Как правильно строить безопасные автоматизированные системы?

Валерий Андреев,
заместитель директора по науке
и развитию компании ИВК

АСЗИ=АС+СЗИ

Прежде чем отвечать на извечный российский вопрос №1 в отношении автоматизированных систем (АС) необходимо договориться о терминах и определениях. Благо для этого имеются все необходимые наработки, так или иначе отраженные в разнообразных документах — ГОСТах, нормативных актах, руководящих документах и пр.

Действительно, в общем случае АС представляет собой организационно-техническую структуру, предназначенную для поддержки принятия решений на основе автоматизации информационных процессов управления, производства и т.п. на инфокоммуникационной инфраструктуре заказчика. АС выполняет некоторую совокупность или последовательность прикладных или функциональных операций (задач, приложений, процедур и пр.) в автоматическом или автоматизированном режимах. Если процессы в системе не автоматизированы, то тогда об описываемой структуре говорят, как об информационной системе (ИС), если же автоматизация частично касается каких-то объектов структуры, то следует говорить об АИС, как об автоматизированной информационной системе.

Одной из отличительных черт таких систем является их изначальная разнородность. Это касается не столько очевидного функционирования объектов АС на разных программно-аппаратных платформах (разные версии операционных систем (ОС), разное компьютерное "железо", разные каналы связи и пр.), сколько одновременной работы различных прикладных задач, не имеющих возможности исчерпывающего взаимодействия друг с другом, например, в силу различной архитектуры, разных форматов представления данных и пр. Поэтому очевидным требованием к любой АС должен быть учет такой особенности как изначальная гетерогенность (неоднородность) системы, как аппаратная, так и программная.

Кроме того, к особенностям АС можно отнести высокую степень ее территориального "покрытия". Тогда существует необходимость объединения объектов автоматизации АС в единый информационный организм посредством указанной инфокоммуникационной составляющей АС.

Отвечая на основной вопрос, можно сказать, что создание АС всегда связано с нормативно-правовой базой, лежащей в основе любого проекта по созданию. Часто самым первым документом заказчика, определяющем пути создания или развития АС является Концепция информатизации (автоматизации) той организационно-штатной структуры, владельцем которой является заказчик. Она может быть создана как самим заказчиком, так и любой иной организацией, выигравшей соответствующий конкурс. На основании этого документа может быть написано подробное техническое задание (ТЗ), выполнение которого и является обязанностью системного или проектного интегратора. Таким образом, разработка и внедрение вновь создаваемой или модернизируемой АС производится в соответствии с ТЗ. ТЗ на АС является основным документом, определяющим требования, предъявляемые к АС в целом, порядок ее создания и приемку заказчика при вводе ее в эксплуатацию. Обычно дополнительно разрабатываются функциональные и прикладные ТЗ (или частные ТЗ — ЧТЗ) на составные части АС: на подсистемы АС, комплексы средств автоматизации (КСА) АС, комплексы задач (КЗ) АС и т.п. Порядок утверждения и согласования ТЗ на АС установлен в ГОСТ 34.602. Утверждение и согласование ТЗ на подсистемы АС также производится в соответствии с порядком, установленным ГОСТ 34.602.

Как видим, вопрос о "правильности" процесса создании АС достаточно изучен и даже стандартизирован. Обязательно следует отметить еще один немаловажный факт, являющийся определяющим в построении многих АС в РФ. Это существование в разных субъектах РФ, ведомствах, предприятиях и организациях вполне работоспособных решений, уже осуществленных заказчиком и стоивших ему немалых средств. Это то, что раньше называлось "лоскутной" (кусочной) информатизацией, а сегодня — "унаследованными" системами. Капитализация ранее осуществленных вложений заказчика при переходе от унаследованных разрозненных систем к построению единой АС сегодня предстает важной задачей практически любого потребителя ИТ-ресурсов. Именно поэтому стали появляться первые реализации неоднородных территориально-распределенных информационных систем органов управления особой значимости для страны, имеющих выраженную разветвленную структуру с объектами во всех субъектах Российской Федерации. Так как задача объединения, интеграции разрозненных информационных ресурсов, в достаточном объеме уже имеющихся как в государственном, так и бизнес-секторе, для обеспечения управляемости этими ресурсами является актуальной, то это сразу же отражается на структуре функциональных подсистем АС, в которой непременно появляются подсистемы интеграции и управления ресурсами.

Следующим важным моментом в решении вопроса №1 является слово "безопасная". В приложении к АС оно трансформируется в "защищенная", а общепринятая аббревиатура — в АСЗИ — автоматизированную систему в защищенном исполнении. Создание АСЗИ заключается в выполнении совокупности мероприятий, направленных на разработку и/или практическое применение таких информационных технологий, которые бы реализовали функции по защите информации в соответствии с требованиями стандартов и нормативных документов по защите информации как во вновь создаваемых, так и в действующих АС. Процесс создания АСЗИ начинается также с реализации научного подхода — создания Концепции информационной безопасности (ИБ) АС, являющейся, наряду с Концепцией автоматизации, вторым основополагающим документом АСЗИ.

Результатом дальнейшего развития подходов Концепции ИБ является формирование раздела ТЗ, в котором будут изложены требования к защите информации в АСЗИ, либо будет сформировано ЧТЗ на подсистему защиты информации в АС. Целью создания такой АСЗИ является определение защищаемых ресурсов АС, исключение или существенное затруднение получения до-

ступа к защищаемой информации злоумышленником не только о самой АС, но и обрабатываемой в АС или являющейся ее продукцией, а также исключение или существенное затруднение несанкционированного и/или непреднамеренного воздействия на защищаемую информацию и ее носители. Защита информации в АСЗИ является видом основной деятельности владельца АС и составной частью работ в области защиты информации.

Основные принципы и положения по созданию и функционированию АСЗИ изложены в требованиях ГОСТ 29339, ГОСТ Р 50543, ГОСТ Р 50739, ГОСТ Р 50972. ГОСТ Р 51275, ГОСТ РВ 50797 и других нормативных документах. Здесь имеется также ряд ограничений, сужающий круг организаций, имеющих возможность работать в АСЗИ. Кооперация исполнителей или единственный проектный интегратор должен иметь лицензии на осуществление работ в области защиты информации и использование средств защиты информации (СЗИ) в своей работе.

Работы по созданию, производству и эксплуатации АСЗИ с использованием криптографических (шифровальных) средств для защиты информации ограниченного доступа, ведутся в соответствии с положениями нормативных актов Российской Федерации, определяющих порядок разработки, изготовления и обеспечения эксплуатации шифровальных средств на основании соответствующих лицензий ФСБ РФ. Если же в АСЗИ обрабатывается информация, относящаяся к государственной тайне РФ, то необходимо наличие лицензии, подтверждающей возможность работы организации с этими сведениями.

Кроме того, ограничения касаются также возможности выбора разнообразных технических средств. Для создания АСЗИ могут применяться как серийно выпускаемые, так и вновь разработанные программные, программно-аппаратные, технические, криптографические СЗИ. Серийно выпускаемые средства должны иметь сертификаты соответствия требованиям по защите информации, полученные в соответствующих системах сертификации по требованиям безопасности информации (ФСТЭК РФ, ФСБ РФ, МО РФ).

Вопросы информационной безопасности, как видим, находятся под постоянным контролем и регулированием, как со стороны государства, так и структур управления организаций. Нормативно-методологической базой для решения вопросов ИБ в АСЗИ являются, в первую очередь, требования российского законодательства, определяющие обязательность защиты информации ограниченного доступа, в том числе и персональных данных граждан, всеми субъектами информационных отношений на всей территории РФ. Эти требования определяются в законах, детализируются и уточняются в руководящих документах Федеральной службы по техническому и экспортному контролю Российской Федерации, ФСБ России и других государственных учреждений, имеющих отношение к обеспечению безопасности информации и безопасному использованию информационных технологий. Эти требования определяют мероприятия и виды технических и программных средств базового уровня безопасности, обязательного для безоговорочного выполнения всеми субъектами информационных отношений, использующих информационные системы, обрабатывающие соответствующие виды информации ограниченного распространения.

Ответственность за несоблюдение этих требований несет, прежде всего, руководитель распределенной структуры, и она (ответственность) определена в таких законодательных актах РФ как: Конституция Российской Федерации, Гражданский Кодекс Российской Федерации, Уголовный Кодекс Российской Федерации, Федеральные законы Российской Федерации "О безопасности", "О государственной тайне", "Об информации, информатизации и защите информации", "О коммерческой тайне", "О связи", "Об участии в международном информационном обмене", "О техническом регулировании", "Об электронной цифровой подписи", "Об информации, информационных технологиях и о защите информации", Указы Президента Российской Федерации, Постановления Правительства Российской Федерации, Доктрина информационной безопасности Российской Федерации, международные договоры и соглашения, заключенные или признанные Российской Федерацией, а также других нормативных правовых актах.

Исходя из общих соображений можно определить ряд обязательных подсистем, которые должны входить в систему комплексной защиты информации в АСЗИ.

1. Подсистема авторизации. Эта подсистема обеспечивает доступ пользователя АСЗИ (в том числе удаленного) к защищаемой информации на основе анализа предъявляемых им своих учетных данных с использованием средств идентификации и аутентификации. Эта подсистема строится на принципах реализации мандатного и дискреционного методов доступа, имеет возможность отказать пользователю в доступе, если его данные будут признаны неподлинными, сигнализировать об этом администратору безопасности и зарегистрировать неудачную попытку доступа для проведения расследования таких коллизий ИБ.

2. Подсистема контроля целостности. Эта подсистема обеспечивает надлежащее функционирование прикладных процессов в АСЗИ на основе контроля идентичности необходимых файлов операционных систем (ОС), функционального и специального программного обеспечения (ПО). Это осуществляется путем сравнения контрольных сумм критичных файлов ОС и ПО с их контрольным суммами, хранящимися в подсистеме, как на этапе загрузки, так и в последующем в процессе функционирования, с возможностью автоматического блокирования сеанса пользователя в АСЗИ и сигнализации администратору безопасности. Кроме того, подсистема осуществляет контроль целостности данных при их передаче по каналам связи посредством применения криптографических СЗИ (симметричное и несимметричное шифрование).

3. Подсистема межсетевого экранирования. Эта подсистема позволяет осуществлять защиту объектов АСЗИ и АСЗИ в целом от несанкционированного доступа и сетевых воздействий (атак) с целью вывода из строя отдельных функций защиты информации, узлов сети, или нарушения функционирования АСЗИ в целом. Подсистема межсетевого экранирования используется также для разграничения доступа по сети к защищаемой информации АСЗИ, как на уровне адресов отдельных узлов, так и на уровне приложений.

4. Подсистема антивирусной защиты. Подсистема осуществляет защиту АСЗИ при взаимодействии со смежными информационными комплексами и системами от вредоносных программ (вирусов, троянских коней, spy-ware и пр.).

5. Подсистема контентного анализа и защиты от нежелательной почты (спама). Подсистема осуществляет защиту АСЗИ при взаимодействии со смежными информационными комплексами и системами от нежелательной (рекламной) информации.

6. Подсистема обнаружения вторжений. Эта подсистема позволяет производить анализ сетевого трафика и передавать сообщения о возможном нападении на централизованную консоль управления. Подсистема обнаружения вторжений позволяет уведомлять администратора безопасности о несанкционированной сетевой активности, регистрировать эти сведения и блокировать доступ нежелательных источников к защищаемой информации в АСЗИ.

7. Подсистема мониторинга уязвимос-

тей и аудита ИБ. Эта подсистема позволяет проводить анализ настроек и оценивать эффективность функционирования СЗИ, предоставляя администратору безопасности информацию о сбоях в работе СЗИ и наличии узких мест, которые могут быть использованы потенциальным злоумышленником для получения несанкционированного доступа к данным АСЗИ, регистрирует коллизии ИБ в журналах регистрации.

8. Подсистема управления ИБ АСЗИ. Подсистема предоставляет возможность централизованного управления конфигурацией всех служб и сервисов комплексной системы защиты АСЗИ. Управление конфигурацией СЗИ позволяет администратору безопасности получать полный доступ к настройкам средств безопасности серверов, рабочих мест, баз данных и средств межсетевого экранирования с использованием защищенных протоколов передачи данных, методами, устойчивыми к пассивному и активному прослушиванию. Система позволяет обнаруживать и устранять причины неисправностей и ошибок авторизации и доступа к данным.

В любом случае, интегратору и заказчику необходимо сформировать и утвердить обоснованную, интегрированную систему взглядов на вопросы обеспечения ИБ на этапах проектирования, создания, ввода в действие, промышленной эксплуатации и модернизации АС для реализации единой политики в области ИБ и выработки взаимосвязанных и согласованных мер организационного и инженерно-технического характера по созданию инфраструктуры информационной безопасности АС. Тогда можно говорить о создании автоматизированной системы в защищенном исполнении, когда в основе принятого технологического решения лежит полное и непротиворечивое решение всех вопросов ИБ, когда ИБ в системе не является отторгаемой, дополнительной опцией системы, но, напротив, является ее непременной функцией.

Вопросы реализации ИБ в АСЗИ станут неотъемлемыми ее частями, если будет решен главный вопрос — вопрос об АРХИТЕКТУРЕ системы — вопрос о выборе того или иного технологического решения для построения АСЗИ. Ведь не секрет, что разнородные СЗИ очень плохо сопрягаемы, что управлять ими сложно, что эксплуатация разнородных и многочисленных СЗИ связана с высокими издержками как на поддержание их в работоспособном состоянии, так и на постоянное совершенствование навыков персонала.

Таким образом, главным решением по созданию функционального обеспечения АСЗИ, в том числе исходя из перечисленных выше подсистем, является решение о единой архитектуре АСЗИ, в которую указанные функции ИБ уже встроены. Практическая деятельность в течение многих лет доказательно убеждает, что только трехуровневая архитектура построения АСЗИ с применением продуктов класса middleware в состоянии решить комплексную задачу ИБ в описываемом здесь понимании. Это означает, что все прикладные подсистемы АСЗИ работают в контексте создаваемой middleware среды исполнения, которая не только нивелирует различия между ними, не только выполняет функции информационно-логического сопряжения разнородных приложений, решая задачи маршрутизации, гарантированного доведения информации, разграничения доступа, контроля целостности, но и обеспечивает АСЗИ встроенными подсистемами ИБ, создает распределенное хранилище данных и т.д.

На наш взгляд, такой архитектурный подход сегодня является наиболее перспективным, позволяющим решить все вопросы совместного функционирования разнородных подсистем, в том числе с точки зрения ИБ. Этот подход может явиться основой для построения АСЗИ произвольной функциональной направленности, которая позволяет использовать в процессе создания АСЗИ любые возможные сертифицированные средства, в том числе зарубежного производства. Используя такую информационную технологию интеграции для любого общего, прикладного программного обеспечения и СЗИ, появляется возможность "правильного построения" защищенных АС для решения задач крупных, социально значимых проектов, к которым, безусловно, и относятся автоматизированные системы в защищенном исполнении (АСЗИ).

РОССИЯ И ИТАЛИЯ ДОГОВОРИЛИСЬ О СОТРУДНИЧЕСТВЕ В СОЗДАНИИ СИСТЕМ БЕЗОПАСНОСТИ ОСОБО ОХРАНЯЕМЫХ ОБЪЕКТОВ И МЕРОПРИЯТИЙ

Итальянская компания SELEX Sistemi Integrati S.p.A. (входит в концерн Finmeccanica) и российские предприятия, действующие под эгидой Государственной корпорации "Ростехнологии", — ОАО "Российская электроника" и Yota (ООО "Скартел") договорились о намерениях вступить в консорциум по созданию систем безопасности особо охраняемых объектов и мероприятий, о чем 7 апреля 2009 г. в Москве президентом и полномочным управляющим концерна Finmeccanica Пьером Франческо Гуаргуальини и генеральным директором Государственной корпорации "Ростехнологии" Сергеем Чемезовым был подписан меморандум.

Церемония подписания состоялась в присутствии Председателя Правительства РФ В.В. Путина в рамках Российско-итальянского экономического форума с участием беспрецедентного количества итальянских и российских предпринимателей — более 900 человек.

В соответствии с подписанным документом, стороны намерены объединить усилия в целях создания систем безопасности для особо охраняемых объектов и мероприятий. Речь идет, в частности, о больших транспортных узлах, таких как аэропорты, морские порты, железнодорожные станции, о потенциально опасных промышленных объектах — нефтебазах, газопроводах, а также о массовых мероприятиях, таких как конгрессы, саммиты или спортивные соревнования. Предусмотрены также создание систем безопасности официальных лиц и делегаций, реагирование на террористические акты.

Эксперты отмечают высокую значимость подписанного документа. Достигнутые договоренности предусматривают использование перспективных разработок обеих сторон, что ускорит развитие высокотехнологической отрасли, а также благотворно скажется на укреплении российско-итальянских отношений.

ГК "Ростехнологии" *учреждена в соответствии с Федеральным законом РФ. Целью деятельности Государственной корпорации "Ростехнологии" является содействие разработке, производству и экспорту высокотехнологичной промышленной продукции путем обеспечения поддержки на внутреннем и внешнем рынках российских организаций — разработчиков и производителей высокотехнологичной промышленной продукции, привлечения инвестиций в организации различных отраслей промышленности.*

ОАО "Российская электроника" *образовано Указом президента РФ от 23 июля 1997 №764 и Постановлением Правительства N 1583 от 18 декабря 1997 г. путем внесения в уставный капитал находящихся в государственной собственности акций акционерных обществ. В соответствии с постановлением Правительства РФ от 21 ноября 2008 г. №873 "О мерах по реализации Указа Президента РФ от 10 июля 2008 г. №1052 акции ОАО "Российская электроника" передаются ГК "Ростехнологии" в качестве имущественного взноса Российской Федерации. Основу ОАО "Российская электроника" составляют 72 предприятия и научно-исследовательских института, работающих в области производства и разработки квантовой электроники, контрольно-измерительной техники, оптоэлектронных и полупроводниковых приборов и СВЧ-техники.*

Yota *— российский разработчик и поставщик мобильных сервисов на базе технологии беспроводного быстрого доступа в интернет — 4G (Mobile WiMAX). Это первая в России сеть Mobile WiMAX™ (стандарт IEEE 802.16-2005), обеспечивающая доступ в интернет со скоростью до 10 Мбит/с и переключение между станциями без обрыва соединения.*

Концерн Finmeccanica со штаб-квартирой в Италии — один их мировых лидеров в вертолетостроении и европейский лидер в области космических услуг и радиоэлектроники.

SELEX Sistemi Integrati *— компания, входящая в концерн Finmeccanica, предлагает последние достижения в области средств противовоздушной обороны, командно-контрольных автоматизированных центров управления, корабельных систем управления, систем управления движением морских и речных судов, береговой охраны, а также систем и средств организации воздушного движения.*