

УТВЕРЖДАЮ
Директор
ГБПОУ РК «РКИГ»
_____ **Пальчук М. И.**

_____ **202**__ г.

Инструкция
о регистрации информации о событиях безопасности
в информационной системе персональных данных
обмена информацией с ИСПДн центра обработки данных ФГБУ ФЦТ

Настоящий перечень мер определяет требования по защите информации о событиях безопасности в информационной системе персональных данных обмена информацией с ИСПДн центра обработки данных ФГБУ ФЦТ (далее - ИСПДн ОИ ФЦТ).

События безопасности, подлежащие регистрации в ИСПДн ОИ ФЦТ, определяются с учетом способов реализации угроз безопасности информации. К событиям безопасности, подлежащим регистрации в ИСПДн ОИ ФЦТ, отнесены любые проявления состояния информационной системы и ее системы защиты информации, указывающие на возможность нарушения конфиденциальности, целостности или доступности информации, доступности компонентов ИСПДн ОИ ФЦТ, нарушения процедур, установленных организационно-распорядительными документами по защите информации ИСПДн ОИ ФЦТ, а также нарушения штатного функционирования средств защиты информации.

В ИСПДн ОИ ФЦТ определены следующие события безопасности, подлежащие регистрации:

1. События, связанные с регистрацией входа (выхода) субъектов доступа в ИСПДн ОИ ФЦТ 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;

2. События, связанные с регистрацией подключения машинных носителей информации и вывода информации на носители информации. Состав и содержание регистрационных записей включает: 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. События, связанные с регистрацией запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации. Состав и содержание регистрационных записей включает: дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный);

4. События, связанные с регистрацией попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. Состав и содержание регистрационных записей включает: дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип);

5. События, связанные с регистрацией попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей). Состав и содержание информации должны включать: дату и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого объекта доступа (логическое имя (номер));

6. События, связанные с регистрацией запланированного обновления антивирусных баз. Состав и содержание информации должны включать дату и время обновления;

7. События, связанные с регистрацией запланированного обновления ОС Windows, ведутся в журнале самой ОС. Состав и содержание информации должны, включать дату и время обновления, состав обновления.

События безопасности, подлежащие регистрации в ИСПДн ОИ ФЦТ, и сроки хранения соответствующих записей регистрационных журналов, обеспечивают возможность обнаружения, идентификации и анализа инцидентов, возникших в ИСПДн ОИ ФЦТ.

Также подлежат регистрации события безопасности, связанные с применением выбранных мер по защите информации в ИСПДн ОИ ФЦТ.

Перечень событий безопасности, регистрация которых осуществляется в текущий момент времени, определяется Администратором безопасности, исходя из возможностей реализации угроз безопасности информации.

Срок хранения информации о зарегистрированных событиях безопасности должен составлять не менее трех месяцев, если иное не установлено требованиями законодательства Российской Федерации.

Защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, определенных в соответствии с методическими документами, и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

Доступ к записям аудита и функциям управления механизмами регистрации (аудита) предоставляется только Администратору безопасности ИСПДн ОИ ФЦТ.

В ИСПДн ОИ ФЦТ для обеспечения защиты информации о событиях безопасности, перед установкой СЗИ осуществляется синхронизация системного времени и даты. Администратор безопасности осуществляет контроль неизменности установленного системного времени и проводит периодическую проверку журналов регистрации событий, для контроля правильности отображения временных меток.

Сбор, запись и хранение информации о событиях безопасности осуществляется с помощью встроенных средств операционной системы Windows и установленных СЗИ.

В целях предотвращения сбоя при регистрации событий безопасности СЗИ и операционной системы в ИСПДн ОИ ФЦТ:

1. Администратору безопасности ИСПДн ОИ ФЦТ необходимо еженедельно проверять журналы регистрации событий СЗИ и операционной системы на наполненность и, в случае необходимости, производить их архивацию;
2. Увеличить при необходимости объём выделяемой под журналы событий безопасности СЗИ и операционной системы памяти;
3. Включить автоматическую перезапись новых событий безопасности поверх устаревших для предотвращения возникновения ошибок переполнения журналов;
4. Настройки прав учетных записей пользователей ИСПДн ОИ ФЦТ должны исключать возможность внесения пользователями изменений в журналы событий безопасности, настройки СЗИ и операционной системы.
5. При появлении в ИСПДн ОИ ФЦТ ошибок операционной системы или СЗИ пользователю необходимо уведомить администратора безопасности и приостановить работу до устранения ошибки.

Ведущий специалист по защите информации

А. О. Грибенников