Приложение №12
к приказу УФИЦ РАН
от «___» _____20___г.
№ _____

ПОЛИТИКА
защиты систем и каналов передачи данных

1 Общие положения

1.1 Настоящая Политика определяет требования к обеспечению защиты систем, средств и каналов передачи данных в информационной инфраструктуре УФИЦ РАН.

2 Разделение в информационной инфраструктуре функций по управлению (администрированию) информационной инфраструктуры, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций

2.1 В информационной инфраструктуре обеспечено разделение функциональных возможностей по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации (функций безопасности) и функциональных возможностей пользователей по обработке информации в соответствии с Политикой управления доступом.

2.2 Функциональные возможности по управлению (администрированию) информационной системой и управлению (администрированию) системой защиты информации включают функции по управлению базами данных, прикладным программным обеспечением, телекоммуникационным оборудованием, рабочими станциями, серверами, средствами защиты информации и иные функции, требующие высоких привилегий.

2.3 Разделение функциональных возможностей обеспечивается на физическом и логическом уровне путем выделения части программно-технических средств информационной системы, реализующих функциональные возможности по управлению (администрированию) информационной системой и управлению (администрированию) системой защиты информации, в отдельный домен, использования различных автоматизированных рабочих мест и серверов, различных типов операционных систем, разных способов аутентификации, различных сетевых адресов, выделенных каналов управления.

3 Обеспечение защиты информации от раскрытия, модификации при ее передаче по каналам связи, имеющим выход за пределы контролируемой зоны

3.1 В УФИЦ РАН обеспечена защита информации от раскрытия, модификации при ее передаче по каналам связи, имеющим выход за пределы контролируемой зоны.

3.2 Защита информации обеспечивается путем защиты каналов связи от несанкционированного физического доступа (подключения) к ним и применения криптографической защиты информации (протоколы SSL, L2TP over IPSec).

4 Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации

4.1 В информационной инфраструктуре обеспечиваются доверенные маршруты передачи данных между администратором (пользователем) и средствами защиты информации.

4.2 В УФИЦ РАН определен перечень целей передачи данных, для которых требуется доверенный канал (маршрут).

4.3 Доверенный канал между пользователем и средствами защиты информации обеспечивается при удаленном и локальном доступе в информационную инфраструктуру (протоколы SSL, L2TP over IPSec).

5 Разбиение информационной инфраструктуры на сегменты и обеспечение защиты периметров сегментов информационной инфраструктуры

5.1 В УФИЦ РАН осуществляется разбиение информационной инфраструктуры на сегменты и обеспечивается защита периметров сегментов информационной инфраструктуры аппаратным средством межсетевого экранирования.

5.2 Сегментирование информационной инфраструктуры проводится с целью построения эшелонированной системы защиты информации путем построения сегментов на различных физических доменах и средах.

5.3 При сегментировании информационной системы обеспечивается защита периметров сегментов информационной системы в соответствии с Политикой управления доступом.

6 Защита периметра информационной инфраструктуры при ее взаимодействии с иными информационными инфраструктурами и информационно-телекоммуникационными сетями

6.1 В информационной инфраструктуре осуществляется защита периметра при ее взаимодействии с иными информационными инфраструктурами и информационно-телекоммуникационными сетями, предусматривающая:

6.1.1 управление (контроль) входящими в информационную инфраструктуру и исходящими из информационной инфраструктуры информационными потоками на физической и логической сегментах информационной инфраструктуры;

6.1.2 обеспечение взаимодействия информационной инфраструктуры и ее сегментов с иными информационными инфраструктурами и сетями только через сетевые интерфейсы, которые обеспечивают управление (контроль) информационными потоками с использованием средств защиты информации (управляемые (контролируемые) сетевые интерфейсы), установленных на физическом и логическом периметре информационной инфраструктуры и ее отдельных сегментов (маршрутизаторов, межсетевых экранов, коммутаторов, прокси-серверов, шлюзов безопасности, средств построения виртуальных частных сетей).