ФОНД СОЦИАЛЬНОГО СТРАХОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСУДАРСТВЕННОЕ УЧРЕЖДЕНИЕ – РЕГИОНАЛЬНОЕ
ОТДЕЛЕНИЕ ФОНДА СОЦИАЛЬНОГО СТРАХОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ХАНТЫ-
МАНСИЙСКОМУ АВТОНОМНОМУ ОКРУГУ-ЮГРЕ

П Р И К А З

21 июня 2019 ХАНТЫ-МАНСИЙСК № 205

Об утверждении инструкций и регламентов в части обеспечения информационной безопасности

С целью исполнения требований законодательства Российской Федерации в части защиты информации и обеспечения информационной безопасности в Государственном учреждении – региональном отделении Фонда социального страхования Российской Федерации по Ханты-Мансийскому автономному округу – Югре (далее – Региональное отделение), **п р и к а з ы в а ю:**

1. Утвердить следующие положения и инструкции:

1.1. Положение об обработке персональных данных в информационной системе персональных данных Регионального отделения (приложение 1);

1.2. Положение об организации защиты информации и доступа к информационным ресурсам в Региональном отделении (приложение 2);

1.3. Инструкцию администратора информационной безопасности (приложение 3);

1.4. Схему границ контролируемой зоны объектов информатизации Регионального отделения (приложение 4);

1.5. Положение об обработке персональных данных работников Регионального отделения (приложение 5);

1.6. Инструкцию пользователя автоматизированного рабочего места и информационных ресурсов Регионального отделения (приложение 6);

1.7. Инструкцию администратора локальной вычислительной сети (приложение 7);

1.8. Инструкцию о порядке действия сотрудников Регионального отделения при возникновении внештатных ситуаций (приложение 8);

1.9. Инструкцию о порядке эксплуатации автоматизированных рабочих мест (приложение 9);

1.10. Инструкцию ответственного за организацию обработки персональных данных (приложение 10);

1.11. Инструкцию по организации антивирусной защиты (приложение 11);

1.12. Инструкцию администратора парольной защиты (приложение 12);

1.13. Инструкцию администратора и порядок работы с ресурсами глобальной сети интернет (приложение 13);

1.14. Инструкцию администратора антивирусной защиты (приложение 14);

1.15. Порядок предоставления данных о работе Регионального отделения (приложение 15);

1.16. Порядок доступа в серверное помещение (приложение 16);

1.17. Инструкцию администратора средств криптографической защиты информации (приложение 17);

1.18. Инструкцию по обращению со средствами криптографической защиты информации (приложение 18);

1.19. Инструкцию по уничтожению криптоключей, ключевых документов и электронных подписей (приложение 19);

1.20. Инструкцию администратора баз данных (приложение 20);

1.21. Инструкцию пользователя баз данных (приложение 21);

1.22. Регламент проведения обновления баз данных и программного обеспечения подсистем ЕИИС «Соцстрах» (приложение 22).

2. Отделу по делопроизводству и организации работы с обращениями граждан (Л. Н. Пилипенко), директорам филиалов, консультантам-руководителям групп работы со страхователями 1,2,3,4 ознакомить сотрудников с настоящим приказом под подпись.

3. Отделу организационно-кадровой работы (Т.В. Сафонова) обеспечить ознакомление вновь принимаемых работников в региональное отделение с настоящим приказом и приложением к нему.

4. Считать утратившими силу приказы Регионального отделения:

4.1. № 39/12 от 25.01.2012 года «Об организации работы по защите персональных данных»;

4.2. № 42/1/11 от 14.02.2011 года «Об утверждении инструкции администратора информационной безопасности»;

4.3. № 1263/11 от 01.12.02011 года «Об утверждении границ контролируемой зоны объектов информатизации»;

4.4. № 98/1/11 от 28.02.2011 года «Об утверждении инструкции администратора локально-вычислительной сети по поддержанию уровня защиты локальной вычислительной сети от несанкционированного доступа»;

4.5. № 55/12 от 27.01.2012 года «Об утверждении инструкции о порядке эксплуатации автоматизированных рабочих мест»;

4.6. № 56/1/11 от 18.02.2011 года «Об утверждении инструкции администратора и порядка организации антивирусной защиты информации»;

4.7. № 1374/11 от 30.12.2011 года «Об утверждении инструкции администратора и инструкции по организации парольной защиты»;

4.8. № 1373/11 от 30.12.2011 года «Об утверждении инструкции администратора доступа в интернет и порядка работы с ресурсами глобальной сети интернет»;

4.9. № 1329/11 от 16.12.2011 года «Об утверждении порядка доступа в серверные помещения»;

4.10. № 52/1/11 от 18.02.2011 года «Об утверждении инструкции администратора средств криптографической защиты информации и инструкции по организации эксплуатации и хранения аппаратно-программных криптографических средств и ключей электронной цифровой подписи»;

4.11. № 297/18 от 28.05.2018 года «Об утверждении инструкции и постоянно действующей комиссии по уничтожению криптоключей, ключевых документов и электронных подписей»;

4.12. № 38/12 от 25.01.2012 года «Об утверждении инструкции администратора и пользователя баз данных»;

5. Контроль за исполнением настоящего приказа возложить на заместителя управляющего региональным отделением Крюкова В.А.

Управляющий М.В. Рыбьяков

Приложение 1 к приказу
Государственного учреждения
-регионального отделения
Фонда социального
страхования Российской
Федерации по Ханты-
Мансийскому автономному
округу – Югре

от «28» июня 2019 г.

№ 205

Положение об обработке персональных данных в информационной системе персональных данных Государственного учреждения - регионального отделения Фонда социального страхования Российской Федерации по Ханты-Мансийскому автономному округу - Югре

1. Термины, определения.

1.1. Персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

1.2. Обработка персональных данных — действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

1.3. Конфиденциальность персональных данных — обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным, требование не допускать их распространения без согласия субъекта или иного законного основания.

1.4. Распространение персональных данных — действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

1.5. Использование персональных данных — действия (операции) с персональными данными, совершаемые должностным лицом Организации в

целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъектов либо иным образом затрагивающих их права и свободы или права и свободы других лиц.

1.6. Блокирование персональных данных — временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

1.7. Уничтожение персональных данных — действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

1.8. Обезличивание персональных данных — действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту.

1.9. Общедоступные персональные данные — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

1.10. Информация — сведения (сообщения, данные) независимо от формы их представления.

2. Сокращения

АРМ	– автоматизированное рабочее место;
АПК	– аппаратно-программный комплекс;
ЕИИС «Соцстрах»	– Единая интегрированная информационная система «Соцстрах» Фонда;
ЕКСПД	– Единая корпоративная сеть передачи данных Фонда;
ИБ	– информационная безопасность;
ИОФ	– исполнительный орган Фонда;
ИСПДн	– информационная система персональных данных;
НСД	– несанкционированный доступ;
ОИ	– отдел информатизации РО;
ПАВЗ	– подсистема антивирусной защиты;
ПДн	– персональные данные;
ПЗПДн	– комплекс подсистем защиты персональных данных, обрабатываемых в ИСПДн;
ПО	– программное обеспечение;
ПЭВМ	– персональная электронно-вычислительная машина;
РО	– региональное отделение Фонда;
РФ	– Российская Федерация;
СВТ	– средства вычислительной техники;
СЗИ	– средства защиты информации;
Фонд	– Фонд социального страхования Российской Федерации;

3. Общие положения

Настоящее Положение об обработке персональных данных (далее — Положение) разработано в соответствии с Трудовым кодексом Российской Федерации, Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом N 149 от 27.07.2006 «Об информации, информационных технологиях и о защите информации», Федеральным законом 152-ФЗ от 27.07.2006 «О персональных данных», иными федеральными законами.

Цель разработки Положения — определение порядка обработки персональных данных всех субъектов персональных данных, данные которых подлежат обработке, на основании полномочий оператора; обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

Положение определяет содержание и порядок осуществления мероприятий по защите персональных данных в ЕИИС «Соцстрах» в Государственном учреждении - региональном отделении Фонда социального страхования Российской Федерации по Ханты-Мансийскому автономному округу - Югре (далее – региональное отделение).

Положение разработано применительно к информационной системе персональных данных ЕИИС «Соцстрах», уничтожение или искажение которых может нанести существенный материальный ущерб региональному отделению.

К персональным данным ЕИИС «Соцстрах» относится любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и другая информация.

Положение одинаково применимо к серверам, периферийному оборудованию, автоматизированным рабочим местам и персональным компьютерам в составе ЕИИС «Соцстрах», а также ко всем лицам, имеющим отношение к ЕИИС «Соцстрах», включая всех работников регионального отделения.

Все работники регионального отделения, связанные с обработкой персональных данных в ЕИИС «Соцстрах», должны быть ознакомлены с настоящим положением, в том числе работники регионального отделения, должны быть ознакомлены с «Обязательством о неразглашении сведений конфиденциального характера» (приложение) под роспись.

4. Условия проведения обработки персональных данных

К работе со сведениями, содержащими персональные данные, допускаются работники, которым по роду их деятельности и по должностным обязанностям доступ к таким сведения необходим.

Допуск работника к таким сведениям осуществляется в соответствии с трудовым договором и функциональными обязанностями по решению руководителя структурного подразделения регионального отделения. Данная процедура предусматривает:

– ознакомление с законодательными актами Российской Федерации, нормативными правовыми документами Правительства Российской Федерации и Фонда, регламентирующими работу со сведениями конфиденциального характера, а также предусматривающими ответственность за нарушение правил работы с указанными сведениями;

– принятие обязательств о неразглашении сведений конфиденциального характера;

– ознакомление с перечнем сведений конфиденциального характера имеющихся в региональном отделении, к которым работник получает право доступа.

– допуск работника к сведениям конфиденциального характера осуществляется только после подписания им «Обязательства о неразглашении сведений конфиденциального характера» (приложение).

5. Состав персональных данных обрабатываемых в ЕИИС «Соцстрах»

Обработка персональных данных в РО осуществляется в информационной системе персональных данных «Единая интегрированная информационная система «Соцстрах», включающей:

– фамилия, имя, отчество;
– пол;
– день, месяц, год рождения;
– номер, серия, дата выдачи документа, удостоверяющего личность;
– адрес места регистрации;
– фактическое место жительства;
– страховой номер индивидуального лицевого счета (СНИЛС);
– номер индивидуальной программы реабилитации (ИПР);
– категория, тип и шифр изделия/услуги на протезирование;
– серия, номер полиса обязательного медицинского страхования (ОМС);
– состояние здоровья;
– дата оказания помощи;
– вредный производственный фактор;
– код результата обращения пациента;
– вид первичной медико-санитарной помощи;

– страховые выплаты;
– номер индивидуального лицевого счета получателя выплат;
– номер лицевого счета получателя выплат в кредитном учреждении;
– информация о путевках;
– профиль лечения;
– история лечения;
– сведения о заработке пострадавшего;
– программа реабилитации;
– квалификация страхового случая;
– вина пострадавшего;
– вид происшествия;
– травма;
– диагноз производственной травмы;
– сопутствующие заболевания;
– диагноз основного заболевания (по МКБ-10);
– степень тяжести несчастного случая;
– степень ограничения трудоспособности;
– степень утраты трудоспособности;
– утраченный заработок;
– суммы страховых выплат;
– виды и период реабилитационных мероприятий;
– дата акта, номер личного дела;
– стаж работы;
– профессия;
– вредные факторы;
– дата, время, вид, причина, исход происшествия;
– дата, номер, тип экспертизы;
– серия, дата и номер медицинского заключения;
– степень опьянения,
– диагноз;
– группа инвалидности;
– серия, номер, дата выдачи документа, удостоверяющего право на льготу;
– профиль санаторно-курортного лечения;
– номер индивидуального плана реабилитации (ИПР);
– дата постановки на учет;
– дата начала и окончания наблюдения за пациенткой;
– дата родов;
– полное число недель беременности на момент выдачи сертификата;
– исход родов (код по МКБ-10);
– серия, номер, дата выдачи, закрытия листка нетрудоспособности;
– номер, дата выдачи обменной карты;

– многоплодная беременность;
– успешные преждевременные роды;
– количество новорождённых;
– количество детей, включая рожденных ранее;
– пол, вес, рост новорожденного;
– лицевой счет, номер кредитной карты;
– номер справки по инвалидности;
– дата выдачи, срок, группа;
– суммы надбавок, премий, вычетов, дотаций, доход;
– семейное положение;
– сведения о родственниках;
– сведения о трудовой деятельности;
– вид и стаж работы во вредных условиях; ИНН;
– образование;
– гражданство;
– информация по воинскому учету;
– номер телефона;
– категория льготника;
– вид нетрудоспособности;
– категория заболевания ребенка;
– информация об инвалидности ребенка;
– номер водительского удостоверения;
– должностной оклад, надбавки к должностному окладу, количество вакансий.

В Организации создаются и хранятся следующие документы, содержащие данные о субъектах персональных данных:

– Анкета (клиента - физического лица (открытие банковского счета, счета по вкладу (депозиту), оформление переводов, клиента - юридического лица (с данными об учредителях, директорах)).

– Копии документов, удостоверяющих личность, а также иных документов, предоставляемых субъектами персональных данных, и содержащих персональные данные. - Свидетельство о государственной регистрации в качестве индивидуального предпринимателя (оригинал или копия, заверенная надлежащим образом).

– Трудовые книжки.

– Анкета работника – субъекта персональных данных.

– Заявления работника – субъекта персональных данных.

Порядок получения (сбора) персональных данных:

1. Все персональные данные субъекта следует получать у него лично с его письменного согласия, кроме случаев, определенных в п. 3 и 5 настоящего Положения и иных случаях, предусмотренных законами.

2. Согласие субъекта на использование его персональных данных хранятся в бумажном виде в структурном подразделении по направлению деятельности.

3. Если персональные данные субъекта возможно получить только у третьей стороны, субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Третье лицо, предоставляющее персональные данные субъекта, должно обладать согласием субъекта на передачу персональных данных Организации. Организация обязана получить подтверждение от третьего лица, передающего персональные данные субъекта персональных данных о том, что персональные данные передаются с согласия субъекта. Региональное отделение обязана при взаимодействии с третьими лицами заключить с ними соглашение о конфиденциальности информации, касающейся персональных данных субъектов.

4. Организация обязана сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта персональных данных дать письменное согласие на их получение.

5. Обработка персональных данных субъектов без их согласия осуществляется в следующих случаях:

1) Персональные данные являются общедоступными.

2) По требованию полномочных государственных органов в случаях, предусмотренных федеральным законом.

3) Обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора.

4) Обработка персональных данных осуществляется в целях заключения и исполнения государственного контракта, одной из сторон которого является субъект персональных данных.

5) Обработка персональных данных осуществляется для статистических целей при условии обязательного обезличивания персональных данных.

6) В иных случаях, предусмотренных законом.

6. Субъект персональных данных предоставляет сотруднику регионального отделения, ответственному за ведение информационной системы достоверные сведения о себе.

6.1. На основании полученной информации сотрудник регионального отделения проверяет наличие данного субъекта, зарегистрированного в информационной системе. Если субъект отсутствует в информационной системе, то сотрудник заносит полную информацию о субъекте, после получения письменного согласия последнего. В случае наличия информации о субъекте в информационной системе – сверяет данные с ранее предоставленными (при необходимости вносит соответствующие изменения).

6.2. При определении объема и содержания, обрабатываемых персональных данных региональное отделение руководствоваться

требованиями Центрального Банка, ФСБ, ФСТЭК и иных контролирующих органов, Конституцией Российской Федерации, закона о персональных данных, Трудовым кодексом Российской Федерации и иными федеральными законами.

6. Блокировка, обезличивание, уничтожение персональных данных

6.1. Порядок блокировки и разблокировки персональных данных:
Блокировка персональных данных субъектов осуществляется с письменного заявления субъекта персональных данных.

6.2. Блокировка персональных данных подразумевает:

– запрет редактирования персональных данных.

– запрет распространения персональных данных любыми средствами (e-mail, сотовая связь, материальные носители).

– запрет использования персональных данных в массовых рассылках (sms, e-mail, почта).

– изъятие бумажных документов, относящихся к субъекту персональных данных и содержащих его персональные данные из внутреннего документооборота регионального отделения и запрет их использования.

6.3. Блокировка персональных данных субъекта может быть временно снята, если это требуется для соблюдения законодательства.

6.4. Разблокировка персональных данных субъекта осуществляется с его письменного согласия или заявления.

6.5. Повторное согласие субъекта персональных данных на обработку его данных влечет разблокирование его персональных данных.

6.6. Порядок обезличивания и уничтожения персональных данных:

– обезличивание персональных данных субъекта происходит по письменному заявлению субъекта персональных данных, при условии, что все договорные отношения завершены и от даты окончания последнего договора прошло не менее 5 лет.

– при обезличивании персональные данные в информационных системах заменяются набором символов, по которому невозможно определить принадлежность персональных данных к конкретному субъекту.

– бумажные носители документов при обезличивании персональных данных уничтожаются.

– операция обезличивания персональных данных субъекта необратима.

– региональное отделение обязано обеспечить конфиденциальность в отношении персональных данных при необходимости проведения испытаний информационных систем на территории разработчика и произвести обезличивание персональных данных в передаваемых разработчику информационных системах.

– уничтожение персональных данных субъекта подразумевает прекращение какого-либо доступа к персональным данным субъекта.

– при уничтожении персональных данных субъекта работники регионального отделения не могут получить доступ к персональным данным субъекта в информационных системах.

– бумажные носители документов при уничтожении персональных данных уничтожаются, персональные данные в информационных системах обезличиваются. Персональные данные восстановлению не подлежат.

– операция уничтожения персональных данных необратима.

– срок, после которого возможна операция уничтожения персональных данных субъекта определяется окончанием срока, указанным в пункте 7.3 настоящего Положения.

7. Передача и хранение персональных данных

7.1. Передача персональных данных:

7.1.1. Под передачей персональных данных субъекта понимается распространение информации по каналам связи и на материальных носителях.

7.1.2. При передаче персональных данных работники Организации должны соблюдать следующие требования:

– разрешать доступ к персональным данным только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения должностных обязанностей.

– передавать персональные данные субъекта представителям субъекта в порядке, установленном законодательством и нормативно-технологической документацией и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функции.

7.2. Хранение и использование персональных данных:

7.2.1. Под хранением персональных данных понимается существование записей в информационных системах и на материальных носителях.

7.2.2. Персональные данные субъектов обрабатываются и хранятся в информационных системах, а также на бумажных носителях в региональном отделении.

7.2.3. Хранение персональных данных субъекта может осуществляться не дольше, чем этого требуют цели обработки, если иное не предусмотрено федеральными законами.

7.3. Сроки хранения персональных данных:

7.3.1. Сроки хранения персональных данных субъектов, относящихся к трудовым правоотношениям, составляют 75 лет. (основание – Перечень типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения, утв. Приказом Министерства культуры Российской Федерации от 25 августа 2010 г. N 558).

7.3.2. Сроки хранения личных дел (заявления, автобиографии, копии приказов и выписки из них, копии личных документов, характеристики, листки по учету кадров, анкеты, аттестационные листы и др.) руководства Организации, членов контрольных органов, а также работников, имеющих государственные и иные звания, премии, награды, ученые степени и звания) - постоянно.

7.3.3. Документы (анкеты, автобиографии, листки по учету кадров, заявления, рекомендательные письма, резюме и др.) лиц, не принятых на работу, хранятся 1 год.

7.3.4. Сроки хранения персональных данных субъектов, относящихся к доходам субъектов, составляют 4 года (основание – Статья 23 НК РФ).

7.3.5. Сроки хранения гражданско-правовых договоров, содержащих персональные данные субъектов, а также сопутствующих документов - 5 лет с момента окончания действия договоров (основание - Перечень типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения, утв. Приказом Министерства культуры Российской Федерации от 25 августа 2010 г. N 558).

7.3.6. В течение срока хранения персональные данные не могут быть обезличены или уничтожены.

7.3.7. По истечении срока хранения персональные данные могут быть обезличены в информационных системах и уничтожены на бумажном носителе.

8. Угрозы в ЕИИС «Соцстрах»

В соответствии с «Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» Приказ ФСТЭК России от 11.02.2013 N 17, для обеспечения безопасности ПДн при их обработке в ИСПДн ЕИИС "Соцстрах" используются мероприятия по техническому обеспечению безопасности ПДн при их обработке в ИСПДн.

В соответствии с «Моделью угроз безопасности персональных данных при их обработке в информационной системе персональных данных единой интегрированной информационной системе Фонда социального страхования Российской Федерации» ИСПДн ЕИИС «Соцстрах» обладает следующими характеристиками:

– категория обрабатываемых в ИСПДн данных – 1 (первая);

– объем обрабатываемых персональных данных – 1 (в информационной системе одновременно обрабатываются персональные данные более чем 100000 субъектов персональных данных);

– характеристики безопасности персональных данных – специальная информационная система;

– структура информационной системы – распределенная;

– наличие подключения к сетям связи общего пользования и (или) сетям международного информационного обмена – информационная система, имеющая подключения;

– режим обработки персональных данных в информационной системе – многопользовательский;

– разграничение прав доступа пользователей к информационной системе - система с разграничением прав доступа;

– местонахождение информационной системы – в пределах Российской Федерации.

Актуальными угрозами безопасности ПДн в ИСПДн ЕИИС "Соцстрах" являются:

– угрозы, реализуемые после загрузки операционной системы;

– угрозы внедрения вредоносных программ;

– угрозы, реализуемые в ходе загрузки операционной системы;

– угрозы внедрения ложного объекта сети как в ИСПДн ЕИИС "Соцстрах", так и во внешних сетях;

– угрозы выявления паролей;

– угрозы удаленного запуска приложений;

– угрозы внедрения по сети вредоносных программ;

– угрозы подмены доверенного объекта.

9. Система защиты персональных данных в ЕИИС «Соцстрах»

В соответствии с Федеральным Законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Защита персональных данных является составной частью работ по созданию и эксплуатации ЕИИС «Соцстрах», должна осуществляться в установленном настоящим положением порядке и реализуется в виде Системы защиты персональных данных ЕИИС «Соцстрах» (СЗПДн ЕИИС «Соцстрах»).

Целями создания СЗПДн ЕИИС "Соцстрах" является обеспечение реализации Федерального закона Российской Федерации от 27 июля 2006 г. №152-ФЗ "О персональных данных", обеспечение реализации постановления Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"

Под защитой персональных данных субъекта понимается комплекс мер (организационно-распорядительных, технических, юридических), направленных на предотвращение неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных субъектов, а также от иных неправомерных действий.

Защита персональных данных субъекта осуществляется за счёт регионального отделения в порядке, установленном федеральным законом.

СЗПДн ЕИИС "Соцстрах" обеспечивает защищенность персональных данных от угроз в ЕИИС «Соцстрах».

Региональное отделение при защите персональных данных субъектов принимает все необходимые организационно-распорядительные, юридические и технические меры, в том числе:

– шифровальные (криптографические) средства;

– антивирусная защита;

– анализ защищённости;

– обнаружение и предотвращение вторжений;

– управления доступом;

– регистрация и учет;

– обеспечение целостности;

– организация нормативно-методических локальных актов, регулирующих защиту персональных данных;

– обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними в соответствии с документацией;

– учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

– учет лиц, допущенных к работе с персональными данными в информационной системе;

– контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

– разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

10. Область ответственности сотрудников

Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе оператором или уполномоченным лицом может назначаться структурное подразделение или должностное лицо, ответственные за обеспечение безопасности персональных данных.

Ответственность за выполнение требований настоящего положения несут:

– заместитель управляющего отвечающий за обеспечение защиты персональных данных;

– ответственные за защиту персональных данных в структурных подразделениях регионального отделения;

– сотрудники, осуществляющие обработку ПДн согласно должностным обязанностям.

Администратор информационной безопасности осуществляет контроль мероприятий, связанных с функционированием СЗПДн, в соответствии с «Инструкцией администратора информационной безопасности».

Ответственные за защиту персональных данных в структурных подразделениях регионального отделения:

– несут ответственность за нарушения порядка допуска работника к сведениям конфиденциального характера;

– проводят регулярно, не реже одного раза в квартал, инструктаж с работниками регионального отделения по вопросу обеспечения защиты сведений конфиденциального характера;

– организуют выполнение требований настоящего положения и иных нормативных документов по обеспечению режима защиты информации сотрудниками на рабочих местах;

– определяют информационные ресурсы подразделения, подлежащие защите, уязвимые места, проводят анализ риска их использования и реализации рентабельных средств защиты;

– организуют обучение сотрудников основам информационной безопасности;

– информируют отдел информатизации об изменениях в статусе любого сотрудника, использующего информационные ресурсы ИСПДн.

Ответственные за защиту персональных данных в структурных подразделениях регионального отделения обязаны:

– осуществлять мероприятия по обеспечению соблюдения режима обработки ПДн;

– сообщать руководителю регионального отделения, или его заместителю, или администратору безопасности о фактах и попытках НСД к ПДн, случаях утечки и разрушения ПДн;

– вносить предложения по совершенствованию режима конфиденциальности, СЗПДн, принимать меры к усилению безопасности в ИСПДн;

Пользователи ИСПДн:

– отвечают за соблюдение информационной безопасности, принятой в региональном отделении и докладывают руководству о любом подозрении при нарушении информационной защиты.

Пользователи ИСПДн обязаны:

– до получения доступа к конфиденциальным документам и сведениям изучить требования настоящего положения, других нормативных документов

по защите ПДн, действующих в региональном отделении в части их касающейся;

– хранить в тайне ПДн, ставшие им известными по работе или иным путем, пресекать действия других лиц, которые могут привести к разглашению ПДн, докладывать о фактах НСД и действий со стороны других исполнителей, случаях утечки и разрушения обрабатываемой информации;

– знакомиться с конфиденциальными документами и сведениями, к которым получили доступ в силу своих служебных обязанностей, правильно определять конфиденциальность документов, строго соблюдать правила их пользования, порядок учета и хранения;

– при составлении конфиденциальных документов, содержащими ПДн, ограничиваться минимальными, действительно необходимыми конфиденциальными сведениями; определять количество экземпляров конфиденциальных документов, в строгом соответствии со служебной необходимостью и не допускать рассылки их адресатам, к которым они не имеют отношения;

– при работе с конфиденциальными документами, содержащими ПДн, на рабочем месте держать только те конфиденциальные документы, с которыми осуществляется работа; все остальные хранить в сейфе (в металлическом шкафу);

– соблюдать правила работы с СЗИ и установленный режим разграничения доступа, принятый в СЗПДн к техническим средствам, программам, данным, файлам с ПДн при ее обработке и другие требования, установленные в региональном отделении;

– при увольнении, переходе в другое подразделение регионального отделения, уходе в отпуск, отъезде в длительную командировку сдавать или отчитываться перед ответственным за защиту персональных данных в структурном подразделении регионального отделения за учет и хранение конфиденциальных сведений, содержащими ПДн, за все числящиеся за ними конфиденциальные документы;

– знакомить представителей других организаций с конфиденциальными документами, содержащими ПДн, только по согласованию и с письменного разрешения соответствующих руководителей регионального отделения, при наличии документов у представителей других организаций, удостоверяющих их личность.

Пользователям ИСПДн запрещается:

– сообщать свои пароли кому бы то ни было, и разрешать входить в сеть под своим именем, подбирать или отгадывать чужие пароли;

– изменять конфигурационную настройку операционной системы; добавлять, изменять или удалять программное обеспечение, отдельные компоненты операционной системы;

– модифицировать чужие файлы, если по каким-то причинам у них есть доступ на запись;

– использовать ПДн в открытых документах, на АРМ, не предназначенных для обработки (хранения) ПДн;

– сообщать устно или письменно посторонним лицам ПДн;

– выполнять работы, связанные с обработкой ПДн, на дому;

– снимать копии с документов, содержащих ПДн, или производить выписки из них без письменного разрешения руководителя подразделения;

– передавать и принимать без росписи конфиденциальные документы и содержащие ПДн;

– уничтожать самостоятельно (без согласования с руководителем подразделения) ПДн;

– не санкционированно тиражировать, передавать и модифицировать программные СЗИ.

Детальные обязанности сотрудников Регионального отделения в части защите информации должны быть указаны в должностных инструкциях и положениях о соответствующих подразделениях.

Отказ соблюдать настоящее положение может подвергнуть защищаемую информацию регионального отделения недопустимому риску потери конфиденциальности, целостности или доступности при ее хранении, обработке или передаче.

При выявлении фактов нарушения прав доступа к сведениям конфиденциального характера руководителям структурных подразделений регионального отделения необходимо немедленно информировать об этом руководство регионального отделения. По всем выявленным фактам проводятся служебные разбирательства с выяснением причин и обстоятельств происшедшего и с принятием дисциплинарных мер в отношении виновных нарушителей. При этом учитывается, что работники регионального отделения, разгласившие сведения конфиденциального характера, а также работники, по вине которых произошла утеря документов, несут ответственность, предусмотренную действующим законодательством Российской Федерации, внутренними документами регионального отделения и условиями трудового договора.

Приложение
к положению об обработке
персональных данных в
информационной системе
персональных данных
Государственного учреждения -
регионального отделения Фонда
социального страхования РФ
по ХМАО - Югре

Обязательство о неразглашении сведений конфиденциального характера

1. Я, _____, являясь работником Государственного учреждения – регионального отделения Фонда социального страхования Российской Федерации по Ханты-Мансийскому автономному округу - Югре (далее – региональное отделение), настоящим документом добровольно заявляю о своем согласии соблюдать следующие условия в течение всего срока действия своего трудового договора:

1.1. Не разглашать сведения конфиденциального характера, которые мне будут доверены или станут известны в процессе работы в региональном отделении.

1.2. Не передавать третьим лицам и не раскрывать публично сведения конфиденциального характера без согласия руководства регионального отделения.

1.3. Выполнять относящиеся ко мне требования приказов, инструкций и положений по обеспечению сохранности сведений конфиденциального характера регионального отделения.

1.4. В случае попытки посторонних лиц получить от меня сведения об отделении Фонда конфиденциального характера немедленно сообщить об этом непосредственному руководителю.

1.5. В случае моего увольнения все носители конфиденциальной информации регионального отделения (черновики, диски, дискеты, распечатки на бумажных носителях и пр.), которые находились в моем распоряжении в связи с выполнением мною служебных обязанностей во время работы в региональном отделении, передать региональному отделению.

1.6. Об утере или недостаче носителей конфиденциальной информации, удостоверений, пропусков, ключей от режимных помещений, хранилищ, сейфов (металлических шкафов), личных печатей и о других фактах, которые могут привести к разглашению данных регионального отделения конфиденциального характера, а также сведений о ставших мне известными фактах, причинах и условиях возможной утечки информации конфиденциального характера, нанесения ущерба региональному отделению немедленно сообщать непосредственному руководителю.

2. Настоящим я выражаю свое понимание и согласие с тем, что:

2.1. Сведения конфиденциального характера определяются руководством регионального отделения и отражаются в Перечне сведений конфиденциального характера, имеющихся в региональном отделении.

2.2. Я, как работник регионального отделения, имею право работать только с теми сведениями и документами, содержащими сведения конфиденциального характера регионального отделения, к которым я получил доступ в силу своих трудовых функций.

2.3. При участии в работе сторонних организаций я могу знакомить их представителей со сведениями конфиденциального характера регионального отделения только с письменного разрешения своего руководителя.

2.4. Я обязан по первому требованию управляющего региональным отделением, его заместителей, руководителя структурного подразделения предъявить для проверки все числящиеся за мной материалы, содержащие сведения конфиденциального характера регионального отделения, представлять письменные или устные объяснения о нарушениях установленных правил, а также о фактах их разглашения, утере документов и изделий, содержащих такие сведения.

2.5. Мне известно, что нарушение настоящего обязательства может повлечь уголовную, материальную и дисциплинарную ответственность в соответствии
с действующим законодательством Российской Федерации.

Должность работника	_____ Подпись	И. О. Фамилия	_____ Дата
Руководитель структурного подразделения, принявший решение о допуске	_____ Подпись	И. О. Фамилия	_____ Дата