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. № 148 а/х

Нижний Новгород

Об утверждении инструкций по эксплуатации информационных систем персональных данных

Во исполнение Федерального закона Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», 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 Инструкцию пользователя по работе в информационных системах персональных данных в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики Российской академии наук» (Приложение 1).

2. Утвердить Инструкцию по организации парольной защиты в информационных системах персональных данных в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики Российской академии наук» (Приложение 2).

3. Утвердить Инструкцию по организации антивирусной защиты в информационных системах персональных данных в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики Российской академии наук» (Приложение 3).

4. Утвердить Инструкцию по организации обновления программного обеспечения и средств защиты информации в информационных системах персональных данных в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики Российской академии наук» (Приложение 4).

5. Утвердить Инструкцию о порядке организации резервирования и восстановления работоспособности программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных в Федеральном государственном бюджетном

научном учреждении «Федеральный исследовательский центр Институт прикладной физики Российской академии наук» (Приложение 5).

6. Требования настоящего приказа довести до работников, осуществляющих обработку персональных данных в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики Российской академии наук».

7. Контроль за исполнением настоящего приказа оставляю за собой.

Директор
член-корреспондент РАН  Г.Г. Денисов

Приложение № 1 к приказу
от 11.09. 2020 г. № 148 а/х

ИНСТРУКЦИЯ
пользователя по работе в информационных системах персональных данных в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики Российской академии наук»

1. Общие положения

1.1 Настоящая инструкция определяет обязанности, права и ответственность пользователей при работе в информационных системах персональных данных Федерального государственного бюджетного научного учреждения «Федеральный исследовательский центр Институт прикладной физики Российской академии наук» (далее по тексту - Информационная система).

1.2 Пользователь информационной системы персональных данных в своей работе руководствуется настоящей инструкцией.

1.3 Настоящая инструкция является дополнением к действующим нормативным документам по вопросам защиты информации, и не исключает обязательного выполнения их требований.

2. Обязанности

2.1 Пользователь обязан:

- знать и выполнять требования настоящей инструкции, а также действующих нормативных и руководящих документов регламентирующих порядок действий по защите информации;
- выполнять на автоматизированном рабочем месте только те процедуры, которые требуются для выполнения его должностных обязанностей;
- работать в сетях общего доступа и (или) международного обмена, только при служебной необходимости;
- соблюдать установленные правила разграничения доступа к информации, обрабатываемой в информационной системе персональных данных;
- покидая свое рабочее место на кратковременный срок блокировать доступ к операционной среде автоматизированного рабочего места;
- знать и выполнять правила работы со средствами защиты информации, установленными в информационной системе;
- немедленно ставить в известность ответственного за защиту информации в информационной системе и (или) администратора информационной системы персональных данных, об обнаруженных инцидентах, в которые входят:
  - факты попыток и успешной реализации несанкционированного доступа в системы обработки информации, в помещения обработки информации и к хранилищам информации;
  - факты сбоя или некорректной работы систем обработки информации;
  - факты сбоя или некорректной работы средств защиты информации;
  - факты разглашения информации, содержащей персональные данные;
  - факты разглашения информации о методах и способах защиты и обработки информации.

2.3 Пользователю категорически запрещается:

- разглашать сведения ограниченного доступа, ставшие известными ему по роду работы;
- производить действия в информационной системе персональных данных в обход процедур идентификации и аутентификации в операционной системе;
- использовать неучтенные внешние машинные носители информации;

- подключать к автоматизированному рабочему месту мобильные устройства;
- самостоятельно устанавливать или модифицировать программное и (или) аппаратное обеспечение информационной системы;
- отключать средства защиты информации;
- использовать компоненты программного и аппаратного обеспечения информационной системы персональных данных в неслужебных (личных) целях;
- оставлять автоматизированное рабочее место без присмотра, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры);
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к инцидентам информационной безопасности.

3. Ответственность

3.1 Пользователи информационной системы персональных данных несут ответственность по действующему законодательству за разглашение сведений ограниченного доступа, ставших известными им по роду работы.

Приложение № 2 к приказу
от 11.09. 2020 г. № 148 а/х

ИНСТРУКЦИЯ
по организации парольной защиты в информационных системах персональных данных в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики Российской академии наук»

4. Общие положения

1.1 Настоящая инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей пользователей информационных систем персональных данных Федерального государственного бюджетного научного учреждения «Федеральный исследовательский центр Институт прикладной физики Российской академии наук» (далее по тексту - Информационная система).

1.2 Пользователь информационной системы персональных данных в своей работе руководствуется настоящей инструкцией.

1.3 Настоящая инструкция является дополнением к действующим нормативным документам по вопросам защиты информации, и не исключает обязательного выполнения их требований.

5. Основные требования к парольной защите

2.1 Личные пароли доступа к автоматизированному рабочему месту из состава информационной системы персональных данных создаются пользователем самостоятельно.

2.2 Личные пароли доступа к автоматизированному рабочему месту из состава информационной системы персональных данных должны соответствовать следующим требованиям:

- длина пароля не менее 6 символов;
- алфавит пароля не менее 60 символов;
- максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток;
- блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 5 до 30 минут;
- смена паролей не более чем через 120 дней;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, даты рождения и т.д.), а также общепринятые сокращения (anonymous, user, пользователь и т.п.).

6. Правила использования паролей

3.1 Правила хранения парольной информации:

- запрещается записывать пароли на бумажные носители, в файл, в электронную записную книжку и другие носители информации, в том числе на предметы;
- запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

3.2 Правила ввода пароля:

- ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан;
- во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.3 Правила смены паролей:

– в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п., технологической необходимости использования имен и паролей сотрудников (исполнителей) в их отсутствие, пользователи обязаны сразу после исчерпания инцидента сменить пароль;

– внеплановая смена личного пароля или удаление учетной записи пользователя в случае прекращения его полномочий (увольнение, переход на другую работу внутри предприятия и т.п.) должна производиться немедленно после окончания последнего сеанса работы данного пользователя с системой;

– внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри предприятия и другие обстоятельства) администратора информационной системы персональных данных.

3.4 Владельцы паролей обязаны своевременно сообщать администратору информационной системы персональных данных об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

7. Ответственность

4.1 Ответственность за соблюдение пользователями правил настоящей инструкции возлагается на администратора информационной системы персональных данных.

4.2 Ответственность за хранение и ввод парольной информации возлагается персонально на владельца пароля.

4.3 Пользователи информационной системы персональных данных несут ответственность по действующему законодательству за разглашение сведений ограниченного доступа, ставших известными им по роду работы.

Приложение № 3 к приказу
от 11.09. 2020 г. № 148 а/х

ИНСТРУКЦИЯ
по организации антивирусной защиты в информационных системах персональных данных в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики Российской академии наук»

1.Общие положения

1.1 Настоящая инструкция определяет порядок применения средств антивирусной защиты в информационных системах персональных данных Федерального государственного бюджетного научного учреждения «Федеральный исследовательский центр Институт прикладной физики Российской академии наук» (далее по тексту - Информационная система).

1.2 Пользователь информационной системы персональных данных в своей работе руководствуется настоящей инструкцией.

1.3 Настоящая инструкция является дополнением к действующим нормативным документам по вопросам защиты информации, и не исключает обязательного выполнения их требований.

2. Порядок применения средств антивирусной защиты

2.1 Средства антивирусной защиты должны устанавливаться на всех средствах вычислительной техники, эксплуатируемых в информационной системе персональных данных.

2.2 Инсталляция и настройка средств антивирусной защиты информации осуществляются в соответствии с программной и эксплуатационной документацией, поставляемой в комплекте с ними.

2.3 Реализация антивирусной защиты должна предусматривать:

- проведение периодических проверок автоматизированных рабочих мест на наличие вредоносных компьютерных программ (вирусов);
- проверку в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съемных машинных носителей информации, сетевых подключений, в том числе к сетям общего пользования, и других внешних источников) при загрузке, открытии или исполнении таких файлов;
- оповещение в масштабе времени, близком к реальному, об обнаружении вредоносных компьютерных программ (вирусов);
- определение и выполнение действий по реагированию на обнаружение в информационной системе объектов, подвергшихся заражению вредоносными компьютерными программами (вирусами).

2.4 При резервном копировании информации, файлы, помещаемые в электронный архив, должны проходить антивирусный контроль с целью выявления вредоносных компьютерных программ.

3.Порядок обновлений баз данных признаков вредоносных компьютерных программ (вирусов)

3.1 Своевременное обновление баз данных средств антивирусной защиты является неотъемлемой частью обеспечения эффективной политики антивирусной защиты информации.

3.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов) производится один раз в сутки в автоматическом режиме.

3.3 Обновление базы данных признаков вредоносных компьютерных программ (вирусов) должно предусматривать:

- получение уведомлений о необходимости обновлений и непосредственном обновлении базы данных признаков вредоносных компьютерных программ (вирусов);

– получение из доверенных источников и установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов);

– контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов).

4.Обязанности пользователей средств антивирусной защиты

4.1 Пользователям запрещается:

– отключать средства антивирусной защиты во время работы;

– использовать средства антивирусной защиты, отличные от установленных средств;

– без разрешения копировать любые файлы, устанавливать и использовать любое программное обеспечение, не предназначенное для выполнения служебных задач.

4.2 Ввод информации с магнитных, оптических, магнитооптических и любых других съемных носителей информации неслужебного характера должен осуществляться пользователем только с разрешения ответственного за защиту информации в информационной системе.

5.Порядок действий по при обнаружении вирусов

5.1 В случае появления подозрений на наличие программных вирусов пользователи должны немедленно проинформировать об этом ответственного за защиту информации.

5.2 В случае обнаружения программных вирусов при входном контроле отчуждаемых носителей информации, файлов или почтовых сообщений, поступивших в формационной системе, пользователь должен:

– приостановить процесс приема-передачи информации;

– сообщить ответственному за защиту информации о факте обнаружения программного вируса;

– принять по согласованию с ответственным за защиту информации меры по локализации и удалению программного вируса с использованием средств антивирусной защиты информации;

– в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, передать зараженный вирусом файл в организацию, с которой заключен договор на антивирусную поддержку;

– по факту обнаружения зараженных вирусом файлов составить служебную записку, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

6.Ответственность

6.1 Ответственность за соблюдение пользователями правил настоящей инструкции возлагается на ответственного за защиту информации.

6.2 За нарушение требований настоящей Инструкции ответственный за защиту информации и пользователи несут ответственность, установленную действующим законодательством Российской Федерации и нормативными правовыми актами.

6.3 Пользователи информационной системы несут ответственность по действующему законодательству за разглашение сведений ограниченного доступа, ставших известными им по роду работы.

Приложение № 4 к приказу
от 11.09. 2020 г. № 148 а/х

ИНСТРУКЦИЯ
по организации обновления программного обеспечения и средств защиты информации в информационных системах персональных данных в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики Российской академии наук»

1.Общие положения

1.1 Настоящая инструкция регламентирует процессы обновления программного обеспечения и средств защиты информации в информационных системах персональных данных Федерального государственного бюджетного научного учреждения «Федеральный исследовательский центр Институт прикладной физики Российской академии наук» (далее по тексту - Информационная система).

1.2 Администратор информационной системы персональных данных в своей работе руководствуется настоящей инструкцией.

1.3 Настоящая инструкция является дополнением к действующим нормативным документам по вопросам защиты информации, и не исключает обязательного выполнения их требований.

2.Правила установки обновлений программного обеспечения

2.1 Установке обновлений должно предшествовать тестирование информационной инфраструктуры на отсутствие негативных воздействий от вновь устанавливаемых обновлений.

2.2 В случае обнаружения негативного воздействия устанавливаемого обновления на штатное функционирование информационной инфраструктуры, данное обновление устанавливаться не должно.

2.3 Установке новых версий программного обеспечения или внесению изменений и дополнений в действующее программное обеспечение должно предшествовать тестирование информационной инфраструктуры на отсутствие негативных воздействий указанного программного обеспечения.

2.4 Установка протестированных обновлений может быть произведена только администратором информационной системы на основании решения ответственного за защиту информации в информационной системе.

2.5 Установка новых версий программного обеспечения или внесение изменений и дополнений в действующее программного обеспечения может быть произведено только администратором информационной системы персональных данных на основании решения ответственного за защиту информации.

3.Ответственность

3.1 Ответственность за соблюдение пользователями правил настоящей инструкции возлагается на администратора информационной системы персональных данных.

3.2 Ответственность за организацию обновления программного обеспечения и средств защиты информации в информационной системе несут ответственный за защиту информации и администратор информационной системы персональных данных.

Приложение № 5 к приказу
от 11.09. 2020 г. № 148 а/х

ИНСТРУКЦИЯ
о порядке организации резервирования и восстановления работоспособности программного обеспечения, баз данных и средств защиты информации 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 инструкция регламентирует процессы организации резервирования и восстановления работоспособности программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных Федерального государственного бюджетного научного учреждения «Федеральный исследовательский центр Институт прикладной физики Российской академии наук» (далее по тексту - Информационная система).

1.2 Администратор информационной системы персональных данных в своей работе руководствуется настоящей инструкцией.

1.3 Настоящая инструкция является дополнением к действующим нормативным документам по вопросам защиты информации, и не исключает обязательного выполнения их требований.

2.Порядок организации резервирования и восстановления работоспособности программного обеспечения, баз данных и средств защиты информации

2.1 Резервирование программного обеспечения и баз данных выполняется администратором информационной системы персональных данных.

2.2 Резервирование средств защиты информации информационной системы выполняется ответственным за защиту информации.

2.3. Определяется 2 вида резервирования баз, данных:

- полное резервирование – резервное копирование всех данных;
- неполное резервирование– резервное копирование части данных.

2.4 Целью неполного резервирования является сохранение изменений в информационной системе с момента полного резервирования баз данных.

2.5 Периодичность проведения работ по резервированию баз данных должна составлять не менее 1 раза в месяц для полного резервирования и 1 раза в неделю для неполного резервирования.

2.6 Для организации резервирования и восстановления работоспособности программного обеспечения, должно быть обеспечено ведение двух копий программных средств и их периодическое обновление, и контроль работоспособности.

2.7 Для организации резервирования и восстановления работоспособности программного обеспечения, перед каждым обновлением программного обеспечения необходимо делать контрольную точку восстановления операционной системы.

2.8 При организации резервирования и восстановления работоспособности программного обеспечения сначала осуществляется резервное копирование баз данных, затем производится полная деинсталляция некорректно работающего программного обеспечения.

2.9 При восстановлении работоспособности средств защиты информации следует выполнить их настройку в соответствии с требованиями безопасности информации, изложенными в техническом задании на создание системы защиты информации.

3.Ответственность

3.1 Ответственность за проведение мероприятий по восстановлению программного обеспечения и баз данных возлагается на администратора информационной системы персональных данных.

3.2 Ответственность за проведение мероприятий по восстановлению средств защиты информации возлагается на ответственного за защиту информации.