Приложение 2
к приказу УФИЦ РАН
от «___» _____20___г.
№ _____

ПОЛИТИКА
управления доступом субъектов доступа к объектам доступа
в информационной инфраструктуре УФИЦ РАН

1 Общие положения

1.1 Настоящая Политика определяет права и привилегии работников, допущенных к информационной инфраструктуре (далее – Пользователи), описывает разграничение доступа пользователей к объектам информационной инфраструктуры на основе совокупности правил разграничения доступа, установленных в УФИЦ РАН, а также контроль соблюдения этих правил.

2 Управление учетными записями пользователей

2.1 В УФИЦ РАН реализованы следующие функции управления учетными записями пользователей:

2.1.1 определены типы учетной записи (пользователя, системная, временная);

2.1.2 учетные записи разделены на группы администраторов и пользователей;

2.1.3 перед выдачей идентификатору пользователем ответственный за управление подсистемой безопасности проверяет необходимые приказы, должностные инструкции пользователя, прежде чем выдать идентификатор с определенным типом учетной записи;

2.1.4 при увольнении сотрудника учетные записи удаляются;

2.1.5 удаление временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в информационной инфраструктуре;

2.1.6 оповещение администратора, осуществляющего управление учетными записями пользователей, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях;

2.1.7 предоставление пользователям прав доступа к объектам доступа информационной инфраструктуры, основываясь на задачах, решаемых пользователями в информационной инфраструктуре;

2.1.8 в информационной инфраструктуре должно осуществляться автоматическое блокирование неактивных (неиспользуемых) учетных записей пользователей после 45 дней неиспользования.

2.2 Ответственным за управление доступом, назначение прав доступа назначается Ответственный за обеспечение безопасности информационной инфраструктуры.

3 Реализация модели управления доступом

3.1 В информационной инфраструктуре реализованы дискреционный и ролевой методы управления доступом, предусматривающие управление доступом субъектов доступа к объектам доступа следующего вида:

3.1.1 Дискреционный: на основе идентификационной информации субъекта и для каждого объекта доступа – списка, содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа;

3.1.2 ролевой: на основе ролей субъектов доступа (совокупность действий и обязанностей, связанных с определенным видом деятельности).

3.2 Типы доступа для каждого пользователя включают операции по чтению, записи, удалению, выполнению и иные операции, разрешенные к выполнению пользователем (группе пользователей) при доступе к объектам доступа.

3.3 Правила разграничения доступа реализуются на основе установленных УФИЦ РАН матриц доступа и обеспечивают управление доступом пользователей (групп пользователей) при входе в систему, доступе к техническим средствам, устройствам, объектам файловой системы, запускаемым и исполняемым модулям, объектам систем управления базами данных, объектам, создаваемым прикладным и специальным программным обеспечением, параметрам настройки средств защиты информации, информации о конфигурации системы защиты информации и иной информации о функционировании системы защиты информации, а также иным объектам доступа.

3.4 Разрешенные доступы до определенных ресурсов по отношению к конкретным лицам фиксируются в матрице доступа.

4 Управление информационными потоками между устройствами, сегментами информационной инфраструктуры

4.1 В УФИЦ РАН осуществляется управление информационными потоками при передаче информации между устройствами, сегментами в рамках информационной инфраструктуры, включающее:

4.1.1 фильтрацию информационных потоков в соответствии с правилами управления потоками, установленными в УФИЦ РАН;

4.1.2 разрешение передачи информации в информационной инфраструктуре только по ранее установленным безопасным каналам передачи данных;

4.2 Управление информационными потоками должно обеспечивать разрешенный (установленный УФИЦ РАН) маршрут прохождения информации между пользователями, устройствами, сегментами в рамках информационной инфраструктуры, а также при взаимодействии с сетью Интернет на основе правил управления информационными потоками, включающих контроль конфигурации информационной инфраструктуры, источника и получателя передаваемой информации, структуры передаваемой информации, характеристик информационных потоков и (или) канала связи (без анализа содержания информации).

4.3 Управление информационными потоками блокирует передачу защищаемой информации через сеть Интернет по незащищенным линиям связи, сетевые запросы и трафик, несанкционированно исходящие из информационной инфраструктуры и (или) входящие в информационную инфраструктуру.

5 Разделение полномочий (ролей) пользователей, администраторов

5.1 В УФИЦ РАН обеспечено разделение полномочий пользователей, администраторов безопасности и лиц, обеспечивающих функционирование информационной инфраструктуры, в соответствии с их должностными обязанностями, с фиксацией их полномочий в должностных инструкциях, а также санкционирование доступа к объектам доступа в соответствии с разделением полномочий.

5.2 Разделение полномочий указывается в матрице доступа.

5.3 В УФИЦ РАН обеспечено исключение наделения одного должностного лица полномочиями по обработке информации и полномочиями по администрированию информационной инфраструктуры и (или) ее системы защиты информации, контролю за обеспечением защищенности информации, обеспечению функционирования информационной инфраструктуры.

6 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной инфраструктуры

6.1. В УФИЦ РАН обеспечено назначение прав и привилегий пользователям и запускаемым от их имени процессам, администраторам и лицам, обеспечивающим функционирование информационной инфраструктуры, минимально необходимых для выполнения ими своих должностных обязанностей, и санкционирование доступа к объектам доступа в соответствии с минимально необходимыми правами и привилегиями.

6.2. Разделение полномочий происходит на основании матрицы доступа, указанной в Приложении.

7 Ограничение числа параллельных сеансов доступа

7.1 В информационной инфраструктуре обеспечивается ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной инфраструктуры и не превышает более одного.

8 Блокирование сеанса доступа в информационную инфраструктуру после установленного времени бездействия (неактивности) пользователя или по его запросу

8.1 В информационной инфраструктуре обеспечивается блокирование сеанса доступа пользователя после 15 минут неактивности в информационной инфраструктуре или по запросу пользователя.

8.2 При заблокированном сеансе осуществляется блокирование любых действий по доступу к информации и устройствам отображения, кроме необходимых для разблокирования сеанса.

8.3 Блокирование сеанса доступа пользователя в информационную инфраструктуру сохраняется до прохождения им повторной идентификации и аутентификации.

8.4 На мониторе после блокировки сеанса не отображается информация сеанса пользователя.

9 Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети

9.1 В УФИЦ РАН обеспечивается защита информации при доступе пользователей к объектам доступа информационной инфраструктуры через информационно-телекоммуникационные сети, в том числе сети связи общего пользования, с использованием стационарных и мобильных технических средств.

9.2 Защита удаленного доступа обеспечивается при всех видах доступа (беспроводной, проводной) и включает:

9.2.1 ограниченные виды удаленного доступа к объектам доступа информационной инфраструктуры:

9.2.1.1 через шлюз удаленных рабочих столов, обеспечивая защищенное соединение, с помощью протокола SSL, с сервером по RDP по нестандартному порту;

9.2.1.2 через VPN сервер по протоколу L2TP over IPSec.

9.2.2 предоставление удаленного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей в соответствии с матрицей доступа;

9.2.3 мониторинг и контроль удаленного доступа на предмет выявления несанкционированного удаленного доступа к объектам доступа информационной инфраструктуры;

9.2.4 применение криптографической защиты средствами службы сертификации Active Directory Certificate Services.

10 Регламентация и контроль использования в информационной инфраструктуре технологий беспроводного доступа

10.1 В УФИЦ РАН обеспечивается регламентация и контроль использования технологий беспроводного доступа пользователей к объектам доступа, направленные на защиту информации в информационной инфраструктуре.

10.2 Регламентация и контроль использования технологий беспроводного доступа включают:

10.2.1 ограничение на использование технологий беспроводного доступа в соответствии с задачами пользователей, для решения которых такой доступ необходим, и предоставление беспроводного доступа в соответствии с главой 2 настоящей Политики;

10.2.2 предоставление технологий беспроводного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей;

10.2.3 мониторинг и контроль применения технологий беспроводного доступа на предмет выявления несанкционированного использования технологий беспроводного доступа к объектам доступа информационной инфраструктуры.

10.3 Беспроводной доступ для администрирования информационной инфраструктуры и систем защиты информации запрещен;

10.4 Возможность изменения пользователем устройств и настроек беспроводного доступа исключена;

10.5 В случае выявления подключенного несанкционированного беспроводного устройства подключение блокируется в кратчайшие сроки.

11 Регламентация и контроль использования в информационной инфраструктуре мобильных технических средств

11.1 В УФИЦ РАН обеспечивается регламентация и контроль использования мобильных технических средств, направленные на защиту информации в информационной инфраструктуре;

11.2 В качестве мобильных технических средств рассматриваются съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства), портативные вычислительные устройства и устройства связи с возможностью обработки информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные устройства);

11.3 Регламентация и контроль использования мобильных технических средств включают:

11.3.1 установление видов доступа (беспроводной, проводной), разрешенных для доступа к объектам информационной инфраструктуры с использованием мобильных технических средств, входящих в состав информационной инфраструктуры;

11.3.2 ограничение на использование мобильных технических средств в соответствии с задачами пользователя, для решения которых использование таких средств необходимо, и предоставление доступа с использованием мобильных технических средств в соответствии с главой 2 настоящей Политики;

11.3.3 мониторинг и контроль применения мобильных технических средств на предмет выявления несанкционированного использования мобильных технических средств для доступа к информационной инфраструктуре;

11.3.4 обеспечение очистки машинного носителя информации мобильного технического средства, переустановка программного обеспечения и выполнение иных мер по защите информации мобильных технических средств, после их использования за пределами УФИЦ РАН.

12 Управление взаимодействием с информационными инфраструктурами сторонних организаций

12.1 В УФИЦ РАН обеспечивается управление взаимодействием с внешними информационными инфраструктурами сторонних организаций, с которыми установлено информационное взаимодействие на основании заключенного договора (соглашения), а также с иными информационными инфраструктурами, информационное взаимодействие с которыми необходимо для функционирования информационной инфраструктуры УФИЦ РАН.

12.2 Управление взаимодействием с внешними информационными инфраструктурами включает в себя:

12.2.1 предоставление доступа к информационной инфраструктуре только авторизованным пользователям в соответствии с главой 2 настоящей Политики;

12.2.2 определение типов прикладного программного обеспечения информационной инфраструктуры, к которым разрешен доступ авторизованным пользователям из внешних информационных инфраструктур;

12.2.3 определение системных учетных записей, используемых в рамках данного взаимодействия;

12.2.4 определение порядка предоставления доступа к информационной инфраструктуре авторизованными пользователями из внешних информационных инфраструктур;

12.2.5 определение порядка обработки, хранения и передачи информации с использованием внешних информационных инфраструктур.

13 Обеспечение доверенной загрузки средств вычислительной техники

13.1 В информационной инфраструктуре обеспечивается исключение несанкционированного доступа к программным и (или) техническим ресурсам средства вычислительной техники на этапе его загрузки.

13.2 Доверенная загрузка обеспечивает:

13.2.1 блокирование попыток несанкционированной загрузки нештатной операционной системы (среды) или недоступность информационных ресурсов для чтения или модификации в случае загрузки нештатной операционной системы;

13.2.2 контроль доступа пользователей к процессу загрузки операционной системы;

13.2.3 контроль целостности программного обеспечения и аппаратных компонентов средств вычислительной техники.

13.3 В информационной инфраструктуре обеспечение доверенной загрузки на уровне базовой системы ввода-вывода осуществляется путем установления пароля на BIOS, опечатывания средств вычислительной техники УФИЦ РАН и контролируемой зоны для исключения несанкционированного физического доступа к средствам вычислительной техники.

ПРИЛОЖЕНИЕ

Должность	Active Directory	Kaspersky Security Center	Управление удаленным доступом (Выдача клиентов VPN)	Резервное копирование данных	Zabbix	Администрирование серверов	Администрирование сетевого оборудования	Другие должностные обязанности
Ответственный за обеспечение безопасности информационной инфраструктуры	ЧЗМП							
Пользователи, работающие в информационной инфраструктуре	ЧЗМП							
Пользователи, обеспечивающие функционирование информационной инфраструктуры	ЧЗМП							
Лица, ответственные за управление подсистемами безопасности информационной инфраструктуры	ЧЗМПА							
Лица, ответственные за выявление компьютерных инцидентов и реагирование на них	ЧЗМП							
Лица, которым разрешены действия по внесению изменений в конфигурацию информационной инфраструктуры и ее подсистем безопасности	ЧЗМПА							

Ч — чтение
З — запись
А — администрирование
М — модификация
П — передача