Приложение №7
к приказу УФИЦ РАН
от «___» _____20___г.
№ _____

ПОЛИТИКА
контроля и анализа защищенности

1 Общие положения

1.1 Настоящая Политика определяет требования к контролю и анализу защищенности информационной инфраструктуры УФИЦ РАН для анализа и устранения уязвимостей.

2 Выявление, анализ и устранение уязвимостей

2.1 В УФИЦ РАН осуществляются выявление (поиск), анализ и устранение уязвимостей в информационной инфраструктуре.

2.2 При выявлении (поиске), анализе и устранении уязвимостей в информационной инфраструктуре должны проводиться:

2.2.1 выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении средств защиты информации, правильностью установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректностью работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;

2.2.2 разработка по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению;

2.2.3 анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации; устранение выявленных уязвимостей, в том числе путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств;

2.2.4 информирование должностных лиц (пользователей, администраторов, подразделения по защите информации) о результатах поиска уязвимостей и оценки достаточности реализованных мер защиты информации.

2.3 В качестве источников информации об уязвимостях используются опубликованные данные разработчиков средств защиты информации, общесистемного, прикладного и специального программного обеспечения, технических средств, а также другие базы данных уязвимостей.

2.4 Выявление (поиск), анализ и устранение уязвимостей должны проводиться на этапах создания и эксплуатации информационной инфраструктуры. На этапе эксплуатации поиск и анализ уязвимостей проводится с постоянной периодичностью. При этом в обязательном порядке для критических уязвимостей проводится поиск и анализ уязвимостей в случае опубликования в общедоступных источниках информации о новых уязвимостях в

средствах защиты информации, технических средствах и программном обеспечении, применяемом в информационной инфраструктуре.

2.5 В случае невозможности устранения выявленных уязвимостей путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств необходимо предпринять действия (настройки средств защиты информации, изменение режима и порядка использования информационной инфраструктуры), направленные на устранение возможности использования выявленных уязвимостей.

2.6 Ответственное лицо должно получать и устанавливать обновления базы признаков уязвимостей только из доверенных источников.

3 Контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации

3.1 В УФИЦ РАН осуществляется контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.

3.2 В УФИЦ РАН осуществляется получение из доверенных источников и установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.

3.3 При контроле установки обновлений осуществляются проверки соответствия версий общесистемного, прикладного и специального программного (микропрограммного) обеспечения, включая программное обеспечение средств защиты информации, установленного в информационной инфраструктуре и выпущенного разработчиком, а также наличие отметок в эксплуатационной документации (формуляр или паспорт) об установке (применении) обновлений.

3.4 Контроль установки обновлений проводится с постоянной периодичностью.

3.5 При контроле установки обновлений осуществляются проверки установки обновлений баз данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной защиты в соответствии с главой 3 Политики антивирусной защиты, баз признаков уязвимостей средств анализа защищенности и иных баз данных, необходимых для реализации функций безопасности средств защиты информации.

4 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации

4.1 В УФИЦ РАН проводится контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации.

4.2 При контроле работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации осуществляется:

4.2.1 контроль работоспособности (неотключения) программного обеспечения и средств защиты информации;

4.2.2 проверка правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) программного обеспечения и средств защиты информации;

4.2.3 контроль соответствия настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации;

4.2.4 восстановление работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов.

4.3 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации проводится с постоянной периодичностью.

5 Контроль состава технических средств, программного обеспечения и средств защиты информации

5.1 В УФИЦ РАН должен проводиться контроль состава технических средств, программного обеспечения и средств защиты информации, применяемых в информационной инфраструктуре (инвентаризация).

5.2 При контроле состава технических средств, программного обеспечения и средств защиты информации осуществляется:

5.2.1 контроль соответствия состава технических средств, программного обеспечения и средств защиты информации приведенному в эксплуатационной документации с целью поддержания актуальной конфигурации информационной инфраструктуры и принятие мер, направленных на устранение выявленных недостатков;

5.2.2 контроль состава технических средств, программного обеспечения и средств защиты информации на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков;

5.2.3 контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;

5.2.4 исключение (восстановление) из состава информационной инфраструктуры несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

5.3 Контроль состава технических средств, программного обеспечения и средств защиты информации проводится с постоянной периодичностью.