|  |  |  |
| --- | --- | --- |
| СИБУР Холдинг |  | ООО «БИАКСПЛЕН» |
|  |  |  |
|  |  | Дата введения |
|  |  | «\_\_» \_\_\_\_\_\_\_\_\_ 2021 г. |
| Владелец процесса |  | Менеджер процесса |
| Генеральный директор |  | Руководитель направления, Экономическая безопасность |
|  СТП БКП/09-01-01/ЗМУ01 |
| Методические указания по обеспечению безопасности персональных данных |
| Редакция 2.0 |
| п. Гидроторф Нижегородской обл.2021 г. |

Содержание

[1. Область применения 3](#_Toc27567732)

[2. Основные требования 3](#_Toc27567733)

[3. Ответственный за организацию обработки ПДн 4](#_Toc27567734)

[4. Требования к предоставлению доступа к ПДн 5](#_Toc27567735)

[5. Требования к предоставлению доступа к ПДн третьим лицам 5](#_Toc27567736)

[6. Требования к сбору, хранению и уточнению ПДн 6](#_Toc27567737)

[7. Требования к взаимодействию с субъектами ПДн 8](#_Toc27567738)

[8. Требования к уничтожению ПДн 11](#_Toc27567739)

[9. Требования к предоставлению доступа работникам в помещения 11](#_Toc27567740)

[10. Требования к организации защиты ПДн 12](#_Toc27567741)

[11. Ответственность за нарушение требований по обеспечению порядка обработки и защиты ПДн 1](#_Toc27567742)6

1. [Термины, определения и сокращения 17](#_Toc27567743)
2. [Ссылочные документы 17](#_Toc27567744)

Регистрация изменений

| Редакция | Дата утверждения | Дата ввода в действие | Реквизиты утвердившего документа |
| --- | --- | --- | --- |
| 1.0 | 31.08.2012 | 31.08.2012 | Приказ от «31» августа 2012г. № 94/1/ББ |
| 1.1 | 30.05.2016 | 30.05.2016 | Приказ от «30» мая 2016г. 63/Б |
| 2.0 |  |  |  |

# Область применения

Настоящий Стандарт разработан в рамках процесса 09-01-01 «Обеспечение безопасности информационных ресурсов».

Целью документа является определение единых принципов и подходов к обработке персональных данных (далее – ПДн) в ООО «БИАКСПЛЕН», обеспечивающих защиту прав субъектов ПДн.

Настоящий Стандарт распространяется на ООО «БИАКСПЛЕН» (далее – Оператор) и его, персонал, сторонних консультантов, контрагентов и любое физическое или юридическое лицо, которому предоставлен доступ к информационным активам Оператора.

Предметом рассмотрения данного Стандарта не является:

* обработка обезличенных ПДн;
* деятельность по организации хранения, комплектования, учета и использования содержащих ПДн архивных документов, в соответствии с Федеральным законом №125-ФЗ «Об архивном деле в Российской Федерации».

# Основные требования

Требования к определению целей обработки ПДн

* + 1. Необходимость обработки и состав обрабатываемых ПДн определяется исходя из принципа целесообразности такой обработки, при этом должны учитываться:
* цели обработки ПДн;
* планируемые характер и способы обработки ПДн;
* значимость обработки ПДн для достижения целей деятельности Оператора;
* возникающие риски, связанные с обработкой ПДн;
* затраты на осуществление обработки ПДн, в том числе затраты на обеспечение требуемого уровня безопасности ПДн.
	+ 1. Оператор может обрабатывать ПДн следующих категорий субъектов ПДн:
* работников Оператора и их близких родственников (в том числе бывших работников), их представителей, с их согласия;
* кандидатов на трудоустройство;
* физических лиц – работников (их представителей) контрагентов;
* физических лиц – посетителей объектов Оператора или участников проводимых Оператором мероприятий;
* субъектов, ПДн которых переданы Оператору третьими лицами в рамках заключенных договоров.
	+ 1. Оператор не имеет права получать и обрабатывать ПДн, касающиеся расовой и национальной принадлежности, политических, религиозных и философских убеждениях, состояния здоровья, интимной жизни, за исключением случаев, предусмотренных федеральными законами.

# Ответственный за организацию обработки ПДн

3.1. Ответственный за организацию обработки ПДн назначается приказом и получает указания непосредственно от Руководителя Оператора.

3.2. Ответственный за организацию обработки ПДн отвечает за организацию процессов:

* своевременного уведомления уполномоченного органа по защите прав субъектов ПДн об изменении сведений об Операторе, внесенных в реестр операторов ПДн;
* подготовки, своевременного внесения изменений (актуализацию), ввода в действие локальных нормативных актов Оператора, регламентирующих вопросы обработки и обеспечения безопасности ПДн Оператора;
* оперативного контроля над соблюдением Оператором законодательства Российской Федерации и положений локальных нормативных актов по вопросам обработки ПДн и обеспечения безопасности ПДн;
* доведения до сведений работников Оператора положения законодательства Российской Федерации о ПДн, локальных нормативных актов по вопросам обработки ПДн, требований к защите ПДн;
* организации приёма обращений и запросов субъектов ПДн или их законных представителей и осуществления обработки таких обращений и запросов;
* применения правовых, организационных и технических мер по обеспечению безопасности ПДн в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
* организации оценки эффективности принимаемых мер по обеспечению безопасности ПДн в информационных системах ПДн;
* осуществления или организации внутреннего контроля и (или) аудита соответствия обработки ПДн Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, политике Оператора в отношении обработки ПДн;
* организации, проведения контроля над принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности информационных систем ПДн;
* осуществления контроля ознакомления работников Оператора, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, действующих у Оператора политики обработки ПДн и других локальных нормативных актов, определяющих вопросы обработки ПДн и обеспечения их безопасности.

3.3. Ответственный за организацию обработки ПДн также вправе делегировать выполняемые им функции по 3.2. настоящего Стандарта на работников соответствующих структурных подразделений Оператора.

# Требования к предоставлению доступа к ПДн

Доступ к ПДн субъекта имеют работники Оператора, которым ПДн необходимы в связи с выполнением ими должностных обязанностей. Перечень должностей работников, имеющих допуск к ПДн, обрабатываемым в информационных системах Оператора, обрабатывающих ПДн, подготавливается Владельцами информационных активов и утверждается Ответственным лицом или уполномоченным им лицом. Ответственность за актуальность сведений в перечне должностей работников, имеющих допуск к ПДн, обрабатываемым в информационной системе, возлагается на Владельца информационного актива.

Доступ работника к ПДн, обрабатываемым в информационной системе, предоставляется по соответствующей заявке при условии ознакомления работника с Федеральным законом от 27.07.2006 152-ФЗ «О персональных данных», настоящими Методическими указаниями, а также внутренними организационно-распорядительными документами Оператора, регулирующими обработку и защиту ПДн субъектов.

Ответственное лицо или уполномоченное им лицо по представлению Владельца информационного актива утверждает Перечень должностей работников Оператора, допущенных к ПДн, обрабатываемым в информационной системе или изменения в данный Перечень.

# Требования к предоставлению доступа к ПДн третьим лицам

Оператор вправе поручить обработку ПДн третьим лицам с согласия субъекта ПДн на основании заключаемого с этими лицами договора.

Передача ПДн судебным и контрольно-надзорным органам (включая налоговые инспекции, правоохранительные органы, органы социального страхования, пенсионные фонды, другие организации) может осуществляться без письменного согласия субъекта в тех случаях, когда необходимость такой передачи определена нормативно-правовыми актами или установлена применимым законодательством, либо это необходимо в целях предупреждения угрозы жизни и здоровья субъекта, если получить согласие последнего невозможно.

Ответы на письменные запросы других организаций и учреждений в пределах их компетенции и предоставленных полномочий даются с согласия Ответственного лица или уполномоченного им лица в письменной форме, на бланке Оператора и в том объеме, который соответствует требованиям действующего законодательства и позволяет не разглашать излишний объем сведений о субъектах ПДн.

Ответственность за соблюдение вышеуказанного порядка предоставления ПДн субъекта несет работник Оператора, а также руководитель функциональной области, осуществляющий передачу ПДн субъекта третьим лицам.

ПДн субъекта могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого субъекта, за исключением случаев, когда передача ПДн субъекта без его согласия допускается действующим законодательством Российской Федерации.

ПДн в электронном виде, передаваемые по телекоммуникационным каналам связи общего пользования (Интернет, электронная почта и др.), могут передаваться только в защищенном виде (с использованием сертифицированных средств криптографической защиты). Передача персональных данных по открытым каналам связи (в том числе по телефону/факсу) запрещается.

Документы, содержащие ПДн, могут быть предоставлены лично ответственным работником Оператора или отправлены через организацию почтовой связи.

# Требования к сбору, хранению и уточнению ПДн

Сбор ПДн субъектов осуществляется работниками Оператора в соответствии с целями обработки ПДн.

Обработка ПДн разрешается только с согласия субъектов, кроме следующих случаев, когда такое согласие не требуется:

* обработка ПДн необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Оператора функций, полномочий и обязанностей;
* обработка ПДн необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;
* обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому, является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем;
* обработка ПДн осуществляется для статистических или иных научных целей с соблюдением ограничений, предусмотренных действующим законодательством, и при условии обязательного обезличивания ПДн;
* обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно;
* обработка ПДн необходима для осуществления прав и законных интересов Оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;
* обработка ПДн осуществляется в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта ПДн;
* осуществляется обработка ПДн, доступ неограниченного круга лиц к которым предоставлен субъектом ПДн либо по его просьбе;
* осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.
	+ 1. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя:
* фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
* фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
* наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;
* цель обработки персональных данных;
* перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
* наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;
* перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
* срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
* подпись субъекта персональных данных.
	+ 1. На основе изложенных в п.6.2.1 требований Оператор разрабатывает необходимые формы Согласий на обработку ПДн, согласовывает с Юридической поддержкой и Ответственным лицом или уполномоченным им лицом и размещает, при необходимости, на внутренних сетевых ресурсах.

Оператор обязан сообщить субъекту о целях и способах, а также о характере подлежащих получению ПДн и возможных последствиях отказа субъекта дать письменное согласие на их получение.

ПДн субъектов могут храниться в бумажном и электронном виде. Способ хранения ПДн определяется исходя из характера обработки ПДн.

Доступ в места хранения материальных носителей, содержащих ПДн, должен быть ограничен. Должны быть реализованы организационные и технические меры (в том числе с применением СКУД), исключающие доступ к ним третьих лиц (несанкционированный доступ).

Материальные носители, содержащие ПДн, должны храниться в служебных помещениях, предназначенных для обработки ПДн, в запираемых шкафах, ящиках. При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

Помещения, предназначенные для обработки ПДн, определяются руководителями подразделений в вверенной им области и учитываются Ответственным лицом или уполномоченным им лицом.

Бумажные носители ПДн, обрабатываемых в сходных целях, могут храниться в общих хранилищах. Запрещается хранить совместно на бумажных и электронных носителях ПДн, обрабатываемые в несовместимых целях.

# Требования к взаимодействию с субъектами ПДн

Выдача работникам Оператора документов, связанных с их трудовой деятельностью (к примеру, копий приказов о приеме на работу, переводах на другую работу, увольнении с работы; выписок из трудовой книжки, справок о месте работы, заработной плате, периоде работы) регулируется трудовым законодательством Российской Федерации и локальными нормативными актами Оператора. Взаимодействие с работниками Оператора по этим вопросам осуществляют уполномоченные работники ответственные за ведение кадрового делопроизводства.

Все запросы и обращения субъектов, их законных представителей, а также уполномоченного органа по защите прав субъектов ПДн, регистрируются согласно СТП СР/09-03-02/ПР01 «Порядок обработки входящих, исходящих и внутренних документов» и рассматриваются Ответственным лицом или уполномоченным им лицом.

Субъект ПДн или его законный представитель имеет право на получение информации о ПДн, относящихся к соответствующему субъекту ПДн, в том числе содержащей:

* подтверждение факта обработки ПДн оператором;
* правовые основания и цели обработки ПДн;
* цели и применяемые оператором способы обработки ПДн;
* 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 федерального закона;
* обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
* сроки обработки ПДн, в том числе сроки их хранения;
* порядок осуществления субъектом ПДн прав, предусмотренных законодательством Российской Федерации в области обработки ПДн;
* информацию об осуществленной или о предполагаемой трансграничной передаче данных;
* наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка поручена или будет поручена такому лицу;
* иные сведения, предусмотренные законодательством Российской Федерации в области обработки ПДн

Субъект ПДн или его законный представитель имеет право на ознакомление с ПДн, которые имеются у Оператора и относятся к соответствующему субъекту ПДн.

Субъект ПДн или его законный представитель имеет право заявлять возражения против принятия на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы.

Письменные запросы на предоставление сведений, указанных в пункте 7.3, рассматривает Ответственное лицо или уполномоченное им лицо и в течение тридцати дней со дня обращения субъекта ПДн подготавливает соответствующий ответ, либо предоставляет возможность ознакомиться с ПДн. В случае требования предоставления иных, непредусмотренных законодательством сведений, Ответственное лицо или уполномоченное им лицо подготавливает мотивированный отказ в письменной форме, содержащий ссылку на положение части 8 статьи 14 Федерального закона №152-ФЗ «О персональных данных» или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта ПДн или его представителя, либо с даты получения запроса субъекта ПДн или его представителя.

В случае требования (письменное заявление) субъекта об исключении или исправлении неверных или неполных ПДн Ответственное лицо или уполномоченное им лицо проверяет подтверждающие документы и вносит необходимые исправления. После чего в течение тридцати дней оповещает субъекта о внесенных изменениях.

В случае отзыва субъектом ранее переданного Оператору согласия на обработку его ПДн, Ответственное лицо или уполномоченное им лицо обязано:

* уведомить субъекта ПДн о возможных последствиях отзыва им согласия;
* в случае наличия законных оснований для обработки ПДн субъекта: прекратить обработку ПДн в целях, выходящих за рамки законных оснований;
* в случае отсутствия законных оснований для обработки ПДн субъекта: прекратить обработку ПДн субъекта и уничтожить ПДн (или обеспечить уничтожение ПДн) в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено действующим законодательством;
* уведомить субъекта ПДн в письменной форме о прекращении обработки ПДн (части ПДн) или о невозможности прекращения обработки ПДн с указанием оснований невозможности прекращения обработки.

В случае отзыва субъектом ПДн согласия на обработку ПДн Оператор вправе продолжить обработку ПДн без согласия субъекта ПДн при наличии следующих оснований:

* обработка ПДн необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;
* обработка ПДн необходима для исполнения договора, одной стороной которого является Оператор, а другой стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн;
* обработка ПДн необходима для заключения договора с Оператором по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем;
* обработка ПДн необходима для осуществления прав и законных интересов Оператора при условии, что при этом не нарушаются права и свободы субъекта ПДн;
* осуществляется обработка ПДн, доступ неограниченного круга лиц к которым предоставлен субъектом ПДн либо по его просьбе;
* осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом;
* осуществляется обработка специальных категорий ПДн, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни в соответствии с согласием субъекта данных в письменной форме на обработку своих ПДн либо в силу того, что ПДн сделаны общедоступными субъектом ПДн.

# Требования к уничтожению ПДн

Уничтожение ПДн, если иное не определено законом, а также требованиями нормативных правовых актов, должно производиться в течение тридцати рабочих дней по достижении целей обработки ПДн, а также в случае утраты необходимости достижения целей обработки.

При получении от субъекта, его законного представителя или уполномоченного органа запроса на уничтожение (блокирование) неполных, устаревших, недостоверных, незаконно полученных или избыточных для заявленной цели обработки ПДн, Ответственное лицо или уполномоченное им лицо обязано удостовериться в правомерности требований и в течение семи рабочих дней со времени поступления запроса уничтожить ПДн субъекта, после чего письменно уведомить его об этом.

Уничтожение ПДн должно производиться способом, исключающим возможность восстановления этих ПДн на носителе.

Уничтожение ПДн с носителя (в случае отсутствия необходимости уничтожения самого носителя) производится в установленный законодательством срок.

Уничтожение бумажного носителя ПДн производится одним из способов, не позволяющим восстановить исходную информацию, например: специальными устройствами для измельчения бумаги (шредерами); путем передачи на уничтожение в специализированные организации по договору и др.

Уничтожение ПДн на машинных носителях без уничтожения носителя информации производится путем удаления с электронных носителей информации методами и средствами гарантированного удаления (в соответствии с ГОСТ P 50739-95).

Уничтожение машинного носителя ПДн (в случае выхода носителя из строя, в случае невозможности стирания данных с носителя (компакт-диск и др.) производится путем механического разрушения на составные элементы, гарантирующего невозможность последующего чтения носителя и восстановления с него информации.

Уничтожение ПДн, принадлежащих конкретному субъекту ПДн, содержащихся в ИСПДн (базе данных ИСПДн) удаляется (или обезличивается) штатными средствами ПО ИСПДн или СУБД, без удаления информации о других субъектах ПДн.

# Требования к предоставлению доступа работникам в помещения

Доступ в помещения, в которых установлены средства обеспечения функционирования ИСПДн (серверные помещения) может предоставляться отдельным работникам Оператора, которым такой доступ необходим для исполнения функциональных обязанностей, а также работникам организаций, с которыми Оператор заключил соответствующие договоры на обслуживание инфраструктуры информационных технологий.

Предоставление или прекращение доступа работников Оператора и работников организаций, с которыми Оператор заключил соответствующие договоры на обслуживание инфраструктуры информационных технологий, осуществляется в соответствии с СТП СР/09-01-03/ПР01 «Порядок организации пропускного и внутриобъектового режима» и согласовывается с Ответственны лицом или уполномоченным им лицом.

Предоставление временного доступа в помещения может осуществляться при обязательном сопровождении лица работником Оператора, которому ранее был предоставлен доступ на постоянной основе.

Должен осуществляется периодический пересмотр перечня лиц, которым разрешен доступ в помещения, с целью определения актуальности и выявления избыточности перечня допущенных.

# Требования к организации защиты ПДн

Оператор обеспечивает защиту ПДн субъекта от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн. В отдельных случаях для выполнения части функций по обеспечению безопасности ПДн могут привлекаться сторонние организации.

Общую организацию защиты ПДн субъектов и контроль за соблюдением мероприятий по защите ПДн осуществляет Ответственное лицо или уполномоченное им лицо.

Защите подлежат все обрабатываемые Оператором ПДн за исключением обезличенных ПДн. Необходимые для защиты ПДн мероприятия определяются Ответственным лицом или уполномоченным им лицом.

К мероприятиям, направленным на создание (или поддержание в актуальном состоянии) комплексной системы защиты ПДн относятся:

* выявление (или уточнение) и документальное описание процессов, предусматривающих обработку ПДн;
* выявление (или уточнение) и документальное описание информационных систем ПДн, в рамках которых осуществляется обработка ПДн с использованием или без использования средств автоматизации;
* разработка (или уточнение) организационных мер защиты, направленных на обеспечение безопасности ПДн при их обработке без использования средств автоматизации, а также при необходимости изменение порядка обработки ПДн, осуществляемой без использования средств автоматизации;
* разработка (или уточнение) организационно-технических мер защиты, направленных на обеспечение безопасности ПДн при их обработке с использованием средств автоматизации;
* внедрение комплексной системы защиты ПДн как совокупности организационных и технических мер, направленных на обеспечение безопасности ПДн при их обработке, как с использованием средств автоматизации, так их использования.

Работы, направленные на обеспечение безопасности ПДн при их обработке с использованием средств автоматизации, осуществляются в рамках 3-х стадий: предпроектной стадии, стадии проектирования и реализации, стадии ввода в действие системы защиты ПДн.

* + 1. На предпроектной стадии:
* устанавливается необходимость обработки ПДн в информационных системах ПДн;
* определяется перечень ПДн, подлежащих защите;
* определяются условия расположения информационных систем ПДн относительно границ контролируемой зоны;
* определяются конфигурация и топология информационных систем ПДн в целом и их отдельных компонентов, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;
* определяются технические средства и системы, предполагаемые к использованию в информационных системах ПДн, условия их расположения, общесистемные и прикладные программные средства, имеющиеся и предлагаемые к разработке;
* определяются режимы обработки ПДн в информационных системах ПДн в целом и в отдельных компонентах;
* уточняется степень участия работников в обработке ПДн, характер их взаимодействия между собой;
* определяются (уточняются) угрозы безопасности ПДн и уровни защищенности ПДн применительно к конкретным условиям функционирования информационных систем ПДн (к примеру, может быть проведена разработка частной модели угроз).

По результатам предпроектного обследования, с учетом действующих законодательных актов Российской Федерации в области защиты ПДн, уровней защищённости ПДн конкретные требования по обеспечению безопасности ПДн включаются в техническое (частное техническое) задание на разработку системы защиты ПДн либо принимается решения о достаточности уже использующихся мер по обеспечению безопасности ПДн и отсутствия необходимости реализации дополнительных мер по обеспечению безопасности ПДн.

* + 1. В случае принятия решения о необходимости реализации дополнительных мер по обеспечению безопасности ПДн на стадии проектирования и реализации осуществляется:
* разработка задания и проекта проведения работ (в том числе строительных и строительно-монтажных) по созданию (реконструкции) ИСПДн в соответствии с требованиями технического (частного технического) задания на разработку системы защиты ПДн;
* выполнение работ в соответствии с проектной документацией;
* обоснование и закупка совокупности используемых в ИСПДн серийно выпускаемых технических средств обработки, передачи и хранения информации;
* разработка мероприятий по защите информации в соответствии с предъявляемыми требованиями;
* обоснование и закупка совокупности используемых в ИСПДн сертифицированных технических, программных и программно-технических средств защиты информации и их установка;
* проведение сертификации по требованиям безопасности информации технических, программных и программно-технических средств защиты информации в случае, когда на рынке отсутствуют требуемые сертифицированные средства защиты информации;
* разработка и реализация разрешительной системы доступа пользователей к обрабатываемой в ИСПДн информации;
* разработка эксплуатационной документации на ИСПДн и средства защиты информации, а также организационно-распорядительной документации по защите информации;
* выполнение мероприятий, характерных для конкретных ИСПДн и направлений обеспечения безопасности ПДн.
	+ 1. На стадии ввода в действие системы защиты ПДн осуществляется:
* опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн;
* приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации;
* организация охраны и физической защиты помещений ИСПДн, исключающих несанкционированный доступ к техническим средствам ИСПДн, их хищение и нарушение работоспособности, хищение носителей информации;
* оценка соответствия ИСПДн требованиям безопасности ПДн;
* оценка эффективности принимаемых мер по обеспечению безопасности ПДн.
	+ 1. Результаты приёмочных испытаний ИСПДн и её подсистемы безопасности (СЗИ) с выводом о её соответствии установленным требованиям включаются в акт приёмки ИСПДн в эксплуатацию.

Ввод в действие ИСПДн и её подсистемы безопасности осуществляется только при положительном заключении (выводе) в акте приёмки (или в аттестате соответствия) о соответствии ИСПДн установленным требованиям по обеспечению безопасности.

При модернизации эксплуатирующейся ИСПДн анализируются исходные данные, вносимые в ИСПДн изменения, подсистема обеспечения безопасности и определяется необходимость внесения изменений с подсистему безопасности ИСПДн. При необходимости внесения изменений в подсистему безопасности ИСПДн выполняются необходимые мероприятия в соответствии с п.10.5

Конкретный перечень мероприятий по защите ПДн при их автоматизированной обработке устанавливается Ответственным лицом или уполномоченным им лицом по результатам оценки актуальности угроз безопасности ПДн для информационных систем ПДн.

Конкретный перечень мероприятий по защите ПДн при их обработке без использования средств автоматизации устанавливается Ответственным лицом или уполномоченным им лицом по результатам обследования процессов и информационных систем (подсистем) ПДн, в которых осуществляется обработка без использования средств автоматизации, с учетом требований законодательства в области ПДн, нормативных правовых актов и методических документов.

С целью поддержания в актуальном состоянии системы защиты ПДн Ответственное лицо или уполномоченное им лицо организует непрерывный процесс проверки выполнения требований законодательства в области ПДн, в том числе нормативных актов в части выявления актуальных угроз безопасности ПДн, а также организует поддержку в актуальном состоянии организационно-распорядительной, проектной, эксплуатационной и прочей вспомогательной документации системы защиты ПДн.

Регулярный пересмотр актуальности угроз безопасности ПДн, организационно-распорядительной, проектной, эксплуатационной и прочей вспомогательной документации системы защиты ПДн, а также адекватности применяемых средств и методов защиты, осуществляется с периодичностью не менее одного раза в 3 года.

Учёт средств защиты информации, применяемых в системе защиты ПДн, а также сопутствующей документации к средствам защиты информации ведёт структурное подразделение, обеспечивающее функционирование ИСПДн.

# Ответственность за нарушение требований по обеспечению порядка обработки и защиты ПДн

Работники, виновные в нарушении требований, регулирующих получение, обработку и защиту ПДн субъектов, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами.

Разглашение ПДн субъекта (передача их посторонним лицам, в том числе, работникам Оператора, не имеющим к ним доступа), их публичное раскрытие, утрата документов и иных носителей, содержащих ПДн субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных настоящими Методическими Указаниями, внутренними нормативными актами (к примеру, приказами, распоряжениями) Оператора, влечет наложение на работника, виновного в разглашении, дисциплинарного взыскания.

Работники Оператора, имеющие доступ к ПДн субъектов и совершившие указанный в п.11.2 настоящих Методических Указаний дисциплинарный проступок, несут полную материальную ответственность в случае причинения его действиями ущерба Оператору, в соответствии п.7 ст. 243 Трудового кодекса Российской Федерации.

Работники Оператора, имеющие доступ к ПДн субъектов, виновные в незаконном разглашении или использовании ПДн без согласия субъектов из корыстной или иной личной заинтересованности и причинившие крупный ущерб, несут уголовную ответственность в соответствии с Уголовным кодексом Российской Федерации.

Приложение № 1

Термины, определения и сокращения

[Термины корпоративного словаря](http://msk03portal.sibur.local/helpful_information/glossary/)

Сокращения

|  |  |
| --- | --- |
| Термин | Сокращение |
| Персональные данные | ПДн |
| Информационная система персональных данных | ИСПДн |

Приложение № 2

Ссылочные документы

1. Внутренние регламентирующие документы:
	1. СР/09-03-02/ПР01 Порядок обработки входящих, исходящих и внутренних документов.
	2. СР/09-01-03/ПР01 Порядок организации пропускного и внутриобъектового режима.
	3. СР/09-01-01/МУ32 Методические указания по обеспечению информационной безопасности при реализации ИТ процессов.
2. Внешние регламентирующие документы:
	1. Федеральный закон Российской Федерации от 27.07.2006 г № 152-ФЗ «О персональных данных».
	2. Федеральный закон Российской Федерации от 27.07.2006 г № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
	3. Федеральный закон Российской Федерации от 22.10.2004 г № 125-ФЗ «Об архивном деле в Российской Федерации».
	4. Гражданский кодекс Российской Федерации.
	5. Трудовой кодекс Российской Федерации.
	6. Конституция Российской Федерации.