



ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ РЕСПУБЛИКИ ХАКАСИЯ
«РЕСПУБЛИКАНСКИЙ ДОМ-ИНТЕРНАТ ДЛЯ ДЕТЕЙ «ТЕРЕМОК»
ХАКАС РЕСПУБЛИКАНЫҢ ХАЗНА БЮДЖЕТ УЧРЕЖДЕГИЕЗИ
РЕСПУБЛИКАДАҒЫ ОЛҒАННАРНЫҢ «ТЕРЕМОК» ТУРА-ИНТЕРНАДЫ

ПРИКАЗ

«25» *апреля* 2021 г.

№ *12* -Д

г. Абакан

**Об ответственных должностных
лицах и организации работы по защите
персональных данных**

В соответствии с Федеральным законом от 27.06.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», 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. Ввести в Государственном бюджетном учреждении Республики Хакасия «Республиканский дом-интернат для детей «Теремок» (далее – Учреждение) режим защиты персональных данных (далее – ПДн).

2. Утвердить Положение о защите персональных данных работников, воспитанников, их родителей (законных представителей) Государственного бюджетного учреждения Республики Хакасия «Республиканский дом-интернат для детей «Теремок» (приложение 1).

3. Утвердить:

перечень информационных систем по защите персональных данных в Государственном бюджетном учреждении Республики Хакасия «Республиканском доме-интернате для детей «Теремок» (приложение 2);

перечень защищаемых данных в информационных системах по защите персональных данных Государственном бюджетном учреждении Республики Хакасия «Республиканский дом-интернат для детей «Теремок» (приложение 3);

перечень программного обеспечения в информационных системах по защите персональных данных в Государственном бюджетном учреждении Республики Хакасия «Республиканском доме-интернате для детей «Теремок» (приложение 4).

4. Назначить ответственным за организацию обработки персональных данных сотрудников и за обеспечение безопасности персональных данных в Учреждении, Аванесян Сашу Сашевну начальника отдела Учреждения, Володину

Марину Анатольевну бухгалтера расчетной группы Учреждения, воспитанников, их родителей (законных представителей), специалистов по социальной работе Учреждения, Задорожникову Марину Викторовну, Рачеву Татьяну Владимировну, Скрыбикову Екатерину Олеговну.

5. На период отпуска, болезни, командировки Аванесян Саши Сашевны ответственного за организацию обработки персональных данных и за обеспечение безопасности персональных данных в ГБУ РХ «Республиканском доме-интернате для детей «Теремок» возложить на Балыбину Евгению Викторовну, специалиста по управлению кадрами Учреждения.

6. Должностным лицам, указанным в пунктах 4 и 5 настоящего приказа, в работе по выполнению обязанностей по организации обработки персональных данных и обеспечению безопасности персональных данных в Учреждении руководствоваться Положением, утвержденное приказом Учреждения.

7. Приказ Государственного бюджетного учреждения Республики Хакасия «Республиканский дом-интернат для умственно отсталых детей «Теремок» от 30.08.2018 № 387-Д «Об утверждении Положения о защите, хранении, обработке и передаче персональных данных воспитанников и родителей (законных представителей) в ГБУ РХ «Республиканский дом-интернат для детей «Теремок» признать утратившим силу.

Директор



Н.В. Кеберле

УТВЕРЖДЕНО
приказом ГБУ РХ «Республиканский
дом-интернат для детей «Теремок»
от «25» апреля 2021 г. № 82-Д

ПОЛОЖЕНИЕ

о защите персональных данных работников, воспитанников, их родителей
(законных представителей)
Государственного бюджетного учреждения Республики Хакасия «Республиканский
дом-интернат для детей «Теремок»

1. Общие положения

1. Целью положения о защите, хранении, обработке и передаче персональных данных работников, воспитанников и родителей (законных представителей) в ГБУ РХ «Республиканский дом-интернат для детей «Теремок» (далее – Положение) является защита персональных данных работников, воспитанников Учреждения, их родителей (законных представителей) (далее – граждане) от несанкционированного доступа, неправомерного их использования или утраты, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

2. Положение разработано в соответствии с Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

3. Порядок ввода в действие и изменения Положения.

Положение вступает в силу с момента его утверждения и действует бессрочно, до замены его новым положением.

Все изменения в Положение вносятся соответствующим приказом.

4. Все граждане, имеющие доступ к персональным данным, должны быть ознакомлены с настоящим Положением под подпись.

5. Режим конфиденциальности персональных данных снимается в случае их обезличивания и по истечении 75 лет срока их хранения, если иное не определено законом.

2. Основные понятия

6. Для целей настоящего Положения используются следующие основные понятия:

персональные данные гражданина – любая информация, относящаяся к определенному или определяемому на основании такой информации воспитаннику, его родителю (законному представителю), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая Учреждению в связи с осуществлением деятельности;

обработка персональных данных – сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных;

конфиденциальность персональных данных – обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным, требование не допускать их распространения без согласия гражданина или иного законного основания;

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;

использование персональных данных – действия (операции) с персональными данными, совершаемые должностным лицом Учреждения в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении гражданина либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных или в результате которых уничтожаются материальные носители персональных данных;

обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному лицу;

общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия работника, воспитанника, его родителя (законного представителя) или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

информация – сведения (сообщения, данные) независимо от формы их представления.

документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

3. Состав персональных данных работников

7. В состав персональных данных входят:

анкетные и биографические данные;

образование;

сведения о месте работы, трудовом и общем стаже;

сведения о составе семьи;

паспортные данные;

сведения о воинском учете;

сведения о заработной плате;
 сведения о социальных льготах;
 специальность,
 занимаемая должность;
 наличие/отсутствие судимостей;
 адрес места жительства;
 домашний телефон;
 пакет документов, содержащие личные сведения о работнике;
 место работы или учебы членов семьи и родственников;
 документы, хранящиеся в личных делах воспитанников;
 состояние здоровья воспитанников;
 сведения о денежных средствах, находящихся на личных счетах
 воспитанников.

8. Данные документы являются конфиденциальными, при этом, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

4. Обработка персональных данных

9. В целях обеспечения прав и свобод гражданина Учреждение и его представители при обработке персональных данных обязаны соблюдать следующие общие требования:

обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов;

при определении объема и содержания обрабатываемых персональных данных Учреждение должно руководствоваться Конституцией Российской Федерации и иными федеральными законами;

получение персональных данных может осуществляться как путем представления их самим гражданином, так и путем получения их из иных источников;

персональные данные гражданина следует получать у него самого. Если персональные данные возможно получить только у третьей стороны, то гражданин должен быть уведомлен об этом заранее. Учреждение должно сообщить гражданину о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать согласие на их получение;

учреждение не имеет права получать и обрабатывать персональные данные гражданина о его политических, религиозных и иных убеждениях и частной жизни;

учреждение не имеет право получать и обрабатывать персональные данные гражданина о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

10. К обработке, передаче и хранению персональных данных воспитанников, родителей (законных представителей), указанных в п. 7 настоящего Положения могут иметь доступ сотрудники:

Директор Учреждения, заместители директора;

специалисты по социальной работе;

юрисконсульт;

медицинские работники;

делопроизводитель.

11. К обработке, передаче и хранению персональных данных работников Учреждения, указанных в п. 7 настоящего Положения могут иметь доступ сотрудники:

директор Учреждения, заместители директора;
начальник отдела;
специалист по кадрам;
главный бухгалтер;
бухгалтер расчетной группы;
делопроизводитель.

12. Использование персональных данных возможно только в соответствии с целями, определившими их получение.

Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с действующим законодательством.

13. Передача персональных данных возможна только с согласия гражданина или в случаях, прямо предусмотренных законодательством.

При передаче персональных данных Учреждение должно соблюдать следующие требования:

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

не сообщать персональные данные в коммерческих целях без письменного согласия;

предупредить лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные, обязаны соблюдать режим секретности (конфиденциальности);

разрешать доступ к персональным данным только специально уполномоченным лицам, определенным приказом по Учреждению, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций.

14. Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

15. При передаче персональных данных потребителям (в том числе и в коммерческих целях) за пределы Учреждения учреждение не должно сообщать эти данные третьей стороне без письменного согласия гражданина, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью или в случаях, установленных федеральным законом.

16. Все меры конфиденциальности при сборе, обработке и хранении персональных данных распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

17. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

18. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

19. Персональные данные работника содержатся в основном документе персонального учета работников – в личные карточки формы Т-2, которая заполняется после издания приказа о его приеме на работу.

Личные карточки работников хранятся в отделе кадров в специально оборудованных негорючих шкафах в алфавитном порядке.

20. Работодатель обеспечивает ограничение доступа к персональным данным работников лицам, не уполномоченным законом либо работодателем для получения соответствующих сведений.

21. При принятии решений, затрагивающих интересы гражданина, Учреждение не имеет права основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

5. Доступ к персональным данным.

22. Внутренний доступ (доступ внутри Учреждения).

Право доступа к персональным данным имеют лица, указанные в пунктах 10,11 настоящего Положения.

23. Внешний доступ.

К числу массовых потребителей персональных данных вне Учреждения можно отнести государственные и негосударственные структуры:

налоговые инспекции;

правоохранительные органы;

военкоматы;

органы социального страхования;

пенсионные фонды;

подразделения муниципальных органов управления: Управления социальной поддержки населения, Управления образования.

надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

6. Защита персональных данных

24. Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности Учреждения.

25. Защита персональных данных от неправомерного их использования или утраты должна быть обеспечена Учреждением за счет его средств в порядке, установленном федеральным законом.

26. Внутренняя защита.

Для обеспечения внутренней защиты персональных данных необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют доступа к персональным данным.

- строгое избирательное и обоснованное распределение документов и информации между работниками;

- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;

- знание работником требований нормативно-методических документов по защите информации и сохранении тайны;

- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;

- определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором хранятся личные дела работников и воспитанников;

- организация порядка уничтожения информации;

- своевременное выявление нарушения требований разрешительной системы доступа работниками Учреждения;

- воспитательная и разъяснительная работа с сотрудниками Учреждения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;

- не допускается выдача личных дел работников, воспитанников на рабочие места сотрудников Учреждения. Личные дела могут выдаваться на рабочие места только директору и заместителям директора.

27. Защита персональных данных на электронных носителях. Все папки, содержащие персональные данные, должны иметь ограниченный доступ.

Внешняя защита.

Для обеспечения внешней защиты персональных данных необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;

- пропускной режим в Учреждении;

- технические средства охраны (опечатавающее устройство на дверь, электронный ключ, сигнализации);

- порядок охраны территории, зданий, помещений, транспортных средств.

28. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны не разглашать персональные данные.

7. Права и обязанности работников, воспитанников, их родителей (законных представителей).

29. В целях защиты персональных данных, работник, воспитанник, их родители (законные представители) имеют право:

- требовать исключения или исправления неверных, или неполных данных;

получать свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные. определять своих представителей для защиты своих персональных данных; на сохранение и защиту своей личной жизни и семейной тайны.

8. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными.

30. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

31. Каждый сотрудник Учреждения, получающий для работы конфиденциальную информацию, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

32. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.

УТВЕРЖДЕНО

приказом ГБУ РХ «Республиканский
дом-интернат для детей «Теремок»от «05» апреля 2021 г. № 82-8

ПЕРЕЧЕНЬ

информационных систем по защите персональных данных в
Государственном бюджетном учреждении Республики Хакасия «Республиканский
дом-интернате для детей «Теремок»

| Наименование информационной системы (ИС) | Тип ИС | Уровень защищенности ИСПДн | Класс защищенности ИС |
|---|--|----------------------------|-----------------------|
| ИС «Зарплата и кадры государственного учреждения 1С: Предприятие» | Информационная система по защите персональных данных (ИСПДн) | третий | третий |

УТВЕРЖДЕНО

приказом ГБУ РХ «Республиканский
дом-интернат для детей «Теремок»от «05» апреля 2021 г. № 82-Д

ПЕРЕЧЕНЬ

защищаемых данных в информационных системах по защите персональных данных Государственном бюджетном учреждении Республики Хакасия «Республиканского дома-интерната для детей «Теремок»

1. Перечень защищаемых персональных данных

1. Конфиденциальность персональных данных - обязательное для соблюдения сотрудниками ГБУ РХ «Республиканский дом-интернат для детей «Теремок», требование не допускать распространения персональных данных без согласия субъекта персональных данных или наличия иного законного основания.

2. Защищаемыми информационными ресурсами в информационной системе персональных данных (ПДн) ГБУ РХ «Республиканский дом-интернат для детей «Теремок» являются:

Персональные данные субъектов ПДн включают:

ФИО;

дата рождения;

контактный телефон;

адрес прописки;

адрес фактического проживания;

паспортные данные;

данные о месте рождения;

данные о смерти;

данные об усыновлении, установлении отцовства;

данные о браке;

данные об изменении имени, фамилии, отчества;

данные о родственниках;

гражданство;

национальность;

данные о состоянии здоровья.

Персональные данные сотрудников ГБУ РХ «Республиканского дома-интерната для детей «Теремок» включают:

ФИО;

место и дата рождения;

гражданство;

адрес по прописке;

паспортные данные (серия, номер паспорта, кем и когда выдан), в том числе загранпаспорт;

информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающие образование: наименование, номер, серия, дата выдачи, специальность, квалификация);

информация о трудовой деятельности до приема на работу (место работы, должность, период работы, причины увольнения);

информация о трудовом стаже;

адрес проживания (фактический);

телефонный номер (домашний, рабочий, мобильный);

семейное положение и состав семьи (муж/жена, дети);

информация о знании иностранных языков;

допуск к государственной тайне;

оклад, надбавки;

отношение к судимости;

пребывание за границей;

сведения о доходах, имуществе, обязательствах имущественного характера своих, супруга и несовершеннолетних детей;

данные о трудовом договоре, дата его заключения, дата начала и дата окончания, вид работы, срок действия, наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, длительность дополнительного отпуска за ненормированный рабочий день, должностные обязанности работника, дополнительные социальные льготы и гарантии, № и число изменения к трудовому договору, характер работы, форма оплаты труда, категория персонала, условия труда, продолжительность рабочей (служебной) недели, система оплаты);

сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета, состав (профиль), ВУС, отношение к воинскому учету, бронирование);

ИНН;

СНИЛС;

данные об аттестации работников;

данные о повышении квалификации, профессиональная переподготовка;

данные о наградах, медалях, поощрениях, почетных званиях;

информация о приеме на работу, перемещении по должности, увольнении;

информация об отпусках;

информация о командировках;

информация о состоянии здоровья, о временной нетрудоспособности;

информация о медицинском страховании;

информация о негосударственном пенсионном обеспечении.

2. Перечень защищаемой информации

3. Технологическая информация, подлежащая защите, включает:
управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);

сведения о проведенных служебных проверках, дисциплинарных взысканиях;

информация о квалификационных экзаменах;

сведения о кадровом резерве;

технологическая информация средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);

информация на съемных носителях информации (бумажные, магнитные, оптические и пр.), содержащие защищаемую технологическую информацию системы управления ресурсами или средств доступа к этим системам управления;

информация о СЗПДн, их составе и структуре, принципах и технических решениях защиты;

информационные ресурсы (базы данных, файлы и другие), содержащие информацию о информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;

служебные данные (метаданные) появляющиеся при работе программного обеспечения, сообщений и протоколов межсетевого взаимодействия, в результате обработки Обрабатываемой информации.

4. Программно-технические средства включают в себя:

общесистемное и специальное программное обеспечение (операционные системы, СУБД, клиент-серверные приложения и другие);

резервные копии общесистемного программного обеспечения;

инструментальные средства и утилиты систем управления ресурсами ИСПДн;

аппаратные средства обработки ПДн (АРМ и сервера);

сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.).

5. Средства защиты данных состоят из аппаратно-программных средств, включают в себя:

средства управления и разграничения доступа пользователей;

средства обеспечения регистрации и учета действий с информацией;

средства, обеспечивающие целостность данных;

средства антивирусной защиты;

средства анализа защищенности;

средства обнаружения вторжений

средства межсетевого экранирования;

средства криптографической защиты ПДн, при их передачи по каналам связи сетей общего и (или) международного обмена.

3. Каналы информационного обмена и телекоммуникации

Каналы информационного обмена и телекоммуникации являются объектами защиты, если по ним передаются обрабатываемая и технологическая информация.

4. Объекты и помещения, в которых размещены компоненты ИС

Объекты и помещения являются объектами защиты, если в них происходит обработка обрабатываемой и технологической информации, установлены технические средства обработки и защиты.

Данная информация является конфиденциальной, хотя, учитывая ее массовость и единое место обработки и хранения, соответствующий гриф ограничения на них не ставит

УТВЕРЖДЕНО

приказом ГБУ РХ «Республиканский
дом-интернат для детей «Теремок»
от «05» апреля 2021 г. № 82-80

Перечень программного обеспечения в информационной системе по защите персональных данных «Зарплата и кадры государственного учреждения 1С: Предприятие» в ГБУ РХ «Республиканском доме-интернате для детей «Теремок»

| № п/п | Наименование ПО | Назначение программы | Лицензия |
|-------|--|--|---|
| 3 | 1С:Предприятие 8.3 | Программный комплекс автоматизации бухгалтерского и управленческого учётов | Договор от 26 мая 2011 года № 260502, Лицензия № 8000230669 |
| 4 | Kaspersky Endpoint Security 11 для Windows | Антивирусное ПО | Договор от ХХХ № ХХХ (уточнить в бухгалтерии, покупали в Киасофте в ноябре 2020 года), Лицензия № 2D242011180812377132176 |
| 5 | 7-Zip 9.20 (x64) | Архиватор | Свободное распространение |
| 6 | Adobe Reader 9 | Приложение для чтения PDF документов | Свободное распространение |
| 7 | Mozilla Firefox | Веб-браузер | Свободное распространение |
| 8 | Microsoft Visual C++ 2015 | Пакет библиотек для запуска приложений | Свободное распространение |