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

П Р И К А З

06.08.2020 г. № 135 а/х

Нижний Новгород

Об утверждении инструкции ответственного за защиту информации

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 прилагаемую Инструкцию ответственного за защиту информации в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики Российской академии наук» (далее – Инструкция).
2. Ответственному за защиту информации Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики Российской академии наук» в рамках своей деятельности руководствоваться прилагаемой Инструкцией.
3. Требования настоящего приказа довести до ответственного за защиту информации в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики Российской академии наук».
4. Контроль за исполнением настоящего приказа оставляю за собой.

Директор
член-корреспондент РАН Г.Г.Денисов

Приложение № 1 к приказу
от «06» __08__ 2020 г. № 135 а/х

ИНСТРУКЦИЯ
ответственного за защиту информации в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики Российской академии наук»

Общие положения

1.1 Настоящая инструкция определяет функции, обязанности и права ответственного за защиту информации (далее – Ответственный) в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики Российской академии наук» (далее – ИПФ РАН).

1.2 Ответственный назначается приказом директора ИПФ РАН.

1.3 Настоящая инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности сведений конфиденциального характера, и не исключает обязательного выполнения их требований.

1. Функции

2.1 Ответственный выполняет следующие функции:

1) Управляет системами защиты персональных данных информационных систем персональных данных:

- управляет средствами защиты информации;
- восстанавливает работоспособность средств защиты информации;
- устанавливает обновления программного обеспечения средств защиты информации, выпускаемых разработчиками (производителями) средств защиты информации или по их поручению;
- анализирует события в информационных системах персональных данных, связанные с защитой персональных данных (события безопасности);
- информирует пользователей об угрозах безопасности персональных данных;
- информирует пользователей о правилах эксплуатации средств защиты информации;
- обучает пользователей работе со средствами защиты информации;
- управляет доступом к съемным машинным носителям персональных данных (определяет должностные лица, имеющие доступ к съемным машинным носителям персональных данных);
- управляет полномочиями пользователей информационной системы персональных данных;
- сопровождает функционирование системы защиты персональных данных в ходе эксплуатации информационной системы персональных данных;
- поддерживает конфигурацию информационной системы персональных данных и конфигурацию системы защиты персональных данных (структуру системы защиты персональных данных, состава, мест установки и параметров настройки средств защиты информации, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на систему защиты персональных данных; информационной системы персональных данных;
- управляет изменениями базовой конфигурации информационных систем персональных данных и систем защиты персональных данных, в том числе:
  - определяет типы возможных изменений,
  - разрешает или отказывает во внесении изменений,
  - документирует действия по внесению изменений,

- хранит данные об изменениях.

2) Выявляет инциденты (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационных систем персональных данных и (или) к возникновению угроз безопасности персональных данных (далее по тексту - инциденты), и реагирует на них:

- обнаруживает и идентифицирует инциденты, в том числе:
  - отказы в обслуживании,
  - сбои (перезагрузки) в работе средств защиты информации,
  - нарушения правил разграничения доступа,
  - неправомерные действия по сбору информации,
  - иные события, приводящие к возникновению инцидентов;
- анализирует инциденты, в том числе определяет источники и причины возникновения инцидентов, а также оценивает их последствия;
- планирует меры по устранению инцидентов, в том числе:
  - по восстановлению информационной системы и ее сегментов в случае отказа в обслуживании или после сбоев,
  - устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;
- планирует и принимает меры по предотвращению повторного возникновения инцидентов.

3) Контролирует обеспечение уровня защищенности персональных данных, обрабатываемых в информационных системах персональных данных:

- контролирует события безопасности и действия пользователей в информационных системах персональных данных;
- контролирует (анализирует) защищенность персональных данных;
- контролирует перемещение съемных машинных носителей персональных данных за пределы контролируемой зоны лицами, которым оно необходимо для выполнения своих должностных обязанностей (функции);
- анализирует и оценивает функционирование системы защиты персональных данных информационной системы персональных данных, включая выявление, анализ и устранение недостатков в функционировании системы защиты персональных данных информационной системы персональных данных;
- выполняет периодический анализ изменения угроз безопасности персональных данных в информационных системах персональных данных, возникающих в ходе их эксплуатации, и принятие мер защиты персональных данных в случае возникновения новых угроз безопасности персональных данных;
- документирует процедуры и результаты контроля (мониторинга) за обеспечением уровня защищенности персональных данных, обрабатываемых в информационных системах персональных данных;
- принимает решения по результатам контроля (мониторинга) за обеспечением уровня защищенности персональных данных о доработке (модернизации) системы защиты персональных данных информационной системы персональных данных.

4) Ведет учет:

- ведет учет используемых средств защиты информации в информационных системах персональных данных;
- ведет учет используемых шифровальных (криптографических) средств защиты информации в информационных системах персональных данных, эксплуатационной и технической документации к ним;
- ведет учет съемных машинных носителей персональных данных.

5) Обеспечивает защиту персональных данных при выводе из эксплуатации информационных систем персональных данных или после принятия решения об окончании обработки персональных данных:

- обеспечивает архивирование персональных данных, содержащихся в информационных системах персональных данных (архивирование должно осуществляться при необходимости дальнейшего использования персональных данных в деятельности оператора);
- обеспечивает уничтожение (стирание) персональных данных и остаточной информации со съемных машинных носителей персональных данных, при необходимости передачи съемного машинного носителя персональных данных другому пользователю или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения;
- при выводе из эксплуатации съемных машинных носителей персональных данных, на которых осуществлялись хранение и обработка персональных данных, осуществляет физическое уничтожение этих съемных машинных носителей персональных данных.

2. Права

3.1 Ответственный имеет право:

- требовать от работников – пользователей информационных систем персональных данных соблюдения установленной технологии обработки персональных данных и выполнения инструкций по обеспечению безопасности персональных данных;
- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты персональных данных, несанкционированного доступа к персональным данным, утраты и/или порчи персональных данных и технических средств, входящих в состав информационных систем персональных данных;
- требовать прекращения обработки персональных данных в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;
- участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа к персональным данным;
- подавать свои предложения по совершенствованию организационных и технических мер по защите персональных данных.

3. Ответственность

4.1 На ответственного за защиту информации возлагается персональная ответственность за качество проводимых им работ по обеспечению защиты персональных данных.

4.2 Сотрудник, ответственный за защиту информации несет ответственность по действующему законодательству за разглашение сведений ограниченного доступа, ставших известными ему по роду работы.