УТВЕРЖДАЮ:
И.о.директора НИИ КПГПЗ
_____ О.Ю.Коротенко
01 сентября 2026 г.

ПОЛОЖЕНИЕ

об информационной безопасности

1. Общие положения

1.1. Настоящее Положение определяет цели, принципы и порядок обеспечения информационной безопасности в Федеральном государственном бюджетном научном учреждение «Научно - исследовательский институт комплексных проблем гигиены и профессиональных заболеваний» (далее – Организация).

1.2. Положение разработано в соответствии с требованиями действующего законодательства Российской Федерации.

1.3. Положение обязательно к исполнению всеми работниками Организации.

1.4. Целью обеспечения информационной безопасности является минимизация ущерба от угроз информационной безопасности.

1.5. Обеспечение информационной безопасности осуществляется по следующим направлениям:

- организационно-правовая защита – включает в себя законы, нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации и регламентирующие производственно-хозяйственную деятельность;
- инженерно-техническая защита – технические средства, препятствующие нанесению ущерба.

1.6. К объектам информационной безопасности относятся:

- информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера;
- информация, защита которой предусмотрена законодательными актами РФ, в том числе персональные данные;
- средства и системы информатизации, программные средства, автоматизированные системы управления, связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации с ограниченным доступом.

1.7. Система информационной безопасности направлена на предупреждение угроз, их своевременное выявление, обнаружение, локализацию и ликвидацию. Система информационной безопасности должна обеспечивать:

- конфиденциальность (защиту информации от несанкционированного раскрытия или перехвата);
- целостность (точность и полноту информации);
- доступность (возможность получения информации в пределах компетенции пользователей).

1.8. Организация вправе определять состав, объем и порядок защиты сведений конфиденциального характера и персональных данных, требовать от работников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз.

2. Защита информации

2.1. Защита информации в Организации представляет собой принятие правовых, организационных и технических мер, направленных:

- на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- соблюдение конфиденциальности информации ограниченного доступа;
- реализацию права на доступ к информации.

2.2. Организация как обладатель информации и/или оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязана обеспечить:

- предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- своевременное обнаружение фактов несанкционированного доступа к информации;
- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- постоянный контроль за обеспечением уровня защищенности информации;
- нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации;
- документирование доказательств неправомерного доступа к компьютерной информации, создания, использования и распространения вредоносных компьютерных программ, нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, нарушения правил защиты информации, незаконной деятельности в области защиты информации, разглашения информации с ограниченным доступом, воспрепятствования уверенной работе сайтов в сети Интернет, нарушения требований законодательства о хранении документов и информации, содержащейся в информационных системах;
- сопровождение исполнения заключенных Организацией договоров на закупку товаров, работ и услуг по темам развития и обеспечения защиты информации;

- ведение реестра приобретенных средств защиты информации;
- проведение служебных расследований по фактам нарушения требований защиты информации;
- взаимодействие с Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации по вопросам защиты информации в Организации;
- обеспечение устойчивости и адаптивности информационных систем;
- финансирование мероприятий по защите информации в Организации;
- закупка товаров, работ и услуг, направленных на обеспечение защиты информации.

2.3. Информация, полученная работниками Организации при исполнении ими профессиональных обязанностей или самой Организацией при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

2.4. Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда.

2.5. Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия Организации или лица, предоставившего такую информацию о себе.

2.6. Порядок доступа к персональным данным граждан устанавливается Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

2.7. Документирование информации осуществляется в соответствии с установленными правилами делопроизводства.

2.8. Право собственности и иные вещные права на материальные носители, содержащие документированную информацию, устанавливаются гражданским законодательством.

2.9. Защита государственной тайны, коммерческой тайны, конфиденциальной информации обеспечивается в соответствии с федеральным законодательством и принятыми локальными нормативно-правовыми актами.

3. Контроль доступа к информационным системам

3.1. Все работы в Организации выполняются в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию в Организации. Личные компьютеры и внешние носители информации (диски, дискеты, флеш-карты и т. п.) разрешено использовать только при согласовании с руководителем отдела защиты информации Организации.

Руководители подразделений должны периодически пересматривать права доступа своих работников и других пользователей к соответствующим информационным ресурсам.

3.2. Для обеспечения санкционированного доступа к информационному ресурсу вход в систему производится только с использованием уникального имени пользователя и пароля. Работники должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и

последующего использования. Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим, в том числе членам своей семьи и близким, если работа выполняется дома.

Работники обязаны постоянно использовать режим «Экранной заставки» с парольной защитой. Рекомендуется устанавливать максимальное время «простоя» компьютера до появления экранной заставки не дольше 15 минут.

3.3. Работники обязаны немедленно уведомлять руководителя отдела защиты информации обо всех случаях предоставления доступа третьим лицам к ресурсам корпоративной сети. Доступ третьих лиц к информационным системам Организации возможен только по согласованию с непосредственным руководителем.

3.4. Работникам, которые используют в работе портативные компьютеры Организации, может быть предоставлен удаленный доступ к сетевым ресурсам Организации в соответствии с правами в корпоративной информационной системе.

Работникам, работающим за пределами Организации с использованием компьютера, не принадлежащего Организации, запрещено копировать данные на компьютер, с которого осуществляется удаленный доступ.

Работники и третьи лица, имеющие право удаленного доступа к информационным ресурсам, должны соблюдать требование, исключающее одновременное подключение их компьютера к сети Организации и к каким-либо другим сетям, не принадлежащим Организации.

Все компьютеры, подключаемые посредством удаленного доступа к информационной сети, должны иметь программное обеспечение антивирусной защиты, имеющее последние обновления.

4. Доступ к сети Интернет

4.1. Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности.

4.2. Работникам запрещается использовать сеть Интернет в личных целях.

4.3. Работникам запрещается использовать сеть Интернет для хранения корпоративных данных.

4.4. Работа с интернет-ресурсами допускается только в режиме просмотра, исключая возможность передачи информации Организации в сеть Интернет.

4.5. Работникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем Организации.

4.6. Работники перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов.

4.7. Запрещен доступ в Интернет для лиц, не являющихся работниками Организации.

4.8. Работникам запрещается направлять партнерам конфиденциальную информацию Организации по электронной почте без использования систем шифрования. Строго конфиденциальная информация Организации ни при каких обстоятельствах не подлежит пересылке третьим лицам по электронной почте. Также запрещено использовать публичные почтовые ящики электронной почты для осуществления какого-либо из видов корпоративной деятельности.

4.9. Недопустимые действия и случаи использования электронной почты:

- рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;
- групповая рассылка всем работникам Организации сообщений/писем;
- рассылка рекламных материалов, не связанных с трудовой деятельностью;
- подписка на рассылку, участие в дискуссиях и подобные услуги, использующие значительные ресурсы электронной почты в личных целях;
- поиск и чтение сообщений, направленных другим лицам (независимо от способа их хранения);
- пересылка любых материалов, как сообщений, так и приложений, содержание которых является противозаконным, непристойным, злонамеренным, оскорбительным, угрожающим, клеветническим, злобным или способствует поведению, которое может рассматриваться как уголовное преступление или административный проступок либо приводит к возникновению гражданско-правовой ответственности, беспорядков или противоречит корпоративным стандартам в области этики.

4.10. Специалисты отдела защиты информации обеспечивают контроль содержания всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.

5. Защита оборудования

5.1. Работникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производят авторизованные специалисты Организации.

5.2. Каждый работник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности как в офисе, так и по месту проживания. В ситуациях, когда возрастает степень риска кражи портативных компьютеров, например в гостиницах, аэропортах, в офисах деловых партнеров и т. д., пользователи обязаны ни при каких обстоятельств не оставлять их без присмотра. Во время поездки в автомобиле портативный компьютер должен находиться в багажнике. На ночь его следует перенести из автомобиля в гостиничный номер.

5.3. Все компьютеры должны защищаться паролем при загрузке системы, активации по горячей клавише и после выхода из режима «Экранной заставки». Для установки режимов защиты пользователь должен обратиться в службу технической поддержки.

5.4. При записи информации на носитель для передачи его контрагентам или партнерам по бизнесу необходимо убедиться в том, что носитель чист и не содержит никаких иных данных. Простое переформатирование носителя не дает гарантии полного удаления записанной на нем информации.

5.5. Карманные персональные компьютеры, а также мобильные телефоны, имеющие функцию электронной почты, и прочие переносные устройства не относятся к числу устройств, имеющих надежные механизмы защиты данных. В подобном устройстве не рекомендуется хранить конфиденциальную информацию.

5.6. Порты передачи данных, в том числе FD- и CD-дисководы в стационарных компьютерах работников Организации блокируются, за исключением тех случаев, когда работником получено разрешение на запись информации у отдела защиты информации.

6. Программное обеспечение

6.1. Все программное обеспечение, установленное на предоставленном Организацией компьютерном оборудовании, является собственностью Организации и должно использоваться исключительно в производственных целях.

6.2. Работникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности. Если в ходе выполнения технического обслуживания будет обнаружено не разрешенное к установке программное обеспечение, оно будет удалено, а сообщение о нарушении будет направлено непосредственному руководителю работника и в отдел защиты информации.

6.3. Работникам запрещается:

- блокировать антивирусное программное обеспечение;
- устанавливать другое антивирусное программное обеспечение;
- изменять настройки и конфигурацию антивирусного программного обеспечения.

7. Управление сетью

7.1. Работники отдела информационных технологий и отдела защиты информации контролируют содержание всех потоков данных, проходящих через сеть Организации.

7.2. Работникам Организации запрещается:

- нарушать информационную безопасность и работу сети Организации;
- сканировать порты или систему безопасности;
- контролировать работу сети с перехватом данных;
- получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;
- использовать любые программы, скрипты, команды или передавать сообщения с целью вмешаться в работу или отключить пользователя оконечного устройства;
- передавать информацию о работниках или списки работников Организации посторонним лицам;
- создавать, обновлять или распространять компьютерные вирусы и прочее разрушительное программное обеспечение.

8. Организация защиты иных информационные ресурсов

8.1. В систему организации делопроизводства входит:

- учет всей документации Организации, в том числе и на электронных носителях, с классификацией по сфере применения, дате, содержанию;
- регистрация и учет всех входящих (исходящих) документов в соответствующих журналах информации о дате получения (отправления) документа, откуда поступил или куда отправлен, классификация (письмо, приказ, распоряжение и т. д.);
- регистрация документов, с которых делаются копии, в специальном журнале (дата копирования, количество копий, для кого или с какой целью производится копирование);
- особый режим уничтожения документов.

8.2. В ходе использования, передачи, копирования и исполнения документов работники Организации обязаны:

- все документы, независимо от грифа, передать исполнителю под роспись в журнале учета документов. Документы с грифом «Для служебного пользования» («Ограниченного пользования») хранить в служебных помещениях в запираемых и опечатываемых шкафах;
- выданные для работы дела и документы с грифом «Для служебного пользования» («Ограниченного пользования») возвратить в секретариат в тот же день;
- не выносить документы с грифом «Для служебного пользования» за пределы Организации;
- при смене работников, ответственных за учет и хранение документов, составлять акт приема-передачи документов.

8.3. Для организации делопроизводства приказом директора Организации назначается ответственное лицо. Делопроизводство ведется на основании инструкции по организации делопроизводства, утвержденной директором Организации.

9. Сообщение об инцидентах информационной безопасности, реагирование и отчетность

9.1. Все работники должны быть осведомлены о своей обязанности сообщать об известных или подозреваемых ими нарушениях информационной безопасности, а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

9.2. В случае кражи документов или переносного компьютера следует незамедлительно сообщить об инциденте руководителю отдела защиты информации.

9.3. В случае подозрения или выявления наличия вирусов или иных разрушительных компьютерных кодов сразу после их обнаружения работник обязан:

- проинформировать специалистов отдела информационных технологий;
- не пользоваться и не выключать зараженный компьютер;
- не подсоединять этот компьютер к компьютерной сети Организации до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование специалистами отдела информационных технологий.

10. Защита и сохранность данных

10.1. Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на работниках.

10.2. Специалисты отдела информационных технологий обязаны оказывать работникам содействие в проведении резервного копирования данных на соответствующие носители.

10.3. Специалисты отдела информационных технологий на основании заявок руководителей подразделений вправе создавать и удалять совместно используемые сетевые ресурсы и папки общего пользования, а также управлять полномочиями доступа к ним.

10.4. Работники имеют право создавать, модифицировать и удалять файлы и директории в совместно используемых сетевых ресурсах только на тех участках, которые выделены лично для них, для их рабочих групп или к которым они имеют санкционированный доступ. Все заявки на проведение технического обслуживания компьютеров должны направляться в отдел информационных технологий.

11. Ответственность

11.1. Нарушение требований настоящего Положения влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

12. Заключительные положения

12.1. Изменения в настоящее Положение вносятся приказом Работодателя.

12.2. Настоящее Положение вступает в силу с момента его утверждения и действует бессрочно, до принятия нового Положения.

Начальник ОКБ  Е.А. Буглаева

01.09.2026 г