Приложение № 15
к приказу УФИЦ РАН
от «___» _____20___г.
№ _____

ИНСТРУКЦИЯ
ответственного за обеспечение безопасности
информационной инфраструктуры УФИЦ РАН

1. Общие положения

1.1. Назначение документа

Определяет основные обязанности, права и ответственность Ответственного за обеспечение безопасности информационной инфраструктуры УФИЦ РАН. Документ направлен на обеспечение работоспособности средств вычислительной техники и системы защиты информации в информационной инфраструктуре.

1.2. Вводимые определения терминов, сокращений и ролей

Таблица 1. Перечень сокращений

Сокращение	Расшифровка сокращения
ИИ	Информационная инфраструктура
АРМ	Автоматизированное рабочее место пользователя
ИБ	Информационная безопасность
НСД	Несанкционированный доступ
ПО	Программное обеспечение
СВТ	Средства вычислительной техники
СЗИ	Система защиты информации

Таблица 2. Перечень ролей

Наименование роли	Описание роли
Ответственный за обеспечение безопасности ИИ	Работник, обеспечивающий контроль работоспособности информационной инфраструктуры, безопасности информации, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники в информационной инфраструктуре
Пользователь	Работник, который в силу своих должностных обязанностей выполняет работы в информационной инфраструктуре

2. Содержание инструкции

2.1. Основные положения

Ответственный за обеспечение безопасности ИИ назначается приказом Руководителя УФИЦ РАН и функционально подчиняется непосредственному руководителю структурного подразделения, в штате которого он состоит.

Ответственный за обеспечение безопасности ИИ руководствуется требованиями законодательства Российской Федерации, настоящей Инструкции и иных внутренних нормативных и распорядительных документов УФИЦ РАН.

Ответственный за обеспечение безопасности ИИ в пределах своих должностных обязанностей осуществляет организацию защиты информационной инфраструктуры, назначает ответственных за обеспечение отдельных функций безопасности информационной инфраструктуры.

Ответственный за обеспечение безопасности ИИ обязан, в случае прекращения (отстранения от) исполнения обязанностей по работе с информационной инфраструктурой, все носители защищаемой информации (рукописи, черновики, чертежи, диски, дискеты, распечатки с принтеров, модели, материалы, изделия и пр.), которые находились в его распоряжении в связи с выполнением им должностных обязанностей во время работы в информационной инфраструктуре, передать непосредственному руководителю структурного подразделения, в штате которого он состоит, с оформлением двустороннего акта приема-передачи.

2.2. Обязанности Ответственного

Ответственный за обеспечение безопасности ИИ обязан:

- Знать перечень установленных в ИИ средств вычислительной техники и перечень задач, решаемых с их использованием;
- Участвовать в разработке и исполнении плана работ по обеспечению безопасности информации в ИИ;
- Участвовать в проведении служебных расследований фактов нарушения или угрозы нарушения безопасности защищаемой информации;
- Участвовать в разработке внутренних документов, связанных с функционированием СВТ и применением средств защиты информации, выполнением мероприятий по обеспечению защиты информации;
- Создавать, присваивать, уничтожать идентификаторы пользователей и устройств;
- Выдавать, инициализировать, хранить, блокировать средства аутентификации;
- Регулярно анализировать работу любых элементов информационной инфраструктуры, электронных системных журналов средств защиты для выявления и устранения неисправностей, а также для оптимизации ее функционирования;
- Выявлять недостатки по обеспечению безопасности ИИ по результатам исполнения плана;
- Подготавливать рекомендации по устранению недостатков в обеспечении безопасности ИИ и включению дополнительных мероприятий в план работ обеспечению безопасности ИИ на следующий период;

- Устанавливать и настраивать средства защиты информации в соответствии с инструкцией по эксплуатации средств защиты информации в ИИ или организовывать такую установку;
- Проводить мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них;
- Выявлять и устранять уязвимости в информационной инфраструктуре;
- Выполнять своевременное обновление программного обеспечения элементов ИИ и системы защиты по мере появления таких обновлений или организовывать обновление;
- Контролировать выполнение резервного копирования и восстановления данных.
- Осуществлять контроль над работой Пользователей, вести работу по выявлению попыток НСД к защищаемым информационным ресурсам и техническим средствам ИИ;
- Осуществлять настройку средств защиты, выполнять другие действия по изменению элементов ИИ;
- Поддержание установленного порядка и соблюдение требований Политик УФИЦ РАН;
- Осуществлять учет всех защищаемых носителей информации с использованием уникального, неизменяемого серийного номера устройства и/или нанесением не удаляемой маркировки (гравировка) на корпус устройства и с занесением учетных данных в специальный журнал (учетную карточку). Осуществлять контроль работы средств и систем защиты информации;
- На машинные носители маркировать информацию о возможности использования машинного носителя информации вне информационной системы;
- Осуществлять текущий контроль технологического процесса обработки защищаемой информации;
- Периодически осуществлять тестирование всех функций системы защиты с помощью тестовых программ, имитирующих попытки НСД, при изменении программной среды и персонала УФИЦ РАН;
- Обновление базы «черных» («белых») списков и контроль целостности базы «черных» («белых») списков, реагирование на поступление незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы;
- Участвовать в разработке внутренних документов, связанных с функционированием СВТ и применением средств защиты информации, выполнением мероприятий по обеспечению защиты информации;
- Регулярно анализировать работу любых элементов информационной инфраструктуры, электронных системных журналов средств защиты для выявления и устранения неисправностей, а также для оптимизации ее функционирования;
- Анализировать потенциальное воздействие планируемых изменений в конфигурации информационной инфраструктуры и системы защиты на обеспечение защиты ИИ;
- Документировать изменения в конфигурации системы защиты ИИ;
- Обеспечивать защиту архивных файлов, параметров настройки средств защиты информации и программного обеспечения, иных данных, не подлежащих изменению в процессе обработки информации;
- Сегментирование информационной инфраструктуры и поддержание защиты периметров сегментов информационной инфраструктуры;

- Контролировать входящие в информационную инфраструктуру и исходящие из информационной инфраструктуры информационные потоки на физических и логических сегментах информационной инфраструктуры;
- Должна обеспечиваться защита информации при ее передаче по каналам связи, имеющим выход за пределы контролируемой зоны, путем применения криптографических методов;

3. Ответственность за неисполнение (ненадлежащее исполнение) настоящей Инструкции

Ответственный за обеспечение безопасности ИИ несет ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных трудовым договором, настоящей Инструкцией, другими внутренними документами УФИЦ РАН, в соответствии с трудовым законодательством Российской Федерации.

С инструкцией ознакомлен: Ответственный за обеспечение безопасности ИИ

_____

(должность, ФИО, подпись)