



ПРАВИТЕЛЬСТВО СВЕРДЛОВСКОЙ ОБЛАСТИ
МИНИСТЕРСТВО
МЕЖДУНАРОДНЫХ И ВНЕШНЕЭКОНОМИЧЕСКИХ СВЯЗЕЙ
СВЕРДЛОВСКОЙ ОБЛАСТИ

ПРИКАЗ

23.07.2020

№ 28

г. Екатеринбург

Об утверждении политики обработки персональных данных на портале внешнеэкономической деятельности Свердловской области «Made-in-Ural» и Положения о порядке обработки и защиты персональных данных в программном комплексе «Информационная система управления финансами» (ПК «ИСУФ») в части модуля управления в отрасли внешнеторговой деятельности Свердловской области

В соответствии с подпунктом 2 пункта 1 статьи 18.1 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», руководствуясь постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие политику обработки персональных данных на портале внешнеэкономической деятельности Свердловской области «Made-in-Ural» (прилагается).

2. Установить, что обработка и защита персональных данных в программном комплексе «Информационная система управления финансами» (ПК «ИСУФ») в части модуля управления в отрасли внешнеторговой деятельности Свердловской области осуществляется в соответствии с Положением о порядке обработки и защиты персональных данных в программном комплексе «Информационная система управления финансами» (ПК «ИСУФ») в части модуля управления в отрасли внешнеторговой деятельности Свердловской области (прилагается).

3. Департаменту внешнеэкономического и гуманитарного сотрудничества Министерства международных и внешнеэкономических связей Свердловской области обеспечить размещение политики обработки персональных данных на портале внешнеэкономической деятельности Свердловской области «Made-in-Ural», утвержденной пунктом 1 настоящего приказа, на портале внешнеэкономической деятельности Свердловской области «Made-in-Ural».

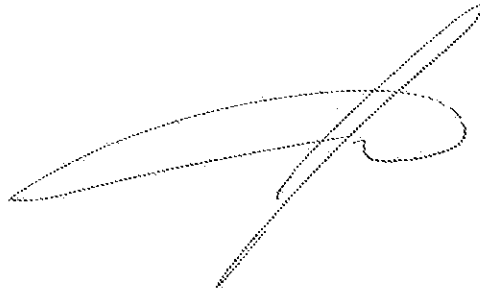
4. Контроль за исполнением настоящего приказа возложить на Заместителя Министра международных и внешнеэкономических связей Свердловской области В.Ю. Ярина.

5. Отделу государственной службы, организационной работы, бюджетного планирования и учета Министерства международных и внешнеэкономических связей Свердловской области обеспечить:

1) официальное опубликование настоящего приказа на «Официальном интернет-портале правовой информации Свердловской области» (www.pravo.gov66.ru), размещение на «Официальном интернет-портале правовой информации» (www.pravo.gov.ru) и официальном сайте Министерства международных и внешнеэкономических связей Свердловской области в информационно-телекоммуникационной сети «Интернет» (mvs.midural.ru);

2) направление копий настоящего приказа в Прокуратуру Свердловской области и в Главное управление Министерства юстиции Российской Федерации по Свердловской области.

Министр



В.В. Козлов

УТВЕРЖДЕНА
приказом Министерства
международных
и внешнеэкономических связей
Свердловской области
№ 28 от 23.04.2020
«Об утверждении политики обработки
персональных данных на портале
внешнеэкономической деятельности
Свердловской области «Made-in-Ural»
и Положения о порядке обработки
и защиты персональных данных
в программном комплексе
«Информационная система управления
финансами» (ПК «ИСУФ») в части
модуля управления в отрасли
внешнеторговой деятельности
Свердловской области»

ПОЛИТИКА
обработки персональных данных на портале внешнеэкономической деятельности
Свердловской области «Made-in-Ural»

1. Общие положения

1.1. Настоящая политика обработки персональных данных на портале внешнеэкономической деятельности Свердловской области «Made-in-Ural» (далее — Политика) разработана в соответствии с частью 2 статьи 18.1 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» в целях обеспечения защиты прав и свобод субъектов персональных данных (далее – субъект ПДн, пользователь) при обработке их персональных данных (далее – персональные данные, ПДн).

1.2. Оператором ПДн, обрабатываемых на портале внешнеэкономической деятельности Свердловской области «Made-in-Ural» (далее – Портал), является Министерство международных и внешнеэкономических связей Свердловской области, расположенное по адресу: 620075, г. Екатеринбург, ул. Горького, 21/23 (далее – Оператор).

1.3. Политика действует в отношении всех ПДн, которые Оператор может получить от пользователя Портала.

1.4. Политика распространяется на ПДн, полученные как до, так и после подписания настоящей Политики.

1.5. Оператор обеспечивает защиту обрабатываемых персональных данных от несанкционированного доступа и разглашения, неправомерного использования или утраты в соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

1.6. Оператор вправе вносить изменения в настоящую Политику.

При внесении изменений в заголовке Политики указывается дата последнего обновления редакции. Новая редакция Политики вступает в силу с момента ее размещения на Портале, если иное не предусмотрено изменениями.

2. Термины и принятые сокращения

2.1. В целях настоящей Политики используются термины «персональные данные», «обработка персональных данных», «автоматизированная обработка персональных данных», «информационная система персональных данных», «блокирование персональных данных», «передача персональных данных» и «уничтожение персональных данных» в значениях, определенных статьей 3 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

2.2. **Оператор** – организация, самостоятельно или совместно с другими лицами организующая обработку персональных данных, а также определяющая цели обработки персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

2.3. **Персональные данные, сделанные общедоступными пользователем** – персональные данные, доступ неограниченного круга лиц к которым предоставлен пользователем либо по его просьбе.

2.4. **СЗПДн** – система защиты персональных данных.

3. Обработка персональных данных

3.1. Все персональные данные следует получать от самого субъекта ПДн. Если персональные данные субъекта ПДн можно получить только у третьей стороны, то субъект ПДн должен быть уведомлен об этом или от него должно быть получено согласие.

Оператор должен сообщить субъекту ПДн о целях, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению ПДн, перечне действий с ПДн, сроке, в течение которого действует согласие, и порядке его отзыва, а также о последствиях отказа субъекта дать письменное согласие на их получение.

3.2. Обработка персональных данных.

Обработка персональных данных осуществляется:

- с согласия субъекта ПДн на обработку его персональных данных, оформляемого по форме в соответствии с Приложением № 1 к Политике;

- в случаях, когда обработка персональных данных необходима Оператору для осуществления и выполнения возложенных на него законодательством Российской Федерации функций, полномочий и обязанностей;

- в случаях, когда осуществляется обработка персональных данных, сделанные общедоступными пользователем.

3.3. Категории субъектов персональных данных.

Обрабатываются персональные данные следующих субъектов ПДн:

- физические лица, являющиеся сотрудниками предприятий Свердловской области, информация о которых размещается на Портале;

- физические лица, осуществляющие передачу своих персональных данных при регистрации на Портале.

3.4. Цель обработки персональных данных – предоставление информации об экспорте ориентированных предприятиях Свердловской области.

3.5. Содержание и объем обрабатываемых ПДн соответствуют заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

3.6. Персональные данные, обрабатываемые Оператором, получены от пользователей Портала.

3.7. Обработка персональных данных ведется с использованием средств автоматизации.

3.8. Хранение персональных данных.

Персональные данные субъектов ПДн могут быть получены, проходить дальнейшую обработку и храниться только в электронном виде.

Не допускается хранение и размещение документов, содержащих персональные данные, в открытых электронных каталогах (файлообменниках) в информационной системе персональных данных (далее – ИСПДн).

Хранение персональных данных в форме, позволяющей определить субъекта ПДн, осуществляется не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

3.9. Уничтожение персональных данных.

ПДн на электронных носителях уничтожаются путем стирания или форматирования носителя.

Факт уничтожения ПДн подтверждается документально актом об уничтожении персональных данных / съемных носителей информации, содержащей персональные данные, согласно Приложению № 2 к Политике.

3.10. Передача персональных данных.

Оператор передает персональные данные третьим лицам в случаях, если:

- субъект ПДн выразил свое согласие на такие действия;
- передача ПДн предусмотрена российским законодательством в рамках установленной законодательством процедуры.

4. Защита персональных данных

4.1. В соответствии с требованиями нормативных документов Оператором создана СЗПДн, состоящая из подсистем правовой, организационной и технической защиты.

Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование СЗПДн.

Подсистема организационной защиты включает в себя организацию структуры управления СЗПДн, разрешительной системы, защиты информации при работе с сотрудниками, партнерами и сторонними лицами.

Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту персональных данных.

4.2. Основными мерами защиты ПДн, используемыми Оператором, являются:

– назначение лица, ответственного за обработку ПДн, которое осуществляет организацию обработки персональных данных, обучение и инструктаж, внутренний контроль за соблюдением Оператором и его сотрудниками требований к защите персональных данных;

– определение актуальных угроз безопасности ПДн при их обработке в ИСПДн и разработка мер и мероприятий по защите персональных данных;

– разработка политики в отношении обработки персональных данных;

- установление правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечение регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;
- установление индивидуальных паролей доступа сотрудников в ИСПДн в соответствии с их производственными обязанностями;
- соблюдение условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ;
- обнаружение фактов несанкционированного доступа к ПДн и принятие мер;
- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- обучение сотрудников Оператора, непосредственно осуществляющих обработку ПДн, положениям законодательства Российской Федерации о персональных данных, документам, определяющим политику Оператора в отношении обработки ПДн, и другим правовым актам Оператора по вопросам обработки ПДн.

5. Основные права субъекта персональных данных и обязанности Оператора

5.1. Субъект ПДн имеет право на доступ к его ПДн и следующим сведениям:

- подтверждение факта обработки его персональных данных Оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые Оператором способы обработки персональных данных;
- наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Оператором или на основании требований законодательства Российской Федерации;
- сроки обработки персональных данных, в том числе сроки их хранения;
- наименование или фамилия, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Оператора, если обработка поручена или будет поручена такому лицу;
- порядок обжалования действий или бездействия Оператора.

5.2. Оператор обязан:

- при сборе ПДн предоставить информацию об обработке персональных данных;
- в случаях если персональные данные были получены не от субъекта ПДн, уведомить субъекта ПДн;
- при отказе в предоставлении персональных данных пользователю разъясняются последствия такого отказа;
- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных;
- принимать необходимые правовые, организационные и технические меры, или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении ПДн;
- давать ответы на запросы и обращения субъектов ПДн, их представителей и уполномоченного органа по защите прав субъектов персональных данных.

Форма

**Пользовательское соглашение
(согласие на обработку персональных данных), оформляемое при прохождении
регистрации на портале внешнеэкономической деятельности Свердловской
области «Made-in-Ural»**

1. Общие положения

1.1. В рамках настоящего согласия под персональными данными (ПДн) пользователя понимаются:

– персональная информация, которую пользователь предоставляет о себе самостоятельно при регистрации (создании учетной записи) или в процессе использования Личного кабинета экспортера на портале внешнеэкономической деятельности Свердловской области «Made-in-Ural» (далее – Сервисов), включая персональные данные пользователя в разделе Профиль. Обязательная для предоставления Сервиса информация помечена специальным образом. Иная информация предоставляется пользователем на его усмотрение.

– данные, которые автоматически передаются Сервисом в процессе их использования с помощью установленного на устройстве пользователя программного обеспечения, в том числе IP-адрес, данные файлов cookie, информация о браузере пользователя (или иной программе, с помощью которой осуществляется доступ к Сервису), технические характеристики оборудования и программного обеспечения, используемых пользователем, дата и время доступа к сервисам, адреса запрашиваемых страниц и иная подобная информация.

– иная информация о пользователе, обработка которой предусмотрена Соглашением об использовании Сервиса.

1.2. Настоящее Пользовательское соглашение применяется только к Сервису доступному по веб-адресу <https://made-in-ural.ru>

1.3. Сервис не контролирует и не несет ответственности за сайты третьих лиц, на которые Пользователь может перейти по ссылкам, доступным в данном Сервисе.

2. Цели обработки персональной информации пользователей

2.1. Сервис собирает и хранит только ту персональную информацию, которая необходима для предоставления сервисов или исполнения соглашений и договоров с пользователем, за исключением случаев, когда законодательством Российской Федерации предусмотрено обязательное хранение персональной информации в течение определенного законом срока.

2.2. Персональная информация пользователя обрабатывается в следующих целях:

– идентификации пользователя, зарегистрированного в Сервисе, для сбора необходимой статистической информации и предоставления ему соответствующих сервисов и услуг;

- предоставления пользователю доступа к персонализированным ресурсам Сервиса;
- установления с пользователем обратной связи, включая направление уведомлений, запросов, касающихся использования Сервиса, оказания услуг, обработку запросов и заявок от пользователя;
- определения места нахождения пользователя для обеспечения безопасности, предотвращения мошенничества;
- подтверждения достоверности и полноты ПДн, предоставленных Пользователем;
- создания учетной записи пользователя для доступа к закрытым услугам Сервиса, если пользователь дал согласие на создание учетной записи;
- предоставления пользователю эффективной клиентской и технической поддержки при возникновении проблем, связанных с использованием Сервиса.

3. Условия обработки персональной информации пользователя и ее передачи третьим лицам

3.1. В отношении персональной информации пользователя сохраняется ее конфиденциальность, кроме случаев добровольного предоставления пользователем информации о себе для общего доступа неограниченному кругу лиц. При использовании отдельных сервисов пользователь соглашается с тем, что определенная часть его персональной информации становится общедоступной.

3.2. Сервис вправе передать ПДн пользователя третьим лицам в следующих случаях:

- пользователь выразил согласие на такие действия;
- передача необходима для использования пользователем определенного сервиса, либо для исполнения определенного соглашения или договора с пользователем;
- передача ПДн предусмотрена законодательством Российской Федерации в рамках установленной процедуры.

3.3. Обработка персональных данных пользователя осуществляется без ограничения срока любым законным способом, в том числе в информационных системах персональных данных с использованием средств автоматизации или без использования таких средств. Обработка персональных данных пользователей осуществляется в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных».

3.4. Администратор Сервиса принимает необходимые организационные и технические меры для защиты персональной информации пользователя от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий третьих лиц.

3.5. Администратор Сервиса совместно с пользователем принимает все необходимые меры по предотвращению убытков или иных отрицательных последствий, вызванных утратой или разглашением персональных данных пользователя.

4. Обязательства сторон

4.1. Пользователь обязан:

- предоставить информацию о персональных данных, необходимую для пользования Сервисом;
- обновлять, дополнять предоставленную информацию о персональных данных в случае изменения данной информации.

4.2. Администратор Сервиса обязан:

– использовать полученную информацию исключительно для целей, указанных в настоящем Пользовательском соглашении;

– обеспечить хранение ПДн в тайне, не разглашать без предварительного письменного разрешения пользователя, а также не осуществлять продажу, обмен, опубликование либо разглашение иными возможными способами переданных персональных данных пользователя, за исключением случаев, предусмотренных настоящим Пользовательским соглашением;

– принимать меры предосторожности для защиты конфиденциальности персональных данных пользователя согласно порядку, обычно используемому для защиты такого рода информации в существующем деловом обороте;

– осуществить блокирование ПДн, относящихся к соответствующему пользователю, с момента обращения или запроса пользователя или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных на период проверки в случае выявления недостоверных персональных данных или неправомерных действий.

5. Ответственность сторон

5.1. Администратор Сервиса, не исполнивший свои обязательства, несет ответственность за убытки, понесенные пользователем в связи с неправомерным использованием ПДн, в соответствии с законодательством Российской Федерации.

5.2. В случае утраты или разглашения ПДн Администратор Сервиса не несет ответственности, если данная конфиденциальная информация:

- стала публичным достоянием до ее утраты или разглашения;
- была получена от третьей стороны до момента ее получения Администратором Сервиса;
- была разглашена с согласия пользователя.

Приложение № 2
к политике обработки персональных
данных на портале
внешнеэкономической деятельности
Свердловской области «Made-in-Ural»

Форма

АКТ
об уничтожении персональных данных / съемных носителей информации,
содержащей персональные данные

_____ место составления акта

_____ число, месяц, год

Комиссия, наделенная полномочиями приказом Министерства международных и внешнеэкономических связей Свердловской области от _____ № _____, в составе:

- 1) _____
(должность, фамилия, инициалы)
- 2) _____
(должность, фамилия, инициалы)
- 3) _____
(должность, фамилия, инициалы)

Зафиксировала уничтожение персональных данных / провела отбор съемных носителей персональных данных, не подлежащих дальнейшему хранению:

№ п/п	Учетный номер съемного носителя	ПДн, содержащиеся на съемном носителе
1		
2		

Всего съемных носителей: _____ штук.
(количество цифрами и прописью)

На съемных носителях уничтожена информация, содержащая ПДн, путем

_____ (указать способ уничтожения)

Вышеперечисленные съемные носители уничтожены путем / сданы для уничтожения предприятию по утилизации вторичного сырья

_____ (указать способ уничтожения / наименование предприятия)

Председатель комиссии:

_____ (должность, фамилия, инициалы)

Секретарь комиссии:

_____ (должность, фамилия, инициалы)

Члены комиссии:

_____ (должность, фамилия, инициалы)

_____ (должность, фамилия, инициалы)

К приказу Министерства
международных
и внешнеэкономических связей
Свердловской области

№ 28 от 23.09.2020

ПОЛОЖЕНИЕ

о порядке обработки и защиты персональных данных
в программном комплексе «Информационная система управления финансами»
(ПК «ИСУФ») в части модуля управления в отрасли внешнеторговой деятельности
Свердловской области

1. Общие положения

1.1. Настоящее Положение регламентирует вопросы обеспечения безопасности персональных данных (далее – персональные данные, ПДн) при их обработке в программном комплексе «Информационная система управления финансами» (ПК «ИСУФ») в части модуля управления в отрасли внешнеторговой деятельности Свердловской области (далее – ИС) и определяет порядок обработки и защиты ПДн.

1.2. Настоящее Положение разработано на основании следующих основных нормативных правовых актов и документов в области обеспечения безопасности ПДн:

– Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

– постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.3. В целях настоящего Положения используются термины «персональные данные», «обработка персональных данных», «автоматизированная обработка персональных данных», «информационная система персональных данных», «блокирование персональных данных», «передача персональных данных» и «уничтожение персональных данных» в значениях, определенных статьей 3 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

1.4. **Оператор** – организация, самостоятельно или совместно с другими лицами организующая обработку персональных данных, а также определяющая цели обработки персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

1.5. **Персональные данные, сделанные общедоступными субъектом персональных данных** – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом ПДн либо по его просьбе.

1.6. **СЗПДн** – система защиты персональных данных.

2. Состав и цели обработки персональных данных

2.1. В ИС обрабатываются данные физических лиц, являющихся сотрудниками предприятий Свердловской области, информация о которых размещается на портале внешнеэкономической деятельности Свердловской области «Made-in-Ural» (далее – Портал), а также осуществляющих передачу своих персональных данных при регистрации на Портале.

2.2. В ИС обрабатываются следующие ПДн:

- фамилия, имя, отчество;
- должность;
- номер телефона и адрес электронной почты.

2.3. Цели обработки ПДн:

- предоставление информации об экспорте ориентированных предприятиях Свердловской области;
- организация взаимодействия с посетителями Портала.

3. Должностные лица и их обязанности

3.1. В ИС определены следующие роли:

- администраторы ИС;
- операторы ИС.

3.2. Администраторы и операторы ИС являются пользователями ИСПДн, доступ которых к ПДн, обрабатываемым в ИС, необходим для выполнения ими служебных (трудовых) обязанностей, и назначаются приказом Министерства международных и внешнеэкономических связей Свердловской области (далее – Министерство).

3.3. Учётные записи администраторов и операторов ИС должны быть внесены в Журнал учетных записей лиц, допущенных для работы с персональными данными, оформляемом согласно Приложению № 1 к настоящему Положению.

3.4. После назначения приказом Министерства до начала работы с ИС оператор ИС должен пройти первичный инструктаж, включающий ознакомление с нормами законодательства Российской Федерации об ответственности за неисполнение требований по обеспечению безопасности ПДн в ИС и изучение следующих правовых документов о работе с ПДн:

- Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»,
- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,
- приказ Министерства об утверждении политики обработки персональных данных на портале внешнеэкономической деятельности Свердловской области «Made-in-Ural»,
- приказ Министерства об утверждении перечня сотрудников, допущенных к обработке персональных данных в ИСУФ в части модуля управления в отрасли внешнеторговой деятельности Свердловской области,
- инструкция о порядке резервирования и восстановления информационной системы (Приложение № 2 к настоящему Положению),
- настоящее Положение и иные правовые акты Министерства по вопросам обработки ПДн.

4. Порядок обработки ПДн

4.1. Обработка ПДн осуществляется после регистрации субъекта персональных данных (далее – субъект ПДн, пользователь) на Портале при условии обязательного согласия с обработкой ПДн и ознакомления с политикой обработки ПДн на Портале.

4.2. Соглашаясь на обработку ПДн, пользователь делает их общедоступными, разрешая публикацию своих ПДн на Портале. Министерство обеспечивает защиту ПДн от неправомерного их использования или утраты. Обработка ПДн осуществляется только с использованием средств автоматизации.

4.3. При обработке ПДн уполномоченные должностные лица Министерства обязаны соблюдать следующие требования:

- объем и характер обрабатываемых ПДн, способы обработки ПДн должны соответствовать целям обработки ПДн;

- защита ПДн от неправомерного их использования или уничтожения обеспечивается в порядке, установленном законодательством Российской Федерации;

- хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн не дольше, чем этого требует цели их обработки. Указанные сведения подлежат уничтожению по достижению цели их обработки или в случае утраты необходимости в их достижении, если иное не установлено законодательством Российской Федерации. Факт уничтожения ПДн оформляется соответствующим актом.

4.4. В целях обеспечения защиты ПДн пользователи вправе:

- получать полную информацию о своих ПДн и способе обработки этих данных (в том числе автоматизированной);

- осуществлять свободный бесплатный доступ к своим ПДн, включая право получать копии любой записи, за исключением случаев, предусмотренных законодательством Российской Федерации;

- требовать внесения необходимых изменений, уничтожения или блокирования соответствующих ПДн, которые являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

- обжаловать в порядке, установленном законодательством Российской Федерации, действия (бездействия) уполномоченных должностных лиц.

4.5. Классификация ИСПДн осуществляется в порядке, установленном законодательством Российской Федерации. Безопасность ПДн, обрабатываемых с использованием средств автоматизации, достигается путем исключения несанкционированного, в том числе случайного доступа к ПДн.

4.6. Обмен ПДн при их обработке в ИС осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения программных и технических средств.

4.7. Доступ операторов ИС к ПДн должен требовать обязательного прохождения процедуры идентификации и аутентификации.

4.8. Структурными подразделениями (должностными лицами) Министерства, ответственными за обеспечение безопасности ПДн при их обработке в информационных системах, должно быть обеспечено:

- своевременное обнаружение фактов несанкционированного доступа к ПДн и немедленное доведение этой информации до руководства;

- недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;

- возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- постоянный контроль за обеспечением уровня защищенности ПДн;
- знание и соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- при обнаружении нарушений порядка предоставления ПДн незамедлительное приостановление предоставления ПДн пользователям ИС до выявления причин нарушений и устранения этих причин;
- разбирательство и составление заключений по фактам несоблюдения условий хранения носителей ПДн, использования средств защиты информации, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

4.9. Носители информации, на которых хранятся ПДн ИС, а также резервные копии, содержащие ПДн, должны быть учтены в Журнале учета машинных носителей, содержащих информацию ограниченного доступа по форме согласно Приложению № 3 к настоящему Положению.

4.10. Министерство осуществляет внутренний контроль (мониторинг) соответствия обработки ПДн требованиям законодательства Российской Федерации о персональных данных, документов, определяющих политику Министерства в отношении обработки ПДн, настоящего Положения и других правовых актов Министерства по вопросам обработки персональных данных. Указанный контроль проводится не реже одного раза в три года в сроки, определяемые Министерством.

4.11. В случае выявления нарушений порядка обработки ПДн в информационных системах, уполномоченными должностными лицами принимаются меры по установлению причин нарушений и их устранению.

5. Ответственность за нарушение требований законодательства

5.1. Сотрудники Министерства, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном законодательством Российской Федерации.

6. Порядок приостановления предоставления персональных данных и их обработки

6.1. При обнаружении нарушений порядка предоставления ПДн по результатам внутреннего контроля или аудита сторонней организации необходимо незамедлительно приостановить предоставление ПДн пользователями ИСПДн до выявления причин нарушений и устранения этих причин.

6.2. Принятие решения о приостановлении обработки ПДн принимается Министром международных и внешнеэкономических связей Свердловской области.

6.3. Администратор ИС запрещает доступ операторов к ИС при обнаружении нарушений и восстанавливает доступ после устранения причин, приведших к нарушениям.

6.4. По факту нарушения требований по обеспечению безопасности, повлекшего приостановление обработки ПДн, может быть проведено служебное расследование.

7. Порядок уничтожения персональных данных

7.1. Уничтожение ПДн должно быть проведено в случаях:

- достижения целей обработки ПДн или утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством Российской Федерации;
- отзыва субъектом ПДн согласия на обработку его ПДн;
- выявления фактов неправомерной обработки ПДн (в том числе при обращении субъекта ПДн), если обеспечить их правомерность не предоставляется возможным.

7.2. Перед уничтожением ПДн необходимо убедиться:

- в правовых основаниях уничтожения ПДн;
- в том, что уничтожаются именно те ПДн, которые предназначены для уничтожения;
- в способе, подходящем для уничтожения в соответствии с требованиями законодательства Российской Федерации;
- в соблюдении порядка уведомления субъекта ПДн (его представителя, или третьих лиц – в случаях, установленных законодательством Российской Федерации) об уничтожении его персональных данных.

7.3. Уничтожение ПДн возможно осуществить одним из следующих способов:

- физическое уничтожение носителя ПДн;
- уничтожение ПДн с носителя ПДн.

7.4. Уничтожение информации на машинных носителях ПДн необходимо осуществлять путем стирания информации с использованием программного обеспечения с гарантированным уничтожением. При уничтожении ПДн необходимо учитывать возможность их наличия в архивных базах данных и производить уничтожение во всех копиях базы данных, если иное не установлено действующим законодательством Российской Федерации.

7.5. Если ПДн хранятся на машинном носителе ПДн, пришедшем в негодность, отслужившем установленный срок или утратившем практическое значение, такой машинный носитель ПДн подлежит физическому уничтожению. Перед уничтожением машинного носителя ПДн на нем производится стирание ПДн путем использования программного обеспечения с гарантированным уничтожением информации.

7.6. После стирания ПДн машинный носитель ПДн уничтожается одним из следующих способов: разрезание, сжигание, механическое уничтожение, сдача предприятию по утилизации вторичного сырья или иными методами, исключающими возможность восстановления содержания ПДн.

7.7. По факту уничтожения ПДн составляется акт об уничтожении персональных данных / съемных носителей информации, содержащей персональные данные.

8. Порядок работы с электронными журналами аудита

8.1. Правила и порядок протоколирования и анализа (аудита) значимых событий в ИСПДн направлены на превентивную фиксацию и изучение действий субъектов ПДн и объектов в ИСПДн, а также на своевременное выявление фактов несанкционированного доступа к защищаемой информации.

8.2. Все события, происходящие в операционной системе, ИСПДн и других критических приложениях должны протоколироваться в специальные электронные журналы аудита.

8.3. Проверке подлежат следующие электронные журналы:

- журнал событий, формируемых программным обеспечением ИС и системы управления базами данных;
- журналы, формируемые операционной системой и прикладным программным обеспечением.

8.4. На технических средствах, входящих в состав ИСПДн, на которых установлены средства защиты информации от несанкционированного доступа, проверка соответствующего электронного журнала событий, формируемых данными средствами, производится в соответствии с прилагаемой к ним технической и эксплуатационной документацией.

8.5. Аудит событий, зафиксированных в электронных журналах, анализируется в плановом порядке на постоянной основе не реже одного раза в неделю администратором ИС.

Приложение № 1
к Положению о порядке обработки
и защиты персональных данных
в программном комплексе
«Информационная система управления
финансами» (ПК «ИСУФ») в части
модуля управления в отрасли
внешнеторговой деятельности
Свердловской области»

ИНСТРУКЦИЯ

о порядке резервирования и восстановления информационной системы

1. Назначение и область действия

Настоящая Инструкция определяет действия, связанные с мерами и средствами поддержания непрерывной работы и восстановления работоспособности информационной системы Модуль управления в отрасли внешнеторговой деятельности Свердловской области программного комплекса «Информационная система управления финансами» (далее – ИС).

Инструкция регламентирует:

- меры защиты от потери информации;
- действия по восстановлению ИС в случае потери информации.

Действие настоящей Инструкции распространяется на Администраторов ИС, ответственных за резервное копирование информации.

2. Меры обеспечения надежной работы и восстановления ресурсов при возникновении инцидентов

2.1. Технические меры.

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения инцидентов, такие как:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Системы жизнеобеспечения ИС включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

Помещения, в которых размещаются элементы ИС, должны быть оборудованы средствами пожарной сигнализации и кондиционирования воздуха.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИС должны подключаться к сети электропитания через источники бесперебойного питания.

С целью обеспечения отказоустойчивости ИС данные и системные разделы следует размещать на дисковых массивах, обеспечивающих отказоустойчивость при выходе из строя одного из дисков.

Системы резервного копирования и хранения данных должны обеспечивать надежное хранение защищаемой информации.

2.2. Организационные меры

Резервное копирование данных должно осуществляться на периодической основе:

- для обрабатываемых персональных данных – на ежедневной основе или по требованию пользователя ИС;
- для системной информации – не реже одного раза в месяц;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение), с которых осуществляется их установка на элементы ИС, – каждый раз при внесении изменений в эталонные копии (при переходе на новые версии программного обеспечения).

Носители, на которые производится резервное копирование персональных данных, должны быть учтены в журнале учета машинных носителей, содержащих информацию ограниченного доступа.

3. Порядок проведения восстановления информации

Перед проведением процедуры восстановления информации необходимо убедиться в том, что все пользователи ИС завершили свою работу с ИС.

Восстановление информации следует проводить из наиболее актуальной резервной копии.

Восстановление информации в ИС проводится при помощи штатных средств, поставляемых в составе специализированного программного обеспечения для построения ИС, либо, в случае отсутствия таковых, штатными средствами операционной системы или системы управления базами данных (при использовании таковой).

После завершения процедуры восстановления необходимо убедиться в работоспособности ИС. В случае успешного восстановления оповестить пользователей ИС о возможности продолжения работы. В противном случае – изучить документацию, прилагаемую к программному обеспечению либо обратиться в службу технической поддержки.

