Приложение №5
к приказу УФИЦ РАН
от «___» _____20___г.
№ _____

ПОЛИТИКА
регистрации событий безопасности

1 Общие положения

1.1 Настоящая Политика регламентирует порядок регистрации событий безопасности информационной инфраструктуры в УФИЦ РАН.

2 Определение событий безопасности, подлежащих регистрации, и сроков их хранения

2.1 В УФИЦ РАН определены следующие события безопасности в информационной инфраструктуре, подлежащие регистрации, и сроки их хранения:

2.1.1 вход (выход), а также попытки входа субъектов доступа в информационную инфраструктуру и загрузки операционной системы;

2.1.2 подключение машинных носителей информации и вывод информации на носители информации;

2.1.3 запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации;

2.1.4 попытки доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;

2.1.5 попытки удаленного доступа;

2.1.6 события, связанные с изменением привилегий учетных записей;

3 Определение состава и содержания информации о событиях безопасности, подлежащих регистрации

3.1 В УФИЦ РАН определены следующие состав и содержание информации о событиях безопасности, подлежащих регистрации:

3.1.1 при регистрации входа (выхода) субъектов доступа в информационную инфраструктуру и загрузки операционной системы состав и содержание информации включают дату и время входа (выхода) в систему (из системы) или загрузки операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа;

3.1.2 при регистрации подключения машинных носителей информации и вывода информации на носители информации состав и содержание регистрационных записей включают дату и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации;

3.1.3 при регистрации запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации состав и содержание регистрационных записей, включают дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный);

3.1.4 при регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам состав и содержание регистрационных записей включают дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип);

3.1.5 при регистрации попыток удаленного доступа к информационной инфраструктуре состав и содержание информации включают дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной инфраструктуре.

4 Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения

4.1 В УФИЦ РАН осуществляется сбор, запись и хранение информации о событиях безопасности в течение 6 месяцев средством Zabbix.

4.2 Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения предусматривает следующее:

4.2.1 возможность выбора администратором безопасности событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности определенных в соответствии с главой 2 настоящей Политики;

4.2.2 генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с главой 2 настоящей Политики с составом и содержанием информации, определенными в соответствии с главой 3 настоящей Политики;

4.2.3 хранение информации о событиях безопасности в течение времени, установленного в соответствии с главой 2 настоящей Политики.

4.3 Объем памяти для хранения информации о событиях безопасности должен быть рассчитан и выделен с учетом типов событий безопасности, подлежащих регистрации в соответствии с главой 2 настоящей Политики, составом и содержанием информации о событиях безопасности, подлежащих регистрации, в соответствии с главой 3 настоящей Политики, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности в соответствии с главой 2 настоящей Политики.

5 Реагирование на сбои при регистрации событий безопасности

5.1 В информационной инфраструктуре осуществляется реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости)

памяти.

5.2 Реагирование на сбои при регистрации событий безопасности предусматривает:

5.2.1 предупреждение (сигнализация, индикация) администраторов о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности;

5.2.2 реагирование на сбои при регистрации событий безопасности путем изменения администраторами параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов информационной инфраструктуры, запись поверх устаревших хранимых записей событий безопасности.

6 Мониторинг результатов регистрации событий безопасности и реагирование на них

6.1 В УФИЦ РАН осуществляется мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них.

6.2 Мониторинг (просмотр и анализ) событий безопасности проводится для всех событий, подлежащих регистрации в соответствии с главой 2 настоящей Политики, и с периодичностью, обеспечивающей своевременное выявление признаков инцидентов безопасности в информационной инфраструктуре.

6.3 В случае выявление признаков инцидентов безопасности в информационной инфраструктуре осуществляется планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности.

7 Защита информации о событиях безопасности

7.1 В информационной инфраструктуре обеспечивается защита информации о событиях безопасности средствами Kaspersky Endpoint Security.

7.2 Защита информации о событиях безопасности обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, и в том числе включает защиту средств ведения регистрации настроек механизмов регистрации событий.

7.3 Доступ к записям аудита и функциям управления механизмами регистрации предоставляется только уполномоченным должностным лицам.