКОБО и отображается на мониторе сотрудника службы безопасности (рис. 8.).

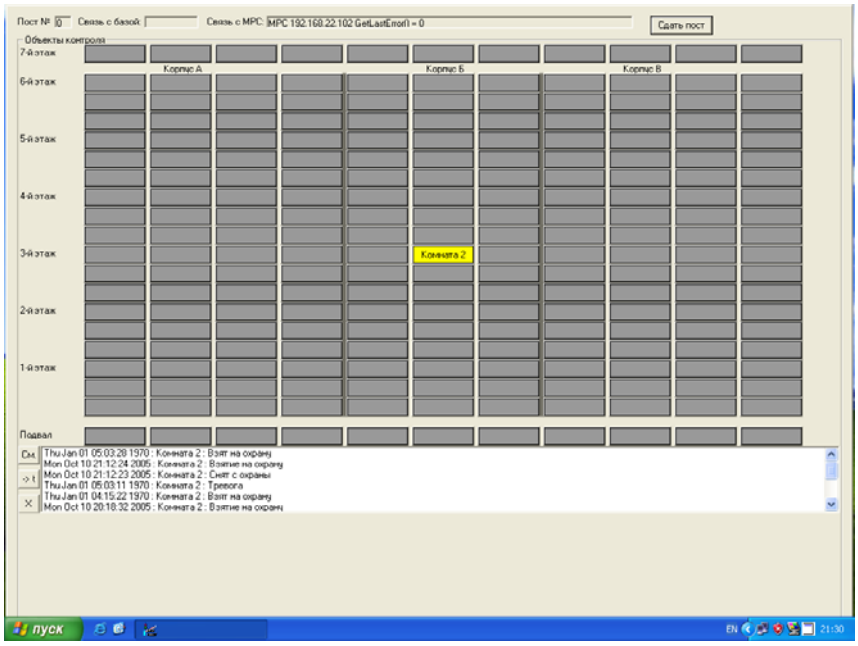

Рис. 8. Окно АРМ системы охраны (демонстрационный режим)

3.2.9. Охрана помещения при помощи телефонной линии

Этот способ охраны помещений отличается от предыдущего организацией охранного шлейфа. Чтобы отказаться от лишней протяжки проводов, можно использовать проводные мощности телефонной сети учреждения. В течение дня телефонная линия используется по своему предназначению, но когда сотрудник уходит с работы, он может перевести линию в режим охраны. При помощи тумблера, расположенного в помещении, специализированное оборудование отключит линию

от АТС и через несколько минут автоматически поставит помещение на охрану. Помещение снимается с охраны в начале следующего рабочего дня.

3.3. Модуль противопожарной безопасности СКОБО

3.3.1. Пожарная сигнализация

В общем случае система пожарной сигнализации отличается от охранной конечным оборудованием. Вместо датчиков на открытие и изменение объема устанавливаются датчики, чувствительные к дыму. Состояние пожарных шлейфов отслеживается на специализированном АРМ “Пожарная сигнализация” (рис. 9).

В некоторых случаях возможна интеграция с уже установленной системой пожарной сигнализации. Существует готовое решение интеграции комплекса СКОБО с системой “Сигнал” производства компании “Болид”. При этом состояние пожарных шлейфов отражается на АРМ “Пожарная сигнализация и управление пожаротушением” СКОБО.

3.3.2. Адресная система включения повысительных пожарных насосов (АСВППН)

Позволяет автоматически включать противопожарные насосы по сигналам пожарной сигнализации, а также отслеживать давление в водопроводной сети и поддерживать его на необходимом уровне. АСВППН можно привести в действие нажатием адресного пускателя, расположенного непосредственно рядом с гидрантом. Включение АСВППН автоматически логгируется и на терминале наблюдения появляется информация о том, с какой группы пожарных датчиков или ручного пускателя пришел сигнал о включении повысительных насосов (см. рис. 9.).

Возможен режим задержки включения пожарных насосов, во время которого сотрудники службы безопасности, проанализировав ситуацию при помощи видеонаблюдения или воочию, могут блокировать запуск АСВППН.

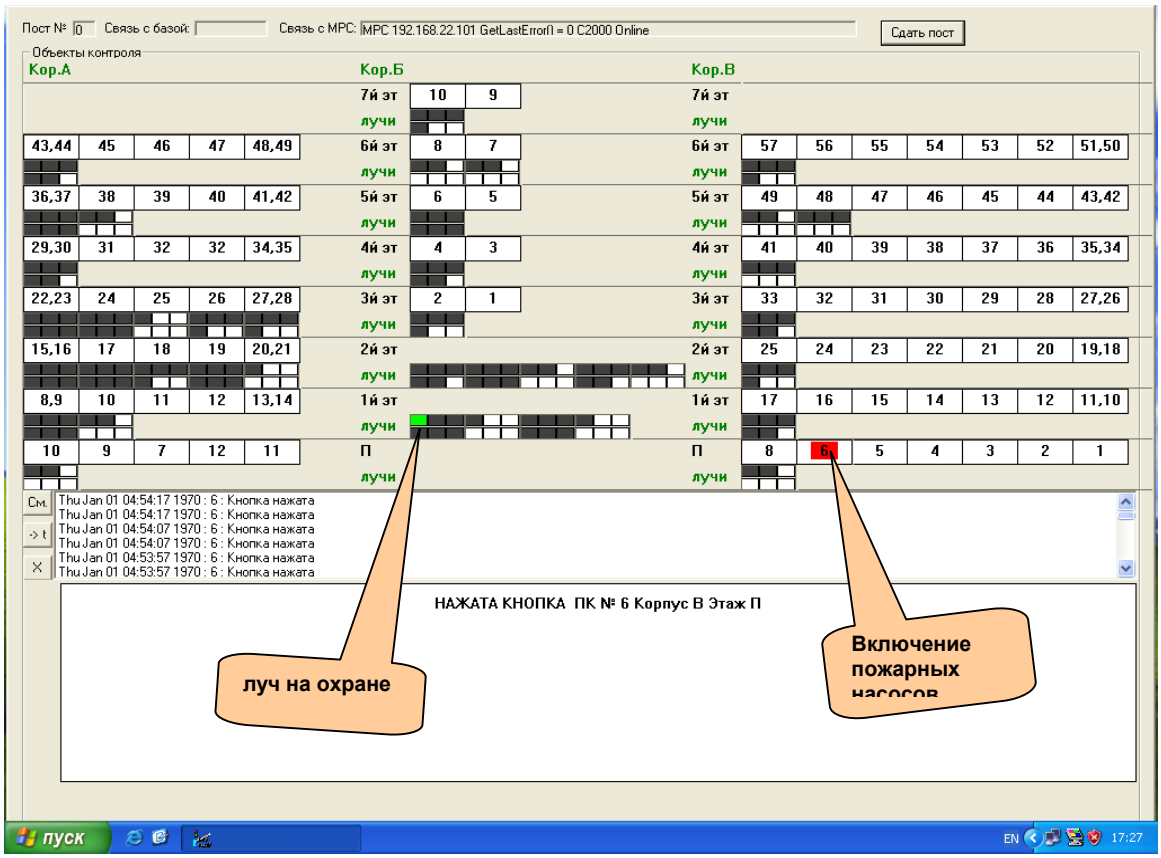

Рис. 9. Визуализация срабатывания системы запуска повысительных насосов на АРМ пожарной сигнализации

3.4. Компоненты информационной системы вуза, используемые в СКОБО

СКОБО работает с данными, формируемыми единой информационной системой вуза. В частности, списочный состав контингента посетителей формируется компонентами автоматизации приемной комиссии, деканата, отдела имущественных отношений, службой подготовительного отделения и др.

3.5. Система видеонаблюдения

Интегрированная система видеонаблюдения является одной из важнейших составляющих СКБ, причем максимальный эффект от использования этой системы достигается в том случае, если события от охранной системы, системы пожарной сигнализации и системы контроля доступа влияют на поведение видеокамер и мониторов визуализации видео. Например, в случае срабатывания шлейфа или несанкционированного доступа на мониторе происходит акцентирование внимание наблюдающего путем звукового сигнала и увеличения размеров наблюдаемой

области, а запись видео начинает производиться с максимальным качеством изображения.

3.6. Система экстренного оповещения и экстренной эвакуации

Система звукового оповещения основана на эффективном управлении сетью громкоговорителей, подключенных к аналоговой шине усилителя мощности (рис. 10).

Рис.10. Система оповещения и управления экстренной эвакуацией

Система позволяет осуществлять следующие функции:

— управление громкоговорителями по зонам

— транслирование разных сообщений в различные зоны

— управление громкостью громкоговорителей в отдельных зонах

— интеграция с противопожарной подсистемой, транслирование сообщений с учетом плана эвакуации и места возгорания

— управление вторичными часовыми механизмами

— управление звонковой сигнализацией начала и окончания занятий

— транслирование информационно-развлекательных блоков в зонах максимального скопления учащихся во время перемен (холлы, буфеты и т. д.).

В качестве управляющего распределенного механизма используются контроллеры МАТИ МПК-3, расположенные в здании. Монтаж системы возможен с использованием существующего аудиооборудования и коммуникаций.

Концепция единой системы СКОБО определяет однозначное взаимодействие собственных компонентов, что позволяет более эффективно решать возложенные на нее задачи.

Комплексная безопасность подразумевает соблюдение и выполнение норм антитеррористической, криминогенной, пожарной, техногенной безопасности. Поскольку эти нормы разрабатываются различными ведомствами, иногда они не стыкуются друг с другом. Например,: нормы криминальной безопасности требуют жесткого ограничения доступа в неиспользуемые помещения и на лестничные пролеты, а режим эвакуации предполагает максимально возможное количество путей выхода из здания. Единая система безопасности вуза, реализующая комплексный подход, позволяет наиболее гибко разрешать подобные проблемы.

Предлагаемый комплекс уже более 5 лет обеспечивает комплексную безопасность в “МАТИ” — Российском государственном технологическом университете им. К.Э.Циолковского.