РЕКОМЕНДАЦИИ В ОБЛАСТИ
СТАНДАРТИЗАЦИИ
БАНКА РОССИИ

РС БР ИББС-2.8-2015

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИИ ВИРТУАЛИЗАЦИИ

Дата введения: 2015-05-01

Москва
2015

Предисловие

ВВЕДЕНЫ в действие приказом Банка России от 19 февраля 2015 года № ОД-393.

Содержание

Введение

В соответствии с действующим стандартом Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения” (далее – СТО БР ИББС-1.0) условием реализации деятельности организаций банковской системы (БС) Российской Федерации (РФ) является обеспечение необходимого и достаточного уровня информационной безопасности вне зависимости от применяемых информационных технологий.

Настоящий документ устанавливает рекомендации по обеспечению информационной безопасности при использовании технологии виртуализации, расширяющие и уточняющие базовый набор требований к системе информационной безопасности организаций БС РФ, определенный положениями подразделов 7.2–7.11 СТО БР ИББС-1.0.

РЕКОМЕНДАЦИИ В ОБЛАСТИ СТАНДАРТИЗАЦИИ БАНКА РОССИИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИИ ВИРТУАЛИЗАЦИИ

Дата введения 2015-05-01

1. Область применения

Настоящий документ распространяется на организации БС РФ, использующие технологию виртуализации в рамках реализации банковских технологических процессов.

Настоящий документ рекомендован для применения путем использования установленных в нем положений, а также путем включения ссылок на них и (или) их прямого использования во внутренних документах организации БС РФ.

Настоящий документ применяется организациями БС РФ на добровольной основе. В конкретной организации БС РФ для обеспечения ИБ при использовании технологии виртуализации могут применяться иные подходы, отражающие специфику и сложившуюся практику организации БС РФ.

2. Нормативные ссылки

В настоящих рекомендациях в области стандартизации Банка России использованы нормативные ссылки на СТО БР ИББС-1.0.

3. Термины и определения

В настоящих рекомендациях применяются термины в соответствии со СТО БР ИББС-1.0, а также следующие термины с соответствующими определениями:

3.1. **Технология виртуализации** – информационная технология, позволяющая с использованием аппаратно-программных средств эмулировать на одном физическом средстве вычислительной техники (хост-сервере) функционирование нескольких средств вычислительной техники, включая их программное обеспечение (ПО).

3.2. **Техническое средство** – аппаратное, программное или аппаратно-программное средство.

3.3. **Средство виртуализации (гипервизор)** – программное средство, используемое для реализации технологии виртуализации, которое обеспечивает эмуляцию на одном физическом средстве вычислительной техники (хост-сервере) нескольких виртуальных машин.

3.4. **Виртуальная машина** – средство вычислительной техники, функционирование которого осуществляется с использованием гипервизора, способное выполнять собственную операционную систему (ОС), системное и иное ПО.

3.5. **Серверные компоненты виртуализации** – совокупность гипервизора, технических средств, необходимых для функционирования гипервизора, технических средств, предназначенных для управления и администрирования гипервизора, ПО, предназначенного для предоставления доступа к виртуальным машинам с АРМ пользователей (брокер соединений).

3.6. **Образ виртуальной машины** – набор файлов, представляющий собой настройки виртуальной машины, системное, прикладное и иное ПО виртуальной машины и данных, обрабатываемый с использованием указанного ПО.

3.7. **Базовый образ виртуальной машины** – образ виртуальной машины, используемый в качестве первоначального образа при запуске (загрузке) виртуальной машины.

3.8. **Информационный обмен между виртуальными машинами** – межпроцессорное взаимодействие, а также сетевые информационные потоки между виртуальными машинами, в том числе реализуемые средствами гипервизора в оперативной разделяемой памяти хост-сервера.

3.9. **Текущий образ виртуальной машины** – образ виртуальной машины в определенный (текущий) момент времени ее функционирования.

3.10. **Контур безопасности** – совокупность аппаратно-программных средств и информационных ресурсов, для которых в организации БС РФ установлен единый набор требований к обеспечению информационной безопасности.

Примечание: в организации БС РФ в числе прочих рекомендуется выделять:

– контур безопасности, в который включаются аппаратно-программные средства и информационные ресурсы, используемые для выполнения банковского платежного технологического процесса (далее – контур безопасности ПТП);
– контуры безопасности, в которые включаются аппаратно-программные средства и информационные ресурсы, используемые для выполнения банковских информационных технологических процессов разной степени критичности, в том числе банковского информационного технологического процесса, в рамках которого осуществляется обработка персональных данных в информационных системах персональных данных (далее – контур безопасности ИСПДн).

3.11. **Система хранения данных** – совокупность технических средств, предназначенных для хранения данных, используемых при реализации технологии виртуализации, в том числе образов виртуальных машин и данных, обрабатываемых виртуальными машинами.

3.12. **Защита от воздействия вредоносного кода на уровне гипервизора** – способ защиты от воздействия вредоносного кода с использованием программных средств, функционирующих как отдельные виртуальные машины на уровне гипервизора без установки специального ПО на защищаемые виртуальные машины.

3.13. **Эксплуатационный персонал** – субъекты доступа, которые решают задачи обеспечения эксплуатации и администрирования, в том числе эксплуатации и администрирования автоматизированных банковских систем (АБС) организации БС РФ, систем управления базами данных, сетевого оборудования, прикладных программных комплексов, а также задачи, связанные с эксплуатацией и администрированием средств и систем обеспечения информационной безопасности.

4. Обозначения и сокращения

АБС – автоматизированная банковская система;
АРМ – автоматизированное рабочее место;
БС – банковская система;
ИБ – информационная безопасность;
ОС – операционная система;
ПО – программное обеспечение;
РФ – Российская Федерация;
СВТ – средство вычислительной техники;
СЗИ – средство защиты информации;
СХД – система хранения данных.

5. Общие положения

5.1. Настоящий документ устанавливает рекомендации по:

– разделению потоков информации и изоляции виртуальных машин;
– обеспечению ИБ образов виртуальных машин;
– обеспечению ИБ серверных компонентов виртуализации;
– обеспечению ИБ виртуальных машин;
– обеспечению ИБ АРМ пользователей (терминалов и персональных электронных вычислительных машин), используемых при реализации технологии виртуализации рабочих мест пользователей;
– мониторингу ИБ;
– составу ролей и разграничению полномочий эксплуатационного персонала;
– обеспечению ИБ СХД.

5.2. Рекомендации настоящего документа применяются среди прочего при создании и модернизации АБС организации БС РФ, реализующих технологию виртуализации, и АБС организации БС РФ, функционирование которых организуется с использованием технологии виртуализации, а также при разработке технических заданий, технорабочих проектов и эксплуатационной документации на АБС организации БС РФ, реализующих технологию виртуализации.

5.3. Создание и модернизация АБС организации БС РФ, реализующих технологию виртуализации, в части вопросов обеспечения ИБ осуществляется по согласованию и под контролем службы ИБ организации БС РФ.

6. Рекомендации по разделению потоков информации и изоляции виртуальных машин

6.1. Рекомендации по разделению потоков информации и изоляции виртуальных машин применяются с целью обеспечения независимого выполнения:

– банковских платежных технологических процессов;
– банковских информационных технологических процессов разной степени критичности для деятельности организации БС РФ, реализуемых в пределах разных контуров безопасности;
– банковских информационных технологических процессов, реализуемых в пределах контура безопасности ИСПДн.

6.2. Рекомендуется размещение совокупности виртуальных машин, входящих в разные контуры безопасности, в первую очередь контур безопасности ПТП и контур безопасности ИСПДн, на отдельных физических СВТ (хост-серверах).

6.3. Доступ к виртуальным машинам, включенным в контур безопасности ПТП, рекомендуется осуществлять только с АРМ, включенных в контур безопасности ПТП.

Доступ к виртуальным машинам, включенным в контур безопасности ИСПДн, рекомендуется осуществлять только с АРМ, включенным в контур безопасности ИСПДн.

Для иных контуров безопасности организации БС РФ рекомендуется реализовать правила, ограничивающие доступ к виртуальным машинам только с АРМ конкретных (установленных) контуров безопасности.

6.4. Реализацию требований и правил ограничения доступа к виртуальным машинам с АРМ, установленных в пункте 6.3 настоящего документа, рекомендуется осуществлять на уровне не выше третьего (сетевой уровень) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ 28906-91, путем применения технических средств, прошедших в соответствии с законодательством РФ оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации (далее – сертифицированные сетевые технические средства).

6.5. Средствами (настройками) гипервизора и (или) иными техническими средствами рекомендуется обеспечивать:

– выделение для групп виртуальных машин, включенных в разные контуры безопасности, в том числе контур безопасности ПТП и контур безопасности ИСПДн, отдельных используемых только для работы данных групп виртуальных машин, логических областей оперативной памяти физического СВТ (хост-сервера);
– запрет нерегламентированного в эксплуатационной документации информационного обмена между виртуальными машинами с использованием общих ресурсов физического СВТ (хост-сервера), в том числе общих областей оперативной памяти физического СВТ (хост-сервера);
– запрет нерегламентированного информационного обмена между виртуальными машинами и программными процессами и ОС физического СВТ (хост-сервера), на котором функционирует гипервизор, с использованием общих ресурсов физического СВТ (хост-сервера), в том числе общих областей оперативной памяти физического СВТ (хост-сервера).

6.6. Не рекомендуется использовать физическое СВТ (хост-сервер), предназначенное для размещения гипервизора, для организации функционирования ПО, реализующего банковские технологические процессы, вне виртуальной машины.

6.7. Совокупность виртуальных машин, включенных в разные контуры безопасности, в том числе в контур безопасности ПТП и контур безопасности ИСПДн, рекомендуется размещать в отдельных сегментах (группах сегментов) вычислительных сетей, в том числе виртуальных вычислительных сетей, реализованных с использованием функциональных возможностей гипервизора.

Информационный обмен между указанными сегментами (группами сегментов) вычислительных сетей рекомендуется обеспечивать только физическим сетевым оборудованием.

6.8. В соответствии с требованиями законодательства РФ для защиты контура безопасности ИСПДн следует применять СЗИ, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации.

6.9. Для организации информационного обмена между сегментами вычислительных сетей, используемыми для размещения виртуальных машин, включенных в контур безопасности ПТП и контур безопасности ИСПДн, и сегментами вычислительных сетей, используемыми для размещения АРМ, включенных в контур безопасности ПТП и контур безопасности ИСПДн соответственно, рекомендуется использовать сертифицированные сетевые технические средства.

6.10. Средствами гипервизора и (или) иными техническими средствами рекомендуется реализовывать запрет нерегламентированного информационного обмена между виртуальными машинами, включенными в контур безопасности ПТП и контур безопасности ИСПДн, используемыми для эксплуатации различных АБС организации БС РФ.

6.11. Рекомендуемым решением является использование гипервизоров, прошедших в соответствии с законодательством РФ оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации.

7. Рекомендации по обеспечению ИБ образов виртуальных машин

7.1. В организации БС РФ рекомендуется регламентировать процессы жизненного цикла базовых образов виртуальных машин, в том числе процесс создания и модернизации базовых образов виртуальных машин.

7.2. Состав ПО каждого из базовых образов виртуальных машин рекомендуется согласовывать со службой ИБ организации БС РФ.

7.3. Для каждого из серверных компонентов АБС организации БС РФ рекомендуется использовать отдельный образ виртуальной машины. Не рекомендуется организовывать функционирование более чем одного серверного компонента АБС организации БС РФ на одной виртуальной машине.

7.4. В случае использования разделяемых (общих) СЗИ, эксплуатируемых с использованием технологии виртуализации для целей обеспечения защиты информации более чем двух виртуальных машин, указанные СЗИ рекомендуется размещать на отдельной виртуальной машине, предназначенной только для этой цели, или физическом СВТ.

7.5. При создании базовых образов виртуальных машин рекомендуется проводить процедуры, необходимые для выполнения последующего контроля их целостности.

7.6. В образ виртуальной машины рекомендуется включать прикладное ПО АБС организации БС РФ, предназначенное для работы только в одном из контуров безопасности.

7.7. На этапах создания и (или) модернизации АБС организации БС РФ, в том числе тестирования ПО в виртуальной среде, рекомендуется организовывать виртуальный тестовый сегмент, доступ к которому рекомендуется осуществлять по отдельному физическому сетевому интерфейсу. Виртуальные машины тестового сегмента рекомендуется размещать на отдельном физическом СВТ.

7.8. Созданный или измененный базовый образ виртуальной машины перед размещением на основном оборудовании, реализующем технологию виртуализации, рекомендуется проверять в тестовом сегменте на:

- корректность работы программных компонентов;
- отсутствие вредоносного кода;
- соответствие настроек включенных в образ программных компонентов СЗИ требованиям, установленным соответствующей эксплуатационной документацией.

7.9. Для каждого базового образа виртуальной машины рекомендуется выполнять регламентированные процедуры контроля:

- соответствия настроек, включенных в образ программных компонентов СЗИ, требованиям, установленным эксплуатационной документацией;
- целостности ПО, включенного в образ виртуальной машины.

7.10. Для каждого базового образа виртуальной машины рекомендуется выполнять регламентированные процедуры обновления:

- средств защиты от воздействия вредоносного кода, в том числе сигнатурных баз средств защиты от воздействия вредоносного кода;
- программных компонентов СЗИ и их настроек, включенных в образ;
- системного и прикладного ПО, в том числе ОС, обеспечивающих устранение уязвимостей ПО.

После выполнения указанных процедур обновления рекомендуется проводить процедуры, необходимые для выполнения последующего контроля целостности образов виртуальных машин.

7.11. Средствами гипервизора и (или) иными техническими средствами рекомендуется реализовать запрет копирования текущих образов виртуальных машин, используемых для реализации технологии виртуализации рабочих мест пользователей.

Копирование текущих образов виртуальных машин, используемых для функционирования серверных компонентов АБС организации БС РФ, рекомендуется осуществлять только для цели создания резервных копий в соответствии с установленными регламентами.

Не допускается копирование текущих образов виртуальных машин, использующих средства криптографической защиты информации, с загруженными криптографическими ключами.

7.12. Рекомендуется регламентировать и выполнять процедуры учета используемых базовых образов виртуальных машин, предусматривающие среди прочего их вывод из эксплуатации и удаление.

8. Рекомендации по обеспечению ИБ серверных компонентов виртуализации

8.1. АРМ, используемые для выполнения задач администрирования серверных компонентов виртуализации, рекомендуется располагать в специально выделенном сегменте вычислительных сетей. Размещение в указанном выделенном сегменте вычислительных сетей СВТ, не связанных с выполнением задач управления и администрирования, не рекомендуется. Рекомендуется использование сертифицированных сетевых технических средств для реализации запрета использования иных АРМ для выполнения задач управления и администрирования серверных компонентов виртуализации.

8.2. Доступ к средствам управления и администрирования серверных компонентов виртуализации рекомендуется осуществлять с использованием СЗИ от несанкционированного доступа, прошедшим оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации.

8.3. СЗИ от несанкционированного доступа, используемые для организации доступа к серверным компонентам виртуализации, рекомендуется размещать только на физическом СВТ.

8.4. Не рекомендуется организация функционирования серверных компонентов виртуализации в рамках виртуальных машин.

8.5. Для обеспечения штатного функционирования серверных компонентов виртуализации рекомендуется использовать минимально необходимый и регламентированный набор ПО СВТ, используемых для размещения серверных компонентов виртуализации. Для указанных СВТ рекомендуется выполнять регламентированные процедуры контроля целостности ПО, в том числе выполняемые при загрузке указанного ПО.

Установка и наличие средств, предназначенных для разработки и отладки ПО, на АРМ, используемых для выполнения задач управления и администрирования серверных компонентов виртуализации, не рекомендуется.

8.6. Для обеспечения штатного функционирования серверных компонентов виртуализации рекомендуется использовать минимально необходимый и регламентированный набор устройств (портов) ввода-вывода информации на СВТ, используемых для функционирования серверных компонентов виртуализации.

С применением технических средств рекомендуется осуществлять контроль использования устройств (портов) ввода-вывода информации на СВТ, используемых для функционирования серверных компонентов виртуализации.

8.7. Техническими средствами, в том числе средствами серверных компонентов виртуализации, рекомендуется осуществлять протоколирование следующих событий:

- запуск (остановка) виртуальных машин;
- изменение настроек виртуальных сетевых сегментов, реализованных средствами гипервизора;
- создание и удаление виртуальных машин;
- создание, изменение, копирование, удаление образов виртуальных машин;
- копирование текущих образов виртуальных машин;
- изменение полномочий доступа к серверным компонентам виртуализации, создание и удаление учетных записей, необходимых для доступа к серверным компонентам виртуализации;
- изменение настроек серверных компонентов виртуализации;
- аутентификация и авторизация эксплуатационного персонала при осуществлении доступа к серверным компонентам виртуализации;
- запуск (остановка) ПО серверных компонентов виртуализации, в том числе ПО гипервизора;
- изменение настроек физических СВТ (хост-серверов), используемых для функционирования серверных компонентов виртуализации;
- изменение настроек СЗИ, используемых для реализации доступа к серверным компонентам виртуализации;
- изменение настроек СЗИ, используемых для целей обеспечения защиты информации виртуальных машин.

8.8. Средствами гипервизора или иными техническими средствами рекомендуется осуществлять:
– контроль информационного обмена (взаимодействия) между виртуальными машинами с использованием общих (разделяемых) ресурсов физического СВТ (хост-сервера);
– контроль использования виртуальными машинами оперативной памяти физического СВТ (хост-сервера);
– выявление проявлений ПО, функционирующего на виртуальных машинах, связанного с возможными нарушениями установленного режима использования ресурсов физического СВТ (хост-сервера);
– выявление вредоносного кода.

8.9. Для серверных компонентов виртуализации рекомендуется осуществлять защиту от воздействия вредоносного кода, реализованную в соответствии с требованиями, установленными в организации БС РФ, в том числе функционирующую на уровне гипервизора.

9. Рекомендации по обеспечению ИБ виртуальных машин

9.1. Для обеспечения ИБ АБС организации БС РФ, эксплуатируемых на виртуальных машинах, применяются требования, установленные в организации БС РФ для соответствующих контуров безопасности.

9.2. При реализации технологии виртуализации рабочих мест пользователей рекомендуется исключить возможность одновременной работы пользователя с разными виртуальными машинами, включенными в разные контуры безопасности.

9.3. Для каждой виртуальной машины рекомендуется осуществлять защиту от воздействия вредоносного кода, реализованную в соответствии с требованиями, установленными в организации БС РФ и предусматривающую:
– централизованное управление средствами защиты от воздействия вредоносного кода;
– реализацию постоянной защиты от воздействия вредоносного кода;
– автоматическое обновление сигнатурных баз средств защиты от воздействия вредоносного кода.

9.4. Для виртуальных машин, размещенных на физическом СВТ (хост-сервере), используемом для размещения виртуальных машин, включенных в контур безопасности ПТП и контур безопасности ИСПДн, техническими средствами рекомендуется реализовать:
– контроль целостности ПО виртуальных машин, в том числе выполняемый на этапе загрузки виртуальных машин;
– контроль и регистрацию доступа пользователей и эксплуатационного персонала к виртуальной машине, выполняемый техническими средствами, прошедшими в соответствии с законодательством Российской Федерации оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации.

9.5. Средствами управления доступом к виртуальным машинам рекомендуется обеспечивать возможность интеграции с системами управления учетными записями и правами доступа, применяемыми в организации БС РФ.

9.6. Рекомендуемым решением является использование средств защиты от воздействия вредоносного кода на уровне гипервизора без установки агентского ПО на виртуальные машины.

9.7. В случае использования централизованных (общих) средств защиты информации, эксплуатируемых с использованием технологии виртуализации для целей обеспечения защиты информации более чем двух виртуальных машин, указанные средства защиты информации рекомендуется размещать на отдельной виртуальной машине, предназначенной только для этой цели.

10. Рекомендации по обеспечению ИБ АРМ пользователей, используемых при реализации технологии виртуализации рабочих мест пользователей

10.1. На АРМ пользователей рекомендуется использование минимально необходимого для выполнения служебных обязанностей и регламентированного набора доступных портов ввода-вывода информации.

Техническими средствами и (или) организационными мерами рекомендуется организовывать контроль использования (портов) ввода-вывода информации АРМ пользователей.

10.2. Техническими и (или) организационными мерами рекомендуется ограничить возможность самостоятельного:
– изменения пользователем настроек АРМ, включая аппаратные и программные компоненты АРМ;
– подключения и использования пользователем дополнительных (несанкционированных) периферийных устройств, в том числе взамен ранее подключенных.

10.3. Для АРМ пользователей, используемых для доступа к виртуальным машинам, включенным в контур безопасности ПТП и контур безопасности ИСПДн, рекомендуется реализовать процедуры доверенной загрузки ОС.

10.4. Рекомендуется осуществлять идентификацию и аутентификацию пользователей серверными компонентами виртуализации до предоставления доступа к виртуальным машинам.

10.5. Для доступа пользователей к виртуальным машинам, включенным в контур безопасности ПТП и контур безопасности ИСПДн посредством АРМ пользователя, рекомендуется применять двухфакторную аутентификацию с использованием аппаратных средств.

10.6. Рекомендуется реализовать механизмы принудительной блокировки (выключения) сессии работы пользователя с виртуальной машиной, установленной с помощью компонента централизованного управления хост-серверами.

10.7. На АРМ пользователей, включенных в контур безопасности ПТП и контур безопасности ИСПДн, техническими средствами рекомендуется реализовать запрет нерегламентированного информационного обмена между программными процессами, используемыми для доступа пользователей к виртуальным машинам, и иными программными процессами с использованием общих, разделяемых ресурсов.

10.8. Создание базовых образов виртуальных машин, используемых при реализации технологии виртуализации рабочих мест пользователей, рекомендуется реализовать в соответствии с ролевой моделью предоставления доступа.

10.9. При загрузке виртуальной машины всегда рекомендуется использовать соответствующий базовый образ виртуальной машины. Средствами гипервизора и (или) иными техническими средствами рекомендуется реализовать запрет сохранения изменений в базовом образе виртуальной машины, произведенных в процессе работы виртуальной машины.

10.10. При реализации технологии виртуализации рабочих мест пользователей для каждого пользователя рекомендуется единовременно обеспечивать возможность работы только с одной виртуальной машиной в каждом из контуров безопасности.

10.11. Техническими средствами рекомендуется исключить возможность доступа пользователей к нескольким разным экземплярам виртуальных машин, включенных в один контур безопасности, с использованием одних (общих) аутентификационных данных.

11. Рекомендации по мониторингу ИБ

11.1. Рекомендуется применять автоматизированные процедуры мониторинга ИБ, реализуемые:
- серверными компонентами виртуализации, в том числе гипервизором;
- ОС физического СВТ (хост-сервера), используемого для функционирования гипервизора;
- функциональными средствами ПО виртуальных машин;
- СЗИ, в том числе функционирующими в среде виртуализации.

11.2. Рекомендуется реализовать процедуры мониторинга ИБ, обеспечивающие выявление нарушений требований к обеспечению ИБ, установленных в организации БС РФ, связанных с:
- несанкционированными действиями эксплуатационного персонала при осуществлении управления и администрирования серверных компонентов виртуализации, СХД и АРМ пользователей;
- несанкционированными действиями пользователей при использовании АРМ и доступе к виртуальным машинам;
- несанкционированными действиями эксплуатационного персонала при выполнении операций с образами виртуальных машин и несанкционированным доступом пользователей к образам виртуальных машин;
- несанкционированными действиями по изменению настроек применяемых СЗИ;
- распределением ролей и полномочий эксплуатационного персонала.

11.3. Рекомендуется реализовать регламентированные процедуры автоматизированного контроля корректной работоспособности СЗИ, применяемых для реализации требований настоящего документа, в том числе СЗИ, функционирующих в среде виртуализации.

11.4. Рекомендуется организовать регистрацию и контроль событий и действий пользователей и персонала в СХД.

11.5. Обработку, анализ и хранение журналов (протоколов), связанных с обеспечением ИБ виртуальной среды, формируемых техническими средствами и используемых для цели мониторинга ИБ, в том числе журналов (протоколов) событий, определенных в пункте 8.7 настоящего документа, рекомендуется осуществлять на физическом СВТ, не являющемся частью СХД и обособленном от СВТ (хост-сервера), используемом для функционирования серверных компонентов виртуализации.

12. Рекомендации по составу ролей и разграничению полномочий эксплуатационного персонала

12.1. В организации БС РФ рекомендуется выделение следующих ролей эксплуатационного персонала:

12.1.1. Администратор виртуальных машин и администратор информационной безопасности (АИБ) виртуальных машин, выполняющие обязанности, предусмотренные для администраторов и АИБ АБС организации БС РФ, эксплуатируемых на виртуальных машинах.

Администратору виртуальных машин и АИБ виртуальных машин не рекомендуется иметь прав доступа:

- по управлению серверными компонентами виртуализации, в том числе гипервизором и физическим СВТ (хост-сервером), на котором он установлен, и СЗИ от несанкционированного доступа, используемыми для организации доступа к серверным компонентам виртуализации;
- по управлению СХД;
- к информации, хранимой в СХД;
- по управлению физическим сетевым оборудованием, используемым для разделения сегментов вычислительной сети в соответствии с требованиями, установленными в разделе 6 настоящих рекомендаций.

12.1.2. Администратор по управлению серверными компонентами виртуализации, выполняющий среди прочих обязанности по созданию виртуальных машин, управлению образами виртуальных машин на этапах их жизненно цикла.

Администратору по управлению серверными компонентами виртуализации не рекомендуется иметь прав доступа:

- предусмотренных для администратора виртуальных машин и АИБ виртуальных машин;
- по предоставлению доступа к виртуальным машинам, включая настройку виртуальных сегментов вычислительных сетей, в которых размещаются виртуальные машины, и настройку программно-аппаратных средств, используемых для сопоставления загружаемых образов виртуальных машин с предъявляемыми пользователями аппаратными идентификаторами;
- по управлению СЗИ от несанкционированного доступа, используемыми для организации доступа к серверным компонентам виртуализации;
- по управлению СХД;
- по управлению физическим сетевым оборудованием, используемым для разделения сегментов вычислительной сети в соответствии с требованиями, установленными в разделе 6 настоящих рекомендаций.

12.1.3. АИБ по управлению серверными компонентами виртуализации, выполняющий среди прочего следующие обязанности:

- по предоставлению доступа к виртуальным машинам, включая настройку виртуальных сегментов вычислительных сетей, в которых размещаются виртуальные машины, по настройке программно-аппаратных средств, используемых для сопоставления загружаемых образов виртуальных машин с предъявляемыми пользователями аппаратными идентификаторами;
- по контролю доступа и мониторингу событий и действий персонала в СХД;
- по управлению СЗИ от несанкционированного доступа, используемыми для организации доступа к серверным компонентам виртуализации;
- по управлению средствами защиты от воздействий вредоносного кода на уровне гипервизора;
- по настройке/обновлению сигнатурных баз средств защиты от воздействий вредоносного кода на уровне гипервизора;
- по применению групповых политик безопасности средств защиты от воздействий вредоносного кода на уровне гипервизора;
- по контролю отсутствия вредоносного кода;
- по просмотру журналов средств защиты от воздействий вредоносного кода на уровне гипервизора.

АИБ по управлению серверными компонентами виртуализации не рекомендуется иметь прав доступа:

- предусмотренных для администратора и АИБ автоматизированных систем организации БС РФ, эксплуатируемых на виртуальных машинах;
- по созданию виртуальных машин, управлению образами виртуальных машин на этапах их жизненного цикла;
- по управлению СХД;
- к информации, хранимой в СХД;
- по управлению физическим сетевым оборудованием, используемым для разделения сегментов вычислительной сети в соответствии с требованиями, установленными в разделе 6 настоящих рекомендаций.

12.1.4. Администратор СХД, выполняющий среди прочего обязанности по управлению СХД, включая управление оборудованием СХД и управление логическими разделами СХД.

Администратору СХД не рекомендуется иметь прав доступа:

– к информации, хранимой в СХД;
– предусмотренных для администраторов виртуальных машин и АИБ виртуальных машин;
– предусмотренных для администратора и АИБ по управлению серверными компонентами виртуализации;
– по управлению физическим сетевым оборудованием, используемым для разделения сегментов вычислительной сети в соответствии с требованиями, установленными в разделе 6 настоящих рекомендаций.

12.2. Не рекомендуется назначение двух или более ролей, указанных в пункте 12.1 настоящего документа, одному лицу.

12.3. Разделение полномочий администратора и АИБ виртуальных машин рекомендуется осуществлять в соответствии с требованиями, установленными в организации БС РФ для соответствующих контуров безопасности.

13. Рекомендации по обеспечению ИБ системы хранения данных

13.1. В СХД рекомендуется выделять отдельные логические разделы для каждого контура безопасности, в том числе:

– для контура безопасности ПТП – разделы для хранения образов виртуальных машин и разделы для хранения данных пользователей (далее – разделы ПТП);
– для контура безопасности ИСПДн – разделы для хранения образов виртуальных машин и разделы для хранения данных пользователей (далее – разделы ИСПДн);
– разделы для хранения данных гипервизора, разделы для хранения ПО, необходимого для функционирования гипервизора, и разделы для хранения базовых образов виртуальных машин (далее – системные разделы).

13.2. Доступ к СХД рекомендуется осуществлять только с использованием средства виртуализации (гипервизора), АРМ, используемых для выполнения задач управления и администрирования СХД, и технических средств, используемых для резервного копирования информации.

13.3. Контроль доступа к логическим разделам СХД рекомендуется организовывать с использованием технических средств следующим образом:

13.3.1. Доступ к разделам ПТП рекомендуется предоставлять только со стороны виртуальных машин, включенных в контур безопасности ПТП, и при необходимости системы резервного копирования.

13.3.2. Доступ к логическим разделам ИСПДн рекомендуется предоставлять со стороны виртуальных машин, включенных в контур безопасности ИСПДн, и при необходимости системы резервного копирования.

13.3.3. Доступ к логическим системным разделам рекомендуется предоставлять со стороны АРМ администраторов серверных компонентов виртуализации и АРМ администраторов СХД соответственно и при необходимости системы резервного копирования.

13.3.4. Рекомендуемым решением является применение сертифицированных сетевых технических средств для контроля доступа к логическим разделам СХД.

13.4. АРМ, используемые для выполнения задач управления и администрирования СХД, рекомендуется располагать в специально выделенном сегменте вычислительных сетей. Размещение в указанных сетевых сегментах СВТ, не связанных с выполнением задач управления и администрирования, не рекомендуется. Выполнение задач, связанных с управлением и администрированием СХД, с использованием иных АРМ, рекомендуется ограничивать сертифицированными сетевыми техническими средствами.

13.5. Для выполнения задач управления и администрирования СХД рекомендуется использование минимально необходимого и регламентированного набора ПО, установленного на СВТ, используемого для выполнения указанных задач. Для данных СВТ рекомендуется выполнять регламентированные процедуры контроля целостности ПО, в том числе выполняемые при загрузке указанного ПО. Установка средств, предназначенных для разработки и отладки ПО, на указанных СВТ не рекомендуется.

13.6. Для организации защищенного доступа к средствам управления и администрирования СХД рекомендуется использовать двухфакторную идентификацию, реализуемую СЗИ от несанкционированного доступа, прошедшими оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации.

Библиография

[1] NIST 800-125 Recommendations of the National Institute of Standards and Technology. Guide to Security for Full Virtualization Technologies.

Ключевые слова: банковская система Российской Федерации, технология виртуализации, гипервизор, виртуальная машина, образ виртуальной машины, система хранения данных, разделение потоков информации, изоляция виртуальных машин.