Минобрнауки России
Федеральное государственное бюджетное научное учреждение
«Федеральный исследовательский центр
Институт прикладной физики Российской академии наук»
(ИПФ РАН)

П Р И К А З

11.09.2020 г. № 149 а/х

Нижний Новгород

**Об утверждении регламента реагирования
на инциденты информационной безопасности
в информационных системах персональных данных**

Во исполнение требований Федерального закона №152-ФЗ от 27.07.2006 г.
«О персональных данных» и прочих нормативных документов по защите информации

П Р И К А З Ы В А Ю:

1. Утвердить прилагаемый Регламент реагирования на инциденты информационной безопасности в информационных системах персональных данных Федерального государственного бюджетного научного учреждения «Федеральный исследовательский центр Институт прикладной физики Российской академии наук» (далее – Регламент).

2. Требования прилагаемого Регламента довести до работников, непосредственно осуществляющих защиту персональных данных в информационных системах персональных данных Федерального государственного бюджетного научного учреждения «Федеральный исследовательский центр Институт прикладной физики Российской академии наук».

3. Контроль за исполнением настоящего приказа оставляю за собой.

Директор
член-корреспондент РАН Г.Г.Денисов

Приложение № 1 к приказу
от 11.09.2020 г. № 149 а/х

РЕГЛАМЕНТ
реагирования на инциденты информационной безопасности в информационных системах персональных данных Федерального государственного бюджетного научного учреждения «Федеральный исследовательский центр Институт прикладной физики Российской академии наук»

1. Общие положения

1.1 Настоящая Регламент реагирования на инциденты информационной безопасности (далее – Регламент) в информационных системах персональных данных Федерального государственного бюджетного научного учреждения «Федеральный исследовательский центр Институт прикладной физики Российской академии наук» (далее – ИПФ РАН), разработан в соответствии с законодательством Российской Федерации в области защиты информации.

1.2 Настоящий Регламент определяет:

- порядок регистрации событий безопасности;
- порядок выявления инцидентов информационной безопасности и реагированию на них;
- порядок проведения анализа инцидентов информационной безопасности, в том числе определение источников и причин возникновения инцидентов.

1.3 Инцидент информационной безопасности - одно событие или группа событий, которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности информации.

1.4 Настоящий Регламент вступает в силу с момента его утверждения директора ИПФ РАН и действует бессрочно, до замены его новым Регламентом.

1.5 Все изменения в Регламент вносятся приказом директора ИПФ РАН.

1.6 Регламент обязателен для исполнения всеми работниками организации, непосредственно осуществляющими защиту персональных данных в информационных системах персональных данных.

2. Порядок регистрации событий безопасности

2.1 Регистрация событий безопасности в информационных системах персональных данных, осуществляется в следующей последовательности:

1) Определение событий безопасности, подлежащих регистрации, и сроков их хранения.
2) Определение состава и содержания информации о событиях безопасности, подлежащих регистрации.
3) Сбор, запись и хранение информации о событиях безопасности
4) Реагирование на сбои при регистрации событий безопасности
5) Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
6) Генерирование временных меток и (или) синхронизация системного времени в информационных системах персональных данных
7) Защита информации о событиях безопасности

2.2 Определение событий безопасности, подлежащих регистрации, и сроков их хранения.

2.2.1 События безопасности, подлежащие регистрации в информационных системах персональных данных, должны определяться с учетом способов реализации угроз безопасности для информационной системы. К событиям безопасности, подлежащим регистрации в информационных системах персональных данных, должны быть отнесены любые проявления состояния информационной системы и ее системы защиты персональных данных, указывающие

на возможность нарушения конфиденциальности, целостности или доступности персональных данных, доступности компонентов информационной системы, нарушения процедур, установленных организационно-распорядительными документами по защите персональных данных, а также на нарушение штатного функционирования средств защиты информации.

2.2.2 События безопасности, подлежащие регистрации в информационных системах персональных данных, и сроки их хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов информационной безопасности, возникших в информационной системе.

2.2.3 В информационных системах персональных данных подлежат регистрации следующие события:

- вход (выход), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы;
- подключение съемных машинных носителей персональных данных и вывод персональных данных на съемные машинные носители;
- запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой персональных данных;
- попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;
- попытки удаленного доступа.

2.3 Определение состава и содержания информации о событиях безопасности, подлежащих регистрации.

2.3.1 Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны, как минимум, обеспечить возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъекта доступа (пользователя и (или) процесса), связанного с данным событием безопасности.

2.3.2 При регистрации входа (выхода) субъектов доступа в информационную систему персональных данных и загрузки (останова) операционной системы состав и содержание информации должны, как минимум, включать дату и время входа (выхода) в систему (из системы) или загрузки (останова) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.

2.3.3 При регистрации подключения съемных машинных носителей персональных данных и вывода персональных данных на съемные носители состав и содержание регистрационных записей должны, как минимум, включать дату и время подключения съемных машинных носителей персональных данных и вывода персональных данных на съемные носители, логическое имя (номер) подключаемого съемного машинного носителя персональных данных, идентификатор субъекта доступа, осуществляющего вывод персональных данных на съемный носитель персональных данных.

2.3.4 При регистрации запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой персональных данных состав и содержание регистрационных записей должны, как минимум, включать дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).

2.3.5 При регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам состав и содержание регистрационных записей должны, как минимум, включать дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип).

2.3.6 При регистрации 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, как минимум, 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).

2.3.7 При регистрации попыток удаленного доступа к информационной системе персональных данных состав и содержание информации должны, как минимум, включать 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 системе персональных данных.

2.4 Сбор, запись и хранение информации о событиях безопасности

2.4.1 Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения должен предусматривать:

- возможность выбора ответственным за защиту информации и (или) администратором информационной системы персональных данных событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности, определенных в пункте 2.2.3 настоящего Регламента;
- генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с составом и содержанием информации, определенными в соответствии с пунктами 2.3.2 – 2.3.7 настоящего Регламента;
- хранение информации о событиях безопасности в течение времени, установленного в пункте 2.2.2 настоящего Регламента.

2.4.2 Объем памяти для хранения информации о событиях безопасности должен быть рассчитан и выделен с учетом типов событий безопасности, подлежащих регистрации в соответствии с составом и содержанием информации о событиях безопасности, подлежащих регистрации, в соответствии с пунктами 2.3.2 – 2.3.7 настоящего Регламента, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности.

2.5 Реагирование на сбои при регистрации событий безопасности

2.5.1 В информационных системах персональных данных должно осуществляться 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.

2.5.2 Реагирование на сбои при регистрации событий безопасности должно предусматривать:

- предупреждение (сигнализация, индикация) о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности;
- реагирование на сбои при регистрации событий безопасности путем изменения ответственным за защиту информации и (или) администратором информационной системы персональных данных параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов информационной системы, запись поверх устаревших хранимых записей событий безопасности.

2.6 Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них

2.6.1 Мониторинг (просмотр и анализ) записей регистрации (аудита) должен проводиться для всех событий, подлежащих регистрации в соответствии и с периодичностью, установленной оператором, и обеспечивающей своевременное выявление признаков инцидентов информационной безопасности в информационных системах персональных данных.

2.6.2 В случае выявление признаков инцидентов информационной безопасности в информационных системах персональных данных осуществляется планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности в соответствии с Порядком проведения разбирательств по фактам возникновения инцидентов в информационной системе.

2.7 Генерирование временных меток и (или) синхронизация системного времени в информационных системах персональных данных

2.7.1 Получение меток времени, включающих дату и время, используемых при генерации записей регистрации (аудита) событий безопасности в информационных системах персональных данных достигается посредством применения внутренних системных часов информационных систем.

2.8 Защита информации о событиях безопасности

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

2.8.2 Доступ к записям аудита и функциям управления механизмами регистрации (аудита) должен предоставляться только уполномоченным должностным лицам:

- ответственному за защиту информации;
- администратору информационных систем персональных данных.

3. Порядок выявления инцидентов информационной безопасности и реагирования на них

3.1 За выявление инцидентов информационной безопасности и реагирование на них отвечают:

- ответственный за защиту информации;
- администратор информационных систем персональных данных.

3.2 Работники организации, должны сообщать ответственным за выявление инцидентов информационной безопасности, любые инциденты, в которые входят:

- факты попыток и успешной реализации несанкционированного доступа в системы обработки персональных данных, в помещения обработки персональных данных и к хранилищам персональных данных;
- факты сбоя или некорректной работы систем обработки персональных данных;
- факты сбоя или некорректной работы средств защиты информации;
- факты разглашения персональных данных;
- факты разглашения информации о методах и способах защиты и обработки персональных данных.

3.3 Все нештатные ситуаций, факты вскрытия и опечатывания технических средств, выполнения профилактических работ, установки и модификации аппаратных и программных средств обработки персональных данных в информационных системах персональных данных должны быть занесены ответственными за выявление инцидентов информационной безопасности в "Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания технических средств, выполнения профилактических работ, установки и модификации аппаратных и программных средств обработки персональных данных в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики Российской академии наук» " (Приложение 1).

3.4 Анализ инцидентов информационной безопасности, в том числе определение источников и причин возникновения инцидентов, осуществляется согласно Порядку проведения разбирательств по фактам возникновения инцидентов информационной безопасности в информационных системах персональных данных.

3.5 Меры по устранению последствий инцидентов информационной безопасности, планированию и принятию мер по предотвращению повторного возникновения инцидентов, возлагаются на ответственных за выявление инцидентов.

4. Порядок проведения разбирательств по фактам возникновения инцидентов информационной безопасности

4.1 Для проведения разбирательств по фактам возникновения инцидентов информационной безопасности создаётся комиссия, состоящая не менее чем из трех человек с обязательным включением в её состав:

- ответственного за защиту информации;
- администратора информационных систем персональных данных.

4.2 Председатель комиссии организует работу комиссии, решает вопросы взаимодействия комиссии с руководителями и работниками структурных подразделений организации, готовит и ведёт заседания комиссии, подписывает протоколы заседаний. По окончании работы комиссии готовится заключение по результатам проведённого разбирательства, которое передается на рассмотрение директору ИПФ РАН.

4.3 При проведении разбирательства устанавливаются:

- наличие самого факта совершения инцидента информационной безопасности, служащего основанием для вынесения соответствующего решения;
- время, место и обстоятельства возникновения инцидента, а также оценка его последствий;
- конкретный работник, совершивший инцидент информационной безопасности или повлекший своими действиями возникновения инцидента;
- наличие и степень вины работника, совершившего инцидент информационной безопасности или повлекшего своими действиями возникновения инцидента;
- цели и мотивы, способствовавшие совершению инцидента информационной безопасности.

4.4 В целях проведения разбирательства все работники обязаны по первому требованию членов комиссии предъявить для проверки все числящиеся за ними материалы и документы, дать устные или письменные объяснения об известных им фактах по существу заданных им вопросов.

4.5 Работник, совершивший инцидент информационной безопасности или повлекший своими действиями возникновения инцидента, обязан по требованию комиссии представить объяснения в письменной форме не позднее трех рабочих дней с момента получения соответствующего требования. Комиссия вправе поставить перед работником перечень вопросов, на которые работник обязан ответить. В случае отказа работника от письменных объяснений, комиссией составляется акт.

4.6 Работник имеет право, по согласованию с председателем комиссии, знакомиться с материалами разбирательства, касающимися лично его, и давать по поводу них свои комментарии, предоставлять дополнительную информацию и документы. По окончании разбирательства работнику для ознакомления предоставляется итоговый акт с выводами комиссии.

4.7 В случае давления на работника со стороны других лиц (не из состава комиссии) в виде просьб, угроз, шантажа и др., по вопросам, связанным с проведением разбирательства, работник обязан сообщить об этом председателю комиссии.

4.8 До окончания работы комиссии и вынесения решения членам комиссии запрещается разглашать сведения о ходе проведения разбирательства и ставшие известные им обстоятельства.

4.9 В процессе проведения разбирательства комиссией выясняются:

- перечень разглашенных сведений;
- причины разглашения информации ограниченного доступа;
- лица, виновные в разглашении информации ограниченного доступа;
- размер (экспертную оценку) причиненного ущерба;
- недостатки и нарушения, допущенные работниками при работе с персональными данными;
- иные обстоятельства, необходимые для определения причин разглашения персональных данных, степени виновности отдельных лиц, возможности применения к ним мер воздействия.

4.10 По завершении разбирательства комиссией составляется заключение. В заключении указываются:

- основание для проведения в разбирательства;
- состав комиссии и время проведения разбирательства;
- сведения о времени, месте и обстоятельствах возникновения инцидента информационной безопасности;
- сведения о работнике, совершившем инцидент информационной безопасности или повлекшем своими действиями возникновения инцидента (должность, фамилия, имя, отчество, год рождения, время работы в учреждении, а также в занимаемая должность);
- цели и мотивы работника, способствовавшие совершению инцидента информационной безопасности;
- причины и условия возникновения инцидента информационной безопасности;
- данные о характере и размерах причиненного в результате инцидента ущерба;
- предложения о мере ответственности работника, совершившего инцидент информационной безопасности или повлекшего своими действиями возникновения инцидента.

4.11 На основании заключения выносится решение о применении мер ответственности к работнику совершившему инцидент или повлекшему своими действиями возникновению инцидента, также о возмещении ущерба виновным работником (или его законным представителем), которое доводится до указанного работника в письменной форме под расписку.

4.12 Все материалы разбирательства относятся к информации ограниченного доступа и хранятся в течение 5 лет. Копии заключения и распоряжения по результатам разбирательства приобщаются к личному делу работника, в отношении которого оно проводилось.

Приложение 1
к Регламенту реагирования на инциденты информационной безопасности в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики Российской академии наук»

Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания технических средств, выполнения профилактических работ, установки и модификации аппаратных и программных средств обработки персональных данных в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики Российской академии наук»

Начат: "___" _____ 20__г.

Окончен: "___" _____ 20__г.

На _____ листах

Инв. № _____

№ п/п	Дата	Краткое описание выполненной работы (нештатной ситуации)	ФИО ответственного за защиту информации, подпись	ФИО администратора информационной системы, подпись	Примечание
1	2	3	4	5	6