**Александр ВЕСЕЛОВ**
руководитель отдела технического консалтинга ООО «С-Терра СиЭсПи»

# СКЗИ В ВИРТУАЛЬНОЙ СРЕДЕ

**Виртуализация не только словом, но и делом, а точнее рублём, доказала свою эффективность. В сфере информационной безопасности (ИБ), например, работа ряда продуктов для защиты от zero-day атак — «песочниц» — основана на виртуализации. Кроме того, упрощается решение задач по предоставлению сервисов безопасности, автоматизации, моделированию и тестированию. Но в силу национальной специфики помимо технологической составляющей не менее важно мнение по этому вопросу регуляторов российского рынка ИБ.**

## НОРМАТИВНАЯ БАЗА

ГНИИИ ПТЗИ ФСТЭК России и Технический комитет по стандартизации «Защита информации» (ТК 362) разработали ГОСТ Р 56938–2016 «Защита информации при использовании технологий виртуализации», содержащий описание объектов, перечень угроз, а также особенности реализации мер защиты в виртуальной среде. Кроме того, в статусе проекта находится документ ГОСТ «Требования по защите информации, обрабатываемой с использованием технологии облачных вычислений» с перечнем угроз ИБ для поставщиков и потребителей облачных услуг. В финансовой сфере также существует отраслевой документ Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности при использовании технологии виртуализации» (РС БР ИББС-2.8–2015), содержащий рекомендации по разделению потоков в виртуальной среде, обеспечению безопасности виртуальных машин (ВМ), их образов и терминалов, а также мониторингу ИБ и разграничению полномочий.

В нормативной базе ФСТЭК России меры по обеспечению защиты среды виртуализации присутствуют в приказах № 17, 21, 31 и 239. При этом ФСТЭК не имеет специальных руководящих документов по сертификации виртуальных сред, но ряд производителей сертифицировали свои продукты на соответствие техническим условиям. Средства защиты, работающие в виртуальной среде, могут быть сертифицированы, например, как межсетевые экраны уровня логических границ сети в программном исполнении (тип «Б»). ФСБ же занимается сертификацией в более узких областях ИБ, в основном криптографией, и ряд сертифицированных средств криптографической защиты информации (СКЗИ) могут работать в виртуальной среде при соблюдении ряда дополнительных требований, указанных в правилах пользования.

## ИСПОЛЬЗОВАНИЕ СКЗИ

Рассмотрим вопрос: реально ли использовать СКЗИ в виртуальной среде с соблюдением правил пользования, согласованных при сертификации?

Сразу нужно сказать, что на данный момент СКЗИ разных производителей, работающие в виртуальной среде, сертифицированы в ФСБ России по классу КС1. Прецедентов повышения класса до КС2 пока не было, связано это с более жёсткими требованиями в части защиты от несанкционированного доступа. Реализовать их можно с помощью средств доверенной загрузки или сертифицировав гипервизор. На российском рынке перечень таких продуктов крайне ограничен, широкого распространения они пока не получили. В связи с этим рассмотрим общие принципы правил пользования для СКЗИ, сертифицированных по классу КС1, при работе в виртуальной среде.

**ВАЖНО!**

*С-Терра Шлюз и С-Терра Клиент, сертифицированные в ФСБ России как СКЗИ по классу КС1, могут использоваться в виртуальной среде.*

## РАЗМЕЩЕНИЕ

При эксплуатации СКЗИ, работающих в виртуальной среде, должны соблюдаться требования по физическому размещению, аналогичные требованиям для аппаратных средств. В частности, охрана, пропускной режим, контроль периметра и т.д. В большинстве современных серверных и тем более в центрах обработки данных эти требования выполняются.

Использование виртуализации подразумевает удалённый доступ к ресурсам с клиентских мест, соответственно потребуется защита самих терминалов, запрещается оставлять их без контроля.

## ГИПЕРВИЗОРЫ

Перечень гипервизоров и их версии фиксируются на этапе тематических исследований. Для каждого гипервизора производитель СКЗИ описывает требования к эксплуатации (например, перечень файлов для контроля целостности). При этом рекомендуется регулярно устанавливать пакеты обновления безопасности, обновлять инструменты виртуализации, а также утилиты, используемые для управления средой виртуализации.

Учитывая наличие множества уязвимостей, а также динамику роста их количества, пренебрегать установкой обновлений точно не стоит. Например, за последний год было выявлено множество уязвимостей аппаратной части — процессоров Intel, начиная от оригинальных Spectre и Meltdown до L1TF (L1 Terminal Fault), которые с разной степенью надёжности закрываются патчами, выпускаемыми производителями гипервизоров. Теоретически возможна ситуация, когда пользователю требуется новая версия гипервизора (или версия с патчем), которая отсутствует в документации производителя СКЗИ. В этом случае производитель СКЗИ инициирует работы испытательной лаборатории по контролю изменений и далее обращается к регулятору. Если производитель СКЗИ имеет аккредитацию испытательной лаборатории, как, например, «С-Терра СиЭсПи», то сроки выполнения таких работ существенно сокращаются.

## АДМИНИСТРИРОВАНИЕ

Гипервизор имеет возможность влиять на функционирование СКЗИ, поэтому потребуется разграничение полномочий администраторов. Необходимо как минимум две роли — администратор виртуальной инфраструктуры, осуществляющий управление ВМ, серверными компонентами, системой хранения данных, а также администратор безопасности, формирующий политику безопасности, ключевую информацию и другие настройки непосредственно СКЗИ. Требование реализуется штатными средствами большинства популярных гипервизоров, а также организационными мерами.

## ВЗАИМОДЕЙСТВИЕ С ДРУГИМИ ВИРТУАЛЬНЫМИ МАШИНАМИ (ВМ)

Для защиты от несанкционированного доступа (НСД) требуется контроль информационного обмена между ВМ, в том числе общих областей оперативной памяти хоста. Актуальность угроз этого типа подтверждает целый ряд указанных выше уязвимостей. Защита реализуется встроенными средствами гипервизора или отдельными средствами защиты от НСД. Помимо этого, нужно помнить, что меры безопасности следует применять не только к ВМ с СКЗИ и гипервизору, но и ко всем другим машинам на этом гипервизоре.

На ВМ с СКЗИ, а также на другие ВМ не должны устанавливаться средства разработки ПО и отладчики. Если средства отладки приложений нужны для технологических потребностей организации, то их использование должно быть санкционировано администратором безопасности. При этом должны быть реализованы меры, исключающие возможность редактирования и просмотр кода и памяти СКЗИ, а также приложений, использующих СКЗИ. Обычно для реализации достаточно организационных мер защиты.

## МИГРАЦИЯ И ОТКЗОУСТОЙЧИВОСТЬ

При передаче (миграции) ВМ с СКЗИ по каналам связи вне контролируемой зоны необходимо обеспечить защиту этих каналов сертифицированными средствами защиты.

После ввода в СКЗИ ключевой информации на файл с образом, а также на последующие снапшоты и резервные копии распространяются требования по обращению с ключевыми носителями.

* * *

**ФСБ России не накладывает вето на сертификацию СКЗИ в виртуальной среде, множество средств защиты сертифицированы по классу КС1. Для каждого продукта существует ряд ограничений и рекомендаций по использованию в виртуальной среде, исходя из специфических угроз виртуализации. Ограничения делают её эксплуатацию менее удобной, но не перечёркивают большинства преимуществ.**

**ВАЖНО!**

*С-Терра Виртуальный Шлюз — виртуальная машина для гипервизоров VMware, Citrix XenServer, Microsoft Hyper-V, KVM и Huawei Fusion, по возможностям аналогичная С-Терра Шлюз в аппаратном исполнении.*

| Параметр | ПАК | ВМ |
|---|---|---|
| Цена | ПО — в рублях, АП — в у.е. | ПО — в рублях |
| Срок поставки | Недели | Дни |
| Масштабирование производительности | Новая (более мощная) АП | Новая лицензия |
| Резервирование | Горячий или холодный резерв с дополнительными затратами | Средствами системы виртуализации без дополнительных затрат |
| Сертификация ФСБ России по требованиям к СКЗИ | КС1, КС2, КС3 | КС1 |
| Сертификация ФСТЭК России по требованиям к МЭ | Тип «А» или «Б» | Тип «Б» |