УДК 681.322

И.В. Брякин, С.В. Корякин
Институт автоматики и информационных технологий
Национальной академии наук Кыргызской Республики, г.Бишкек
bivas2006@yandex.com, s.koryakin@aknet.kg

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СИСТЕМАХ РЕАЛЬНОГО ВРЕМЕНИ

Рассматриваются структура и особенности функционирования систем реального времени (СРВ). Анализируются вопросы обеспечения информационной безопасности в СРВ. Обосновывается вариант методологии создания систем защиты информации (СиЗИ), как функционального компонента СРВ защищенного исполнения (ЗИ).

Ключевые слова: архитектура, защищенное исполнение, информационная безопасность, операционная система, принцип, структура, система реального времени, система защиты информации, ядро.

Введение

Системы реального времени (СРВ) по своей сути являются параллельными системами с временными ограничениями. Они широко распространены в промышленных, коммерческих и военных приложениях. Современная система реального времени немыслима без комплекса достаточно сложной обработки информации, полученной не только путем ручного ввода, но и на основании автоматических измерений. К подобной обработке информации можно отнести: автоматизированный сбор, преобразование, агрегирование, хранение, передачу и представление (визуализация). Результатом этой обработки служит предоставление требуемой и достоверной информации в нужном виде, в нужном месте, и в нужное время, все то, без чего невозможно полноценное управление. Здесь имеется в виду не только информация для поддержки принятия решений, позволяющая операционному менеджменту выполнять свои функции, но и информация, на основании которой система в автоматическом или автоматизированном режиме производит выработку управляющих воздействий и команд, поступающих на реальный объект управления [1].

Система считается СРВ, если правильность ее функционирования зависит не только от логической корректности вычислений, но и от времени, за которое эти вычисления производятся. Иными словами, для событий, происходящих в такой системе, то, когда эти события происходят, так же важно, как логическая корректность самих событий. Кроме того, быстродействие такой системы адекватно скорости протекания физических процессов на объектах контроля или управления, а время генерации выходного сигнала СРВ играет существенную роль.

Это обычно связано с тем, что входной сигнал соответствует каким-то изменениям в физическом процессе, и выходной сигнал должен быть связан с этими же изменениями. Временная задержка от получения входного сигнала до выдачи выходного сигнала должна быть небольшой, чтобы обеспечить приемлемое время реакции. Время реакции является, прежде всего, системной характеристикой: при управлении ракетой требуется реакция в течение нескольких миллисекунд, тогда как для диспетчерского управления движением пароходов требуется время реакции, измеряемое днями.

Следует отметить, что время реакции СРВ имеет порядок миллисекунд; диалоговые системы отличаются временем реакции порядка нескольких секунд, а в

системах пакетной обработки время реакции измеряется часами или днями. Примерами СРВ являются АСУ физическими процессами с применением вычислительных машин, системы торговых автоматов, автоматизированные системы контроля и автоматизированные испытательные комплексы.

Среди АСУ, являющихся СРВ, выделяют следующие основные классы [2]:

• АСУТП – АСУ технологическими процессами (например, система управления ядерным реактором АЭС или система управления конвейером автозавода);

• АСНИ – автоматизированные системы научных исследований и комплексных испытаний (например, система вибрационных испытаний компонентов ракетной техники);

• встроенные системы управления (предназначенные для управления работой простых технических объектов – мобильных телефонов, стиральных машин, станков и т.п.) и бортовые системы управления (предназначенные для управления автомобилями, танками, самолетами, ракетами и т.п.).

Следует отметить, что на практике встречаются частные случаи СРВ:

• если в системе присутствуют только каналы сбора данных и измерения, то данная система является ИИС;

• если принятие решений и управление осуществляется непосредственно человеком, то система представляет собой АСДУ.

В последние годы вместе с техническими факторами, определяющими эффективность использования СРВ, широко обсуждаются и проблемы информационной безопасности подобных систем.

Независимо от того, является ли СРВ распределенной или централизованной, ее можно рассматривать как некоторую совокупность средств обработки, хранения и представления информации. Из этого следует, что в СРВ должны функционировать линии связи между отдельными аппаратными составляющими. В этом случае любое из аппаратных средств и любая линия связи могут быть источником информационной угрозы.

Структура и особенности функционирования СРВ

На практике защита информации представляет собой комплекс регулярно используемых методов и средств, принимаемых мер и осуществляемых мероприятий с целью систематического обеспечения требуемой надежности информации, генерируемой, хранящейся и обрабатываемой, в какой-либо информационной системе, а также передаваемой по каким-либо каналам.

Защита должна носить системный характер, т.е. для получения наилучших результатов все разрозненные виды защиты информации должны быть объединены в единое целое. Она должна функционировать в составе единой системы методов и средств, представляющей собой безотказный механизм взаимодействующих элементов, предназначенных для выполнения задач по обеспечению информационной безопасности.

Качество (надежность и эффективность) защиты зависит не только от видов составляющих частей системы, но и от их полноты, которая может быть обеспечена только при учете всех факторов и обстоятельств, сопутствующих функционированию СРВ. Поэтому комплексная система защиты информации призвана объединить логические и технологические составляющие защиты, учитывающие все факторы, которые оказывают или могут оказывать влияние на качество защиты. Более того, комплексная система защиты информации предназначена обеспечивать, с одной стороны, организацию и обеспечение надежных механизмов защиты, а с другой – управление механизмами защиты информации [3].

В большинстве случаев требования к комплексной системе защиты информации

предъявляются с учетом условий и рабочих характеристик СРВ и стоящих перед ней функциональных задач.

Следует учитывать тот факт, что в настоящее время происходит переосмысление многих вопросов становления и развития информационного рынка, неизбежно порождающих самые разнообразные проблемы, главной из которых является обеспечение информационной безопасности, поэтому образование на этом рынке сектора, в задачи которого входит защита информации, является вполне закономерным и весьма необходимым.

Для более полного понимания специфики решаемых задач, в плане обеспечения необходимого уровня защиты информации СРВ, следует рассмотреть более подробно особенности организации и функционирования таких систем.

Известно, что термин «система реального времени» обычно относится к системе в целом, включающей приложение реального времени, операционную систему реального времени и подсистему ввода/вывода реального времени (рис. 1).

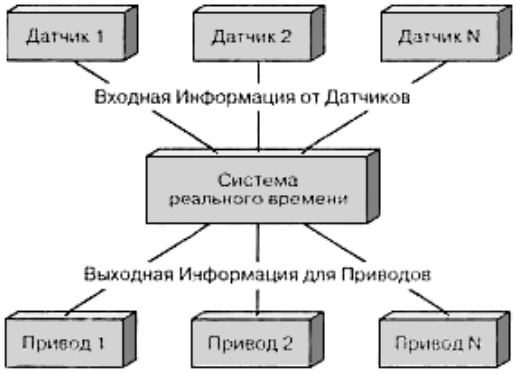


Рисунок 1. Обобщенная блок-схема СРВ

В состав такой системы входят также драйверы специальных устройств, управляющие работой различных датчиков и приводов.

По сравнению с информационными системами, в которых функции получения первичной информации и выдачи управляющих воздействий перекладываются на человека, системы, построенные на основе реальной связи с объектом управления, обладают более высокой оперативностью и достоверностью, не менее важным является и то, что в таких системах практически отсутствует человеческий фактор.

Системы реального времени часто отличаются повышенной сложностью, так как их работа связана с многочисленными независимыми потоками входных событий и продуцированием различной выходной информации. Частота поступления событий обычно непредсказуема, однако реагировать необходимо достаточно быстро, чтобы соблюсти временные ограничения, сформулированные в требованиях к программе. Нередко нельзя предугадать и порядок поступления событий. Кроме того, входная нагрузка может с течением времени значительно и неожиданно изменяться.

Аппаратные и программные средства, обеспечивающие техническую реализацию СРВ, должны отвечать современным требованиям унификации и стандартизации, метрологической, конструктивной, информационной и эксплуатационной совместимости, принципам модульного построения. При выполнении этих требований обеспечивается надежность построенной на основе этих средств информационной системы предприятия, достоверность и оперативность получаемой менеджментом информации, гарантированность исполнения командной информации.

Исходные требования к времени реакции системы и другим временным параметрам определяются или техническим заданием на систему, или просто логикой

ее функционирования. Однако точное определение «приемлемого времени реакции» не всегда является простой задачей, а в системах, где одним из звеньев служит человек, подвержено влиянию субъективных факторов.

Быстродействие СРВ должно быть тем больше, чем больше скорость протекания процессов на объекте контроля и управления. Чтобы оценить необходимое быстродействие для систем, имеющих дело со стационарными процессами, необходимо использовать теорему Котельникова, из которой следует, что частота дискретизации сигналов должна быть как минимум в 2 раза выше граничной частоты их спектра.

При работе с широкополосными по своей природе переходными процессами (транзиент–анализ) следует применять быстродействующие АЦП с буферной памятью, куда с необходимой скоростью записывается реализация сигнала, которая затем анализируется и/или регистрируется вычислительной системой. При этом требуется закончить всю необходимую обработку до следующего переходного процесса, иначе информация будет потеряна.

Подобные системы иногда называют системами квазиреального времени. Различают системы «жесткого» и «мягкого» реального времени [4]:

1. Системой «жесткого» реального времени является система, где неспособность обеспечить реакцию на какие-либо события в заданное время является отказом и ведет к невозможности решения поставленной задачи.

Несмотря на то, что теоретически время реакции в «жестких» системах может составлять и секунды, и часы, и недели, но с точки зрения практики время реакции в системах «жесткого» реального времени должно быть все-таки минимальным. Следует иметь в виду тот факт, что однозначного мнения о том, какое время реакции свойственно «жестким» системам, нет. Более того, с увеличением быстродействия микропроцессоров это время имеет тенденцию к уменьшению, и если раньше в качестве границы называлось значение 1 мс, то сейчас, как правило, называется время порядка 100 мкс.

2. Точного определения «мягкого» реального времени не существует, поэтому считается, что сюда относятся все системы реального времени, не попадающие в категорию «жестких». Кроме того, системы «мягкого» реального времени в настоящее время до конца теоретически не проработаны.

При разработке СРВ следует выбирать наиболее простые конфигурации, характерные для систем «жесткого» реального времени. Иногда это необходимо осуществлять даже в ущерб эффективности использования вычислительных ресурсов.

Причина этого заключается в том, что сложные динамические системы весьма трудно анализировать и отлаживать. Поэтому лучше использовать более мощную дорогостоящую микропроцессорную технику, чем иметь в будущем проблемы из-за непредвиденного поведения системы. В связи с этим большинство существующих СРВ представляют собой статические системы с фиксированными приоритетами. Часто в системе реализуется несколько «режимов» работы, каждый из которых имеет свой набор выполняемых задач с заранее заданными приоритетами.

Программные СРВ имеют дополнительные характеристики, отличающие их от прочих систем:

1. Встраиваемые системы. СРВ часто является частью более крупной программно-аппаратной системы. Примером может служить контроллер робота, входящий в состав робототехнического комплекса, имеющего одну или несколько механических рук. Обычно программная система реального времени состоит из приложения реального времени, ОСРВ и, возможно, дополнительного системного ПО: коммуникационных программ, программ промежуточного слоя или драйверов специальных устройств.

2. Взаимодействие с внешней средой. Как правило, СРВ осуществляет такое

взаимодействие без участия человека. Например, она может управлять механизмами или процессом производства, следить за протеканием химических реакций или поднимать тревогу. Для получения информации о внешней среде обычно требуются датчики, а для управления средой – приводы (см. рис. 2).

3. Временные ограничения. СРВ обязаны тратить на обработку события время, не превышающее заранее заданное. Если в интерактивной системе недостаточно быстрая реакция способна лишь вызвать недовольство, то в системе реального времени последствия бывают катастрофическими. Например, в системе управления воздушным движением это может привести к столкновению самолетов в воздухе. Необходимое время реакции зависит от приложения: иногда оно измеряется миллисекундами, иногда – секундами, а иногда – даже минутами.

4. Управление в реальном масштабе времени. Часто СРВ приходится принимать управляющие решения на основе входных данных, без участия человека. Так, автомобильная система круиз-контроля, призванная поддерживать постоянную скорость машины, должна управлять дросселем в зависимости от текущей скорости. Однако могут быть и некритичные по времени компоненты. Например, система сбора данных в реальном времени должна принимать информацию сразу, иначе она будет потеряна, но анализ полученных сведений допустим и позже.

5. Реактивные системы управляются событиями и должны реагировать на внешние стимулы. Обычно реакция системы зависит от ее текущего состояния, то есть не только от самого внешнего стимула, но и от того, что происходило в системе раньше.

В общем случае операционные системы (ОС) состоят из нескольких «слоев», каждый из которых выполняет свой набор функций (рис. 2).

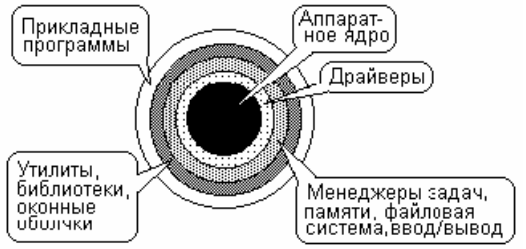


Рисунок 2. Многослойная структура ПО

При умозрительном анализе простых систем следует осторожно относиться к рекламной информации разработчиков ОСРВ, которые из коммерческих соображений показывают, как правило, параметры для «лучшего случая».

Например, если речь идет о максимальном времени обработки прерывания, необходимо в первую очередь понимать, а что, собственно, подразумевается под этим временем: а) время от возникновения запроса на прерывание до передачи управления по вектору прерывания; б) или включая время сохранения контекста текущей задачи и передачи управления подпрограмме обработки прерывания; в) или дополнительно к этому еще и время до завершения подпрограммы обработки прерывания и передачи сообщения, связанной с прерыванием задачи; г) или дополнительно к этому время до момента, когда эта задача наконец получит управление (в предположении, что она является наиболее приоритетной) и начнет реальную обработку события.

Безотносительно к тому, какой вариант рассматривается, необходимо помнить следующее: 1 – если наряду с разработанными вами программами используется программное обеспечение третьих фирм, вы не застрахованы от того, что там не встретятся участки кода, где прерывания запрещены; 2 – практически любая ОСРВ имеет в своих недрах участки такого кода; 3 – всё ядро ОСРВ или его участки могут

быть «невытесняемыми»; 4 – интеллектуальные контроллеры ввода/вывода типа SCSI могут инициировать в системе различные служебные операции, которые способны отразиться на ее характеристиках; 5 – многое зависит от применяемой системы кэширования.

Все ОСРВ являются многозадачными операционными системами. Задачи делят между собой ресурсы вычислительной системы, в том числе и процессорное время.

Четкой границы между ядром (Kernel) и ОС нет. Различают их, как правило, по набору функциональных возможностей.

Ядра предоставляют пользователю такие базовые функции, как планирование и синхронизация задач, межзадачная коммуникация, управление памятью и т. п.

ОС в дополнение к этому имеют файловую систему, сетевую поддержку, интерфейс с оператором и другие средства высокого уровня.

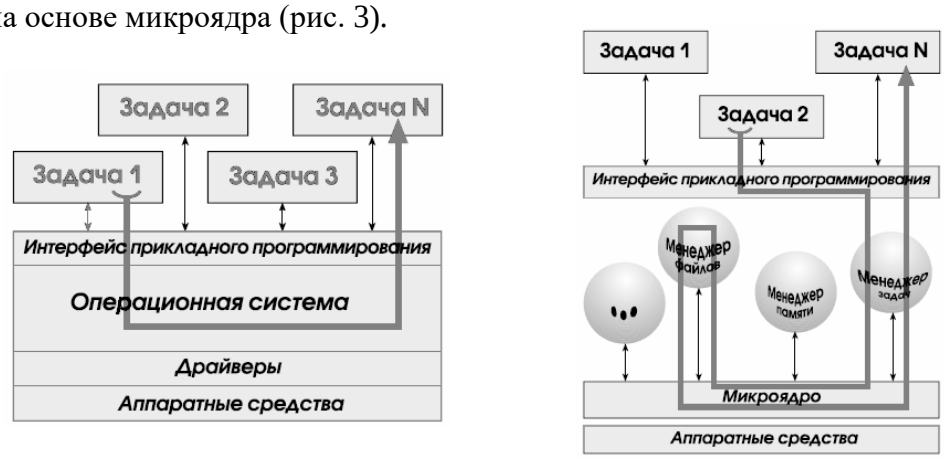
Практически все современные процессоры поддерживают как минимум два режима выполнения программного кода:

• «привилегированный режим» (или «режим супервизора», или «режим ядра», или «kernel mode», или «защищенный режим»);

• «непривилегированный режим» (или «режим приложений»).

Основное различие между ними заключается в том, что программы, работающие в режиме супервизора, имеют непосредственный доступ ко всем ресурсам ЭВМ: к внешним устройствам, к оперативной памяти по физическим адресам и пр. Программы же режима приложений работают в виртуальной среде, сформированной программами режима супервизора.

По своей внутренней архитектуре ОСРВ можно условно разделить на монолитные ОС и ОС на основе микроядра (рис. 3).



а) б)

Рисунок 3. Варианты архитектур ОС: а – монолитная архитектура; б – микроядерная архитектура

Все компоненты «монолитной» ОС работают в режиме супервизора в едином адресном пространстве. Главное достоинство таких ОС – высокая производительность. Главный недостаток – невозможность внесения каких-либо изменений в структуру операционной системы в процессе ее эксплуатации, т.е. плохая масштабируемость. Другой недостаток – невысокая реактивность системы, т.к. если внешнее событие, требующее немедленной реакции, происходит во время выполнения задач уровня ядра, то обработка этого события задерживается до возвращения на уровень приложений.

Особенность «микроядерных» ОС – наличие компактного и быстродействующего «микроядра», работающего в режиме супервизора, а все остальные компоненты операционной системы, включая менеджеры ресурсов, при этом работают в непривилегированном режиме. «Микроядерный» подход обеспечивает хорошую

гибкость и масштабируемость операционной системы, малое время реакции на внешние события. С другой стороны, «микроядерные» операционные системы отличаются относительно невысокой производительностью, т.к. при работе происходят частые переключения из режима в режим.

Встраиваемые ОСРВ преимущественно строятся в соответствии с «микроядерной» архитектурой. В фирменной документации на ОСРВ обычно указывают числовые значения временных характеристик, таких как: предельное время переключения с задачи на задачу; предельная задержка между возникновением прерывания и началом его обработки; предельное время выполнения запроса прикладной программы к ядру ОС; предельное время переключения из режима «супервизора» в «непривилегированный» режим и обратно, и т.п.

Прежде чем устанавливать СРВ на реальном объекте, рекомендуется проверить ее работоспособность с помощью интенсивных тестов. Это особенно важно для сложных динамических систем. Во время такого тестирования желательно смоделировать наиболее неприятные и «тяжелые» режимы работы, аварийные ситуации и т. п. Кроме того, следует учитывать тот факт, что значительная часть особо ответственных систем фактически реализуется без применения коммерческих ОСРВ.

Общие требования по информационной безопасности СРВ

СРВ фактически представляет собой организационно-техническую систему, обеспечивающую выработку решений на основе автоматизации информационных процессов в различных сферах деятельности (управление, проектирование, производство и т.д.) или их сочетаниях.

СРВ реализует информационную технологию в виде определенной последовательности информационно связанных функций, задач или процедур, выполняемых в автоматизированном или автоматическом режимах. Целесообразность создания и внедрения АС определяется социальным, научно-техническим или другими полезными эффектами, получаемыми в результате автоматизации [4].

Под защищенным исполнением СРВ следует понимать наличие в ее составе организационных и программно-технических средств защиты информации от несанкционированного доступа (НСД) [5]. Тогда сам процесс создания СРВ защищенного исполнения будет представлять собой фактически выполнение совокупности мероприятий, направленных на разработку и/или практическое применение информационной технологии, реализующей функции по ЗИ, установленные в соответствии с требованиями стандартов и/или НД по ЗИ как во вновь создаваемых, так и в действующих СРВ.

Общие принципы проектирования СРВ защищенного исполнения основаны на структурном подходе к анализу и самому проектированию СРВ. Исходя из этого, для защиты информации можно сформулировать следующие основные принципы: 1 – системности; 2 – комплексности; 3 – непрерывности защиты; 4 – разумной достаточности; 5 – гибкости управления и применения; 6 – открытости алгоритмов и механизмов защиты; 7 – простоты применения защитных мер и средств.

С точки зрения прикладной значимости, при организации ИБ СРВ в первую очередь следует акцентировать внимание на двух базовых принципах: комплексности и системности.

Собственно, комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонированно. Внешняя

защита должна обеспечиваться физическими средствами, организационными, технологическими и правовыми мерами. При построении комплексной защиты СРВ используется ряд основных мер, на которых данная система строится:

- правовые (законодательные);
- организационные (административные и процедурные);
- технические (аппаратурные и программные);
- физические;
- технологические;
- морально-этические.

Связь данных принципов представлена в виде соответствующей блок-схемы на рис. 4, где 1 – нормативные и организационно-распорядительные документы составляются с учетом и на основе существующих норм морали и этики; 2 – организационные меры обеспечивают исполнение существующих нормативных актов и строятся с учетом существующих правил поведения, принятых в стране и/или организации; 3 – воплощение организационных мер требует разработки соответствующих нормативных и организационно-распорядительных документов; 4 – для эффективного применения организационные меры должны быть поддержаны физическими и техническими средствами; 5 – применение и использование технических средств защиты требует соответствующей организационной поддержки.

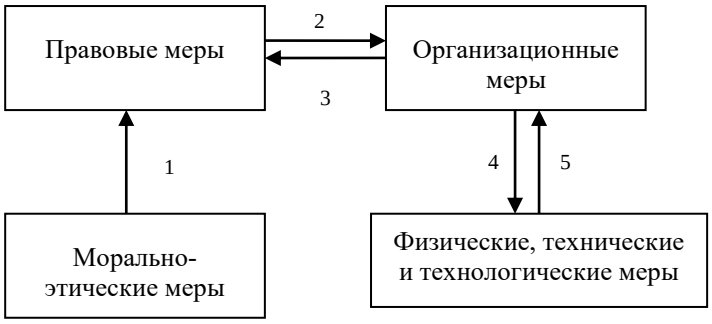


Рисунок 4. Взаимосвязь мер обеспечения безопасности

Системный подход к защите информации в СРВ предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения информационной безопасности в СРВ.

Принцип системности является одним из основных концептуальных и методологических принципов построения СРВ защищенного исполнения и предполагает:

- анализ всех возможных угроз безопасности информации;
- обеспечение защиты на всех жизненных циклах СРВ;
- защиту информации во всех звеньях СРВ;
- комплексное использование механизмов защиты.

Основной проблемой, которую приходится решать при создании больших систем любой природы, является проблема сложности. Правильная декомпозиция системы является главным способом преодоления сложностей больших систем [6].

Понятие *правильно* по отношению к декомпозиции означает следующее: 1 – количество связей между отдельными подсистемами должно быть минимальным; 2 – связанность отдельных частей внутри каждой подсистемы должна быть максимальной.

Структура системы должна быть такой, чтобы все взаимодействия между ее

подсистемами укладывались в ограничения: 1 – каждая подсистема должна инкапсулировать своё содержимое; 2 – каждая подсистема должна иметь четко определенный интерфейс с другими подсистемами

Используют два основных подхода к декомпозиции систем:

1. Функционально-модульный (структурный подход) – в основу положен принцип функциональной декомпозиции, при которой структура системы описывается в терминах иерархии ее функций и передачей информацией между отдельными функциональными элементами.

2. Объектно-ориентированный подход – использует объектную декомпозицию, при которой структура системы описывается в терминах объекта и связей между ними, а поведение системы описывается в терминах обмена сообщениями между объектами.

Кроме того, следует отметить, что одним из важнейших принципов построения защищенных СРВ является так же использование блочной архитектуры, позволяющее получить, в свою очередь, целый ряд преимуществ: а – упрощается разработка, отладка, контроль и верификация устройств (программ, алгоритмов); б – допускается параллельность разработки блоков; в – используются унифицированные стандартные блоки; г - упрощается модернизация систем; д – удобство и простота эксплуатации.

Основываясь на принципе блочной архитектуры защищенной СРВ, можно представить структуру идеальной защищенной системы.

В такой системе имеется минимальное ядро защиты, отвечающее нижней границе защищенности систем определенного класса (например, ПЭВМ). Если в системе необходимо обеспечить более высокий уровень защиты, то это достигается за счет согласованного подключения аппаратных блоков или инсталляции дополнительных программных средств (аналог режима «Plug and Play» в ОС Windows). В случае необходимости могут быть использованы более совершенные блоки СРВ, чтобы не допустить снижения эффективности применения системы по прямому назначению. Это объясняется потреблением части ресурсов СРВ вводимыми блоками защиты.

Стандартные входные и выходные интерфейсы блоков позволяют упростить процесс модернизации систем защиты информации (СиЗИ), альтернативно использовать аппаратные или программные блоки. Здесь просматривается аналогия с семиуровневой моделью OSI.

Очевидно, что степень соответствия этому принципу зависит от конкретной ОС, для которой создается СиЗИ. Эта зависимость определяется принципами построения и взаимодействия компонентов ОС, а также возможностью применения современных методов объектно-ориентированного проектирования.

Обобщая, можно констатировать, что в настоящее время существуют две концепции к проектированию СРВ защищенного исполнения (ЗИ):

- В первом случае СиЗИ разрабатываются одновременно с защищенной СРВ как таковой, т.е. СРВ создается как единое целое, включая, в частности, общее, специальное и функциональное ПО, аппаратную часть и средства защиты. При этом средства защиты включают компоненты уровня ОС, отвечающие за выполнение базовых функций защиты, и компоненты прикладного уровня, размещающиеся в общем, специальном и функциональном ПО. Взаимодействие указанных компонент СиЗИ позволяет создать необходимые условия для выполнения заданных требований по защищенности информации в СРВ.
- Вторая концепция обусловлена особенностями развития технологий разработки системного ПО в странах СНГ, которые привели к отсутствию сколь-либо распространенных ОС, производимых в этих странах. Разработка защищенных информационных систем в рамках СНГ выполнялась преимущественно путем переработки некоторой системы-прототипа с целью ее адаптации и доработки средств

защиты до требуемого уровня. На первый взгляд, этот путь представляется менее трудоемким, чем создание средств защиты с нуля. Однако на практике доработка уже существующей системы при отсутствии достаточной информации о ней не только приводит к непроизводительным потерям рабочего времени, но и предопределяет большую вероятность неудачи. При таком подходе разработчики СиЗИ из стран СНГ за основу брали, как правило, штатную систему защиты конкретной ОС и дорабатывали ее под требования РД ГТК, используя декларированные функции и возможности. Для целого ряда некритичных приложений подобный подход вполне приемлем, так как обеспечивает достижение определенного уровня информационной безопасности при относительно небольших затратах на разработку. Однако для использования в областях, где присутствует государственная тайна, например в изделиях, предназначенных для Министерств обороны стран СНГ, данный подход неприемлем в принципе.

При различных вариациях второй концепции основой СиЗИ все равно остается базовая система иностранного производства. При этом отсутствие исходных текстов и достоверных сведений о недекларированных возможностях не позволяет гарантировать необходимую реакцию СиЗИ на угрожающее воздействие. Это справедливо и тогда, когда разработчики СРВ ЗИ обеспечивают частичное вскрытие и доработку базовой системы защиты с целью обеспечения требуемой реакции в соответствии с определенными правилами.

СиЗИ, как основной функциональный компонент СРВ защищенного исполнения

В сложившихся условиях принципиальным решением указанной проблемы является разработка своего комплекса средств защиты информации (СрЗИ), с использованием которого можно было бы создавать полнофункциональные СиЗИ, в максимальной степени не зависимые от ОС импортного производства и полностью не зависимые от базовой системы защиты этой ОС.

Поэтому разрабатываемая СиЗИ должна выполняться с более высоким приоритетом, чем уже существующая базовая, и обеспечивать функции защиты как при активированной, так и при выключенной базовой СиЗИ.

В целом, совокупность требований к СиЗИ можно представить в виде соответствующей блок-схемы (рис. 5).

Выделяют четыре основных типа структуры СиЗИ [3]:

• однокомпонентные СиЗИ, которые строятся на базе одного, как правило, узкоспециализированного продукта по защите информации (в большинстве случаев таким продуктом становился антивирусный пакет);

• многокомпонентные СиЗИ, строящиеся уже на базе нескольких продуктов, каждый из которых решает свою конкретную задачу. При этом используемые в многокомпонентной СЗИ продукты и технологии по защите информации никак не связаны между собой ни на техническом, ни на организационном уровнях;

• комплексные СиЗИ – дальнейшее развитие многокомпонентных СиЗИ, в которых используемые продукты, технологии и решения объединяются в единую систему на организационном уровне с тем, чтобы обеспечить максимальную степень защищенности всей КИС в целом. Очевидно, что при этом стойкость всей СиЗИ эквивалентна стойкости самого «слабого» ее звена;

• интегрированные СиЗИ, в которых все элементы комплексных СиЗИ объединяются (вернее интегрируются) не только на организационном, но и на техническом и даже технологическом уровнях. В такой интегрированной системе компрометация одного из элементов защиты должна надежно компенсироваться

противодействием других ее элементов.

Рисунок 5. Совокупность требований к СиЗИ

СиЗИ относятся к классу сложных систем и для их построения могут использоваться основные принципы построения сложных систем с учетом специфики решаемых задач СРВ: 1 – параллельная разработка СРВ и СиЗИ; 2 – системный подход к построению СРВ защищенного исполнения (ЗИ); 3 – многоуровневая структура СиЗИ; 4 – иерархическая система управления СиЗИ; 5 – блочная архитектура СРВ ЗИ; 6 – возможность развития СиЗИ; 7 – дружественный интерфейс СРВ ЗИ с пользователями и обслуживающим персоналом.

Первый из приведенных принципов построения СиЗИ требует проведения одновременной параллельной разработки СРВ и механизмов защиты. Только в этом случае можно эффективно обеспечить реализацию всех остальных принципов. Причем в процессе разработки СРВ ЗИ должен соблюдаться разумный компромисс между созданием встроенных неразделимых механизмов защиты и блочных унифицированных средств и процедур защиты.

Только на этапе разработки СРВ можно полностью учесть взаимное влияние блоков и устройств собственно СРВ и механизмов защиты, добиться системности защиты оптимальным образом.

Как показывает практика, СиЗИ чаще всего имеет несколько уровней, перекрывающих друг друга, т. е. такие системы организованы по принципу построения «матрешек». В этом случае злоумышленнику, чтобы добраться до закрытой информации, необходимо «взломать» все уровни защиты (рис. 6).

Например, для отдельного объекта СРВ можно выделить 6 уровней (рубежей) защиты: 1 – охрана по периметру территории объекта; 2 – охрана по периметру здания; 3 – охрана помещения; 4 – защита аппаратных средств; 5 – защита программных средств; 6 – защита информации.

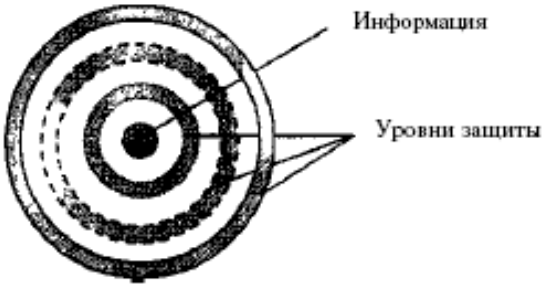


Рисунок 6. Многоуровневая СиЗИ

Несмотря на то, что СиЗИ всегда должны иметь централизованное управление, в распределенных СиЗИ допускается управление защитой осуществлять и по иерархическому принципу.

Централизация управления защитой информации объясняется необходимостью проведения единой политики в области безопасности информационных ресурсов в рамках предприятия, организации, корпорации, министерства. Для осуществления централизованного управления в СиЗИ должны быть предусмотрены специальные средства дистанционного контроля, распределения ключей, разграничения доступа, изготовления атрибутов идентификации и другие.

При создании СиЗИ должны учитываться все слабые и наиболее уязвимые места системы обработки информации, а также характер, возможные объекты и направления атак на систему со стороны нарушителей, пути проникновения в распределенные системы и несанкционированный доступ (НСД) к информации. СиЗИ должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

На современном этапе развития технологий обеспечения ИБ использование явления синергизма в масштабах всей корпоративной СиЗИ пока еще невозможно, т.к. на IT-рынке отсутствуют соответствующие реальные решения, позволяющие строить именно интегрированные СиЗИ. С одной стороны, это объясняется недостаточной зрелостью международных стандартов в области защиты информации, хотя движение в этом направлении прослеживается уже достаточно явно, а с другой стороны, построение многокомпонентных, а тем более однокомпонентных СиЗИ в большинстве случаев уже не является современным решением проблемы ИБ, особенно для крупных компаний. Поэтому в настоящее время оптимальным решением является построение именно комплексных СиЗИ.

Заключение

С учетом сказанного выше, в качестве системной основы для построения СРВ ЗИ исполнения рекомендуется применять микроядерную архитектуру с использованием сервера безопасности. На каждой рабочей станции защищаемой СРВ компоненты ПО системы защиты структурируются в виде ядра и сервисов. Ядро ориентировано на реализацию наиболее важных и общих функций базиса для всех сервисов защиты. Такой подход позволит минимизировать размер ядра и реализовать взаимодействие компонентов с использованием модели «клиент–сервер».

При разработке сложной СРВ, например, необходимо предусматривать возможность ее развития в двух направлениях: увеличения числа пользователей и наращивания возможностей сети по мере совершенствования информационных технологий. С этой целью при разработке СРВ предусматривается определенный запас ресурсов по сравнению с потребностями на момент разработки. Наибольший запас

производительности необходимо предусмотреть для наиболее консервативной части сложных систем – каналов связи. Часть резерва ресурсов СРВ может быть востребована при развитии СиЗИ.

На практике резерв ресурсов, предусмотренный на этапе разработки, исчерпывается уже на момент полного ввода в эксплуатацию сложных систем. Поэтому при разработке СРВ необходимо предусмотреть возможность модернизации системы. В этом смысле сложные системы должны быть развивающимися или открытыми.

Причем механизмы защиты, постоянно совершенствуясь, вызывают необходимость наращивания ресурсов СРВ. Новые возможности, режимы СРВ, а также появление новых угроз в свою очередь стимулируют развитие новых механизмов защиты. Важное место в процессе создания открытых систем играют международные стандарты в области взаимодействия устройств, подсистем. Они позволяют использовать подсистемы различных типов, имеющих стандартные интерфейсы взаимодействия.

Следует отметить, что разработка средств защиты уровня ОС позволит создать необходимый базис для проектирования СРВ ЗИ. Однако, как указывалось выше, для получения эффективной СиЗИ необходимо иметь средства не только защиты уровня ОС, но и прикладного уровня, встроенные в прикладное ПО. На практике решение этой задачи достигается путем разработки соответствующих (руководящих документов) РД, используя которые, программист создает защищенное ПО. В случае реализации такого подхода к проектированию без использования серьезной инструментально-технологической оснастки разработанные средства защиты могут оказаться слабо типизированными и недостаточно унифицированными [6].

Практическое применение изложенных методологических аспектов проектирования АСЗИ позволит эффективно решать многосторонний комплекс существующих вопросов, связанных с достижением таких целей, как безопасность, безотказность и деловая добросовестность.

Литература

1. Нестеров, А.Л. Проектирование АСУТП: методическое пособие. Кн.1. – М.: Деан, 2006. – 552 с
2. Брякин, И.В. Методология итерационного проектирования магнитовариационной ИИС // Проблемы автоматики и управления. – 2011. – №1. – С. 20–30.
3. Брякин И.В. Проектирование автоматизированных систем защищенного исполнения: научно-методическое пособие. – Бишкек: ИАИТ, 2017. – 81 с.
4. Емельянова, Н.З., Партыка, Т.Л., Попов, И.И. Основы построения автоматизированных информационных систем. – М.: ФОРУМ-ИНФРА-М, 2007. – 416 с.
5. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. – М.: Горячая линия-Телеком, 2004. – 280 с.
6. Тарасюк, М.В. Защищенные информационные технологии: Проектирование и применение. – М.: СО-ЛОН-Пресс, 2004. – 192 с.