Приложение №1
к приказу УФИЦ РАН
от «___» _____20___г.
№ _____

ПОЛИТИКА
идентификации и аутентификации субъектов доступа и объектов доступа в информационной инфраструктуре УФИЦ РАН

1 Общие положения

1.1 Настоящая Политика регламентирует порядок и процедуры присвоения субъектам и объектам доступа уникального признака (идентификатора), сравнения предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, проверки принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности), а также организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) для информационной инфраструктуры УФИЦ РАН и контроль за действиями пользователей информационной инфраструктуры (далее – Пользователь) и обслуживающего персонала при работе с паролями.

2 Регламентация правил и процедур идентификации и аутентификации

2.1 В информационной инфраструктуре УФИЦ РАН обеспечивается идентификация и аутентификация пользователей.

2.2 В информационной инфраструктуре УФИЦ РАН обеспечивается идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных.

2.3 В информационной инфраструктуре УФИЦ РАН обеспечивается управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов.

2.4 В информационной инфраструктуре УФИЦ РАН обеспечивается управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации.

2.5 В информационной инфраструктуре УФИЦ РАН обеспечивается защита обратной связи при вводе аутентификационной информации.

3 Идентификация и аутентификация пользователей

3.1 При доступе в информационную инфраструктуру УФИЦ РАН осуществляется идентификация и аутентификация пользователей, и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей.

3.2 В качестве пользователей дополнительно рассматриваются должностные лица обладателя информации, заказчика, а также лица, привлекаемые на договорной основе для обеспечения функционирования информационной инфраструктуры УФИЦ РАН (ремонт, гарантийное обслуживание, регламентные и иные работы) в соответствии с организационно-распорядительными документами УФИЦ РАН и которым в информационной инфраструктуре также присвоены учетные записи.

3.3 Пользователи информационной инфраструктуры УФИЦ РАН однозначно идентифицируются и аутентифицируются для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации.

3.4 Аутентификация пользователя осуществляется с использованием паролей.

3.5 В информационной инфраструктуре обеспечена возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами.

4 Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных

4.1 В информационной инфраструктуре УФИЦ РАН до начала информационного взаимодействия (передачи защищаемой информации от устройства к устройству) осуществляется идентификация и аутентификация устройств (технических средств).

4.2 В УФИЦ РАН определен перечень типов устройств, используемых в информационной инфраструктуре и подлежащих идентификации и аутентификации до начала информационного взаимодействия.

4.3 Идентификация устройств в информационной инфраструктуре обеспечивается по логическим именам (имя устройства), IP-адресам и по MAC-адресам устройства или по комбинации.

4.4 Аутентификация устройств в информационной инфраструктуре обеспечивается с использованием соответствующих протоколов аутентификации и с применением криптографических методов защиты информации.

5 Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов

5.1 В УФИЦ РАН определено должностное лицо (администратор), ответственное за создание, присвоение и уничтожение идентификаторов пользователей и устройств.

5.2 Реализованы следующие функции управления идентификаторами пользователей и устройств в информационной инфраструктуре:

5.2.1 формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство;

5.2.2 присвоение идентификатора пользователю и (или) устройству;

5.2.3 предотвращение повторного использования идентификатора пользователя и (или) устройства в течение установленного Организацией периода времени;

5.2.4 блокирование идентификатора пользователя после установленного Организацией времени неиспользования.

6 Управление средствами аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации

6.1 В УФИЦ РАН определено должностное лицо (администратор), ответственное за хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации.

6.2 Реализованы следующие функции управления средствами аутентификации (аутентификационной информацией) пользователей и устройств в информационной инфраструктуре:

6.2.1 изменение аутентификационной информации (средств аутентификации), заданных их производителями и (или) используемых при внедрении системы защиты информационной инфраструктуры УФИЦ РАН;

6.2.2 выдача средств аутентификации пользователям;

6.2.3 генерация и выдача начальной аутентификационной информации (начальных значений средств аутентификации);

6.2.4 установление характеристик пароля: длина пароля не менее 8 символов, алфавит пароля не менее 8 символов, максимальное количество неуспешных попыток аутентификации до блокировки 5 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации 15 минут, смена паролей не более чем через 60 дней; пароль является комбинацией цифр, букв и специальных символов («@», «#», «$», «&», «*», «%»); пароль должен содержать по меньшей мере одну цифру, одну строчную букву, одну прописную букву, один специальный символ;

6.2.5 блокирование (прекращение действия) и замена утерянных, скомпрометированных или поврежденных средств аутентификации в случае увольнения сотрудника, перевода на другую должность;

6.2.6 назначение необходимых характеристик средств аутентификации (в том числе механизма пароля);

6.2.7 обновление аутентификационной информации (замена средств аутентификации) с периодичностью не более, чем через 60 дней;

6.2.8 защита аутентификационной информации от неправомерного доступа к ней и модифицирования.

6.3 Личный пароль пользователя не должен передаваться никому. Исключением является ситуация, когда необходимо использовать для нескольких пользователей одну учетную запись для организаций доступа к информационным ресурсам.

6.4 В случае компрометации личного пароля пользователя немедленно предпринимаются меры в зависимости от полномочий владельца скомпрометированного пароля:

6.4.1 внеплановая смена личного пароля или удаление учетной записи пользователя в информационной инфраструктуре в случае прекращения его полномочий (увольнение, переход на другую работу внутри УФИЦ РАН и т.п.) производится ответственным за управление (администрирование) подсистемой безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой;

6.4.2 внеплановая полная смена паролей всех пользователей производится в случае прекращения полномочий (увольнение, переход на другую работу внутри УФИЦ РАН и другие обстоятельства) ответственным за управление (администрирование) подсистемой безопасности и других работников, которым были предоставлены полномочия по управлению парольной защитой информационной инфраструктуры.

7 Защита обратной связи при вводе аутентификационной информации

7.1 В информационной инфраструктуре осуществляется защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий.

7.2 Защита обратной связи «система - субъект доступа» в процессе аутентификации обеспечивается исключением отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации.

7.3 Вводимые символы пароля отображаются условными знаками «*».

7.4 Защита аутентификационной информации при ее передаче по каналам связи осуществляется в соответствии с требованиями к защите информационной инфраструктуры.

8 Ответственность при УФИЦ РАН идентификации и аутентификации

8.1 Ответственность за реализацию правил идентификации и аутентификации субъектов доступа и объектов доступа в соответствии с требованиями настоящей Политики возлагается на ответственного за управление (администрирование) подсистемой безопасности.

8.2 Ответственность за поддержание установленного порядка и соблюдение требований настоящей Политики возлагается на ответственного за управление (администрирование) подсистемой безопасности.

8.3 Периодический контроль за выполнением всех требований настоящей Политики осуществляется Ответственным за обеспечение безопасности информационной инфраструктуры.