

МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ



Федеральное государственное автономное учреждение
«Национальный медицинский исследовательский центр
«Межотраслевой научно-технический комплекс «Микрохирургия глаза»
имени академика С.Н. Федорова» Министерства здравоохранения Российской Федерации
(ФГАУ «НМИЦ «МНТК «Микрохирургия глаза» им. акад. С.Н. Федорова» Минздрава России)

П Р И К А З

18.04.2023

Москва

№ 106

**Об утверждении Положения о защите
персональных данных работников ФГАУ
«НМИЦ «МНТК «Микрохирургия глаза»
им. акад. С.Н. Фёдорова» Минздрава России**

В соответствии с Трудовым кодексом Российской Федерации и во исполнение требований Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», а также в целях защиты персональных данных в ФГАУ «НМИЦ «МНТК «Микрохирургия глаза» им. акад. С.Н. Федорова» Минздрава России (далее – Учреждение),

П Р И К А З Ы В А Ю:

1. Утвердить и ввести в действие Положение о защите персональных данных работников ФГАУ «НМИЦ «МНТК «Микрохирургия глаза» им. акад. С.Н. Федорова» Минздрава России (далее - Положение) согласно приложению 1.

2. Распространить действие Положения на Учреждение, в том числе обособленные структурные подразделения (филиалы).

3. Руководителям структурных подразделений головной организации Учреждения в 7-дневный срок со дня утверждения настоящего приказа ознакомить работников своих подразделений с настоящим приказом и представить листы ознакомления согласно приложению 2 в отдел управления персоналом.

4. Начальнику отдела по координации деятельности филиалов Вепринскому Д.В. довести настоящий приказ до директоров филиалов.

5. Директорам филиалов ознакомить работников своих филиалов с настоящим приказом и принять Положение к исполнению.

6. Начальнику отдела научной информации Политовой Е.А. разместить Положение на официальном сайте Учреждения в 2-дневный срок со дня подписания настоящего приказа.

7. Начальнику группы по обеспечению информационной безопасности организации клиники Бадаеву А.В., а также работникам филиалов Учреждения,

ответственным за развитие информационно-телекоммуникационной инфраструктуры и информационной безопасности, ежегодно (или по мере необходимости) представлять предложения о внесении изменений в Положение с целью проверки соответствия Положения реальным условиям применения в информационных системах Учреждения.

8. Контроль за исполнением настоящего приказа оставляю за собой.

Генеральный директор



Д.Г. Арсютов

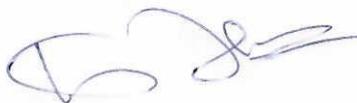
Визы:

Заместитель генерального директора
по научно-клинической работе
«10» 04 _____ 2023 г.



А.В. Дога

Заместитель генерального директора
по научной работе
«10» 04 _____ 2023 г.



Б.Э. Малюгин

Заместитель генерального директора
по экономическим вопросам
«10» 04 _____ 2023 г.



Ю.Л. Лимбир

Заместитель генерального директора
по общим вопросам
«11» 04 _____ 2023 г.



В.И. Егоров

Заместитель генерального директора
по организационно-методической работе
«10» 04 _____ 2023 г.



Н.С. Ходжаев

Заместитель генерального директора
по безопасности
«11» 04 _____ 2023 г.



Д.С. Королев

Начальник юридического отдела
«11» 04 _____ 2023 г.



Н.И. Чижова

Начальник отдела
документационного обеспечения
«10» 04 _____ 2023 г.



Л.Т. Бокова

Начальник группы по обеспечению
информационной безопасности
«10» 04 _____ 2023 г.



А.В. Бадаев

Начальник отдела
управления персоналом
«10» 04 _____ 2023 г.
исполнитель: 89-88



Е.А. Шкляева

к приказу ФГАУ «НМИЦ «МНТК
«Микрохирургия глаза» им. акад.
С.Н. Федорова» Минздрава России
от «18» 04 2023 г. № 106

ПОЛОЖЕНИЕ

О защите персональных данных работников ФГАУ «НМИЦ «МНТК «Микрохирургия глаза» им. акад. С.Н. Федорова» Минздрава России

I. Общие положения

1.1. Настоящее Положение ФГАУ «НМИЦ «МНТК «Микрохирургия глаза» им. акад. С.Н. Федорова» Минздрава России (далее – Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», Трудовым кодексом Российской Федерации, Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», другими действующими нормативными правовыми актами Российской Федерации в области защиты персональных данных, Политикой ФГАУ «НМИЦ «МНТК «Микрохирургия глаза» им. акад. С.Н. Федорова» Минздрава России в отношении обработки персональных данных, Положением «О персональных данных работников» ФГАУ «НМИЦ «МНТК «Микрохирургия глаза» им. акад. С.Н. Федорова» Минздрава России и иными локальными нормативными актами ФГАУ «НМИЦ «МНТК «Микрохирургия глаза» им. акад. С.Н. Федорова» Минздрава России (далее - Учреждение, Работодатель) в области защиты персональных данных.

1.2. Цель настоящего Положения - защита персональных данных работников Учреждения от несанкционированного доступа и разглашения. Персональные данные работников всегда являются конфиденциальной, строго охраняемой информацией, в соответствии с законодательством Российской Федерации.

1.3. Положение является локальным нормативным актом Учреждения, обязательным для соблюдения всеми работниками Учреждения, а также иными лицами, участвующими в обработке персональных данных работников в соответствии с настоящим Положением.

1.4. Положение определяет политику Учреждения, в том числе его обособленных подразделений (филиалов), в отношении защиты персональных данных работников, а также устанавливает процедуры,

направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

1.5. Положение и изменения к нему утверждаются руководителем Учреждения и вводятся его приказом. Все работники должны быть ознакомлены под подпись с данным Положением и изменениями к нему.

II. Понятие и состав персональных данных

2.1. Персональными данными является информация, необходимая Учреждению в связи с трудовыми отношениями, возникающими с работниками, и относящаяся прямо или косвенно к определенному или определяемому работнику (субъекту персональных данных).

2.2. Состав персональных данных работников определяется локальным нормативным актом Учреждения «Положение о персональных данных работников ФГАУ «НМИЦ «МНТК «Микрохирургия глаза» им. акад. С.Н. Федорова» Минздрава России.

2.3. Документами, содержащими персональные данные работников являются в том числе:

- паспорт или иной документ, удостоверяющий личность;
- трудовая книжка и (или) сведения о трудовой деятельности работника;
- документ, подтверждающий регистрацию в системе индивидуального (персонифицированного) учета, в том числе в форме электронного документа, страховое свидетельство обязательного пенсионного страхования;
- документы воинского учета (для военнообязанных и лиц, подлежащих призыву на военную службу);
- свидетельство о постановке на учет в налоговый орган и присвоении ИНН;
- документы об образовании, о квалификации или наличии специальных знаний или специальной подготовки;
- автобиография, анкета, резюме, характеристики, рекомендательные письма и иные подобные документы;
- медицинские заключения о состоянии здоровья и листки нетрудоспособности;
- справки, выданные органами МВД России, о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям (при поступлении на работу, к выполнению которой в соответствии с Трудовым кодексом Российской Федерации или иным федеральным законом не допускаются лица, имеющие или имевшие судимость, подвергающиеся или подвергавшиеся уголовному преследованию);
- личная карточка Т-2;
- свидетельство о заключении брака, свидетельство о рождении детей;
- трудовой договор;
- подлинники и копии приказов по личному составу;

– иные документы, добровольно предоставляемые работником Работодателю.

2.4. Из указанного списка Учреждение вправе получать и использовать только те сведения, которые характеризуют гражданина как сторону трудового договора.

2.5. Сведения и документы указанные в п. 2.2 и 2.3 настоящего Положения являются конфиденциальными.

III. Обязанности Работодателя

3.1. Работодатель обязан принимать правовые, организационные и технические меры, необходимые и достаточные для обеспечения выполнения обязанностей по защите персональных данных работников Учреждения.

3.2. Работодатель обязан осуществлять внутренний контроль и аудит соответствия обработки персональных данных требованиям к защите персональных данных, установленных законодательством Российской Федерации, политике Учреждения в отношении обработки персональных данных, локальным нормативным актам Учреждения.

3.3. Работодатель обязан проводить оценку вреда, который может быть причинен работникам в случае нарушения законодательства Российской Федерации в области защиты персональных данных, а также соотносить указанный вред с принимаемыми Учреждением мерами, направленными на их защиту.

3.4. Защита персональных данных работника от неправомерного их использования или утраты должна обеспечиваться Работодателем за счет его средств в порядке, установленном федеральным законом.

IV. Сбор, обработка и хранение персональных данных работников

4.1. Обработка персональных данных работника - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных работника.

4.2. Обработка персональных данных осуществляется уполномоченными должностными лицами Учреждения, определенными приказом генерального директора, на основании инструкций, предусматривающих выполнение комплекса мероприятий по организации обработки и обеспечению безопасности персональных данных.

4.3. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

4.4. Правила хранения персональных данных работников устанавливаются Положением «О персональных данных работников ФГАУ «НМИЦ «МНТК «Микрохирургия глаза» им. акад. С.Н. Федорова» Минздрава России» и иными локальными актами Учреждения.

V. Передача персональных данных

5.1. При передаче персональных данных работника Работодатель должен соблюдать следующие требования:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом;

- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать конфиденциальность. Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;

- разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

- передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

VI. Доступ к персональным данным работника

6.1. Внутренний доступ (доступ внутри Учреждения).

6.1.1. Список работников, имеющих доступ к персональным данным, определяется локальным актом Учреждения, утвержденным генеральным директором.

6.2. Внешний доступ.

6.2.1. Учреждение вправе осуществлять передачу персональных данных работника третьим лицам, в том числе в коммерческих целях, только с его

предварительного письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных действующим законодательством Российской Федерации.

6.2.2. Перед передачей персональных данных Учреждение должно предупредить третье лицо о том, что они могут быть использованы только в тех целях, для которых были сообщены. При этом у третьего лица необходимо получить подтверждение того, что такое требование будет им соблюдено.

6.2.3. Не требуется согласие работника на передачу персональных данных:

- третьим лицам в целях предупреждения угрозы жизни и здоровью работника;
- в Социальный фонд России в объеме, предусмотренном действующим законодательством Российской Федерации;
- в налоговые органы;
- в военные комиссариаты;
- по запросу профессиональных союзов в целях контроля за соблюдением трудового законодательства работодателем;
- по мотивированному запросу органов прокуратуры;
- по мотивированному требованию правоохранительных органов и органов безопасности;
- по запросу от государственных инспекторов труда при осуществлении ими надзорно-контрольной деятельности;
- по запросу суда;
- в органы и организации, которые должны быть уведомлены о тяжелом несчастном случае, в том числе со смертельным исходом;
- в случаях, связанных с исполнением работником должностных обязанностей;
- в кредитную организацию, обслуживающую платежные карты работников.

6.3. Другие организации.

6.3.1. Сведения о работнике (в том числе уволенном) могут быть предоставлены другой организации только с письменного запроса на бланке организации с приложением копии заявления работника.

6.4. Родственники и члены семей.

6.4.1. Персональные данные работника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого работника.

VII. Конфиденциальность персональных данных работников

7.1. В целях обеспечения сохранности и конфиденциальности персональных данных работников организации все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться

только работниками, допущенными локальными нормативными актами Учреждения к обработке таких данных.

7.2. Ответы на письменные запросы других организаций и учреждений в пределах их компетенции и предоставленных полномочий даются в письменной форме на бланке Учреждения в том объеме, который позволяет не разглашать излишний объем персональных сведений о работниках Учреждения.

7.3. Передача информации, содержащей сведения о персональных данных работников организации, по телефону, факсу, электронной почте без письменного согласия работника запрещается.

7.4. Личные дела и документы, содержащие персональные данные работников, хранятся в запирающихся шкафах (сейфах), обеспечивающих защиту от несанкционированного доступа.

7.5. Помещения, в которых обрабатываются и хранятся персональные данные, оборудуются надежными замками. Должно быть исключено бесконтрольное пребывание посторонних лиц в этих помещениях, при отсутствии в них сотрудников в рабочее время они должны быть закрыты.

Проведение уборки помещений, в которых хранятся персональные данные, должно производиться в присутствии работников этих помещений.

7.6. Персональные компьютеры, в которых содержатся персональные данные, должны быть оснащены средствами защиты от несанкционированного доступа.

VIII. Угрозы безопасности персональных данных

8.1. Под актуальными угрозами безопасности персональных данных работников Учреждения понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным работников Учреждения при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

8.2. Угрозы безопасности персональных данных работников Учреждения делятся на следующие типы:

8.2.1. Угрозы первого типа. В системном программном обеспечении информационной системы есть функциональные возможности программного обеспечения, которые не указаны в описании к нему либо не отвечают характеристикам, которые заявил производитель. И это потенциально может привести к неправомерному использованию персональных данных работников Учреждения.

8.2.2. Угрозы второго типа. Присутствуют потенциальные проблемы с прикладным программным обеспечением — внешними программами, которые установлены на компьютерах работников.

8.2.3. Угрозы третьего типа. Потенциальной опасности ни от системного, ни от программного обеспечения нет.

8.3. Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится Учреждением с учетом оценки возможного вреда, проведенной в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных, который может быть причинен субъектам персональных данных.

IX. Уровни защищенности персональных данных

9.1. При обработке персональных данных работников Учреждения в информационных системах устанавливаются следующие уровни защищенности персональных данных:

9.1.1. Первый уровень защищенности устанавливается в случае, если:

– для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

– для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся работниками Учреждения.

9.1.2. Второй уровень защищенности устанавливается в случае, если:

– для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;

– для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных работников Учреждения или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся работниками Учреждения;

– для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;

– для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся работниками Учреждения;

– для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся работниками Учреждения;

– для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся работниками Учреждения.

9.1.3. Третий уровень защищенности устанавливается в случае, если:

– для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные работников Учреждения или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся работниками Учреждения;

– для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных работников Учреждения или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся работниками Учреждения;

– для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных работников Учреждения или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся работниками Учреждения;

– для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;

– для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся работниками Учреждения.

9.1.4. Четвертый уровень защищенности устанавливается в случае, если:

– для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

– для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных работников Учреждения или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся работниками Учреждения.

Х. Меры по защите персональных данных работников

10.1. Для персональных данных работников, которые хранятся в информационных системах, постоянно действующей комиссией по защите информации, созданной Приказом генерального директора, определяются типы угроз безопасности и уровней защищенности персональных данных.

10.2. При обработке персональных данных, которым присвоен четвертый уровень защищенности Учреждение принимает следующие меры:

– организует режим обеспечения безопасности помещений, в которых размещена информационная система, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

– обеспечивает сохранность носителей персональных данных.

– приказом генерального директора утверждает перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

– использует средства защиты информации, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

10.3. Для обеспечения 3-го уровня защищенности персональных данных работников при их обработке в информационных системах помимо выполнения требований, установленных п. 10.2 настоящего Положения, приказом генерального директора назначается должностное лицо, ответственное за безопасность персональных данных в информационной системе.

10.4. Для обеспечения 2-го уровня защищенности персональных данных работников при их обработке в информационных системах помимо выполнения требований, предусмотренных п. 10.3 настоящего Положения, доступ к содержанию электронного журнала сообщений возможен исключительно для должностных лиц (работников) Учреждения или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

10.5. Для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах помимо требований, предусмотренных п. 10.4 настоящего Положения, устанавливаются следующие требования:

10.5.1. В случае изменения полномочий сотрудника Учреждения по доступу к персональным данным работников, содержащихся в информационной системе, производится автоматическая регистрация указанных изменений в электронном журнале безопасности;

10.5.2. Приказом генерального директора назначается структурное подразделение, ответственное за обеспечение безопасности персональных данных работников в информационной системе.

10.6. Приказом генерального директора назначается лицо, ответственное за обработку персональных данных, которое осуществляет организацию обработки персональных данных, обучение и инструктаж, внутренний контроль за соблюдением работниками требований к защите персональных данных.

10.7. Для защиты информации, обрабатываемой в информационных системах в электронном виде, Учреждение внедряет соответствующее сертифицированное программное обеспечение с регулярно обновляемыми базами.

10.8. Контроль выполнения требований по обработке и обеспечению безопасности персональных данных организуется Учреждением самостоятельно и (или) с привлечением на договорной основе юридических лиц, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Приказом генерального директора назначается лицо, ответственное за контроль выполнения мер по защите персональных данных работников. Периодичность такого контроля

устанавливается локальным нормативным актом Учреждения, но не реже 1 раза в 3 года.

10.9. Для обеспечения безопасности персональных данных работников проводятся мероприятия по контролю за соблюдением требований, установленных законодательством Российской Федерации и локальными актами Учреждения.

10.10. В случае обнаружения факта несанкционированного доступа или разглашения персональных данных лицо, ответственное за обработку персональных данных, проводит расследование с привлечением виновных работников к ответственности и принятием иных мер.

XI. Ответственность за разглашение информации, связанной с персональными данными работника

11.1. Персональная ответственность является одним из главных требований к организации функционирования системы защиты персональных данных и обязательным условием обеспечения эффективности функционирования данной системы.

11.2. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, установленных действующим законодательством и настоящим Положением, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

XII. Заключительные положения

12.1. Настоящее Положение вступает в силу с момента его утверждения приказом генерального директора Учреждения и действует бессрочно, до замены его новым Положением.

12.2. Положение подлежит полному пересмотру при изменении состава технических и программных средств информационных систем Учреждения, приводящих к существенным изменениям технологии обработки информации.

12.3. Полный плановый пересмотр Положения проводится регулярно, раз в год, с целью проверки соответствия положений данного документа реальным условиям применения их в информационных системах Учреждения.

12.4. Все изменения в Положение вносятся приказом генерального директора Учреждения.

12.5. В случае изменений законодательных и иных нормативных актов Российской Федерации, а также Устава Учреждения, настоящее Положение и изменения к нему применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также Уставу Учреждения.

12.6. Во всем остальном, что не предусмотрено настоящим Положением, Учреждение и его работники руководствуются действующим законодательством Российской Федерации.

