ОБЩИЕ ВОПРОСЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И ОБЪЕКТОВ

УДК 004

О проблеме выбора средств защиты информации для инфраструктуры виртуализации

С. С. Лыдин
Закрытое акционерное общество "ОКБ САПР", Москва, Россия

Определение видовых ограничений, налагаемых на используемые средства защиты информации, составляет один из этапов проектирования системы защиты информации. Зачастую встроенные средства защиты информации позиционируются в качестве более предпочтительных к использованию для целей защиты инфраструктуры виртуализации в сравнении с наложенными. При этом отсутствие сертификата безопасности рассматривается как формальное препятствие. Настоящая статья содержит краткий обзор проблемы, которая связана с применением средств защиты информации, встроенных в системное программное обеспечение среды виртуализации.

Ключевые слова: инфраструктура виртуализации, встроенные средства защиты информации, наложенные средства защиты информации, недекларированные возможности.

Проектирование системы защиты информации для информационной системы (ИС), как правило, подразумевает выполнение следующих мероприятий:

- определение состава организационных и технических мер защиты информации, подлежащих реализации;
- определение видов и типов средств защиты информации (СЗИ), обеспечивающих реализацию технических мер защиты информации в соответствии с результатами выполнения первого этапа;
- выбор моделей средств защиты информации в соответствии с результатами выполнения второго этапа, сертифицированных на соответствие требованиям по безопасности информации.

На почве многочисленных дискуссий, ведущихся в профессиональных кругах, у владельца ИС при выполнении второго этапа довольно часто возникают трудности, связанные с принятием решения, о том какие СЗИ предпочтительнее использовать: *встроенные* в системное и прикладное программное обеспечение или *наложенные*.

При этом следует отметить, что в отношении систем, реализующих технологии виртуализации и облачных вычислений, указанная проблема выбора, как правило, неактуальна. Дело в том, что наиболее востребованные программные среды виртуализации не содержат *встроенных* СЗИ, сертифицированных для использования в ИС достаточно высоких классов. Таким образом, область поиска подходящего решения для владельца подобной системы, как правило, ограничивается только множеством *наложенных* СЗИ.

В то же время получил достаточно широкое распространение тезис, согласно которому соотношение сил могло бы оказаться иным в случае наличия у программных комплексов со *встроенными* функциями защиты среды виртуализации необходимых сертификатов безопасности. Зачастую принято считать, что по большинству других показателей превосходство *встроенных* СЗИ над *наложенными* не вызывает сомнений. На практике при выборе СЗИ, обеспечивающих реализацию технических мер защиты информации в системе, справедливо учитываются их стоимость, совместимость с информационными технологиями и техническими средствами. В качестве решающих преимуществ *встроенных* СЗИ перед *наложенными* обыкновенно рассматриваются:

- полная совместимость встроенного СЗИ с системным и прикладным программным обеспечением и, как следствие, высокая общая надежность решения и высокая производительность;
- низкая стоимость решения, сохранение средств заказчика.

Лыдин Сергей Сергеевич, начальник научно-исследовательского отдела.
E-mail: ssl@okbsapr.ru

Статья поступила в редакцию 5 июня 2017 г.

К недостаткам *наложенных* СЗИ последовательно относят отсутствие гарантий совместимости и, соответственно, низкую надежность и производительность. Также в некоторых аналитических материалах в отношении концепции *наложенных* СЗИ выносится заключение вида "конфликт интересов: безопасность против прогресса".

Таким образом, бытует мнение, что по основным технико-экономическим показателям *встроенные* СЗИ превосходят *наложенные*, а полной их доминации препятствуют лишь некоторые ограничения формального характера, связанные с особенностями сертификации по требованиям безопасности информации.

Между тем на поверку оказывается, что заявляемые преимущества *встроенных* механизмов защиты среды виртуализации перед *наложенными* носят умозрительный характер и в целом несостоятельны.

Для того чтобы в этом наглядно убедиться, достаточно обратиться непосредственно к истокам проблемы сертификации таких решений по требованиям безопасности информации, проблемы, которая, по мнению сторонников использования встроенных СЗИ, носит исключительно формальный характер.

Итак, одна из основных сложностей сертификации программного обеспечения для использования в системах высокого класса защищенности заключается в необходимости его контроля на отсутствие недекларированных возможностей, или прохождения так называемой "проверки на НДВ".

Следует сразу отметить, что данная сложность отнюдь не второстепенна, а скорее, представляет собой вершину айсберга. Очевидно, что наличие в программном обеспечении СЗИ недекларированных возможностей в худшем случае равнозначно полной его неработоспособности. При этом нужно иметь в виду, что факт успешного прохождения процедуры "проверки на НДВ" не означает, что в программном обеспечении действительно отсутствуют недекларированные возможности. Выполнение этой процедуры — лишь один из способов обеспечения доверия, степень которого в силу объективного несовершенства применяемых программно-технических средств проверки на НДВ обратно пропорциональна объему анализируемого программного кода.

Например, "динамический" анализ исходных текстов программ, необходимость проведения которого на высоких уровнях определена соответствующим руководящим документом ФСТЭК России, предусматривает организацию фактического выполнения функциональных объектов анализируемого программного обеспечения в рамках всех возможных маршрутов, что практически невыполнимо ввиду огромных объемов современных программных средств [1].

Очевидно, что "полная совместимость" *встроенного* СЗИ с системным и прикладным программным обеспечением подразумевает достаточно высокий уровень их связности. Поскольку выделить ядро защиты в условиях связности высокого уровня крайне трудно или невозможно, при сертификации *встроенных* СЗИ проверке на НДВ должен подвергаться весь программный код комплекса виртуализации вместе с *встроенными* в него СЗИ. Принимая во внимание весьма значительный объем программного кода таких продуктов (общий размер установочных пакетов измеряется в гигабайтах), можно обнаружить следующее. Стремление к достижению "полной совместимости" *встроенного* СЗИ и системного программного обеспечения имеет обратную сторону: повышение уровня связности неизбежно влечет за собой усложнение процедуры исследования программного кода и, как следствие, снижение уверенности в правильном функционировании решения в целом. Таким образом, заявление о более высоком уровне надежности комплексов со встроенными СЗИ хотя, по-видимому, и является верным в плоскости умозрительных рассуждений, с практической точки зрения не может быть подкреплено свидетельствами, характеризующимися высокой степенью доверия.

Относительно "конфликта интересов", который якобы имеет место при использовании *наложенных* СЗИ, легко убедиться, что ситуация диаметрально противоположна заявленной.

В действительности первостепенная задача добросовестного производителя *наложенных* СЗИ заключается в том, чтобы реализовать защитные механизмы, позволяющие выполнить требования. Производитель, конечно, принимает меры для того, чтобы реализованные механизмы не оказывали существенного негативного влияния на функционирование целевой системы, но приоритетной всегда остается задача обеспечения информационной безопасности. Поэтому использование термина "конфликт интересов" куда более оправдано в отношении концепции *встраивания* СЗИ в инфраструктуру виртуализации. Производители таких решений, как правило, конкурируют между собой, прежде всего на уровне показателей масштабируемости, поддержки всевозможных хранилищ данных, сетевых возможностей, производительности и т. п. Очевидно, что уступка по любому из этих параметров пусть даже за счет достижения более высокого уровня информационной безопасности

негативно сказывается на конкурентоспособности продукта. Не случайно один из основных аргументов сторонников использования *встроенных* СЗИ — именно быстродействие системы.

В связи с этим уместно также вспомнить об одном из базовых принципов обеспечения информационной безопасности да и вообще любой коллективной деятельности — разделении ролей, направленном на предотвращение возможного конфликта интересов. На практике при правильной организации производственных процессов всегда имеет место разделение полномочий: администратора виртуальной инфраструктуры и администратора информационной безопасности, администратора информационной безопасности и аудитора и т. д. Любое вольное или невольное нарушение этого принципа — веский повод для усиления мер предосторожности и введения дополнительных процедур контроля. Тем не менее в случае, когда производитель совмещает в одном лице функции разработки прикладного и системного программного обеспечения повышенной сложности, а также функции разработки интегрированных механизмов защиты информации системы, о базовом принципе забывают и правильность реализации функций в рамках этого совмещения принимается на веру.

В тесной связи с описанными побочными эффектами "полной совместимости" состоит проблема обновления *встроенных* СЗИ. В соответствии с установленными регулятором правилами разработчик сертифицированного продукта обязан осуществлять периодический поиск уязвимостей продукта с использованием средств анализа защищенности. В частности, в случае обнаружения уязвимостей необходимо принимать меры по их устранению путем выпуска обновлений безопасности. При этом обновление безопасности должно проходить процедуру проверки со стороны испытательной лаборатории. Разумеется, в условиях, когда защитные функции интегрированы в системное программное обеспечение, длительность выполнения процедуры проверки существенно увеличивается в сравнении с длительностью проверки выделенного ядра защиты небольшого объема, реализованного в *наложенном* СЗИ.

Основная проблема заключается в том, что механизмы защиты информации составляют малую часть от общего объема механизмов, реализованных в комплексе виртуализации. Разумеется, при эксплуатации комплекса виртуализации часто возникает потребность его обновления в связи с изменениями, вносимыми разработчиком в целевой функционал системы — системное и прикладное программное обеспечение. В силу высокого уровня связности последнего с программным обеспечением *встроенных* СЗИ, в сущности, любое обновление системы, даже не связанное с устранением уязвимостей, влечет за собой вопрос о необходимости предварительной проверки со стороны испытательной лаборатории, что существенно усложняет в организационно-техническом отношении эксплуатацию среды виртуализации.

В случае использования *наложенных* СЗИ обновление системного и прикладного программного обеспечения среды виртуализации может быть выполнено незамедлительно после выпуска разработчиком среды виртуализации соответствующих пакетов. Процедуре проверки со стороны испытательной лаборатории должны быть подвергнуты только пакеты обновления *наложенных* СЗИ, подготовленные разработчиком наложенного средства, и только при необходимости устранения соответствующей уязвимости. Таким образом, процедуры обновления различного назначения отделены друг от друга, что создает гораздо меньше сложностей для эксплуатирующей организации.

Наконец, помимо стоимости и совместимости с информационными технологиями, при выборе СЗИ далеко не в последнюю очередь нужно учитывать состав функций безопасности этих средств и особенности их реализации. Использование сред виртуализации со *встроенными* средствами защиты во многих случаях не позволяет обеспечить уровень информационной безопасности, сопоставимый с тем, который может быть достигнут с помощью *наложенных* средств.

Дело в том, что на программном уровне не может быть полноценно реализована важнейшая концепция основания доверия —концепция резидентного компонента безопасности системы как активного элемента, не зависящего от защищаемой системы и реализующего заданный набор процедур ее контроля [2]. Данная концепция положена в основу всех программно-аппаратных комплексов компании "ОКБ САПР" для защиты различных инфраструктур виртуализации ("Аккорд-В" для VMware vSphere; "ГиперАккорд" для Microsoft Hyper-V; "Аккорд-KVM" для KVM), каждый из которых является *наложенным* СЗИ.

Вопрос сравнительной стоимости решений и сохранения средств заказчика сознательно выведен за рамки данной работы. Исследование вопроса ценообразования для сложных продуктов, построенных в парадигме "все включено",

по-видимому, представляет собой бесперспективное занятие. Можно лишь путем логических умозаключений прийти к выводу о том, что реализация защитных функций и последующая сертификация требуют от производителя немалых затрат, что не может не привести к увеличению стоимости продукта.

Литература

1. *Осовецкий Л. Г.* Технология выявления недекларированных возможностей при сертификации промышленного программного обеспечения // Вопросы кибербезопасности. 2015. № 1 (9), С. 61.

2. Конявский В. А. Управление защитой информации на базе СЗИ НСД "Аккорд". — М.: Радио и связь, 1999. — 325 с.

The problem of choosing the information security tools for the virtualization infrastructure

S. S. Lydin
Closed Joint Stock Company "OKB SAPR", Moscow, Russia

The definition of specific restrictions for information security tools is one of the stages of designing an information security system. Built-in information security tools are often considered as more preferable to use for virtualization infrastructure protection purposes in comparison with external tools. At the same time, the absence of a safety certificate is regarded as a formal obstacle. This article contains a brief overview of the problem associated with the use of information security tools built into the system software of the virtualization environment.

Keywords: virtualization infrastructure, built-in information security tools, external information security tools, undeclared capabilities.

Bibliography — 2 references. *Received June 5, 2017*