ИНТЕГРИРОВАННАЯ СИСТЕМА КОНТРОЛЯ ДОСТУПА И ЗАЩИТЫ ИНФОРМАЦИИ

на основе биометрической аутентификации сотрудников

Д.Счастный, С.Конявская, ОКБ САПР

Интеграция систем контроля доступа и защиты информации способна существенно повысить как уровень защищенности системы, так и комфорт ее эксплуатации. Сценарии работы таких объединенных систем могут быть почти бесконечно разнообразны и учитывать самые прихотливые правила и особенности регламентов работы на предприятии. В этой статье обобщены предпосылки, которые необходимо иметь в виду при постановке задачи такой интеграции.

Системы защиты постоянно развиваются, это можно наблюдать во всех областях и сегментах этого обширного и разнообразного рынка. Развивается все: средства идентификации, системы видеонаблюдения, системы контроля и управления доступом (СКУД), системы защиты информации от несанкционированного доступа (СЗИ НСД), системы криптографической защиты информации (СКЗИ). Анализ тенденций развития средств защиты выявляет два основных направления развития: совершенствование и расширение собственных возможностей и интеграция со смежными системами безопасности. Так, в системах видеонаблюдения улучшается качество передаваемого сигнала, в СКЗИ разрабатываются и внедряются новые алгоритмы. А с другой стороны, системы видеонаблюдения объединяются со СКУД, криптография применяется в СЗИ НСД.

Но наблюдаемая интеграция пока касается только смежных систем безопасности: видеонаблюдения и СКУД, СЗИ НСД и криптографии. Примеры интеграции технических средств безопасности (ТСБ) и средств защиты информации

(СЗИ) практически отсутствуют. Можно видеть случаи механического объединения таких систем: например, в СКУД применяются СЗИ НСД, а при передаче данных от видеокамер используются VPN-решения. Однако во всех этих случаях взаимопроникновения систем не происходит: каждая из систем функционирует независимо от других, и данные одной системы в общем случае не влияют на принятие решений при функционировании другой. Причина такой ситуации не только в технологической сложности интеграции, но и в отсутствии спроса со стороны заказчиков, ведь автономность этих систем привычна и воспринимается как должное.

Зачастую первым импульсом к внедрению новых технологических решений является отнюдь не спрос, а предложение, ведь разработчикам в силу большей информированности может быть виднее, какие нераскрытые до сих пор ресурсы содержатся в тех или иных технологиях. Для разработчиков ТСБ информационные технологии являются вспомогательным инструментом, обязанным правильно обеспечить функционирование шлюзовых кабин, систем пожаротушения и видеокамер, а разработчики СЗИ уверены, что созданные ими продукты достаточно универсальны, чтобы применяться везде – нужно только их правильно настроить.

Одним из перспективных направлений интеграции является взаимоувязывание СКУД и СЗИ НСД. С одной стороны, эти системы максимально отдалены друг от друга: СКУД оперирует большими физическими сущностями (двери, турникеты, шлюзовые кабины), а СЗИ НСД работает с программами, томами, файлами, каталогами, записями, полями записей. Но, с другой стороны, все эти сущности связаны с людьми (сотрудниками, пользователями), и в конечном итоге они должны обеспечить комфортное и безопасное выполнение пользователями функциональных обязанностей на рабочих местах. Кроме того, и СЗИ НСД, и СКУД в принципе управляют *доступом*, что позволяет надеяться на выделение общих сущностей в системах и взаимодополнение в результате интеграции.

Рассмотрим принципиальные моменты функционирования типовых СКУД и типовых СЗИ НСД и выделим общие черты у обеих систем.

Во-первых, как уже упоминалось выше, каждая из систем управляет доступом

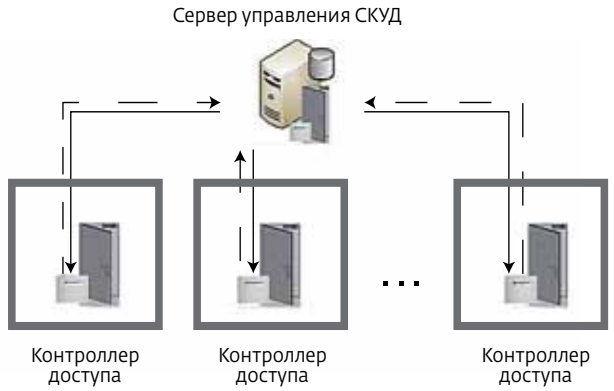

Рис.1. Типовая схема сетевой СКУД

пользователей к некоторым ресурсам. СКУД контролирует физический доступ пользователей в помещения к материальным ресурсам, СЗИ НСД контролирует доступ к информационным ресурсам: дискам, каталогам, файлам. Инструментом контроля является некий обобщенный *замок* – контроллер СКУД, установленный на дверях, или турникет, или шлюзовая кабина в СКУД, или аппаратный модуль доверенной загрузки, установленный в ПЭВМ, – тоже замок, но электронный. Пользователи получают доступ к необходимым ресурсам после успешной процедуры идентификации/аутентификации, предъявив аппаратный идентификатор – RFID-карту, смарт-карту, контактный ключ, TM-идентификатор), токен – и подтвердив легальность обладания этим идентификатором, обычно паролем, PIN-кодом, но, возможно, и с помощью других методов аутентификации.

Во-вторых, каждая из систем имеет некоторую внутреннюю логику работы и некоторый регламент доступа. В общем случае легальный пользователь может получить доступ к ресурсам при условии выполнения некоторых правил разграничения доступа: он может находиться в строго определенных помещениях и в строго определенное время, или не может находиться в двух помещениях одновременно ("антипасбэк" – англ. anti passback), или он может запускать строго определенные программы, или читать файлы из одного каталога, а удалять из другого. Эти правила работы хранятся в базе данных системы и применяются во время ее работы.

В-третьих, архитектурно и СКУД, и СЗИ НСД могут быть как автономными, так и сетевыми. Контроллеры СКУД и программно-аппаратные комплексы (ПАК) СЗИ НСД могут функционировать локально и быть самодостаточными (контролировать доступ к локальным ресурсам на основании правил, хранящихся непосредственно в локальной базе данных) или работать во взаимодействии с некоторой единой (централизованной или распределенной) базой данных – обмениваться данными с другими аналогичными элементами системы или подчиняться воздействиям с некоторого сервера управления.

Все это убедительно доказывает, что СКУД и СЗИ НСД имеют много общего, и позволяет наметить следующие пути интеграции:

- *объединение идентификаторов* представляется наиболее простым и очевидным путем интеграции систем. Один и тот же идентификатор регистрируется в обеих системах и используется штатным образом в каждой из них. Системы связываются между собой через общий элемент – пользователя, что позволяет унифицировать управление пользователями в различных системах. Кроме того, такое объединение позволяет минимизировать число применяемых идентификаторов;
- *объединение объектов доступа* может происходить путем логического взаимоувязывания помещений и компьютеров. Это позволит создать новые правила доступа как к ПЭВМ, так и в помещения, что в целом повысит безопасность каждой из систем. Например, доступ к ПЭВМ будет происходить только в том случае, если пользователь прошел в помещение, в котором установлено это средство вычислительной техники. С другой стороны, при выходе из помещения контроллер СКУД откроет замок на двери только в том случае, если пользователь заблокировал доступ к компьютеру, включив скринсейвер, или выключил компьютер;
- *объединение баз данных* может происходить двумя способами: либо будут модифицированы исходные схемы баз данных добавлением атрибутов из смежной системы и в итоге будет создана единая база данных, либо будет создана третья база данных, которая будет синхронизировать данные из неизменных баз данных каждой из систем. Объединение баз данных

позволит централизовано и единообразно управлять параметрами доступа в каждую из систем;

- *объединение технологий взаимодействия* может происходить путем взаимодействия серверов через сеть по некоторому протоколу для сетевых систем или путем передачи управляющих сигналов через идентификатор для автономных систем. Управляющие воздействия могут записываться в идентификатор в одной системе и считываться в другой системе. Например, в идентификаторе можно зафиксировать факт и время прохода в помещение через контроллер СКУД, а при идентификации в СЗИ НСД считать эти данные и принять решение о старте компьютера. Это объединение позволит оперативно реагировать на инциденты безопасности в смежной системе и предотвращать возможные случаи несанкционированного доступа.

При этом важно помнить, что общим субъектом в обеих системах является человек – сотрудник организации-владельца системы.

Итак, интеграция СКУД и СЗИ НСД возможна. Причем она может осуществляться разными способами и основываться на разных принципах. В качестве примера рассмотрим вариант интеграции сетевых СКУД и СЗИ НСД.

Типовую сетевую СКУД (рис.1) можно описать следующим образом: на местах входа в помещение установлены контроллеры СКУД, которые взаимодействуют со считывателями, управляют замками и в соответствии с собственной базой данных принимают решение об открытии замка на основании предъявленного идентификатора и правил разграничения доступа в помещение. Управление контроллерами осуществляется удаленно с сервера СКУД, который, в свою очередь, выполняет следующие функции:

- сбор событий с подконтрольных контроллеров СКУД и ведение архива событий;
- ведение базы данных пользователей, идентификаторов, правил разграничения доступа в помещения;
- собственно управление контроллерами.

Типовая сетевая СЗИ НСД (рис.2) выглядит следующим образом: на подконтрольных компьютерах установлен модуль доверенной загрузки, который на основании предъявленных идентификатора и аутентифицирующих данных и в соответствии с правилами, описанными в собственной базе данных, принимает решение о старте компьютера. Далее в ОС запускается программная часть СЗИ НСД, которая осуществляет разграничение доступа пользователя к информационным ресурсам. Программная часть СЗИ НСД осуществляет и взаимодействие с сервером управления, который выполняет следующие функции:

- сбор событий с подконтрольных объектов;
- ведение архива событий;
- ведение базы данных пользователей, идентификаторов, правил разграничения доступа к информационным ресурсам;
- собственно управление СЗИ НСД на подконтрольных объектах.

Рассмотрим варианты интеграции этих систем по каждому из направлений. При объединении идентификаторов необходимо остановить свой выбор либо на идентификаторах СКУД, либо на идентификаторах СЗИ НСД. Вероятность того, что в обеих системах используются одни и те же идентификаторы, стремится к нулю, поэтому в объединенной системе необходимо выбрать идентификатор одной из систем в качестве основного (и единственного) и адаптировать другую систему к работе с этим типом идентификаторов. Или выбрать третий тип идентификатора, если для выполнения каких-то новых функций объединенной системы свойства имеющихся идентификаторов не оптимальны.

Например, допустим, объединенную систему предполагается расширить биометрической идентификацией пользователя при доступе к автоматизированному рабочему месту (АРМ). В этом случае ввод пароля с клавиатуры будет

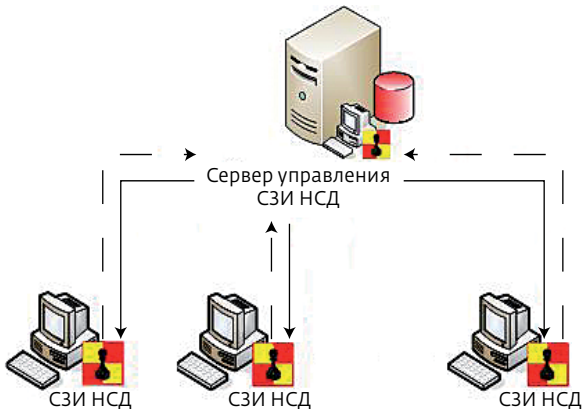

Рис.2. Типовая схема сетевой СЗИ НСД

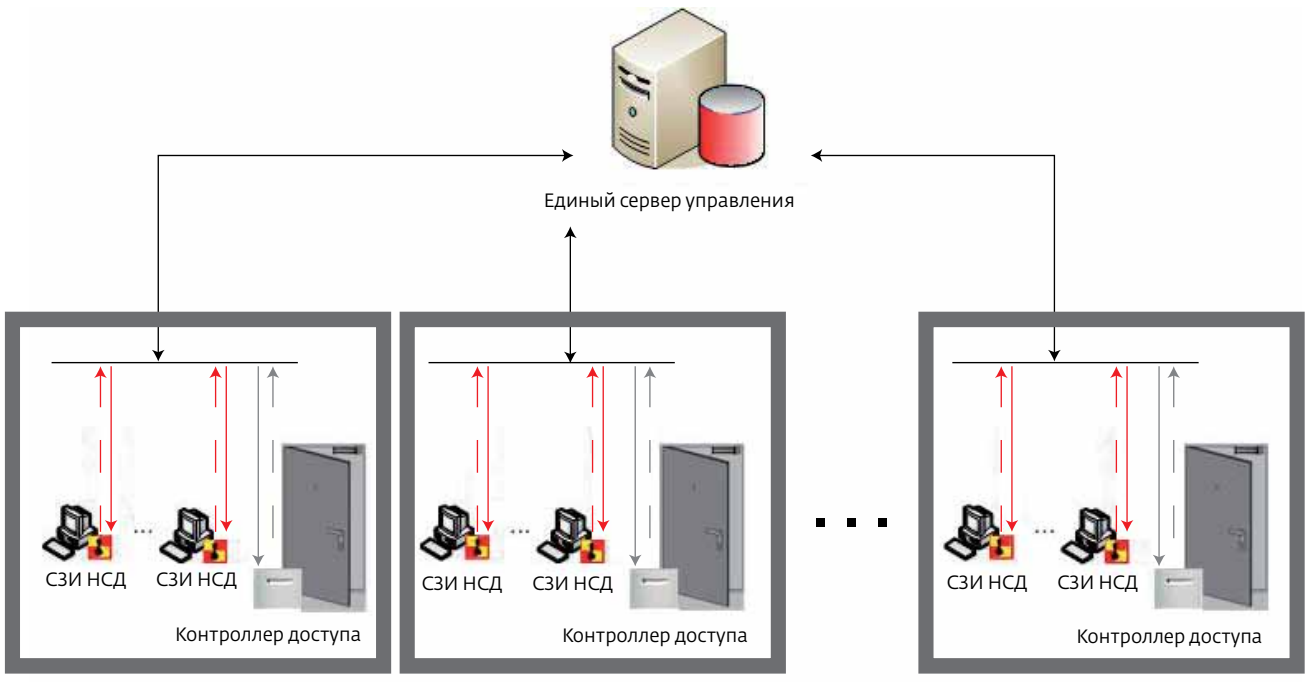

Рис.3. Единая система с общей базой данных

заменяться на предъявление биометрического признака (например, кисти руки для сканирования сосудистого русла ладони). Это позволит избежать инцидентов, связанных с забыванием паролей, что снизит нагрузку на администратора и повысит комфортность работы пользователя.

Понятно, что эталон биометрического признака, по предъявлению которого будет аутентифицироваться пользователь, нерационально хранить в базе данных, так как база биометрических данных – это информационная система персональных данных (ИСПДн), сама нуждающаяся в защите. Значит, эталон своих биометрических данных сотрудник должен носить с собой в защищенном контейнере. Роль такого контейнера прекрасно выполнит токен, смарт-карта или ТМ-идентификатор.

При использовании в СКУД радиокарт, а в СЗИ НСД – ТМ-идентификаторов очевидно, что заменить радиокарту на ТМ-идентификатор не получится. То есть при прочих равных интеграция на уровне идентификаторов вылилась бы в поддержку радиокарт в СЗИ НСД.

Однако не всякая радиокарта допускает возможность применения в качестве хранилища произвольных данных (в нашем случае – эталона снимка сосудистого русла). В этом случае необходимо будет выбрать другой идентификатор и адаптировать к его применению обе системы.

Заметим, что расширить биометрической аутентификацией можно обе подсистемы – не только СЗИ, но и СКУД, – чтобы пользователь для входа в помещение также предъявлял и карту, и руку. Это позволит гарантированно исключить передачу карты "по дружбе", чтобы, допустим, используя карту коллеги, выйти из комнаты, не блокируя свое АРМ.

Интеграция объектов доступа потребует модификации логики работы каждой из систем как с помощью расширения атрибутов баз данных (необходимо добавить атрибуты помещений и компьютеров в соответствующие базы данных), так и путем модификации правил разграничения доступа (необходимо добавить правила работы с новыми атрибутами и взаимоувязать их с существующими правилами).

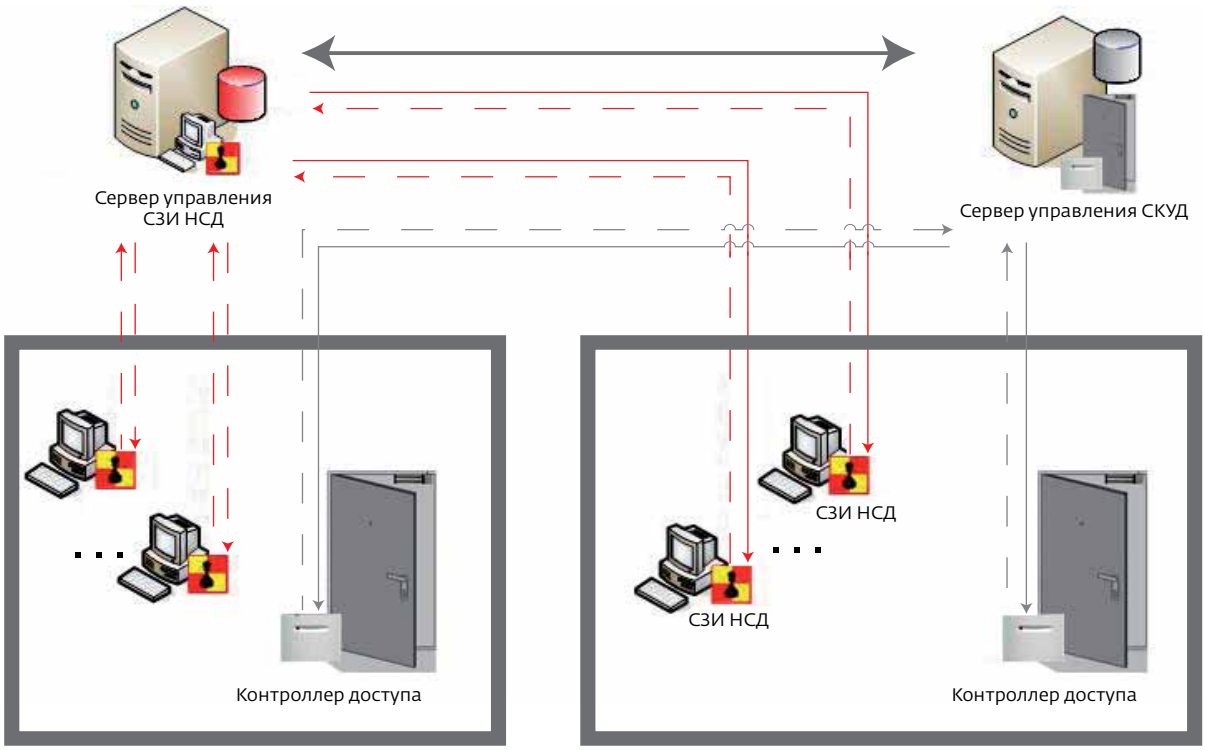

Рис.4. Равноправное взаимодействие серверов СКУД и СЗИ НСД

Объединение баз данных (рис.3) может происходить либо путем создания общей базы данных с записями, либо путем расширения каждой из баз набором дополнительных атрибутов. Объединение функций серверов в одном программном продукте – самый трудоемкий и самый непредсказуемый вариант в части получения конечного результата.

При общей схожести рассматриваемых систем защиты они все-таки очень различаются в деталях. В первую очередь это касается протоколов взаимодействия серверов и оконечного оборудования. Мало того, что эти протоколы отличаются по своей реализации (стандартом взаимодействия контроллеров с сервером СКУД является протокол EIA-485 (RS-485), а компоненты СЗИ НСД чаще всего взаимодействуют через ЛВС на Ethernet) и протоколы взаимодействия часто являются проприетарными и закрытыми, так еще и со стороны регулирующих органов к ним предъявляются различные требования. Кроме того, понятия и атрибуты, которыми оперирует каждая из систем, настолько различны, что процесс изучения разработчиком смежной предметной области может растянуться на значительное время. Еще одним из недостатков этого решения является уникальность разработки – интеграция с другой аналогичной системой будет являться новой работой практически без возможности использования наработок. Уникальность разработки также затруднит и дальнейшее развитие системы: развитие и обновление каждого из продуктов будут требовать внесения изменений и в объединенный вариант. Но в случае правильной реализации этого варианта степень интеграции будет максимальной, что позволит, во-первых, единообразно управлять обеими системами, во-вторых, более тонко осуществлять взаимодействие систем.

Вариант выработки *технологии взаимодействия серверов между собой* позволяет сохранить принципиальную независимость систем. Детали реализации взаимодействия сервера и оконечного оборудования неважны для разработчиков смежной подсистемы, каждая система может развиваться и обновляться самостоятельно и независимо от смежной системы.

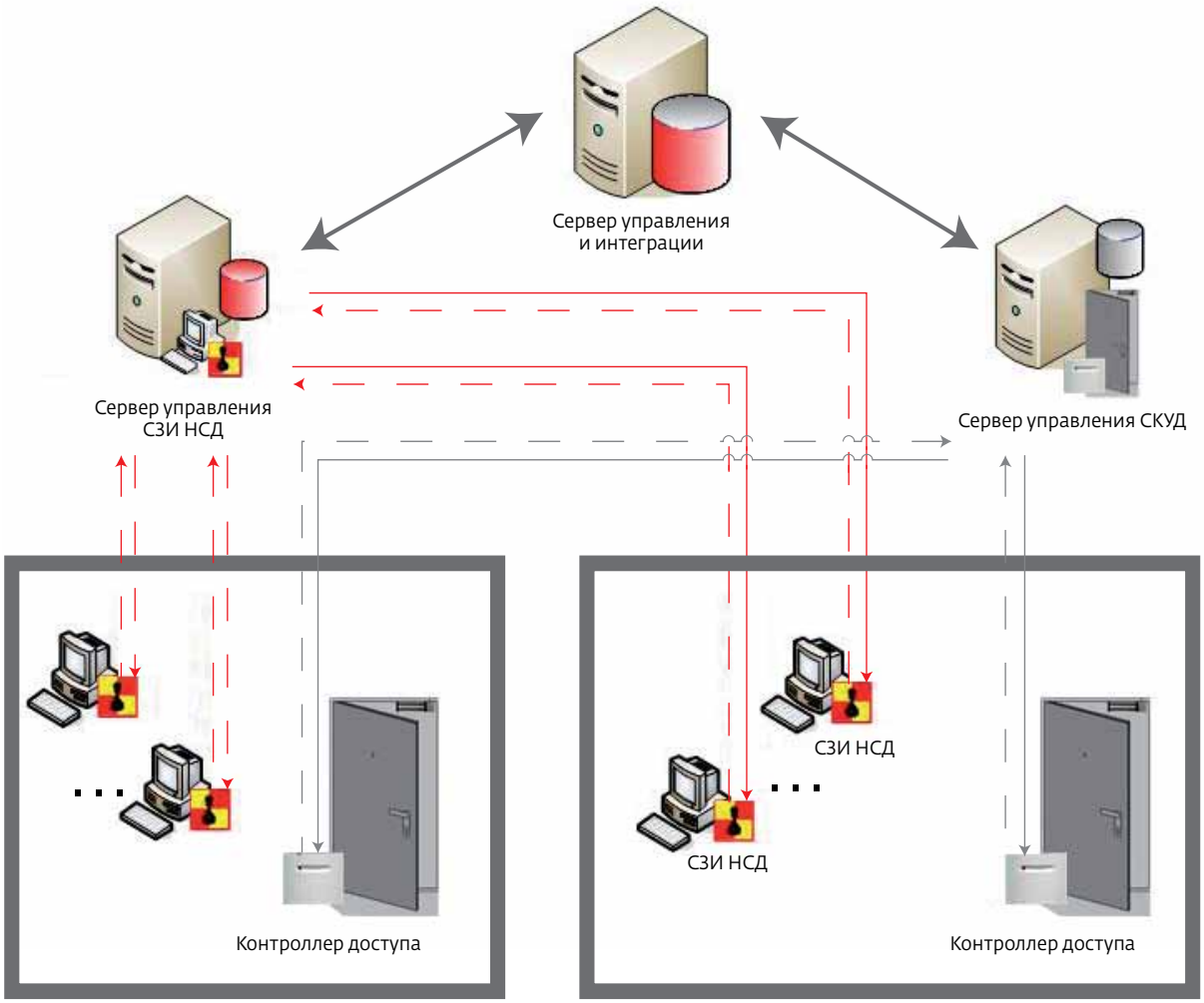

Рис.5. Соподчинение серверов СКУД и СЗИ НСД

Взаимодействие серверов (так как мы рассматриваем вариант взаимодействия сетевых систем) может происходить в трех вариантах.

- подчиненное взаимодействие серверов;
- равноправное взаимодействие серверов (рис.4);
- взаимодействие серверов с третьим управляющим сервером (рис.5).

Каждый вариант имеет свои преимущества и недостатки.

Первые два варианта взаимодействия серверов между собой напрямую требуют разработки, согласования и реализации протокола взаимодействия серверов по синхронизации баз данных (в части выделенных общих частей) и протокола извещения систем о событиях, критичных для обеих систем. Кроме того, для управления каждой из систем используется собственный интерфейс управления, что увеличивает нагрузку на эксплуатирующий персонал по сравнению с первым вариантом.

Третий вариант структурной интеграции поз-волит в одном месте сосредоточить всю информацию о системе и обеспечит единый интерфейс управления системами. Но он потребует как разработки протокола взаимодействия серверов, аналогичного описанному выше, так и разработки отдельного продукта – этого самого третьего сервера. При этом детали работы каждой системы будут скрыты от разработчика, так что теоретически все три сервера могут разрабатываться разными исполнителями.

Сценарий развития событий при попытке сотрудника приступить к работе в начале дня в описываемой условной системе будет выглядеть примерно так.

1. Сотрудник прикладывает радиокарту и руку на КПП при входе на территорию предприятия.
2. На монитор компьютера охранника выводится фото сотрудника, ассоциированного с данной картой, и результаты верификации предъявленного сосудистого русла с эталоном из карты.
3. Охранник оценивает результат верификации и визуально сравнивает фото с сотрудником.
4. Сотрудник проходит на территорию предприятия.
5. Данные о том, что сотрудник успешно прошел, передаются управляющему элементу интегрированной системы контроля доступа для учета попытки сотрудника пройти в одно из помещений предприятия.
6. При необходимости возможно установить правила, регулирующие нормальное время между проходом на территорию и входом в помещение, установить нужную реакцию на нарушение этого времени.
7. При входе в помещение также производится идентификация по карте и аутентификация на основе биометрической верификации, после чего система контроля доступа ждет включения АРМ.
8. При включении АРМ запрашивается карта и рука, производятся контрольные процедуры, на основании которых загружается профиль пользователя, и последний может приступить к работе в рамках установленных для него правил разграничения доступа к информационным ресурсам системы.
9. Работа на АРМ производится при условии наличия карты в считывателе.
10. При съеме карты со считывателя для выхода из помещения АРМ блокируется, и разблокировка производится по повторному предъявлению карты и руки.

Дополнительно система может быть усложнена разными сценариями – работы с контролером или коллективной работы, сигнализации о различных событиях и многими другими.

В зависимости от выбранных путей и способов интеграции возможно получение различных решений с различными трудозатратами и разной степенью эффективности. Но то, что интегрировать СЗИ НСД и СКУД можно и нужно, – не вызывает сомнений.

Дальнейшее развитие интегрированного решения возможно в двух упомянутых в самом начале направлениях: совершенствование и расширение возможностей созданного решения и интеграция со смежными системами безопасности. Совершенствование и расширение возможностей может проходить как путем улучшения эргономических свойств и повышения быстродействия и надежности системы, так и путем расширения списка поддерживаемых идентификаторов, объектов доступа и правил разграничения доступа.

Следующим шагом интеграции со смежными системами безопасности видится интеграция с системами видеонаблюдения, когда наряду с контролем доступа в помещения и контролем доступа к информационным ресурсам будет осуществляться и визуальный контроль за происходящими событиями. Причем не только в помещениях, но и на экранах рабочих мест пользователей. Это заслуживает отдельной статьи. ■