Защита от несанкционированного доступа: что сегодня носят

Требований времени к средствам защиты информации принципиально два – соответствие актуальным СВТ и соответствие актуальным угрозам

беседовала Светлана Конявская, заместитель генерального директора ЗАО «ОКБ САПР»

Применяемые защитные меры тем эффективнее, чем точнее тот, кто их принимает, понимает, от чего он хочет защититься. Можно пытаться защититься от того, что молния попадет в дом, каким-то шаманским образом препятствуя этому, а можно направить усилия на то, чтобы при попадании в дом молния не вызвала пожара.

Защита информации – это ограничение универсальности средств вычислительной техники. Именно в этом состоит цель мероприятий по обеспечению ИБ, если посмотреть на нее с определенной дистанции: нам необходимо добиться того, чтобы все наши (то есть легальные) задачи решались, а задачи злоумышленников (нелегальные) не решались.

Универсальность компьютера обеспечивается архитектурно, самой его «конструкцией», как машины Тьюринга, универсального исполнителя.

Поскольку архитектуру нельзя изменить программным путем, то никакие программные средства не помогут нам защититься от хакеров надежно. Если уязвимость в архитектуре, то и совершенствовать нужно архитектуру.

В этом направлении мы можем:

1. усовершенствовать архитектуру уже существующих технических средств;
2. использовать новые технические средства на базе новой, более совершенной архитектуры.

Следуя первому направлению, эксплуатирующие организации, приобретают универсальную технику и устанавливают на нее те или иные средства защиты, следуя второму – приобретают технику, спроектированную тем или иным особым образом. Возвращаясь к подзаголовку – первые (наложенные средства) должны соответствовать современным (актуальным) СВТ, а вторые (защищенные СВТ) должны быть защищены именно от актуальных атак.

Наложенные средства защиты информации могут быть эффективны только в том случае, если они являются (или включают в свой состав) резидентным компонентом безопасности (РКБ).

Вытащить себя из болота за волосы нельзя, потому что нет точки опоры. А вот если тянуть за ветку дерева, растущего на кочке, – можно, потому что у дерева есть точка опоры.

Точка опоры применительно к принципиально модифицируемой компьютерной системе может означать только одно: контролирующие процедуры должны быть вынесены из этой модифицируемой среды в среду немодифицируемую и легко проверяемую. Значит, это должно быть аппаратное устройство, независимое от компьютера, который оно проверяет.

С появлением более 20 лет назад аппаратных модулей доверенной загрузки (АМДЗ) семейства «Аккорд» принципиально задача проектирования РКБ решена, а задача соответствия времени при таком солидном стаже работы решается тем, что ОКБ САПР систематически выпускает новые модели «Аккорда» для новых шин расширения и инфраструктурных особенностей. Так, вслед за АМДЗ в форм-факторе USB-устройств для внешнего или внутреннего подключения (контроллер «Инаф»), а также в форм-факторе mini PCI-express half size (это как WiFi-модуль, контроллер называется «Аккорд-GXMH»), недавно был выпущен новый контроллер – «Аккорд-GXm.2» для шины расширения m.2, применяемой сейчас в ноутбуках и моноблоках. Ничего подобного больше на рынке сейчас не предложено, в то время как в ближайшем будущем эта шина расширения станет основной.

В тех же случаях, когда бизнес-задачи точно описаны и рабочие места целесообразно создавать на базе специализированных АРМ с вирусным иммунитетом и без лишних функций – например, для фронт- и бэк-офиса, гораздо эффективнее не защищать универсальные машины, а использовать защищенные микрокомпьютеры семейства МКТ.

Естественно, помимо новых шин расширения и новых компьютерных архитектур, новые задачи возникают в связи с распространением новых инфраструктурных решений. Поэтому вслед за продуктами для защиты виртуализации VMware – «Аккорд-В.» и «Сегмент-В.» мы выпустили «ГиперАккорд» и «Аккорд-KVM» для виртуализации Hyper-V и KVM соответственно.

Вместо «продолжение следует» еще одно замечание насчет современных угроз. Наши решения пока остаются единственными, блокирующими угрозу со стороны IntelME. Потому что, не надеясь на шаманов, мы предпочитаем делать громоотводы. NBJ