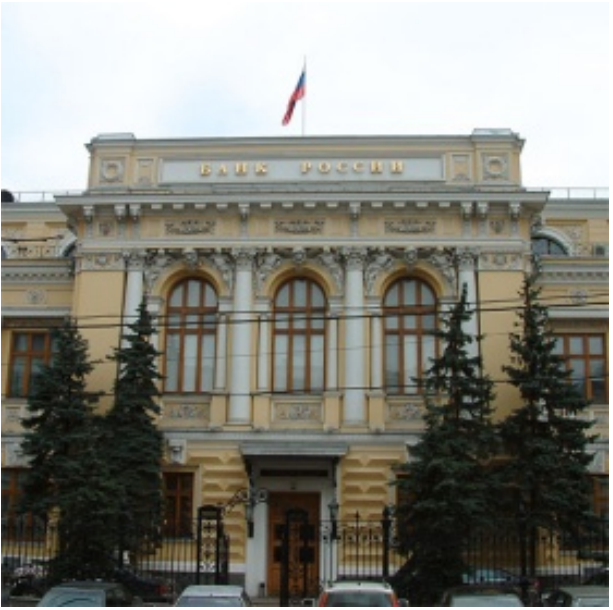
О вопросах обеспечения защиты информации при использовании технологии виртуализации



А.О. Выборнов

Начальник отдела методологии обеспечения безопасности информационных ресурсов Управления безопасности информационных банковских технологий

Главного управления безопасности и защиты информации Банка России

Использованные материалы

1. Требования к обеспечению информационной безопасности, установленные в нормативных актах Банка России

2. NIST Special Publication 800-125

Guide to security for Full Virtualization Technologies

3. PCI Data Security Standard

Information Supplement PCI DSS Virtualization Guidelines

Выделенные группы требований

Требования к разделению потоков информации и изоляции виртуальных машин

Требования к обеспечению информационной безопасности на этапах жизненного цикла образов виртуальных машин

Требования к обеспечению информационной безопасности при доступе к серверным компонентам средств виртуализации, в том числе при доступе к гипервизору

Требования к обеспечению информационной безопасности виртуальных машин

Требования к обеспечению информационной безопасности автоматизированных мест пользователей

Требования к мониторингу событий информационной безопасности

Требования к составу ролей и разграничению полномочий эксплуатационного персонала

Требования к обеспечению информационной безопасности при доступе к системе хранения данных

Требования к разделению потоков информации и изоляции виртуальных машин

Группа требований к разделению потоков информации и изоляции виртуальных машин применяются с целью обеспечения независимого выполнения банковских информационных и платежных технологических процессов

Принятие решения о возможности выполнения различных технологических процессов в рамках разных виртуальных машин на одном физическом оборудование

Определение порядка и технологии защиты информации при доступе с автоматизированных мест пользователей к виртуальным машинам

Контроль изоляции виртуальных машин средствами гипервизора (контроль использования оперативной памяти, контроль информационного обмена между виртуальными машинами, контроль корректного использования виртуальными машинами выделенных им ресурсов)

Контроль информационного обмена между виртуальными машинами (использование внешнего, сертифицированного физического оборудования)

Определения состава, порядка изоляции и порядка информационного обмена виртуальных сегментов вычислительных сетей, реализованных функциональными возможностями гипервизора

Требования к обеспечению информационной безопасности на этапах жизненного цикла образов виртуальных машин

Регламентация выполнения процесса жизненного цикла образов виртуальных машин

Реализация ролевого принципа при определении состава образов виртуальных мест пользователей

Размещение серверных компонент автоматизированных систем в отдельных образах и отдельных виртуальных машинах

Размещение общих (разделяемых) средств защиты информации в отдельных образах и отдельных виртуальных машинах

Реализация контроля целостности образов виртуальных машин, в том числе при запуске (загрузке) виртуальных машин

Контроль состава программного обеспечения образов виртуальных машин

Контроль настроек программных средств защиты информации, размещенных в образах виртуальных машин, контроль отсутствия вредоносного кода

Требования к обеспечению информационной безопасности на этапах жизненного цикла образов виртуальных машин

Регламентация обновления программного, размещенного в образах виртуальных машин

Регламентация и контроль возможности внесения пользователями изменений в образа виртуальных машин

Регламентация и контроль возможности копирования текущих образов виртуальных машин

Реализация учета образов виртуальных машин, а также регламентация процедур вывода из эксплуатации и удаления образов виртуальных машин

Требования к обеспечению информационной безопасности при доступе к серверным компонентам средств виртуализации

- Требования к обеспечению физического доступа к автоматизированным рабочим местам и консолям, используемым для управления серверными компонентами средств виртуализации
- Организация защищенного логического доступа к серверным компонентам средств виртуализации (выделение специализированных сегментов вычислительных сетей и использование двухфакторной аутентификации)
- Организация доступа к серверным компонентам средств виртуализации только посредством специализированного средства защиты, реализующего, среди прочего, контроль и протоколирования доступа эксплуатационного персонала, разделение полномочий эксплуатационного персонала в рамках принятой ролей модели. Размещение указанного средства на специально выделенном физическом средстве вычислительной техники
- Реализация контроля целостности и выполнения обновления программного обеспечения серверных компонент средств виртуализации, в том числе на этапе их загрузки

Требования к обеспечению информационной безопасности виртуальных машин

Регламентация процессов жизненного цикла виртуальных машин, контроль их исполнения

Реализация требований установленных внутренними документами (нормативными актами Банка России)

Реализация защиты от воздействия вредоносного кода

Контроль целостности программного обеспечения виртуальных машин

Контроль и регистрация доступа пользователей и эксплуатационного персонала к виртуальной машине

Обеспечение единого уровня обеспечения информационной безопасности виртуальных машин, размещенных на одном средстве вычислительной техники под управлением единого гипервизора

Требования к обеспечению информационной безопасности автоматизированных мест пользователей

Контроль конфигурации аппаратных и программных компонент автоматизированных рабочих мест пользователей, контроль использования портов ввода-вывода информации

Контроль целостности программного обеспечения автоматизированных мест пользователей, в том числе на этапе загрузки операционной системы (доверенная загрузка программного обеспечения)

Использование аппаратных средств для загрузки виртуальных машин

Реализация контроля информационного обмена между программными процессами, используемыми для реализации технологии виртуализации рабочих мест и иными программными процессами автоматизированных рабочих мест пользователей

Размещение автоматизированных мест пользователей в отдельных сегментах вычислительных сетей, регламентация и контроль разделения указанных сегментов и информационного обмена между указанными сегментами с использованием физического сетевого оборудования

Требования к мониторингу событий информационной безопасности

Регламентация процедур мониторинга и контроля:

- эксплуатационного персонала при осуществлении доступа к серверным компонентам средств виртуализации, в первую очередь при осуществлении доступа к гипервизору;
- пользователей, в соответствии с установленными требованиями (требования, установленных нормативными актами Банка России)

Мониторинг реализуется путем использования функциональных возможностей:

- серверных компонент средств виртуализации, в первую очередь средств гипервизора;
- операционной системы физического средства вычислительной техники, используемого для функционирования гипервизора
- применяемых средств защиты информации, в первую очередь средств защиты информации, применяемых для контроля доступа к серверным компонентам средств виртуализации

Требования к составу ролей и разграничению полномочий эксплуатационного персонала

Реализация принципа разделения полномочий, выделение следующих категорий ролей эксплуатационного персонала, обладающих непересекающимися полномочиями:

- администратор и администратор информационной безопасности виртуальных машин (выполняют обязанности, предусмотренные эксплуатационной документацией на автоматизированные системы, размещенные на виртуальных машинах)
- администратор управления серверными компонентами средств виртуализации (создание виртуальных машин, управление образами виртуальных машин на этапах их жизненного цикла)
- администратор информационной безопасности серверных компонент средств виртуализации (предоставление доступа к виртуальным машинам, управление средствами защиты от несанкционированного доступа к серверным компонентам средств виртуализации)
- администратор средств хранения данных (создание логических разделов, предоставление доступа к логическим разделам)

Требования при осуществлении доступа к системе хранения данных

Выделение отдельных логических разделов для хранения:

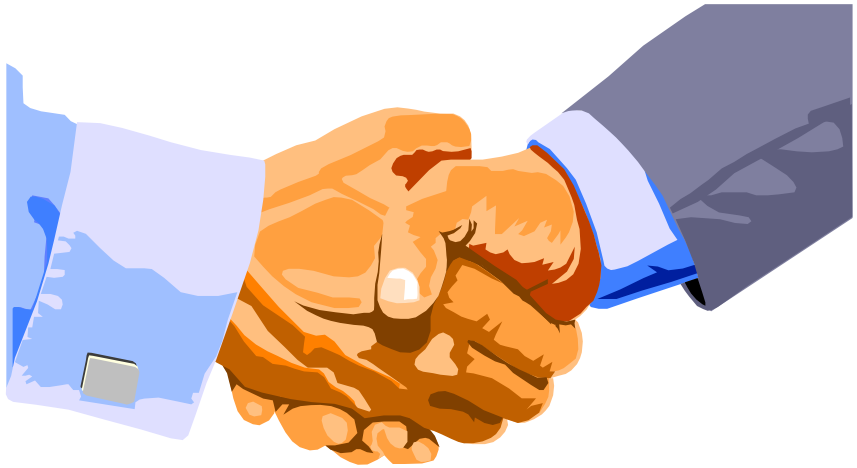
- эталонных образов виртуальных машин
- данных виртуальных машин и данных пользователей для выделенных категорий (типов) информации
- данных гипервизора и программного обеспечения, необходимого для функционирования гипервизора

Определение целесообразности использования отдельных физических систем хранения данных для критичных банковских технологических процессов

Организация контроля доступа к логическим разделам средств хранения данных со стороны виртуальных машин и эксплуатационного персонала

Организация физического доступа к автоматизированным рабочим местам, используемым для выполнения задач управления и администрирования систем хранения данных

Организация защищенного логического доступа эксплуатационного персонала к серверным компонентам средств виртуализации (выделение специализированных сегментов вычислительных сетей и использование двухфакторной аутентификации)



Спасибо за внимание!

Выборнов Андрей Олегович
Начальник отдела методологии обеспечения
безопасности информационных ресурсов
Главного управления безопасности
и защиты информации Банка России