Приложение №10
к приказу УФИЦ РАН
от «___» _____20___г.
№ _____

ПОЛИТИКА
защиты среды виртуализации

1 Общие положения

1.1 Настоящая Политика определяет требования к обеспечению защиты среды виртуализации в информационной инфраструктуре УФИЦ РАН.

2 Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации

2.1 В информационной инфраструктуре обеспечивается идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации, в соответствии с Политикой идентификации и аутентификации.

2.2 При реализации мер по идентификации и аутентификации субъектов доступа и объектов доступа в виртуальной инфраструктуре обеспечиваются:

2.2.1 идентификация и аутентификация администраторов управления средствами виртуализации;

2.2.2 идентификация и аутентификация субъектов доступа при их локальном и удалённом обращении к объектам доступа в виртуальной инфраструктуре;

2.2.3 блокировка доступа к компонентам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;

2.2.4 защита аутентификационной информации субъектов доступа, хранящейся в компонентах виртуальной инфраструктуры от неправомерного доступа к ней, уничтожения или модифицирования;

2.2.5 защита аутентификационной информации в процессе ее ввода для аутентификации в виртуальной инфраструктуре от возможного использования лицами, не имеющими на это полномочий;

2.2.6 идентификация и аутентификация субъектов доступа при осуществлении ими попыток доступа к средствам управления параметрами аппаратного обеспечения виртуальной инфраструктуры.

3 Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин

3.1 В информационной инфраструктуре обеспечивается управление доступом субъектов доступа к объектам доступа, в том числе внутри виртуальных машин, в соответствии с Политикой управления доступом.

3.2 При реализации мер по управлению доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре обеспечиваются:

3.3 контроль доступа субъектов доступа к средствам управления компонентами виртуальной инфраструктуры;

3.4 контроль доступа субъектов доступа к файлам-образам виртуализированного программного обеспечения, виртуальных машин, файлам-образам, служебным данным, используемым для обеспечения работы виртуальных файловых систем, и иным служебным данным средств виртуальной среды;

3.5 управление доступом к виртуальному аппаратному обеспечению информационной системы, являющимся объектом доступа;

3.6 контроль запуска виртуальных машин на основе заданных оператором правил (режима запуска, типа используемого носителя и иных правил).

4 Регистрация событий безопасности в виртуальной инфраструктуре

4.1 В информационной инфраструктуре обеспечивается регистрация событий безопасности в виртуальной инфраструктуре в соответствии с Политикой регистрации событий безопасности.

4.2 При реализации мер по регистрации событий безопасности в виртуальной инфраструктуре дополнительно к событиям, установленным в Политике регистрации событий безопасности, подлежат регистрации следующие события:

4.2.1 запуск (завершение) работы компонентов виртуальной инфраструктуры;

4.2.2 доступ субъектов доступа к компонентам виртуальной инфраструктуры;

4.2.3 изменения в составе и конфигурации компонентов виртуальной инфраструктуры во время их запуска, функционирования и аппаратного отключения;

4.2.4 изменения правил разграничения доступа к компонентам виртуальной инфраструктуры.

5 Управление потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры

5.1 В информационной инфраструктуре осуществляется управление потоками информации между компонентами виртуальной инфраструктуры и по периметру виртуальной инфраструктуры в соответствии с Политикой управления доступом, Политикой защиты систем и каналов передачи данных.

5.2 При реализации мер по управлению потоками информации между компонентами виртуальной инфраструктуры обеспечиваются:

5.2.1 фильтрация сетевого трафика между компонентами виртуальной инфраструктуры, в том числе между внешними по отношению к серверу виртуализации сетями и внутренними по отношению к серверу виртуализации сетями, в том числе при УФИЦ РАН сетевого обмена с сетями связи общего пользования;

5.2.2 обеспечение доверенных канала, маршрута внутри виртуальной инфраструктуры между администратором, пользователем и средствами защиты информации (функциями безопасности);

5.2.3 контроль передачи служебных информационных сообщений, передаваемых в виртуальных сетях гипервизора, хостовой операционной системы, по составу, объёму и иным характеристикам;

5.2.4 отключение неиспользуемых сетевых протоколов компонентами виртуальной инфраструктуры гипервизора, хостовой операционной системы, виртуальной вычислительной сети;

5.2.5 обеспечение подлинности сетевых соединений (сеансов взаимодействия) внутри виртуальной инфраструктуры, в том числе для защиты от подмены сетевых устройств и сервисов;

5.2.6 обеспечение изоляции потоков данных, передаваемых и обрабатываемых компонентами виртуальной инфраструктуры (гипервизором, хостовой операционной системой) и сетевых потоков виртуальной вычислительной сети.

6 Контроль целостности виртуальной инфраструктуры и ее конфигураций

6.1 В информационной инфраструктуре обеспечивается контроль целостности компонентов виртуальной инфраструктуры в соответствии с Политикой обеспечения целостности.

6.2 При реализации мер по контролю целостности компонентов виртуальной инфраструктуры обеспечиваются:

6.2.1 контроль целостности компонентов, критически важных для функционирования хостовой операционной системы, гипервизора, гостевых операционных систем и (или) обеспечения безопасности обрабатываемой в них информации (загрузчика, системных файлов, библиотек операционной системы и иных компонентов);

6.2.2 контроль целостности состава и конфигурации виртуального оборудования; контроль целостности файлов, содержащих параметры настройки виртуализированного программного обеспечения и виртуальных машин;

6.2.3 контроль целостности файлов-образов виртуализированного программного обеспечения и виртуальных машин, файлов-образов, используемых для обеспечения работы виртуальных файловых систем (контроль файлов-образов должен проводиться во время, когда файлы-образы не задействованы).

6.3 В информационной системе обеспечивается контроль целостности резервных копий виртуальных машин (контейнеров).

7 Реализация и управление антивирусной защитой в виртуальной инфраструктуре

7.1 В информационной инфраструктуре обеспечиваются реализация и управление антивирусной защитой в виртуальной инфраструктуре в соответствии с Политикой антивирусной защиты.

7.2 При реализации соответствующих мер обеспечиваются:

7.2.1 проверка наличия вредоносных программ (вирусов) в хостовой операционной системе, включая контроль файловой системы, памяти, запущенных приложений и процессов;

7.2.2 проверка наличия вредоносных программ в гостевой операционной системе, в процессе ее функционирования, включая контроль файловой системы, памяти, запущенных приложений и процессов.