ОБЩИЕ ВОПРОСЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И ОБЪЕКТОВ

УДК 004.056

Особенности обеспечения безопасности виртуальных инфраструктур в банковском секторе

А. С. Рябов
Закрытое акционерное общество "ОКБ САПР", Москва, Россия

Особенности обеспечения безопасности виртуальных инфраструктур в банках и других финансовых организациях. Рассмотрены основные принципы защиты виртуальной инфраструктуры в разрезе рекомендаций Банка России РС БР ИББС-2.8-2015, предложены решения по обеспечению безопасности.

Ключевые слова: информационная безопасность, технологии виртуализации, РС БР ИББС-2.8-2015, банковский сектор, виртуальная машина.

Развитие нормативной базы по информационной безопасности (ИБ) для банковского сектора идет очень активно. В 2014 г. обновился Стандарт Банка России СТО БР ИББС-1.0-2014 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения" [1]. Без внимания не остались и вопросы, связанные с безопасностью технологий виртуализации. В положениях стандарта появились базовые требования по защите виртуальных инфраструктур. Для уточнения базовых требований [1] в 2015 г. Банком России выпущены рекомендации РС БР ИББС-2.8-2015 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности при использовании технологий виртуализации" [2].

Обеспечение ИБ технологий виртуализации в разрезе документа [2] подразумевает эшелонированный подход к защите. В документе даются рекомендации по:

- разделению потоков информации и изоляции виртуальных машин (ВМ);
- обеспечению информационной безопасности образов ВМ;
- обеспечению информационной безопасности серверных компонентов виртуализации;
- обеспечению информационной безопасности ВМ;
- обеспечению информационной безопасности автоматизированных рабочих мест пользователей, используемых при реализации технологии виртуализации рабочих мест пользователей;
- мониторингу информационной безопасности;
- составу ролей и разграничению полномочий эксплуатационного персонала;
- обеспечению информационной безопасности системы хранения данных.

Рассмотрим наиболее важные положения документа [2] и предложим способы реализации защитных мер.

В банковских организациях существуют различные банковские технологические процессы – платежный, информационный, а также банковские технологические процессы, в рамках которых обрабатываются персональные данные [1]. Банковские технологические процессы имеют разные уровни критичности с точки зрения информационной безопасности. Для каждого вида банковского технологического процесса необходимо создать отдельный контур безопасности путем применения отдельного хост-сервера для каждого контура. Информационное взаимодействие между контурами необходимо обеспечивать с помощью сертифицированного сетевого оборудования, обеспечивающего контроль не выше сетевого уровня семиуровневой модели OSI [2].

Необходимо также обеспечить и запрет нерегламентированного информационного обмена между ВМ и другими компонентами виртуализации [2]. Например, в VMware vSphere информационный обмен между ВМ и ESXi обеспечивается с помощью настройки VMCI (*Virtual Machine Communication Interface*). Настройки VMCI хранятся в файлах оборудования ВМ и без надлежащего контроля могут быть подвержены модификации. Для защиты настроек от модификации необходимо применять механизмы (средства защиты), которые позволяют контролировать кон-

Рябов Андрей Сергеевич, исследователь.
E-mail: asr@okbsapr.ru

Статья поступила в редакцию 26 июня 2016 г.

фигурацию оборудования ВМ (например, это может быть программно-аппаратный комплекс "Аккорд-В.").

В рекомендациях по обеспечению ИБ базовых образов ВМ большое внимание уделяется вопросам контроля настроек ВМ, антивирусного контроля, обновления программных средств, а также целостности ОС, прикладного ПО и СЗИ ВМ [2].

При обеспечении безопасности текущих образов ВМ необходимо также позаботиться о вопросах запрета несанкционированного копирования этих образов [2]. С данной задачей может справиться программно-аппаратный комплекс "Сегмент-В." путем запрета клонирования и экспорта ВМ, а также запрета доступа к хранилищу пользователям.

При обеспечении безопасности серверных компонентов виртуализации автоматизированные рабочие места, предназначенные для администрирования, рекомендуется располагать в специально выделенном сегменте вычислительных сетей [2]. При этом для контроля использования иных АРМ для выполнения задач управления и администрирования серверных компонентов виртуализации рекомендуется применение сертифицированных сетевых технических средств [2], например комплекса "Сегмент-В.".

Средства управления и администрирования виртуализации являются сердцем инфраструктуры и подлежат тщательной защите. Для управления доступом к указанным элементам необходимо применять надежные сертифицированные СЗИ от НСД (например, СЗИ от НСД "Аккорд-Win64" (*TSE*)).

В соответствии с положениями [2] для антивирусной защиты виртуальной инфраструктуры рекомендуется применять средства, функционирующие на уровне гипервизора, без установки агентского ПО на ВМ.

Для доступа пользователей к ВМ, включенным в контур безопасности платежного технологического процесса и контур безопасности ИСПДн посредством АРМ пользователя, рекомендуется применять двухфакторную аутентификацию с использованием аппаратных средств [2] (например, персональных идентификаторов "ШИПКА").

Немаловажным аспектом безопасности виртуальной инфраструктуры является мониторинг. Для осуществления такого мониторинга должны обеспечиваться сбор, архивирование и хранение в течение определенного периода времени журналов, в которых регистрируются действия пользователей, нештатные ситуации и события ИБ виртуальной инфраструктуры. Как правило, сертифицированные СЗИ от НСД для виртуальных инфраструктур осуществляют регистрацию событий безопасности и имеют средства для их просмотра и анализа. Для архивации и надежного хранения журналов безопасности рекомендуется использовать мобильное USB-устройство с управляемым доступом "программно-аппаратный журнал" (ПАЖ), которое позволяет осуществлять сбор, архивацию и безопасное хранение журналов безопасности. При необходимости (например, при обнаружении инцидента ИБ) архивы журналов можно экспортировать для исследования в аналитические системы, например в системы SIEM.

Необходимо также определиться с составом ролей и разграничением полномочий эксплуатационного персонала. Для виртуальной инфраструктуры необходимо выделить следующие роли эксплуатационного персонала [2]:

- администратор ВМ и администратор информационной безопасности ВМ;
- администратор ИБ по управлению серверными компонентами виртуализации;
- администратор по управлению серверными компонентами виртуализации;
- администратор СХД.

Заключительным этапом является обеспечение безопасности систем хранения данных (СХД). В соответствии с [2] в СХД рекомендуется выделять отдельные логические разделы для каждого контура безопасности. При этом доступ к СХД рекомендуется осуществлять только с использованием гипервизора, АРМ, применяемых для выполнения задач управления и администрирования СХД, и технических средств, используемых для резервного копирования информации. Для контроля доступа к логическим разделам СХД рекомендуется применять сертифицированные сетевые технические средства, а для доступа к средствам управления и администрирования СХД — двухфакторную идентификацию, реализуемую сертифицированными СЗИ от НСД (например, СЗИ от НСД "Аккорд-Win64").

В рекомендациях [2] также большое внимание уделяется регламентированию (документированию) различных процессов, связанных с обеспечением ИБ технологий виртуализации (например, документирование процессов жизненного цикла базовых образов, документирование состава ПО базовых образов, регламентация обновления программного обеспечения и т. д.). Таким образом, необходима разработка новых или корректировка существующих в банке внутренних документов.

Итак, построение системы защиты виртуальной инфраструктуры в соответствии с рекомендациями

Банка России РС БР ИББС-2.8-2015 является комплексной задачей и обеспечивается организационными и техническими мерами.

При этом в качестве организационных мер можно выделить разработку новых и корректировку действующих внутренних организационных документов банка, как верхнеуровневых (частных политик ИБ), так и низкоуровневых – процессных (регламенты, инструкции, списки, перечни).

К техническим мерам можно отнести:

- настройку и конфигурацию платформы виртуализации;
- сегментирование инфраструктуры;
- установку адаптированных для виртуальной инфраструктуры средств защиты.

Также можно выделить следующий набор необходимых средств защиты для реализации безопасности виртуальной инфраструктуры:

- межсетевые экраны и сетевое оборудование;
- средства защиты информации, адаптированные для виртуальных инфраструктур (например, для популярной в России платформы виртуализации VMware vSphere — программно-аппаратные комплексы "Аккорд-В." и "Сегмент-В.", а для платформы Microsoft Hyper-V — комплекс "ГиперАккорд");
- средства двухфакторной аутентификации (например, персональные идентификаторы "ШИПКА");
- средства антивирусной защиты, адаптированные для виртуальных инфраструктур;
- средства сбора, архивации и надежного хранения журналов безопасности.

Средства защиты должны быть сертифицированы по требованиям безопасности ФСТЭК.

Можно отметить, что методическая база по информационной безопасности банковского сектора серьезно изменилась за последнее время. Банк России не оставил без внимания и вопросы обеспечения информационной безопасности популярного направления – виртуализации. При этом рекомендации Банка России РС БР ИББС-2.8-2015 являются универсальными для популярных на российском рынке платформ VMware vSphere, Microsoft Hyper-V. Несмотря на рекомендательный статус, документ РС БР ИББС-2.8-2015 учитывает специфические особенности организации банковской системы. Поэтому специалистам по информационной безопасности банков, использующим виртуализацию в качестве среды обработки данных, рекомендуется применять положения документа РС БР ИББС-2.8-2015 при реализации системы защиты как "руководство к действию".

Литература

1. Стандарт Банка России СТО БР ИББС-1.0-2014 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения".

2. Рекомендации Банка России РС БР ИББС-2.8-2015 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности при использовании технологий виртуализации".

Features securing virtual infrastructures in the banking sector

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

The article is devoted to the security of the virtual infrastructure in banks and other financial institutions. The basic principles for the protection of your virtual infrastructure in the context of the Recommendations of the Bank of Russia RS BR IBBS-2.8-2015 and proposed solutions for ensuring security.

Keywords: information security, virtualization technology, RS BR IBBS-2.8-2015, banking sector, virtual machine.

Bibliography — 2 references. *Received June 26, 2016*