Российская Федерация
Бюджетное учреждение
Ханты – Мансийского автономного округа - Югры
«Советский комплексный центр социального обслуживания населения»

ПРИКАЗ

«06» сентября 2023 года № 167
г. Советский

О защите информации

В соответствии с требованиями Федерального закона Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных, Постановления 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. Назначить ответственными по защите информации:
1.1. За организацию обработки персональных данных заместителя директора административно-хозяйственной части Иванову Ю.А.;
1.2. За обеспечение безопасности персональных данных в информационных системах персональных данных инженера по автоматизированным системам управления производством отделения информационно-аналитической работы Каправчука А.А.
1.3 За эксплуатацию информационных систем персональных данных:
Кривых О.В., главного бухгалтера;
Погодину Н.Л., экономиста;
бухгалтера;
Печкину Е.А., специалиста по кадрам;
Звягольскую О.В., юрисконсульта.
2. Утвердить перечень должностей в БУ «Советский комплексный центр социального обслуживания населения», доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими должностных (трудовых) обязанностей согласно приложению 1 к настоящему приказу.
3. Создать комиссию по защите информации:
3.1. Утвердить состав комиссии по защите информации согласно приложению 2 к настоящему приказу.

3.2. Утвердить положение о комиссии по защите информации согласно приложению 3 к настоящему приказу.

4. Утвердить типовые формы документов по защите информации:

4.1. Согласие на обработку персональных данных согласно приложению 4 к настоящему приказу.

4.2. Разъяснение субъекту персональных данных согласно приложению 5 к настоящему приказу.

4.3. Обязательство о неразглашении информации, содержащей персональные данные, согласно приложению 6 к настоящему приказу.

4.4. Журналы по защите информации согласно приложению 7 к настоящему приказу.

4.5. Протокол заседания комиссии по защите информации согласно приложению 8 к настоящему приказу.

4.6. Акт определения уровня защищенности персональных данных при их обработке в информационных системах персональных данных и класса защищенности информационных систем персональных данных согласно приложению 9 к настоящему приказу.

4.7. Акт об уничтожении персональных данных субъектов персональных данных согласно приложению 10 к настоящему приказу.

5. Утвердить перечень информационных систем персональных данных согласно приложению 11 к настоящему приказу.

6. Утвердить перечень обрабатываемых персональных данных согласно приложению 12 к настоящему приказу.

7. Утвердить положение об организации режима обеспечения безопасности помещений, в которых размещены информационные системы персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения, согласно приложению 13 к настоящему приказу.

8. Утвердить политику в отношении обработки персональных данных согласно приложению 14 к настоящему приказу.

9. Утвердить инструкции и правила по защите информации:

− Инструкцию ответственного за организацию обработки персональных данных согласно приложению 15 к настоящему приказу;

− Инструкцию ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных согласно приложению 16 к настоящему приказу;

− Инструкцию ответственного за эксплуатацию информационной системы персональных данных согласно приложению 17 к настоящему приказу;

− Инструкцию по организации резервного копирования и восстановления программного обеспечения и баз персональных данных в информационных системах персональных данных согласно приложению 18 к настоящему приказу;

– Инструкцию по идентификации и аутентификации пользователей информационных систем персональных данных согласно приложению 19 к настоящему приказу;

– Инструкцию по организации антивирусной защиты в информационных системах персональных данных согласно приложению 20 к настоящему приказу;

– Инструкцию по регистрации событий безопасности согласно приложению 21 к настоящему приказу;

– Инструкцию о пропускном и внутриобъектовом режимах согласно приложению 22 к настоящему приказу;

– Инструкцию по обработке персональных данных без использования средств автоматизации согласно приложению 23 к настоящему приказу;

– Инструкцию по работе с инцидентами информационной безопасности согласно приложению 24 к настоящему приказу;

– Инструкцию по обращению со средствами криптографической защиты информации согласно приложению 25 к настоящему приказу;

– Правила рассмотрения запросов субъектов персональных данных или их представителей согласно приложению 26 к настоящему приказу;

– Правила работы лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими должностных (трудовых) обязанностей, согласно приложению 27 к настоящему приказу;

– Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных согласно приложению 28 к настоящему приказу;

– Порядок уничтожения персональных данных при достижении целей обработки и (или) при наступлении законных оснований согласно приложению 29 к настоящему приказу.

10. Приказ № 60 от 28.03.2023 признать утратившим силу.
Приказ № 61 от 28.03.2023 признать утратившим силу.
Приказ № 62 от 28.03.2023 признать утратившим силу.
Приказ № 63 от 28.03.2023 признать утратившим силу.
Приказ № 64 от 28.03.2023 признать утратившим силу.

11. Божко О.В., документоведу административно-хозяйственной части, ознакомить работников с настоящим приказом под (Приложение 30).

12. Контроль за исполнением настоящего приказа оставляю за собой.

Директор Прохорова Н.А.

Приложение 1 к приказу
БУ «Советский комплексный
центр социального
обслуживания населения»
от «06» сентября 2023 г. № 167

Перечень должностей в бюджетном учреждении
Ханты – Мансийского автономного округа - Югры
«Советский комплексный центр социального обслуживания населения »,
доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими должностных (трудовых) обязанностей

№ п/п	Должность	ИСПДн	Физический доступ к машинным носителям информации	Способ обработки ПДн
1.	главный бухгалтер	«1С:Зарплата и Кадры»	нет	смешанный
2.	экономист	«1С:Зарплата и Кадры»	нет	смешанный
3.	специалист по кадрам	«1С:Зарплата и Кадры»	нет	смешанный
4.	юрисконсульт	«1С:Зарплата и Кадры»	нет	смешанный
5.	бухгалтер	«1С:Зарплата и Кадры»	нет	смешанный

Приложение 2 к приказу
БУ «Советский комплексный
центр социального
обслуживания населения»
от «06» сентября 2023 г. № 167

Состав комиссии по защите информации

Председатель комиссии	Иванова Ю.А. – заместитель директора
Члены комиссии	Каправчук А.А. - инженер по АСУП отделения информационно-аналитической работы;
	специалист по пожарной профилактике административно-хозяйственной части;
	Кривых О.И.- главный бухгалтер административно-хозяйственной части;
	Звягольская О.В. – юрисконсульт административно-хозяйственной части;
	Печкина Е.А.- специалист по кадрам административно-хозяйственной части

Приложение 3 к приказу
БУ «Советский комплексный
центр социального
обслуживания населения»
от «06» сентября 2023 г. № 167

ПОЛОЖЕНИЕ
о комиссии по защите информации

1. Общие положения

1.1. Настоящее Положение определяет основные задачи, порядок формирования, полномочия и ответственность комиссии по защите информации (далее - Комиссия).

2. Основные задачи комиссии по защите информации

2.1. Основными задачами Комиссии являются:

2.1.1. Сбор и анализ исходных данных по информационным системам персональных данных.

2.1.2. Определение значений параметров для установления уровня защищенности персональных данных в соответствии с постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2.1.3. Определение уровня защищенности персональных данных при их обработке в информационных системах персональных данных.

2.1.4. Принятие решения об уничтожении персональных данных.

2.1.5. Проведение внутренних проверок соответствия обработки персональных данных в БУ «Советский комплексный центр социального обслуживания населения» требованиям законодательства в сфере защиты персональных данных.

3. Порядок формирования комиссии по защите информации

3.1. Комиссия формируется из числа штатных сотрудников в БУ «Советский комплексный центр социального обслуживания населения», участвующих в процессе обработки персональных данных.

3.2. В состав Комиссии входит не менее четырех человек – членов Комиссии, в их числе – председатель Комиссии.

3.3. Члены Комиссии назначаются приказом директора БУ «Советский комплексный центр социального обслуживания населения»

3.4. В случае изменения состава Комиссии, в приказ вносятся соответствующие изменения.

4. Полномочия комиссии по защите информации

4.1. Для осуществления задач, указанных в разделе 2 настоящего Положения, Комиссия имеет право:

- получать необходимые сведения у всех сотрудников БУ «Советский комплексный центр социального обслуживания населения», участвующих в обработке персональных данных;
- просматривать электронные базы данных и бумажные носители, содержащие персональные данные, с целью выявления состава обрабатываемых персональных данных;
- отслеживать технологический процесс обработки персональных данных;
- выявлять или получать готовые сведения о структуре локальной вычислительной сети БУ «Советский комплексный центр социального обслуживания населения»;
- определять или получать готовые сведения о наличии и способах доступа к информационно-телекоммуникационной сети;
- определять или получать готовые сведения о технических и программных средствах обработки персональных данных;
- определять или получать готовые сведения об условиях, местах и способах передачи персональных данных в сторонние организации.

5. Отчетность комиссии по защите информации

5.1. Комиссия при выполнении своих задач должна составить протокол заседания комиссии.

5.2. В результате своей деятельности Комиссия должна составить Акт(ы) определения уровня защищенности персональных данных при их обработке в информационных системах персональных данных/Акт уничтожения персональных данных/Акт проведения внутренней проверки соответствия обработки персональных данных в Учреждении требованиям законодательства в сфере защиты персональных данных.

Приложение 4 к приказу
БУ «Советский комплексный
центр социального
обслуживания населения»
от «06» сентября 2023 г. № 167

СОГЛАСИЕ
сотрудника на обработку персональных данных

г. Советский «__» _____ г.

Я, _____,
(фамилия, имя, отчество)

_____ серия _____ № _____ выдан _____
(вид документа, удостоверяющего личность)

_____
(когда и кем)

проживающий(ая) по адресу: _____
_____

настоящим даю свое согласие на обработку автоматизированным и неавтоматизированным способами моих персональных данных БУ «Советский комплексный центр социального обслуживания населения», расположенному по адресу: 628242, город Советский , ул. Гастелло, дом 39, и подтверждаю, что, давая такое согласие, я действую по своей воле и в своих интересах.

Обработка информации включает в себя следующее любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), блокирование, удаление, уничтожение).

Согласие дается мною для целей обеспечения соблюдения законов и иных нормативных правовых актов, содействия в трудоустройстве, получения образования и продвижения по службе, обеспечения личной безопасности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества, ведения кадрового, бухгалтерского, налогового и воинского учета, размещения на общедоступных источниках персональных данных, предоставления гарантий и компенсаций, установленных действующим законодательством и локальными нормативными актами БУ «Советский комплексный центр социального обслуживания населения», и распространяется на следующую информацию:

1) фамилия, имя, отчество;

2) пол;
3) гражданство;
4) данные документа, удостоверяющего личность;
5) год, месяц и дата рождения; место рождения;
6) адрес регистрации (места жительства);
7) сведения о составе семьи и о близких родственниках (Фамилия, имя, отчество, дата рождения, степень родства);
8) сведения о доходах;
9) семейное положение;
10) сведения об образовании и (или) о квалификации или наличие специальных знаний, наименование образовательного учреждения, сведения о документах, подтверждающих образование (наименование, серия, номер, дата выдачи, годы обучения, направление, специальность или квалификация по документу);
11) профессия;
12) сведения о наградах; поощрениях; почетных званиях; медалях;
13) квалификация;
14) номер и дата трудового договора;
15) сведения об отпусках, в том числе о выезде за пределы РФ;
16) данные идентификационного номера налогоплательщика (ИНН);
17) данные Пенсионного страхового свидетельства (СНИЛС);
18) сведения о воинском учете, данные военного билета;
19) сведения о постановке на учет в налоговом органе;
20) результаты обязательных предварительных (при поступлении на работу) и периодических медицинских осмотров (обследований);
21) сведения о судимости/факте уголовного преследования (наличие/отсутствие);
22) сведения об административных правонарушениях;
23) место работы;
24) должность;
25) табельный номер;
26) сведения, содержащиеся в трудовой книжке, вкладыше в трудовую книжку;
27) сведения, содержащиеся в должностной инструкции;
28) сведения о трудовой деятельности и стаже;
29) данные банковского счета;
30) номер контактного телефона или сведения о других способах связи;
31) фотографическое изображение;
32) сведения, содержащиеся в актах органов записи гражданского состояния;
33) подпись;
34) данные водительского удостоверения;
35) сведения, содержащиеся в медицинской справке о допуске к управлению транспортным средством;

36) сведения, содержащиеся в справке от бюро медико-социальной экспертизы; группа инвалидности;

37) сведения, содержащиеся в индивидуальной программе реабилитации инвалида;

38) сведения о льготах;

39) адрес электронной почты;

40) сведения, содержащиеся в документах, подтверждающих стоимость проезда и провоза багажа в пределах территории Российской Федерации к месту использования отпуска и обратно;

41) сведения, содержащиеся в документах, подтверждающих расходы сотрудников, связанных со служебными командировками;

42) сведения, содержащиеся в листках временной нетрудоспособности,

43) иные сведения, представленные сотрудником по собственной инициативе;

полученных лично от меня для обработки и передачи в документальной и электронной форме в различные государственные органы власти, если этого требует законодательство Российской Федерации или Ханты-Мансийского автономного округа – Югры, а также третьим лицам:

1) Кредитным организациям в целях перечисления денежных средств, выпуска и обслуживания банковских карт;

2) Органы государственной власти Ханты-Мансийского автономного округа – Югры (Департамент труда и занятости населения Ханты-Мансийского автономного округа – Югры) в целях осуществления контроля (надзора) за приемом на работу людей с ограниченными возможностями здоровья в пределах установленной квоты;

3) Медицинские учреждения с целью проведения предрейсового (послерейсового) медицинского осмотра;

4) Образовательные учреждения с целью оказания ими образовательных услуг по обучению сотрудников БУ «Советский комплексный центр социального обслуживания населения»,

с целью исполнения обязательств представителя нанимателя в рамках трудового договора, и в установленных Федеральными законами случаях их обязательного предоставления.

Настоящее согласие дается на период срока действия трудовых правоотношений, а по их завершении - до истечения сроков хранения соответствующей информации или документов, содержащих указанную информацию, определяемых в соответствии с законодательством Российской Федерации.

В случае неправомерного использования предоставленных мною персональных данных согласие отзывается моим письменным заявлением.

_____

(Ф.И.О., подпись лица, давшего согласие)

Примечание:

1. Письменное согласие заполняется и подписывается субъектом персональных данных собственноручно в присутствии должностного лица оператора.

2. Перечень персональных данных уточняется исходя из целей получения согласия.

3. Срок хранения документов определен в приказе Росархива от 20.12.2019 № 236 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения».

БУ «Советский комплексный центр социального обслуживания населения»

адрес: ХМАО-Югра, Тюменская область, г. Советский, ул. Гастелло, д.39

ИНН: 8615011097 ОГРН: 1028601845238

СОГЛАСИЕ

на обработку персональных данных, разрешенных СУБЪЕКТОМ ПЕРСОНАЛЬНЫХ ДАННЫХ для распространения

Я, _____,
(фамилия, имя, отчество (при наличии) субъекта ПДн на русском языке (в русской транскрипции для иностранного гражданина и лица без гражданства)

Контактная информация: _____
(контактная информация (номер телефона, адрес электронной почты или почтовый адрес субъекта ПДн)

настоящим даю свое согласие на передачу (распространение) моих ПДн БУ «Советский комплексный центр социального обслуживания населения» и подтверждаю, что, давая такое согласие, я действую по своей воле и в своих интересах.

Согласие дается мною с целью размещения на общедоступных источниках персональных данных и распространяется на следующую информацию:

Категория ПДн	**Перечень ПДн**	**Разрешаю к распространению (да/нет)**	**Условия и запреты**
Общие ПДн	Фамилия		
	Имя		
	Отчество (при наличии)		
	Сведения о занимаемой должности		
	Номер рабочего телефона		
	Адрес рабочей электронной почты		
	Фотография		
	Сведения о наградах, достижениях, участии в мероприятиях		

Вышеперечисленные персональные данные будут размещены на официальном сайте БУ «Советский комплексный центр социального обслуживания населения», официальных страницах в социальных сетях

,которые являются общедоступными источниками персональных данных, с соблюдением всех условий и запретов, установленных субъектом ПДн.

Настоящее согласие дается на период срока действия трудовых отношений и на период ____ лет по их завершении.

В случае неправомерного использования предоставленных мною персональных данных согласие отзывается моим письменным заявлением.

«____» _____ 20___г. _____/_____/
(подпись) (расшифровка)

Приложение 5 к приказу
БУ «Советский комплексный
центр социального
обслуживания населения»
от «06» сентября 2023 г. № 167

Разъяснение
субъекту персональных данных

Я _____,
(фамилия, имя, отчество)

паспорт (иной документ, удостоверяющий личность) серия _____ № _____ выдан _____
_____
_____ дата выдачи «___» _____ 20 ___г.

получил (а) разъяснения о юридических последствиях отказа предоставить свои персональные данные БУ «Советский комплексный центр социального обслуживания населения» в соответствии с законодательством Российской Федерации.

В соответствии со статьей 65 Трудового кодекса Российской Федерации субъект персональных данных при приеме на работу и заключении трудового договора, обязан предоставить определенный перечень информации о себе.

Без предоставления субъектом персональных данных обязательных для заключения трудового договора сведений, трудовой договор не может быть заключен.

_____	_____	_____
дата	подпись	расшифровка

Юридические последствия отказа предоставить персональные данные разъяснил(а):

_____	_____	_____
должность	подпись	расшифровка

Приложение 6 к приказу
БУ «Советский комплексный
центр социального
обслуживания населения»
от «06» сентября 2023 г. № 167

Обязательство
о неразглашении информации, содержащей персональные данные

Я, _____,
(фамилия, имя, отчество полностью)

являясь сотрудником БУ «Советский комплексный центр социального обслуживания населения», в должности
_____,
_____
(указать должность и наименование структурного подразделения)

обязуюсь прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, в случае расторжения со мной трудового договора.

В соответствии со статьей 7 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией, и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставшие известными мне в связи с исполнением должностных обязанностей.

Я предупрежден(а) о том, что в случае нарушения данного обязательства буду привлечен(а) к ответственности в соответствии с законодательством Российской Федерации.

_____	_____	_____
дата	подпись	расшифровка

Приложение 7 к приказу
БУ «Советский комплексный
центр социального
обслуживания населения»
от «06» сентября 2023 г. № 167

ЖУРНАЛ
учета машинных носителей персональных данных (стационарные носители)

№ п/п	Регистрационный номер	Тип и ёмкость	Дата и место установки (использования)	Ответственное должностное лицо (Ф.И.О)

ЖУРНАЛ
учета лиц, допущенных к работе с персональными данными в информационных системах персональных данных

№ п/п	Сведения о допуске к персональным данным				Сведения о прекращении допуска к персональным данным
	Наименование информационных систем персональных данных /способ обработки ПДн	Ф.И.О, должность получившего допуск	Дата и номер приказа о допуске	Дата и подпись допускаемого лица	Дата и номер приказа о прекращении допуска

ЖУРНАЛ
учета средств защиты информации

№ п/п	Индекс и наименование средства защиты информации	Серийный (заводской) номер	Номер специального защитного знака	Наименование организации, установившей средство защиты информации	Место установки	Примечание

ЖУРНАЛ

учета обращений субъектов персональных данных по вопросам обработки персональных данных

№ п/п	Дата обращения	ФИО обратившегося	Цель обращения	Отметка о предоставлении информации или отказе в ее предоставлении / дата предоставления или отказа в предоставлении информации	Подпись ответственного	Примечание

ЖУРНАЛ

антивирусных проверок информационных систем персональных данных

№ п/п	Дата и время проверки	Наименование ИСПДн (составной части ИСПДн)	Какими средствами проводилась проверка	Результаты проверки		Наименование инфицированных файлов, источника поступления (носитель, организация)	Примечание (принятые меры)	Фамилия и подпись лица, проводившего проверку
				кол-во проверенных файлов	кол-во инфицированных файлов			

ЖУРНАЛ

учета выявленных инцидентов информационной безопасности

№ п/п	Дата и время	Описание инцидента	Ответственный за реагирование на инцидент	Отметка об устранении инцидента	Дата устранения инцидента	Подпись ответственного лица	Примечание

ЖУРНАЛ
периодического тестирования средств защиты информации

№ п/п	Наименование средства защиты информации	Регистрационные номера СЗИ	Дата тестирования	Фамилия и подпись ответственного пользователя, проводившего тестирование	Наименование теста, используемые средства для проведения теста	Результат тестирования (успешный/неуспешный), комментарий	Дата очередного тестирования

ЖУРНАЛ

учета проверок электронных журналов обращений к информационным системам персональных данных

№ п/п	Дата проверки	Наименование ИСПДн, компьютера, технического средства	Наименование проверяемого журнала	Выявленные нарушения требований безопасности, нештатные ситуации	Подпись администратора информационной безопасности	Примечание

ЖУРНАЛ
уничтожения носителей персональных данных

№ п/п	Наименование ИСПДн, в которой уничтожаются персональные данные	Ф.И.О. субъекта, персональные данные которого подлежат уничтожению	Обоснование уничтожения	Наименование файла, и его месторасположение	Дата уничтожения	Ф.И.О. и подпись исполнителя	Ф.И.О. и подпись ответственного за обработку персональных данных

ЖУРНАЛ

ознакомления сотрудников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных

№ п/п	Ф.И.О. инструктируемого	Структурное подразделение, должность инструктируемого	Вид инструктажа	Дата	Ф.И.О. инструктирующего	Структурное подразделение, должность инструктирующего	Подпись инструктирующего	Подпись инструктируемого

ЖУРНАЛ

учета выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн

№ п/п	Дата	Краткое описание выполненной работы	Ф.И.О. исполнителей и их подписи	Ф.И.О. ответственного за эксплуатацию ИСПДн, подпись	Подпись администратора информационной безопасности	Примечание (ссылка на заявку)

Приложение 8 к приказу
БУ «Советский комплексный
центр социального
обслуживания населения»
от «06» сентября 2023 г. № 167

ПРОТОКОЛ № __
заседания комиссии по защите информации

Дата и время проведения _____
Место проведения _____

Председатель комиссии _____ ФИО
Члены комиссии _____ ФИО
_____ ФИО
_____ ФИО

Повестка дня

Определение информационных систем персональных данных (далее - ИСПДн), принадлежащих БУ «Советский комплексный центр социального обслуживания населения».

1. Слушали: _____
доложил(а) исходные данные об ИСПДн « «1С:Зарплата и Кадры»».

Выступил(а): _____
предложил(а) утвердить акт определения уровня защищенности персональных данных и класса защищённости ИС «_____».

Постановили:

Утвердить акт определения уровня защищенности персональных данных и класса защищённости ИС «УЗ4».

Председатель комиссии _____ ФИО
Члены комиссии _____ ФИО
_____ ФИО
_____ ФИО

Приложение 9 к приказу
БУ «Советский комплексный
центр социального
обслуживания населения»
от «06» сентября 2023 г. № 167

АКТ
определения уровня защищенности ПДн при их обработке в ИСПДн и класса защищенности ИС «1С:Зарплата и Кадры»

Председатель комиссии _____ ФИО
Члены комиссии _____ ФИО
_____ ФИО
_____ ФИО

Рассмотрев исходные данные об информационной системе персональных данных (далее - ИСПДн), комиссия определила:

– Категории персональных данных обрабатываемых в ИСПДн: в информационной системе обрабатываются _____ (биометрические, специальные, общедоступные, иные) категории персональных данных;

– Категории субъектов: _____ (субъектов персональных данных, являющихся сотрудниками оператора или субъектов персональных данных, не являющихся сотрудниками оператора);

– Объем обрабатываемых персональных данных: _____ (менее чем 100000, более чем 100000);

– Тип актуальных угроз: для информационной системы актуальны угрозы _____ (первого, второго, третьего) типа;

Комиссия решила, в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и на основании анализа исходных данных, необходимо обеспечить _____ уровень защищенности (УЗ4___) персональных данных.

Председатель комиссии _____ ФИО
Члены комиссии _____ ФИО
_____ ФИО
_____ ФИО

«__»_____20____ г.

Приложение 10 к приказу
БУ «Советский комплексный
центр социального
обслуживания населения»
от «06» сентября 2023 г. № 167

АКТ

об уничтожении персональных данных субъектов персональных данных

Комиссия в составе:

Роль	ФИО	Должность
Председатель		
Члены комиссии		

Установила, что на основании достижения цели обработки персональных данных, в соответствии с требованиями Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» гл. 2, ст. 5, пункт 7, подлежат уничтожению сведения, составляющие персональные данные:

№ п/п	Сведения, содержащие персональные данные	Место хранения	Кол-во ед. хранения	Примечание

Указанные персональные данные уничтожены путем _____

_____

(удаления с помощью средств гарантированного удаления информации, уничтожения носителя и т.п.)

Председатель комиссии: _____ _____

подпись расшифровка

Члены комиссии: _____ _____

подпись расшифровка

_____ _____

подпись расшифровка

_____ _____

подпись расшифровка

Приложение 11 к приказу
БУ «Советский комплексный
центр социального
обслуживания населения»
от «06» сентября 2023 г. № 167

Перечень информационных систем персональных данных

Наименование ИСПДн	Адрес расположения	Структура ИСПДн	Наличие подключений к ССОП и сетям МИО (Интернет)	Разграничение доступа пользователей	Уровень защищенности ИСПДн
«1С: Зарплата и Кадры»	628242 Советский, ул. Гастелло, дом 39	Локальная информационная система	Имеется многоточечное подключение	С разграничением прав доступа	Четвертый (У34)

Приложение 12 к приказу
БУ «Советский комплексный
центр социального
обслуживания населения»
от «06» сентября 2023 г. № 167

ПЕРЕЧЕНЬ
обрабатываемых персональных данных

Таблица 1. Перечень обрабатываемых персональных данных

Группа персональных данных	Состав персональных данных	Цели обработки персональных данных	Способ обработки персональных данных
Сотрудники, в том числе уволенные	1) фамилия, имя, отчество; 2) пол; 3) гражданство; 4) данные документа, удостоверяющего личность; 5) год, месяц и дата рождения; место рождения; 6) адрес регистрации (места жительства); 7) сведения о составе семьи и о близких родственниках (Фамилия, имя, отчество, дата рождения, степень родства); 8) сведения о доходах;	Обеспечение соблюдения законов и иных нормативных правовых актов, содействие в трудоустройстве, получение образования и продвижение по службе, обеспечение личной	Смешанный

Группа персональных данных	Состав персональных данных	Цели обработки персональных данных	Способ обработки персональных данных
	9) семейное положение; 10) сведения об образовании и (или) о квалификации или наличие специальных знаний, наименование образовательного учреждения, сведения о документах, подтверждающих образование (наименование, серия, номер, дата выдачи, годы обучения, направление, специальность или квалификация по документу); 11) профессия; 12) сведения о наградах; поощрениях; почетных званиях; медалях; 13) квалификация; 14) номер и дата трудового договора; 15) сведения об отпусках, в том числе о выезде за пределы РФ; 16) данные идентификационного номера налогоплательщика (ИНН); 17) данные Пенсионного страхового свидетельства (СНИЛС); 18) сведения о воинском учете, данные военного билета; 19) сведения о постановке на учет в налоговом органе; 20) результаты обязательных предварительных	безопасности, контроль количества и качества выполняемой работы и обеспечение сохранности имущества; ведение кадрового, бухгалтерского, налогового и воинского учета; размещение на общедоступных источниках персональных данных; предоставление гарантий и компенсаций, установленных действующим законодательством и локальными	смешанный

Группа персональных данных	Состав персональных данных	Цели обработки персональных данных	Способ обработки персональных данных
	(при поступлении на работу) и периодических медицинских осмотров (обследований); 21) сведения о судимости/факте уголовного преследования (наличие/отсутствие); 22) сведения об административных правонарушениях; 23) место работы; 24) должность; 25) табельный номер; 26) сведения, содержащиеся в трудовой книжке, вкладыше в трудовую книжку; 27) сведения, содержащиеся в должностной инструкции; 28) сведения о трудовой деятельности и стаже; 29) данные банковского счета; 30) номер контактного телефона или сведения о других способах связи; 31) фотографическое изображение; 32) сведения, содержащиеся в актах органов записи гражданского состояния; 33) подпись; 34) данные водительского удостоверения; 35) сведения, содержащиеся в медицинской справке о допуске к управлению транспортным средством;	нормативными актами БУ «Советский комплексный центр социального обслуживания населения»	смешанный

Группа персональных данных	Состав персональных данных	Цели обработки персональных данных	Способ обработки персональных данных
	36) сведения, содержащиеся в справке от бюро медико-социальной экспертизы; группа инвалидности; 37) сведения, содержащиеся в индивидуальной программе реабилитации инвалида; 38) сведения о льготах; 39) адрес электронной почты; 40) сведения, содержащиеся в документах, подтверждающих стоимость проезда и провоза багажа в пределах территории Российской Федерации к месту использования отпуска и обратно; 41) сведения, содержащиеся в документах, подтверждающих расходы сотрудников, связанных со служебными командировками; 42) сведения, содержащиеся в листках временной нетрудоспособности, 43) иные сведения, представленные сотрудником по собственной инициативе;		смешанный
Родственники сотрудников, в том числе уволенных	1) фамилия, имя, отчество; 2) сведения, содержащиеся в актах органов записи гражданского состояния; 3) степень родства; 4) число, месяц и год рождения;	Реализация трудовых отношений, ведение личных дел (карточек), ведение	Смешанный

Группа персональных данных	Состав персональных данных	Цели обработки персональных данных	Способ обработки персональных данных
	5) сведения, содержащиеся в документах, подтверждающих стоимость проезда и провоза багажа в пределах территории Российской Федерации к месту использования отпуска и обратно.	налогового учета, предоставления гарантий и компенсаций, установленных действующим законодательством и локальными нормативными актами БУ «Советский комплексный центр социального обслуживания населения»	смешанный

Таблица 2. Правовое основание обработки персональных данных и сроки их хранения

Группа персональных данных	Правовое основание для обработки персональных данных	Сроки хранения
Сотрудники, в том числе уволенные	1) Трудовой кодекс Российской Федерации (Федеральный закон от 30.12.2001 № 197-ФЗ); 2) Налоговый кодекс Российской Федерации (Федеральный закон от 05.08.2000 № 117-ФЗ); 3) Федеральный закон «Об обязательном пенсионном страховании в Российской Федерации» от 15.12.2001 № 167-ФЗ; 4) Федеральный закон «О воинской обязанности и военной службе» от 28.03.1998 № 53-ФЗ; 5) Федеральный закон «О социальной защите инвалидов в Российской Федерации» от 24.11.1995 № 181-ФЗ; 6) Федеральный закон «О безопасности дорожного движения» от 10.12.1995 № 196-ФЗ; 7) Федеральный закон «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования» от 01.04.1996 № 27-ФЗ; 8) Федеральный закон «О бухгалтерском учете» от 06.12.2011 № 402-ФЗ; 9) Постановление Правительства РФ «Об утверждении Положения о воинском учете» от 27.11.2006 № 719; 10) Закон Ханты-Мансийского автономного округа – Югры «О гарантиях трудовой занятости инвалидов в Ханты-Мансийском автономном округе - Югре» от 23.12.2004 № 89-оз;	По достижению целей обработки*

Группа персональных данных	Правовое основание для обработки персональных данных	Сроки хранения
	11) Закон Ханты-Мансийского автономного округа – Югры «О гарантиях и компенсациях для лиц, проживающих в Ханты-Мансийском автономном округе - Югре, работающих в государственных органах и государственных учреждениях Ханты-Мансийского автономного округа - Югры» от 09.12.2004 № 76-оз; 12) Постановление Правительства Ханты-Мансийского автономного округа – Югры «О порядке возмещения расходов, связанных со служебными командировками, руководителям и работникам государственных учреждений Ханты-Мансийского автономного округа - Югры» от 19.05.2008 № 108-п; 13) Устав БУ «Советский комплексный центр социального обслуживания населения» от 18.12.2014 г.; 14) Коллективный договор БУ «Советский комплексный центр социального обслуживания населения» на 2022-2025 годы; 15) Согласие субъекта персональных данных	
Родственники сотрудников, в том числе уволенных	1) Трудовой кодекс Российской Федерации (Федеральный закон от 30.12.2001 № 197-ФЗ); 2) Налоговый кодекс Российской Федерации (Федеральный закон от 31.07.1998 № 146-ФЗ); 3) Закон Ханты-Мансийского автономного округа – Югры «О гарантиях и компенсациях для лиц, проживающих в Ханты-Мансийском автономном округе - Югре, работающих в государственных органах и государственных учреждениях	По достижению целей обработки*

Группа персональных данных	Правовое основание для обработки персональных данных	Сроки хранения
	Ханты-Мансийского автономного округа - Югры» от 09.12.2004 № 76-оз; 4) Коллективный договор БУ «Советский комплексный центр социального обслуживания населения» от 30.11.2022	

* - Приказ Росархива от 20.12.2019 № 236 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения»

Приложение 13 к приказу
БУ «Советский комплексный
центр социального
обслуживания населения»
от «06» сентября 2023 г. № 167

Положение об организации режима обеспечения безопасности помещений, в которых размещены информационные системы персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения

1. Общие положения

Положение об организации режима обеспечения безопасности помещений БУ «Советский комплексный центр социального обслуживания населения», в которых размещены информационные системы персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения (далее – Положение) разработано в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», приказом ФСТЭК России от 18.02.2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.1. Обеспечение безопасности помещений БУ «Советский комплексный центр социального обслуживания населения», где расположены информационные системы персональных данных (далее – ИСПДн), ведется обработка персональных данных (далее – ПДн), а также где расположено коммутационное оборудование и серверы, направлено на исключение возможности несанкционированного доступа к техническим средствам, входящим в состав ИСПДн, их хищения и нарушения работоспособности, хищения носителей информации.

1.2. Защита от проникновения посторонних лиц в помещения БУ «Советский комплексный центр социального обслуживания населения»

обеспечивается организацией порядка доступа, а также соответствующей инженерно-технической защитой помещений, и видеонаблюдением.

2. Границы контролируемой зоны

Контролируемая зона – границы пространства (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска.

План-схемы контролируемых зон помещений по адресу: 628242, город, ул. Гастелло, дом 39, приведены в приложении 1 к настоящему Положению.

3. Предъявляемые требования к помещениям и порядок доступа к ним

3.1. Помещения БУ «Советский комплексный центр социального обслуживания населения», в которых размещены ИСПДн и ведется обработка ПДн (далее - помещения), должны соответствовать следующим требованиям:

- обеспечивать сохранность технических средств;
- исключать возможность бесконтрольного проникновения в помещения;
- исключать возможность визуального просмотра обрабатываемой информации посторонними лицами;
- двери и окна должны иметь прочные и надежные петли, шпингалеты, крючки или задвижки и быть плотно подогнаны к рамам и дверным коробам. Допускается применение электромеханических, электромагнитных замков и задвижек;
- конструкция оконных рам должна исключать возможность демонтажа с наружной стороны оконного проема стекол. Стекла в рамах должны быть надежно закреплены в пазах. Рамы указанных оконных проемов оборудуются запорными устройствами. На окнах первого этажа, а также верхних этажей – при возможности прямого просмотра помещения с улицы, должны быть установлены жалюзи.

3.2. Перечень должностей в Учреждении, доступ которых в Помещения необходим для выполнения ими должностных (трудовых) обязанностей приведен в приложении 2 к настоящему Положению.

3.3. Неконтролируемое пребывание лиц в помещениях, находящихся в пределах границы контролируемой зоны, указанных в п. 2.2 настоящего Положения, разрешено в период рабочего времени в соответствии с утвержденным графиком работы БУ «Советский комплексный центр социального обслуживания населения», либо вне периода рабочего времени с письменного разрешения ответственного за организацию обработки персональных данных или ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных.

3.4. Лица, не указанные в п. 2.2 настоящего Положения, допускаются в помещения в присутствии лиц, имеющих право пребывания в данных помещениях.

3.5. В случае отсутствия сотрудников в помещении в рабочее время, помещение должно быть закрыто на ключ.

3.6. Вскрытие и закрытие помещений осуществляется сотрудниками данной ИСПДн.

3.7. Перед закрытием помещения по окончании рабочего времени лица, непосредственно обрабатывающие персональные данные, обязаны:

− убрать бумажные и электронные носители, содержащие персональные данные, в металлические шкафы (сейфы);

− отключить технические средства обработки информации и электроприборы от сети.

3.8. Сотрудник, последний покидающий помещение, обязан:

− закрыть окна;

− выключить освещение;

− закрыть дверь помещения.

3.9. Перед открытием помещения первый прибывший сотрудник обязан:

− провести внешний осмотр двери и дверного замка с целью установления их целостности;

− открыть дверь и осмотреть помещение;

− проверить наличие и целостность замков на металлических шкафах (сейфах) с целью установления их целостности.

3.10. При обнаружении факта взлома двери, дверного замка сотрудник обязан:

− не вскрывая помещение, незамедлительно сообщить непосредственному руководителю;

− в присутствии не менее двух лиц и непосредственного руководителя вскрыть помещение и осмотреть его;

− составить акт о факте взлома двери, дверного замка и направить его Перечень помещений, в которых осуществляется обработка персональных данных

3.11. Перечень помещений, в которых осуществляется обработка персональных данных, приведен в приложении 2 к настоящему положению.

4. Организация и порядок производства ремонтно-строительных работ

4.1. Рабочие и специалисты ремонтно-строительных организаций допускаются в помещение для проведения ремонтно-строительных работ на основании заявок, подписанных руководством. Работы проводятся только в присутствии контролирующего лица из числа сотрудников.

4.2. Для предотвращения несанкционированного доступа к информации, содержащей ПДн, осуществляется контроль деятельности рабочих.

5. Организация охраны

5.1. Для охраны помещений БУ «Советский комплексный центр социального обслуживания населения» используется охранная сигнализация.

5.2. Для исключения несанкционированного доступа к информации, содержащей ПДн, при покидании помещения необходимо закрывать его на ключ.

6. Уборка помещений

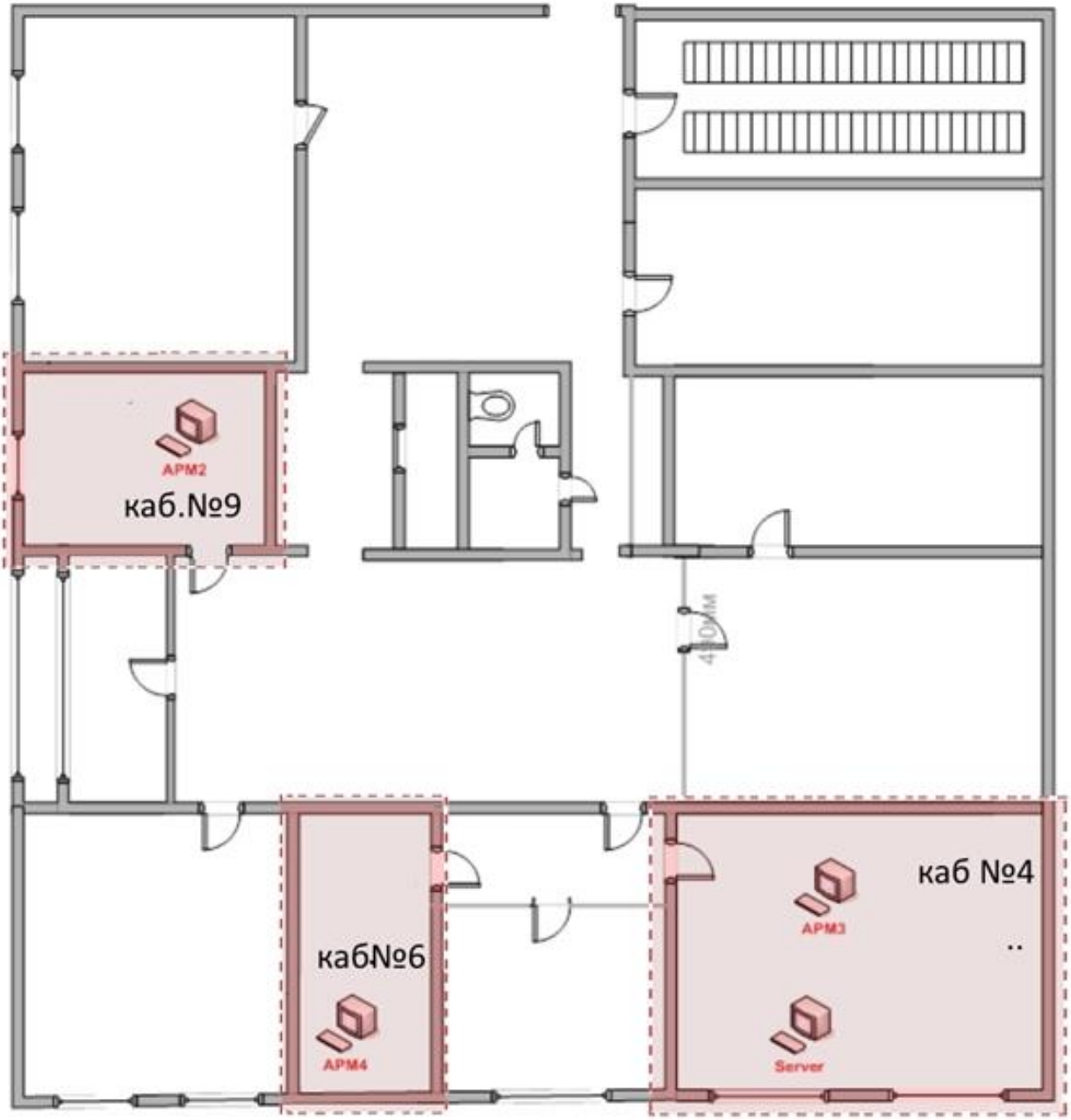
6.1. Уборка помещений должна производиться под контролем сотрудника, имеющего доступ в помещение и постоянно в нем работающего.

6.2. Во время уборки в помещении должна быть приостановлена работа с ПДн, должны быть заблокированы все АРМ, на которых хранятся ПДн, носители, содержащие ПДн, должны быть убраны в сейф.

Приложение 1

- - - - - - граница контролируемой зоны

Рисунок 1. Схема контролируемой зоны ГИС ПДн "1С"
(г.Советский ул.Гастелло д 39 второй этаж)



Приложение 2

Перечень помещений, в которых осуществляется обработка персональных данных

№ п/п	Помещение	Наименование должностей, доступ которых в Помещения необходим для выполнения ими должностных (трудовых) обязанностей
1	Кабинет № 4	Главный Бухгалтер, бухгалтер
2	Кабинет № 6	Специалист по кадрам
3	Кабинет № 9	Экономист

Приложение 14 к приказу
БУ «Советский комплексный
центр социального
обслуживания населения»
от «06» сентября 2023 г. № 167

ПОЛИТИКА
в отношении обработки персональных данных

1. Общие положения

1.1. Политика в отношении обработки персональных данных в БУ Учреждении разработана в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологий и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»), постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», приказом ФСТЭК России от 18.02.2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и другими нормативными правовыми актами, регулирующими отношения, связанные с обработкой персональных данных.

1.2. Политика определяет порядок и условия обработки персональных данных в Учреждении с использованием средств автоматизации и без использования таких средств.

1.3. Политика вступает в силу с момента подписания директором БУ «Советский комплексный центр социального обслуживания населения».

1.4. Политика подлежит пересмотру в ходе периодического анализа со стороны руководства БУ «Советский комплексный центр социального обслуживания населения», а также в случаях изменения законодательства Российской Федерации в области обеспечения безопасности персональных данных (далее - ПДн).

1.5. Основные понятия, используемые в Политике, соответствуют основным понятиям, указанным в статье 3 Федерального закона Российской Федерации от 27.07.2006 № 152 «О персональных данных».

1.6. Политика подлежит опубликованию на официальном сайте БУ «Советский комплексный центр социального обслуживания населения» в течение 10 дней после её утверждения.

2. Цели и правовые основания обработки персональных данных

Обработка ПДн осуществляется БУ «Советский комплексный центр социального обслуживания населения» в следующих целях:

- обеспечения соблюдения законов и иных нормативных правовых актов, содействия в трудоустройстве, получения образования и продвижение по службе, обеспечения личной безопасности, контроль количества и качества выполняемой работы и обеспечение сохранности имущества;
- ведения кадрового, бухгалтерского, налогового и воинского учета;
- размещения на общедоступных источниках персональных данных;
- предоставления гарантий и компенсаций, установленных действующим законодательством и локальными нормативными актами БУ «Советский комплексный центр социального обслуживания населения»,
- реализации трудовых отношений, ведения личных дел (карточек).

Обработка ПДн осуществляется БУ «Советский комплексный центр социального обслуживания населения» на основании следующих нормативно-правовых актов:

- Трудовой кодекс Российской Федерации (Федеральный закон от 30.12.2001 № 197-ФЗ);
- Налоговый кодекс Российской Федерации (Федеральный закон от 05.08.2000 № 117-ФЗ);
- Федеральный закон «Об обязательном пенсионном страховании в Российской Федерации» от 15.12.2001 № 167-ФЗ;
- Федеральный закон «О воинской обязанности и военной службе» от 28.03.1998 № 53-ФЗ;
- Федеральный закон «О социальной защите инвалидов в Российской Федерации» от 24.11.1995 № 181-ФЗ;
- Федеральный закон «О безопасности дорожного движения» от 10.12.1995 № 196-ФЗ;
- Федеральный закон «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования» от 01.04.1996 № 27-ФЗ;
- Федеральный закон «О бухгалтерском учете» от 06.12.2011 № 402-ФЗ;
- Постановление Правительства РФ «Об утверждении Положения о воинском учете» от 27.11.2006 № 719;
- Закон Ханты-Мансийского автономного округа – Югры «О гарантиях трудовой занятости инвалидов в Ханты-Мансийском автономном округе - Югре» от 23.12.2004 № 89-оз;
- Закон Ханты-Мансийского автономного округа – Югры «О гарантиях и компенсациях для лиц, проживающих в Ханты-Мансийском

автономном округе - Югре, работающих в государственных органах и государственных учреждениях Ханты-Мансийского автономного округа - Югры» от 09.12.2004 № 76-оз;

− Постановление Правительства Ханты-Мансийского автономного округа – Югры «О порядке возмещения расходов, связанных со служебными командировками, руководителям и работникам государственных учреждений Ханты-Мансийского автономного округа - Югры» от 19.05.2008 № 108-п;

− Устав БУ «Советский комплексный центр социального обслуживания населения» от 29.12.2014 г. №13р-3334

− Коллективный договор БУ «Советский комплексный центр социального обслуживания населения» в актуальной редакции.

− Согласие субъекта персональных данных.

3. Категории субъектов, персональные данные которых обрабатываются

3.1. В соответствии с целями обработки ПДн, указанными в п. 2. настоящей Политики, в Учреждении осуществляется обработка следующих категорий субъектов персональных данных:

− Сотрудников, в том числе уволенных;

− Родственников сотрудников, в том числе уволенных

4. Принципы обработки персональных данных

4.1. Обработка ПДн осуществляется на законной основе.

4.2. Обработка ПДн ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн.

4.3. Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

4.4. Обработке подлежат только те ПДн, которые отвечают целям их обработки.

4.5. Содержание и объем ПДн соответствуют заявленным целям обработки. Обрабатываемые ПДн не являются избыточным по отношению к заявленным целям их обработки.

4.6. При обработке ПДн обеспечены точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. БУ «Советский комплексный центр социального обслуживания населения» обеспечивается принятие необходимых мер по удалению или уточнению неполных или неточных данных.

4.7. Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн. Обрабатываемые ПДн подлежат уничтожению по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5. Условия обработки персональных данных

5.1. Условия обработки иных категорий ПДн:

5.1.1. Обработки иных категорий ПДн осуществляется БУ «Советский комплексный центр социального обслуживания населения» с соблюдением следующих условий:

– обработка ПДн необходима для осуществления и выполнения возложенных законодательством Российской Федерации на БУ «Советский комплексный центр социального обслуживания населения» функций, полномочий и обязанностей;

– 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 с согласия субъекта ПДн на обработку его ПДн.

5.2. Условия обработки общедоступных категорий ПДн:

5.2.1. Осуществляется обработка ПДн, сделанных общедоступными с согласия субъекта ПДн.

5.3. Поручение обработки ПДн:

5.3.1. БУ «Советский комплексный центр социального обслуживания населения» вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора.

5.3.2. Лицо, осуществляющее обработку ПДн по договору с БУ «Советский комплексный центр социального обслуживания населения», обязано соблюдать принципы и правила обработки ПДн, предусмотренные настоящей Политикой, соблюдать конфиденциальность ПДн, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных настоящей Политикой. В поручении БУ «Советский комплексный центр социального обслуживания населения»определены перечень ПДн, перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн, цели их обработки, установлена обязанность такого лица соблюдать конфиденциальность ПДн, требования, предусмотренные частью 5 статьи 18 и статьей 18.1. 152-ФЗ, обязанность по запросу БУ «Советский комплексный центр социального обслуживания населения» в течение срока действия поручения БУ «Советский комплексный центр социального обслуживания населения», в т.ч. до обработки ПДн, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения БУ «Советский комплексный центр социального обслуживания населения» требований, установленных в соответствии со статьей 6 152-ФЗ, обязанность обеспечивать безопасность ПДн при их обработке, а также указываются

требования к защите обрабатываемых ПДн в соответствии со статьей 19 152-ФЗ, в т.ч. требование об уведомлении БУ «Советский комплексный центр социального обслуживания населения» о случаях, предусмотренных частью 3.1. статьи 21 152-ФЗ.

5.3.3. Лицо, осуществляющее обработку ПДн по поручению БУ «Советский комплексный центр социального обслуживания населения», не обязано получать согласие субъекта ПДн на обработку его ПДн.

5.3.4. В случае, если БУ «Советский комплексный центр социального обслуживания населения» поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет БУ «Советский комплексный центр социального обслуживания населения». Лицо, осуществляющее обработку персональных данных по поручению БУ «Советский комплексный центр социального обслуживания населения», несет ответственность перед БУ «Советский комплексный центр социального обслуживания населения».

6. Конфиденциальность персональных данных

6.1. Сотрудники БУ «Советский комплексный центр социального обслуживания населения», получившие доступ к ПДн, обязаны не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом.

7. Общедоступные источники персональных данных

7.1. В целях информационного обеспечения БУ «Советский комплексный центр социального обслуживания населения» размещает ПДн на общедоступных источниках (информационных стендах). Сведения о субъекте ПДн исключаются из общедоступных источников ПДн по требованию субъекта ПДн либо по решению суда или иных уполномоченных государственных органов. В общедоступные источники ПДн включены следующие сведения о сотрудниках:

- Фамилия, имя, отчество (при наличии);
- Сведения о занимаемой должности;
- Номер рабочего телефона;
- Адрес рабочей электронной почты;
- Фотография;
- Сведения о наградах, достижениях, участии в мероприятиях.

8. Согласие субъекта персональных данных на обработку его персональных данных

8.1. При необходимости обеспечения условий обработки ПДн субъекта может предоставляться согласие субъекта ПДн на обработку его ПДн.

8.2. Субъект ПДн принимает решение о предоставлении его ПДн и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку ПДн должно быть конкретным, информированным и

сознательным. Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, ели иное не установлено федеральным законом. В случае получения согласия на обработку ПДн от представителя субъекта ПДн полномочия данного представителя на дачу согласия от имени субъекта ПДн проверяются БУ «Советский комплексный центр социального обслуживания населения».

8.3. Согласие на обработку ПДн может быть отозвано субъектом ПДн. В случае отзыва субъектом ПДн согласия на обработку ПДн БУ «Советский комплексный центр социального обслуживания населения» вправе продолжить обработку ПДн без согласия субъекта ПДн при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 152-ФЗ.

8.4. Обязанность предоставить доказательство получения согласия субъекта ПДн на обработку его ПДн возлагается на БУ «Советский комплексный центр социального обслуживания населения».

8.5. В случаях, предусмотренных федеральным законом, обработка ПДн осуществляется только с согласия в письменной форме субъекта ПДн. Равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме субъекта ПДн на обработку его ПДн должно включать в себя, в частности:

– 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.

8.6. В случае недееспособности субъекта ПДн согласие на обработку его ПДн дает законный представитель субъекта ПДн.

8.7. В случае смерти субъекта ПДн согласие на обработку его ПДн дают наследники субъекта ПДн, если такое согласие не было дано субъектом ПДн при его жизни.

8.8. Согласие на обработку ПДн, разрешенных субъектом ПДн для распространения, может быть предоставлено БУ «Советский комплексный центр социального обслуживания населения» непосредственно или с использованием информационной системы уполномоченного органа по защите прав субъектов ПДн.

9. Право субъекта персональных данных на доступ к его персональным данным

9.1. Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

– подтверждение факта обработки ПДн БУ «Советский комплексный центр социального обслуживания населения»;

– правовые основания и цели обработки ПДн;

– цели и применяемые БУ «Советский комплексный центр социального обслуживания населения» способы обработки ПДн;

– наименование и место нахождения БУ «Советский комплексный центр социального обслуживания населения», сведения о лицах (за исключением сотрудников БУ «Советский комплексный центр социального обслуживания населения»), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с БУ «Советский комплексный центр социального обслуживания населения» или на основании федерального закона;

– обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок предоставления таких данных не предусмотрен федеральным законом;

– сроки обработки ПДн, в том числе сроки их хранения;

– порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

– информацию об осуществленной или о предполагаемой трансграничной ПДн;

– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению БУ «Советский комплексный центр социального обслуживания населения», если обработка поручена или будет поручена такому лицу;

– информацию о способах исполнения БУ «Советский комплексный центр социального обслуживания населения» обязанностей, установленных статьей 18.1 152-ФЗ;

– иные сведения, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами.

9.2. Субъект ПДн имеет право на получение сведений, указанных в п. 9.1. настоящей Политики, за исключением случаев, при которых доступ субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц.

9.3. Субъект ПДн вправе требовать от БУ «Советский комплексный центр социального обслуживания населения» уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

9.4. Сведения, указанные в п. 9.1. настоящей Политики, должны быть предоставлены субъекту ПДн БУ «Советский комплексный центр социального обслуживания населения» в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

1.1. Сведения, указанные в п. 9.1. настоящей Политики, предоставляются субъекту ПДн или его представителю БУ «Советский комплексный центр социального обслуживания населения» в течение 10 (десяти) рабочих дней с момента обращения либо получения БУ «Советский комплексный центр социального обслуживания населения» запроса субъекта ПДн или его представителя. Указанный срок может быть продлен, но не более чем на 5 рабочих дней в случае направления БУ «Советский комплексный центр социального обслуживания населения» в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации. Запрос должен содержать номер основного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПДн в отношениях с БУ «Советский комплексный центр социального обслуживания населения» (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн БУ «Советский комплексный центр социального обслуживания населения», подпись субъекта ПДн или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации. БУ «Советский комплексный центр социального обслуживания

населения»предоставляет сведения, указанные в пункте 9.1 Политики, субъекту ПДн или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

9.5. В случае, если сведения, указанные в п. 9.1. настоящей Политики, а также обрабатываемые ПДн были предоставлены для ознакомления субъекту ПДн по его запросу, субъект ПДн вправе обратиться повторно к БУ «Советский комплексный центр социального обслуживания населения» или направить ему повторный запрос в целях получения сведений, указанных в п. 9.1. настоящей Политики, и ознакомления с такими ПДн не ранее чем через 30 дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн.

9.6. Субъект ПДн вправе обратиться повторно к БУ «Советский комплексный центр социального обслуживания населения» или направить ему запрос в целях получения сведений, указанных в п. 9.1. настоящей Политики, а также в целях ознакомления с обрабатываемыми ПДн до истечения срока, указанного в п. 9.5. настоящей Политики, в случае, если такие сведения и (или) обрабатываемы ПДн не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду с необходимой для запроса информацией должен содержать основание направления повторного запроса.

9.7. БУ «Советский комплексный центр социального обслуживания населения» вправе отказать субъекту ПДн в выполнении повторного запроса, несоответствующего условиям повторного запроса. Такой отказ должен быть мотивированным. Обязанность предоставления доказательств обоснованности отказа в выполнении повторного запроса лежит на Учреждении.

9.8. Формы запросов субъектов персональных данных или их представителей и уполномоченного органа по защите прав субъектов персональных представлены в приложении к настоящей Политике.

10. Право на обжалование действий или бездействий БУ «Советский комплексный центр социального обслуживания населения»

10.1. Если субъект ПДн считает, что БУ «Советский комплексный центр социального обслуживания населения» осуществляет обработку его ПДн с нарушением требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» или иным образом нарушает его права и свободы, субъект ПДн вправе обжаловать действия или бездействия БУ «Советский комплексный центр социального обслуживания населения» в

уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) или в судебном порядке.

10.2. Субъект ПДн имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

11. Обязанности БУ «Советский комплексный центр социального обслуживания населения»

11.1. При сборе ПДн БУ «Советский комплексный центр социального обслуживания населения» обязано предоставить субъекту ПДн по его просьбе информацию, предусмотренную в пункте 9.1 Политики.

11.2. Если предоставление ПДн является обязательным в соответствии с федеральным законом, БУ «Советский комплексный центр социального обслуживания населения» обязано разъяснить субъекту ПДн юридические последствия отказа предоставить его ПДн и (или) дать согласие на их обработку.

11.3. Если ПДн получены не от субъекта ПДн, БУ «Советский комплексный центр социального обслуживания населения», за исключением случаев, предусмотренных пункте 9.2 Политики, до начала обработки таких ПДн обязано предоставить субъекту ПДн следующую информацию:

11.3.1. Наименование либо фамилия, имя, отчество и адрес БУ «Советский комплексный центр социального обслуживания населения» или его представителя.

11.3.2. Цель обработки ПДн и ее правовое основание.

11.3.3. Перечень ПДн.

11.3.4. Предполагаемые пользователи ПДн.

11.3.5. Установленные Законом № 152-ФЗ права субъекта ПДн.

11.3.6. Источник получения ПДн.

11.4. БУ «Советский комплексный центр социального обслуживания населения» освобождается от обязанности предоставить субъекту ПДн сведения, предусмотренные пункте 9.1 Политики, в случаях, если:

11.4.1. Субъект ПДн уведомлен об осуществлении обработки его ПДн БУ «Советский комплексный центр социального обслуживания населения».

11.4.2. ПДн получены БУ «Советский комплексный центр социального обслуживания населения» на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект ПДн.

11.4.3. Обработка ПДн, разрешенных субъектом ПДн для распространения, осуществляется с соблюдением запретов и условий, предусмотренных статьей 10.1 152-ФЗ.

11.4.4. Предоставление субъекту ПДн сведений, предусмотренных пункте 9.1 Политики, нарушает права и законные интересы третьих лиц.

11.4.5. При сборе ПДн, в том числе посредством информационно-телекоммуникационной сети «Интернет», обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение ПДн граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 152-ФЗ.

11.4.6. Сообщить в порядке, предусмотренном ст. 14 152-ФЗ, субъекту ПДн или его представителю информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн, а также предоставить возможность ознакомления с этими ПДн при обращении субъекта ПДн или его представителя либо в течение 10 (десяти) рабочих дней с даты получения запроса субъекта ПДн или его представителя. Указанный срок может быть продлен, но не более чем на 5 рабочих дней в случае направления БУ «Советский комплексный центр социального обслуживания населения» в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

11.4.7. В случае отказа в предоставлении информации о наличии ПДн о соответствующем субъекте ПДн или ПДн субъекту ПДн или его представителю при их обращении либо при получении запроса субъекта ПДн или его представителя дать в письменной форме мотивированный ответ, содержащий ссылку на положение ч. 8 ст. 14 152-ФЗ или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий 10 (десяти) рабочих дней со дня обращения субъекта ПДн или его представителя либо с даты получения запроса субъекта ПДн или его представителя. Указанный срок может быть продлен, но не более чем на 5 рабочих дней в случае направления оператором в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

11.4.8. Предоставить безвозмездно субъекту ПДн или его представителю возможность ознакомления с ПДн, относящимися к этому субъекту ПДн. В срок, не превышающий 7 рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными, внести в них необходимые изменения. В срок, не

превышающий 7 рабочих дней со дня представления субъектом ПДн или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, уничтожить такие ПДн. Уведомить субъекта ПДн или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы.

11.4.9. Сообщить в уполномоченный орган по защите прав субъектов ПДн по запросу этого органа необходимую информацию в течение 10 (десяти) рабочих дней с даты получения такого запроса. Указанный срок может быть продлен, но не более чем на 5 рабочих дней в случае направления БУ «Советский комплексный центр социального обслуживания населения» в адрес уполномоченного органа по защите прав субъектов ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

11.4.10. В случае выявления неправомерной обработки ПДн при обращении субъекта ПДн или его представителя либо по запросу субъекта ПДн или его представителя, либо уполномоченного органа по защите прав субъектов ПДн осуществить блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту ПДн, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению БУ «Советский комплексный центр социального обслуживания населения» с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных ПДн при обращении субъекта ПДн или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов ПДн осуществить блокирование ПДн, относящихся к этому субъекту ПДн, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению БУ «Советский комплексный центр социального обслуживания населения») с момента такого обращения или получения указанного запроса на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта ПДн или третьих лиц.

11.4.11. В случае подтверждения факта неточности ПДн на основании сведений, представленных субъектом ПДн или его представителем либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов уточнить ПДн либо обеспечить их уточнение (если обработка ПДн осуществляется другим лицом, действующим по поручению БУ «Советский комплексный центр социального обслуживания населения») в

течение 7 рабочих дней со дня представления таких сведений и снять блокирование ПДн.

11.4.12. В случае выявления неправомерной обработки ПДн, осуществляемой БУ «Советский комплексный центр социального обслуживания населения» или лицом, действующим по поручению БУ «Советский комплексный центр социального обслуживания населения», в срок, не превышающий 3 рабочих дней с даты этого выявления, прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению БУ «Советский комплексный центр социального обслуживания населения». В случае, если обеспечить правомерность обработки ПДн невозможно, БУ «Советский комплексный центр социального обслуживания населения» в срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки ПДн, уничтожить такие ПДн или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении ПДн уведомить субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.

11.4.13. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) ПДн, повлекшей нарушение прав субъектов ПДн, с момента выявления такого инцидента БУ «Советский комплексный центр социального обслуживания населения», уполномоченным органом по защите прав субъектов ПДн или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов ПДн:

1) в течение 24 часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов ПДн, и предполагаемом вреде, нанесенном правам субъектов ПДн, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном БУ «Советский комплексный центр социального обслуживания населения» на взаимодействие с уполномоченным органом по защите прав субъектов ПДн, по вопросам, связанным с выявленным инцидентом;

2) в течение 72 часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

11.4.14. В случае достижения цели обработки ПДн прекратить обработку ПДн или обеспечить ее прекращение (если обработка ПДн

осуществляется другим лицом, действующим по поручению БУ «Советский комплексный центр социального обслуживания населения») и уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению БУ «Советский комплексный центр социального обслуживания населения») в срок, не превышающий 30 дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между БУ «Советский комплексный центр социального обслуживания населения». и субъектом ПДн либо если БУ «Советский комплексный центр социального обслуживания населения». не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных 152-ФЗ или другими федеральными законами.

11.4.15. В случае отзыва субъектом ПДн согласия на обработку его ПДн прекратить их обработку или обеспечить прекращение такой обработки (если обработка ПДн осуществляется другим лицом, действующим по поручению БУ «Советский комплексный центр социального обслуживания населения».) и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению БУ «Советский комплексный центр социального обслуживания населения».) в срок, не превышающий 30 дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между БУ «Советский комплексный центр социального обслуживания населения». и субъектом ПДн либо если БУ «Советский комплексный центр социального обслуживания населения». не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных 152-ФЗ или другими федеральными законами.

11.4.16. В случае обращения субъекта ПДн к БУ «Советский комплексный центр социального обслуживания населения». с требованием о прекращении обработки ПДн в срок, не превышающий 10 рабочих дней с даты получения БУ «Советский комплексный центр социального обслуживания населения». соответствующего требования, прекратить их обработку или обеспечить прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку ПДн), за исключением случаев, предусмотренных пунктами 2 - 11 части 1 статьи 6, частью 2 статьи 10 и частью 2 статьи 11 152-ФЗ. Указанный срок может быть продлен, но не более чем на 5 рабочих дней в случае направления БУ

«Советский комплексный центр социального обслуживания населения». в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

11.4.17. В случае отсутствия возможности уничтожения ПДн в течение срока, указанного в ч. 3 - 5 ст. 21 152-ФЗ, осуществляет блокирование таких ПДн или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению БУ «Советский комплексный центр социального обслуживания населения».) и обеспечивает уничтожение ПДн в срок не более чем 6 месяцев, если иной срок не установлен федеральными законами.

11.4.18. В срок не позднее 3 рабочих дней с момента получения соответствующего согласия субъекта ПДн опубликовать информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц ПДн, разрешенных субъектом ПДн для распространения.

11.4.19. Обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных.

12. Меры направленные на обеспечение выполнения БУ «Советский комплексный центр социального обслуживания населения» обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»

12.1. Назначен ответственный за организацию обработки ПДн.

1.2. Изданы документы, определяющие политику БУ «Советский комплексный центр социального обслуживания населения». в отношении обработки ПДн, локальные акты по вопросам обработки ПДн, определяющих для каждой цели обработки ПДн категории и перечень обрабатываемых ПДн, категории субъектов, ПДн которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения ПДн при достижении целей их обработки или при наступлении иных законных оснований, а также локальных актов, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений. Такие документы и локальные акты не содержат положения, ограничивающие права субъектов ПДн, а также возлагающие на БУ «Советский комплексный центр социального обслуживания населения». не предусмотренные законодательством Российской Федерации полномочия и обязанности.

12.2. Применяются правовые, организационные и технические меры по обеспечению безопасности ПДн.

12.3. Утверждены правила проведения внутреннего контроля соответствия обработки ПДн требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и принятых в соответствии с ним БУ «Советский комплексный центр социального обслуживания населения».

12.4. Проведено ознакомление работников, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе, документами, определяющими политику БУ «Советский комплексный центр социального обслуживания населения», в отношении обработки ПДн, локальными актами по вопросам обработки ПДн.

13. Меры по обеспечению безопасности персональных данных при их обработке

13.1. Определены угрозы безопасности ПДн при их обработке в ИСПДн.

13.2. Применяются организационные и технические меры по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимые для выполнения требований к защите ПДн.

13.3. Применяются прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации.

13.4. Ведется учет машинных носителей ПДн.

13.5. Выполняются меры по обнаружению фактов несанкционированного доступа к ПДн и принятию соответствующих мер.

13.6. Определен комплекс мер по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

13.7. Установлены правила доступа к ПДн, обрабатываемым в ИСПДн, обеспечена регистрация и учет всех действий, совершаемых с ПДн в ИСПДн.

13.8. При передаче (подготовке к передаче) ПДн по каналам связи, имеющим выход за пределы контролируемой зоны, защита от раскрытия, модификации или навязывания (ввода ложной информации) осуществляется путем применения в соответствии с законодательством Российской Федерации средств криптографической защиты информации.

13.9. Для исключения несанкционированного просмотра ПДн на устройствах вывода (отображения, печати) информации, как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны, их не размещают напротив оконных проемов, входных дверей, в коридорах, холлах и иных местах, доступных для несанкционированного просмотра.

13.10. Осуществляется выявление, анализ и устранение уязвимостей ИСПДн на этапах создания и эксплуатации ИСПДн. Такие проверки проводятся с периодичностью один раз в месяц, с учетом того, что для

критических уязвимостей проводятся обязательные проверки в случае опубликования в общедоступных источниках информации о новых уязвимостях в средствах защиты информации, технических средствах и программном обеспечении, применяемом в ИСПДн. При выявлении уязвимости составляется отчет и разрабатывается план по их устранению.

13.11. Осуществляется непрерывный контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровнем защищенности персональных данных.

13.12. Проводятся работы по оценке эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн.

Приложение 1
к Политике в отношении обработки
персональных данных

Типовые формы запросов субъектов персональных данных

Форма запроса субъекта персональных данных о наличии и ознакомлении с ПДн

В БУ «Советский комплексный центр социального обслуживания населения»
от _____
адрес:_____
_____
паспорт №_____ выдан _____
_____
_____

ЗАПРОС

Я *состою/не состою* в договорных (трудовых) отношениях с БУ «Советский комплексный центр социального обслуживания населения» и со мной заключен договор № _____ от «___» _____ 20___г.

В соответствии со статьей 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» я имею право получить от вас сведения о наличии моих персональных данных, связанных с вышеуказанными данными.

Прошу вас предоставить мне следующую информацию:

1. осуществляется ли обработка моих персональных данных;
2. перечень обрабатываемых вами моих персональных данных и источник их получения;
3. какими способами эти данные обрабатываются;
4. какие лица имеют доступ или могут получить доступ к моим персональным данным;
5. срок хранения моих персональных данных;
6. осуществлялась ли трансграничная передача моих персональных данных, а, если нет, то предполагается ли такая передача;
7. какие юридические последствия для меня может повлечь обработка моих персональных данных.

Ответ на настоящий запрос прошу направить в письменной форме по вышеуказанному адресу в предусмотренный законом срок.

С уважением, _____
«____» _____ 20___ года

Форма запроса субъекта персональных данных на уточнение ПДн

В БУ «Советский комплексный центр социального обслуживания населения»

от _____

адрес:_____

_____

паспорт №_____ выдан _____

_____

_____

ЗАПРОС

Я *состою/не состою* в договорных (трудовых) отношениях с БУ «Советский комплексный центр социального обслуживания населения» и со мной заключен договор № _____ от «___» _____ 20__г.

В соответствии со статьей 20 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и в связи с _____

_____

_____ прошу внести следующие изменения в мои персональные данные: _____

_____

_____

_____

Ответ на настоящий запрос прошу направить в письменной форме по вышеуказанному адресу в предусмотренный законом срок.

С уважением, _____ «____» _____ 20___ года

Форма запроса субъекта персональных данных на уничтожение ПДн

В БУ «Советский комплексный центр социального обслуживания населения».

от _____

адрес:_____

_____

паспорт №_____ выдан _____

_____

_____

ЗАПРОС

Я *состою/не состою* в договорных (трудовых) отношениях с БУ «Советский комплексный центр социального обслуживания населения». и со мной заключен договор № _____ от «___» _____ 20__г.

В соответствии со статьей 20 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и в связи с _____

_____

_____ прошу Вас уничтожить мои персональные данные: _____

_____

_____

_____

Ответ на настоящий запрос прошу направить в письменной форме по вышеуказанному адресу в предусмотренный законом срок.

С уважением, _____ «____» _____ 20___ года

Форма запроса субъекта персональных данных с отзывом согласия на обработку ПДн

В БУ «Советский комплексный центр социального обслуживания населения».

от _____

адрес:_____

_____

паспорт №_____ выдан _____

_____

_____

ЗАПРОС

Я *состою/не состою* в договорных (трудовых) отношениях с БУ «Советский комплексный центр социального обслуживания населения». и со мной заключен договор № _____ от «___» _____ 20___г.

В соответствии со статьей 20 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и в связи с _____ прошу прекратить обработку следующих моих персональных данных: _____

_____

_____

Ответ на настоящий запрос прошу направить в письменной форме по вышеуказанному адресу в предусмотренный законом срок.

С уважением, _____

«____» _____ 20___ года

Приложение 15 к приказу
БУ «Советский комплексный
центр социального
обслуживания населения»
от «06» сентября 2023 г. № 167

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных

1. Общие положения

1.1. Ответственный за организацию обработки персональных данных в БУ «Советский комплексный центр социального обслуживания населения». назначается приказом директора и отвечает за организацию обеспечения своевременного и квалифицированного выполнения сотрудниками БУ «Советский комплексный центр социального обслуживания населения». требований по организации обработки и обеспечения безопасности персональных данных (далее - ПДн).

1.2. Ответственный за организацию обработки персональных данных (далее - Ответственный) в своей деятельности руководствуется:

- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119;
- Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15.09.2008 № 687;
- Приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Иными нормативными правовыми актами, регламентирующими вопросы обработки и защиты персональных данных;
- Политикой в отношении обработки персональных данных;
- Настоящей Инструкцией.

2. Основные функции и обязанности ответственного за организацию обработки персональных данных

2.1 Функции Ответственного:

2.2.1. Доведение до сведения допущенных к обработке ПДн сотрудников положений законодательства о персональных данных,

локальных актов по вопросам обработки и защиты персональных данных.

2.2.2. Общий контроль за соблюдением сотрудниками законодательства о персональных данных и мер по защите персональных данных.

2.2.3. Осуществление контроля за выполнением разовых и периодических мероприятий по обеспечению безопасности персональных данных.

2.2.4. Взаимодействие с субъектами персональных данных по вопросам обработки и защиты персональных данных.

2.2.5. Взаимодействие с органами, контролирующими обработку и защиту персональных данных, при проведении проверок.

2.2.6. Поддержание локальных организационно-распорядительных документов по организации обработки и обеспечению безопасности персональных данных в актуальном состоянии.

2.2 Ответственный обязан:

2.2.1. Знать:

− перечень ПДн, обрабатываемых в БУ «Советский комплексный центр социального обслуживания населения».

− перечень ИСПДн в БУ «Советский комплексный центр социального обслуживания населения»;

− перечень должностей в БУ «Советский комплексный центр социального обслуживания населения», доступ которых к ПДн, в том числе обрабатываемым в ИСПДн, необходим для выполнения ими должностных (трудовых) обязанностей;

− условия и технологический процесс обработки ПДн в БУ «Советский комплексный центр социального обслуживания населения»;

− законодательство Российской Федерации по вопросам обработки и защиты ПДн.

2.2.2. Представлять по требованию директора БУ «Советский комплексный центр социального обслуживания населения». Отчет о состоянии защиты ИСПДн и о нештатных ситуациях на объектах ИСПДн и допущенных сотрудниками нарушениях установленных требований по защите информации.

2.2.3. Следить за изменениями законодательства Российской Федерации о ПДн, своевременно и точно отражать изменения в локальных организационных актах по вопросам обработки и защиты ПДн.

2.2.4. Осуществлять внутренний контроль за соблюдением БУ «Советский комплексный центр социального обслуживания населения» и его сотрудниками законодательства Российской Федерации о персональных данных, в том числе требований к защите ПДн, а также локальных документов, регламентирующих порядок работы с программными, техническими средствами ИСПДн и ПДн, машинными носителями ПДн.

2.2.5. Доводить до сведения сотрудников БУ «Советский комплексный центр социального обслуживания населения» положения

законодательства Российской Федерации о ПДн, локальных актов по вопросам обеспечения и защиты обработки ПДн, требований к защите ПДн путем проведения занятий и инструктажа сотрудников с периодичностью один раз в год.

2.2.6. Организовать прием и обработку обращений и запросов субъектов персональных данных или их представителей и осуществлять контроль за приемом и обработкой таких обращений и запросов.

2.2.7. По запросу субъекта персональных данных сообщать ему сведения об обработке его персональных данных, в том числе ознакомить с Политикой обработки персональных данных в БУ «Советский комплексный центр социального обслуживания населения».

2.2.8. По запросу субъекта персональных данных организовать уточнение, блокирование или уничтожение персональных данных указанного субъекта.

2.2.9. Вести журнал учета обращений субъектов персональных данных по вопросам обработки персональных данных.

2.2.10. Осуществлять контроль передачи персональных данных по запросам третьих лиц/организаций.

2.2.11. Осуществлять контроль за сбором с сотрудников, допущенных к обработке ПДн, письменного обязательства о соблюдении режима конфиденциальности персональных данных и соблюдении правил их обработки (обязательство о неразглашении информации, содержащей ПДн).

2.2.12. Участвовать в определении полномочий пользователей ИСПДн (оформлении разрешительной системы доступа), минимально необходимых им для выполнения должностных (трудовых) обязанностей.

2.2.13. Осуществлять контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИСПДн с периодичностью один раз в три месяца в соответствии с Инструкцией по идентификации и аутентификации пользователей. А также контролировать наличие документов, подтверждающих разрешение изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей с периодичностью раз в полгода.

2.2.14. Осуществлять сопровождение и решение вопросов проверочной комиссии надзорных органов в сфере обработки ПДн при проведении проверочных мероприятий.

2.2.15. Принимать меры по реагированию в случае возникновения нештатных и аварийных ситуаций с целью ликвидации их последствий.

2.2.16. Вносить свои предложения по совершенствованию мер защиты ПДн в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищённости ПДн вследствие неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления,

распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

2.2.17. Проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей ПДн, нарушения правил работы с документами, содержащими ПДн, или по другим нарушениям, которые могут привести к снижению уровня защищенности ПДн.

3. Права ответственного за организацию обработки персональных данных

3.1. Ответственный имеет право:

3.1.1. Иметь доступ к информации, касающейся обработки персональных данных в БУ «Советский комплексный центр социального обслуживания населения» и включающей:

- цели обработки ПДн;
- категории обрабатываемых ПДн;
- категории субъектов, ПДн которых обрабатываются;
- правовые основания обработки ПДн;
- перечень действий с ПДн, общее описание используемых в БУ «Советский комплексный центр социального обслуживания населения». способов обработки ПДн;
- дату начала обработки ПДн;
- срок или условия прекращения обработки ПДн;
- сведения о наличии или об отсутствии трансграничной передачи ПДн в процессе их обработки;
- сведения об обеспечении безопасности ПДн в соответствии с требованиями к защите ПДн, установленными Правительством Российской Федерации.

3.1.2. Требовать от сотрудников выполнения федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативных правовых актов, а также локальных нормативно-правовых актов в части работы с ПДн.

3.2.2. Требовать от сотрудников БУ «Советский комплексный центр социального обслуживания населения» письменных объяснений при нарушении требований по обработке и обеспечении безопасности ПДн.

3.2.3. Не допускать сотрудников до обработки персональных данных до подписания ими письменного обязательства о неразглашении информации, содержащей персональные данные.

3.2.4. Указывать сотрудникам, допущенным к обработке ПДн, на необходимость выполнения установленных мер по обеспечению безопасности персональных данных.

3.2.5. Указывать сотрудникам, участвующим в обработке персональных данных, на необходимость осуществления уточнения, блокирования или уничтожения персональных данных по запросу субъекта.

3.2.6. Право доступа ко всем локальным нормативным актам в области обработки и защиты персональных данных.

3.2.7. Блокировать доступ к ПДн любых пользователей, если это необходимо для предотвращения нарушения режима защиты ПДн.

3.2.8. Запрашивать и получать от всех сотрудников сведения, справочные и другие материалы, необходимые для осуществления деятельности Ответственного.

3.2.10. Проводить служебные расследования и опрашивать пользователей по фактам несоблюдения условий хранения носителей ПДн, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости ПДн.

3.2.11. Привлекать к реализации мер, направленных на выполнение требований законодательства о ПДн, иных сотрудников БУ «Советский комплексный центр социального обслуживания населения» с возложением на них соответствующих обязанностей и закреплением ответственности.

3.2.12. Проходить обучение по защите ПДн в учебных центрах и центрах повышения квалификации.

3.2.13. Выносить на рассмотрение руководства предложения по совершенствованию работы, связанной с обеспечением безопасности персональных данных.

4. Ответственность

4.1. Ответственный за организацию обработки персональных данных несет ответственность за:

4.1.1. Соблюдение требований настоящей Инструкции, за качество проводимых ими работ по обработке и обеспечению безопасности ПДн.

4.1.2. Осведомленность сотрудников, участвующих в обработке персональных данных, в вопросах обеспечения безопасности ПДн.

4.1.3. Комплектность и содержание локальных нормативных актов в области защиты ПДн.

4.1.4. Выполнение обязанностей перед субъектами ПДн и уполномоченным органом по защите прав субъектов персональных данных.

4.2. За неисполнение (ненадлежащее исполнение) своих должностных обязанностей, предусмотренных настоящей инструкцией, ответственный за организацию обработки персональных данных несет персональную ответственность в соответствии с законодательством Российской Федерации.

Приложение 16 к приказу
БУ «Советский комплексный
центр социального
обслуживания населения»
от «06» сентября 2023 г. № 167

ИНСТРУКЦИЯ
ответственного за обеспечение
безопасности персональных данных в информационных системах
персональных данных

1. Общие положения

1.1. Настоящая инструкция определяет основные обязанности, права и ответственность ответственного за обеспечение безопасности персональных данных (далее – администратор информационной безопасности) в информационных системах персональных данных (далее - ИСПДн).

1.2. Администратор информационной безопасности ИСПДн назначается приказом директора БУ «Советский комплексный центр социального обслуживания населения» и отвечает за обеспечение безопасности заданных характеристик информации (конфиденциальность, целостность и доступность), содержащей персональные данные, в процессе их обработки в ИСПДн БУ «Советский комплексный центр социального обслуживания населения»..

1.3. В своей деятельности администратор информационной безопасности руководствуется:

- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119;
- Приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказом ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения

установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

- Иными нормативными правовыми актами, регламентирующими вопросы обработки и защиты персональных данных;
- Политикой в отношении обработки персональных данных;
- Настоящей Инструкцией.

1.4. Методическое руководство и контроль работы администратора информационной безопасности ИСПДн осуществляет ответственный за организацию обработки персональных данных в ИСПДн.

1.5. Администратор информационной безопасности ИСПДн осуществляет контроль за выполнением требований нормативно-правовых и организационно-распорядительных документов по организации обработки и обеспечению безопасности персональных данных при их обработке в ИСПДн.

2. Основные функции и обязанности ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных

2.1. Основными функциями администратора информационной безопасности ИСПДн являются:

2.1.1. Обеспечение заданных характеристик информации, содержащей персональные данные, (конфиденциальности, целостности и доступности) в процессе их обработки в ИСПДн.

2.1.2. Обеспечение выполнения и контроль за выполнением требований нормативно-правовых и организационно-распорядительных документов по организации обработки и обеспечению безопасности персональных данных при их обработке в ИСПДн.

2.1.3. Администрирование системы защиты информации в составе следующих подсистем:

- идентификации и аутентификации субъектов доступа и объектов доступа (ИАФ);
- управления доступом пользователей ИСПДн к объектам доступа ИСПДн (УПД);
- ограничения программной среды (ОПС);
- защиты машинных носителей персональных данных (ЗНИ);
- регистрации событий безопасности (РСБ);
- антивирусной защиты (АВЗ);
- контроля (анализа) защищенности персональных данных (АНЗ);
- обеспечения целостности информационных систем персональных данных и персональных данных (ОЦЛ);
- защиты информационных систем персональных данных, ее средств и систем связи и передачи данных (ЗИС);
- управления конфигурацией информационной системы и системы защиты персональных данных (УКФ).

2.2. Администратор информационной безопасности ИСПДн обязан:

2.2.1. Знать перечень обрабатываемых персональных данных, состав, структуру, назначение и выполняемые задачи ИСПДн, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку ПДн.

2.2.2. Знать эксплуатационную документацию на применяемые средства защиты информации (далее - СрЗИ), устанавливать и эксплуатировать СрЗИ в соответствии с документацией и поддерживать настройку СрЗИ, соответствующие требованиям нормативных документов по безопасности информации и техническому проекту на ИСПДн. При этом система должна реализовывать в совокупности на каждом автоматизированном рабочем месте ИСПДн функции, необходимые для выполнения требований по защите от несанкционированного доступа (далее - НСД).

2.2.3. Исполнять и требовать исполнения от пользователей ИСПДн установленного комплекса мероприятий по обеспечению безопасности информации и соблюдения действующего законодательства в области информационной безопасности, в том числе иных организационно-распорядительных документов в части обеспечения безопасности информации.

2.2.4. Проводить инструктаж пользователей ИСПДн по правилам обработки ПДн, правилам работы с используемыми техническими средствами и СрЗИ в соответствии с технической документацией на используемые СрЗИ.

2.2.5. Фиксировать и пресекать невыполнение пользователями ИСПДн требований и норм нормативно-методических документов в области безопасности информации и организационно-распорядительных документов БУ «Советский комплексный центр социального обслуживания населения», а также создания пользователями возможностей утечки информации. В случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации требовать прекращения обработки ПДн.

2.2.6. Проверять соответствие прав доступа пользователей к объектам доступа ИСПДн в соответствии с задачами, решаемыми пользователями в ИСПДн, Разрешительной системой доступа к ИСПДн.

2.2.7. Администратор информационной безопасности ИСПДн оказывает методическую помощь и контролирует выполнение ответственным за эксплуатацию ИСПДн следующих действий:

− при смене пользователя ответственный за эксплуатацию ИСПДн инициирует внесение изменений в список сотрудников, допущенных к работе на данной ИСПДн, и в разрешительную систему доступа;

− при исключении пользователя ИСПДн из «Перечня должностей в БУ «Советский комплексный центр социального обслуживания населения», доступ которых к ПДн, в том числе обрабатываемым в ИСПДн, необходим

для выполнения ими должностных (трудовых) обязанностей» ответственным за эксплуатацию ИСПДн принимаются меры по исключению возможности нарушения данным пользователем характеристик безопасности информации ИСПДн.

Администратору информационной безопасности ИСПДн необходимо до момента доведения до сотрудника информации о прекращении его работы в ИСПДн лишить сотрудника возможности доступа к защищаемой информации.

2.2.8. Поддерживать в актуальном состоянии Разрешительную систему доступа и Технический паспорт на ИСПДн.

2.2.9. Участвовать при проведении внутреннего контроля соответствия обработки ПДн установленным требованиям.

2.2.10. Обеспечивать строгое выполнение требований по обеспечению защиты информации при организации технического обслуживания технических средств ИСПДн и отправке их в ремонт, в том числе разрешать проведение работ по обслуживанию технических средств ИСПДн и отправке их в ремонт в присутствии или в сопровождении администратора информационной безопасности ИСПДн.

2.2.11. Проводить ежегодный анализ изменения угроз безопасности информации в ИСПДн, возникающих в ходе ее эксплуатации, и принимать меры защиты информации в случае возникновения новых угроз безопасности информации.

2.2.12. Осуществлять учет средств защиты информации в Журнале учета средств защиты информации (форма журнала приведена в приложении 7 к настоящему Приказу).

2.2.13. Осуществлять ежемесячное тестирование средств защиты информации с отражением результатов в Журнале периодического тестирования средств защиты информации (форма журнала приведена в Приложении 7 к настоящему Приказу).

2.2.14. Присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию АРМ.

2.2.15. Осуществлять администрирование подсистемы идентификации и аутентификации субъектов доступа и объектов доступа:

− осуществлять создание, присвоение и уничтожение идентификаторов внутренних пользователей и устройств;

− исключать повторное использование идентификатора пользователя в течение одного года;

− осуществлять блокирование идентификатора пользователя через период времени неиспользования более 90 дней;

− осуществлять хранение, выдачу, инициализацию, блокирование средств аутентификации (паролей) и принимать меры в случае утраты и (или) компрометации средств аутентификации;

− при администрировании подсистемы идентификации и аутентификации субъектов доступа и объектов доступа руководствоваться

Инструкцией по идентификации и аутентификации пользователей информационных систем персональных данных.

2.2.16. Осуществлять администрирование подсистемы управления доступом субъектов доступа к объектам доступа:

− определять типы учетных записей (внутреннего пользователя, системная, приложения; иные типы записей);

− проверять должностные (функциональные) обязанности пользователя, при заведении учетной записи, на соответствие заявке;

− проверять соответствие прав доступа пользователей к объектам доступа ИСПДн в соответствии с задачами, решаемыми пользователями в ИСПДн и взаимодействующими с ней ИС и Разрешительной системой доступа к ИСПДн;

− осуществлять заведение, активирование, объединение учетных записей в группы (при необходимости), блокирование и уничтожение учетных записей пользователей;

− осуществлять периодический (один раз в месяц) пересмотр и, при необходимости, корректировку учетных записей пользователей (проверять отсутствие в ИСПДн учетных записей уволенных (отстраненных) сотрудников, своевременность удаления временных учетных записей, предоставленных для однократного (ограниченного по времени) выполнения задач в ИСПДн);

− устанавливать права доступа пользователей к информационным и техническим ресурсам ИСПДн в соответствии с принятой и утвержденной Разрешительной системой доступа;

− назначать права и привилегии пользователям, администраторам и лицам, обеспечивающим функционирование ИСПДн, минимально необходимых для выполнения ими своих должностных обязанностей (функций), и осуществление контроля доступа к объектам доступа в соответствии с минимально необходимыми правами;

− осуществлять контроль в части неизменности настроек СрЗИ, которые должны выполнять:

- препятствие передаче ПДн через сеть Интернет и (или) другие информационно-телекоммуникационные сети международного информационного обмена по незащищенным каналам связи;
- ограничение доступа к ИСПДн на 15 минут при 5 неудачных попытках входа в ИСПДн;
- запрет доступа к ИСПДн до прохождения процедур аутентификации и идентификации;
- обеспечение запрета удаленного доступа к ИСПДн по незащищенным каналам связи.

2.2.17. Осуществлять администрирование подсистемы ограничения программной среды:

− проверять перечень программного обеспечения (далее - ПО) в ИСПДн на предмет соответствия его перечню ПО, определенному в

Техническом паспорте на ИСПДн и разрешенному к установке в ИСПДн с периодичностью один раз в месяц;

− осуществлять исключение (восстановление) из состава ИСПДн несанкционированно установленного (удаленного) ПО.

2.2.18. Осуществлять администрирование подсистемы защиты машинных носителей персональных данных:

− осуществлять учет машинных носителей ПДн, используемых в ИСПДн для хранения и обработки информации в журнале (формы журналов учета машинных носителей представлены в Приложении 7 к настоящему Приказу);

− осуществлять выдачу и (или) прием машинных носителей ПДн должностным лицам, доступ которых к машинным носителям персональных данных необходим для выполнения ими должностных (трудовых) обязанностей с внесением соответствующей отметки в журнал;

− осуществлять контроль в части уничтожения (стирания) ПДн с машинных носителей ПДн при их передаче в сторонние организации для ремонта или утилизации.

2.2.19. Осуществлять администрирование подсистемы регистрации событий:

− путем просмотра журналов операционной системы и средств защиты информации осуществлять еженедельный контроль регистрации событий безопасности, которые приведены в Инструкции по регистрации событий безопасности;

− осуществлять настройку СрЗИ (состав событий безопасности и срок их хранения), руководствуясь Инструкцией по регистрации событий безопасности;

− в случае выявления признаков инцидентов информационной безопасности в ИСПДн осуществить планирование и проведение мероприятий по реагированию на выявленные инциденты, согласно Инструкции по работе с инцидентами информационной безопасности.

2.2.20. Осуществлять администрирование подсистемы антивирусной защиты:

– осуществлять еженедельные полные проверки АРМ на наличие вредоносных компьютерных программ (вирусов) средством антивирусной защиты, руководствуясь эксплуатационной документацией на данное СрЗИ;

– осуществлять настройку средства антивирусной защиты на ежедневную автоматическую проверку на наличие вредоносных компьютерных программ (вирусов) в вечернее время и производить проверку результатов сканирования;

– в случае обнаружения не поддающегося лечению вируса, принять меры по удалению инфицированного файла и, в случае необходимости, провести мероприятия по восстановлению работоспособности ПО руководствуясь Инструкцией по организации резервирования и восстановления программного обеспечения и баз ПДн в ИСПДн;

– осуществлять еженедельный контроль над процессом обновления антивирусных баз;

– при администрировании подсистемы антивирусной защиты руководствоваться Инструкцией по организации антивирусной защиты в информационных системах персональных данных.

2.2.21. Осуществлять администрирование подсистемы контроля (анализа) защищенности информации:

− с помощью средства анализа (контроля) защищенности (сканеров безопасности) осуществлять периодический (один раз в три месяца или при опубликовании в общедоступных источниках информации о новых уязвимостях в СрЗИ, технических средствах и ПО, применяемом в ИСПДн) поиск уязвимостей в ИСПДн;

− осуществлять анализ отчета с описанием выявленных уязвимостей, разрабатывать план мероприятий по их устранению;

− осуществлять устранение выявленных уязвимостей с помощью установки обновления ПО СрЗИ, общесистемного ПО, прикладного ПО или настройки СрЗИ, изменения режима и порядка использования ИСПДн;

− осуществлять информирование ответственного за организацию обработки ПДн о выявленных уязвимостях и результатах их устранения;

− контролировать работоспособность параметров настройки и правильность функционирования ПО и СрЗИ с периодичностью один раз в неделю, путем осуществления:

- контроля работоспособности (неотключения) ПО и СрЗИ;
- проверки правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) ПО и СрЗИ;
- контроля соответствия настроек ПО и СрЗИ параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и СрЗИ;
- восстановления работоспособности (правильности функционирования) и параметров настройки ПО и СрЗИ (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов.

− хранить документацию и дистрибутивы СрЗИ в соответствии с техническими условиями (компакт-диск с программным обеспечением системы должен упаковываться согласно требованиям, предусмотренным для оптических носителей), производить, при необходимости, восстановление программной среды СрЗИ или настройки защитных механизмов операционной системы и привилегий пользователей по доступу к ресурсам ИСПДн;

− производить инвентаризацию технических средств, ПО и СрЗИ, применяемых в ИСПДн, не реже одного раза в шесть месяцев:

- осуществлять контроль соответствия состава технических средств, приведенного в техническом паспорте на ИСПДн, с

целью поддержания актуальной конфигурации ИСПДн и принятие мер, направленных на устранение выявленных недостатков;
- осуществлять исключение (восстановление) из состава ИСПДн несанкционированно установленных (удаленных) технических средств;
- осуществлять контроль установленного (инсталлированного) в ИСПДн программного обеспечения на предмет его соответствия перечню программного обеспечения, определенному в техническом паспорте на ИСПДн;
- осуществлять исключение (восстановление) из состава ИСПДн несанкционированно установленного (удаленного) ПО;
- осуществлять контроль соответствия состава СрЗИ, приведенных в техническом паспорте на ИСПДн, с целью поддержания актуальной конфигурации ИСПДн и принятие мер, направленных на устранение выявленных недостатков;
- осуществлять исключение (восстановление) из состава ИСПДн несанкционированно установленных (удаленных) СрЗИ.

− осуществлять учет изменений аппаратно-программной конфигурации (архив заявок, на основании которых были произведены данные изменения) в Техническом паспорте на ИСПДн;

− осуществлять контроль выполнения условий и сроков действия лицензий и сертификатов соответствия на СрЗИ и принятие мер, направленных на устранение выявленных недостатков;

− при установке обновлений ПО, включая ПО СрЗИ и ПО базовой системы ввода-вывода руководствоваться эксплуатационной документацией. После установки обновлений убедиться в работоспособности и правильности функционирования технических средств и СрЗИ, добавить отметки в формуляр;

− осуществлять еженедельный контроль за установкой обновлений ПО, включая ПО СрЗИ и ПО базовой системы ввода-вывода.

2.2.22. Осуществлять администрирование подсистемы обеспечения целостности ИСПДн и ПДн:

− осуществлять восстановление общесистемного и прикладного программного обеспечения, а также программного обеспечения средств защиты информации при возникновении нештатных ситуаций:
- восстановление общесистемного программного обеспечения из резервных копий (дистрибутивов);
- восстановление прикладного программного обеспечения из резервных копий (дистрибутивов);

- восстановление программного обеспечения средств защиты информации из резервных копий (дистрибутивов) программного обеспечения;
- возврат ИСПДн в начальное состояние (до возникновения нештатной ситуации), обеспечивающее ее штатное функционирование, или восстановление отдельных функциональных возможностей ИСПДн, определенных оператором, позволяющих решать задачи по обработке информации;
- восстановление и проверка работоспособности системы защиты информации, обеспечивающие необходимый уровень защищенности информации.

2.2.23. Осуществлять администрирование подсистемы защиты ИСПДн, ее средств и систем связи и передачи данных:

− вести поэкземплярный учет в журнале всех СКЗИ (форма журнала приведена в приложении 7 к настоящему приказу), эксплуатационной и технической документации на СКЗИ;

− проводить ежегодный инструктаж пользователей ИСПДн по правилам работы с используемыми техническими средствами и СКЗИ в соответствии с технической документацией на используемые СКЗИ;

− осуществлять администрирование СКЗИ в соответствии с эксплуатационной документацией на данные средства;

− осуществлять периодический контроль (не реже 1 раза в месяц) сохранности и работоспособности установленных СКЗИ, а также всего используемого совместно с СКЗИ программного обеспечения для предотвращения внесения программно-аппаратных закладок и вирусов;

− осуществлять контроль в части запрета использования в ИСПДн технологий беспроводного доступа и мобильных технических средств;

− осуществлять контроль в части отсутствия доступа к ИСПДн со стороны пользователей ИС сторонних организаций;

− осуществлять контроль в части обеспечения запрета удаленного доступа к ИСПДн.

2.2.24. Осуществлять администрирование подсистемы управления конфигурацией информационной системы и системы защиты персональных данных:

− поддерживать базовую конфигурацию системы защиты информации в соответствии с эксплуатационной документацией на систему защиту информации, определять типы возможных изменений конфигурации системы защиты информации, анализировать потенциальное воздействие планируемых изменений на обеспечение защиты информации, на возникновение дополнительных угроз безопасности информации и работоспособность ИСПДн;

− вносить изменения (при необходимости) в Технический паспорт на ИСПДн и Разрешительную систему доступа пользователей к сведениям конфиденциального характера в ИСПДн;

− принимать решения по результатам изменений о повторной аттестации ИСПДн или проведении дополнительных аттестационных испытаний;

− документировать информацию (данные) об изменениях в конфигурации ИСПДн и системы защиты персональных данных в Журнале учета выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн.

2.3. Администратору информационной безопасности ИСПДн запрещается:

− фиксировать учетные данные пользователя (пароли, идентификаторы, ключи и др.) на твердых носителях, а также сообщать их кому бы то ни было, кроме самого пользователя;

− раскрывать информацию об организации системы защиты ПДн в ***У*** БУ «Советский комплексный центр социального обслуживания населения» и любую информацию, которая может создать предпосылки для возникновения канала утечки информации или создания угрозы безопасности информации.

3. Основные права ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных

3.1. Администратор информационной безопасности имеет право:

− знакомиться с нормативными актами БУ «Советский комплексный центр социального обслуживания населения», регламентирующими процессы обработки ПДн;

− вносить предложения своему непосредственному начальнику и (или) директору БУ «Советский комплексный центр социального обслуживания населения» по совершенствованию существующей системы защиты информации;

− привлекать по согласованию с ответственным за организацию обработки ПДн и директором БУ «Советский комплексный центр социального обслуживания населения» к работе по созданию и совершенствованию системы защиты информации организации, имеющие лицензию ФСТЭК России на право осуществления деятельности по технической защите конфиденциальной информации и лицензию ФСБ России на право осуществления деятельности по предоставлению услуг в области шифрования информации, разработке, производству шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем, распространению шифровальных (криптографических) средств, техническому обслуживанию шифровальных (криптографических) средств. осуществления деятельности по разработке, производству, распространению шифровальных (криптографических) средств;

− требовать от пользователей ИСПДн соблюдения установленной технологии обработки информации, выполнения нормативно-методических документов в области безопасности информации и организационно-распорядительных документов в БУ «Советский комплексный центр социального обслуживания населения»;

− инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения безопасности ПДн;

− требовать прекращения работы в ИСПДн, как в целом, так и отдельных пользователей ИСПДн, в случае выявления нарушений требований по обеспечению безопасности ПДн или в связи с нарушением функционирования ИСПДн;

− обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности ПДн к ответственному за организацию обработки ПДн и/или ответственному за эксплуатацию ИСПДн;

− принимать участие в планировании мероприятий по защите информации в ИСПДн и планировании оснащения средствами защиты информации структурных подразделений.

4. Ответственность ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных

4.1. На администратора информационной безопасности возлагается персональная ответственность за качество проводимых им работ по обеспечению безопасности ПДн в ИСПДн.

4.2. Администратор информационной безопасности в ИСПДн несет ответственность за разглашение сведений ограниченного распространения, ставших известными ему по роду деятельности, в соответствии с действующим законодательством Российской Федерации.

Приложение 17 к приказу
БУ «Советский комплексный
центр социального
обслуживания населения»
от «06» сентября 2023 г. № 167

ИНСТРУКЦИЯ
ответственного за эксплуатацию информационной системы персональных данных

1. Общие положения

1.1. Настоящая инструкция определяет основные функции, обязанности, права и ответственность ответственного за эксплуатацию информационной системы персональных данных (далее - ИСПДн) БУ «Советский комплексный центр социального обслуживания населения» по вопросам защиты персональных данных (далее - ПДн) в ИСПДн.

1.2. Ответственный за эксплуатацию ИСПДн БУ «Советский комплексный центр социального обслуживания населения» назначается приказом директора.

1.3. Ответственный за эксплуатацию ИСПДн осуществляет контроль за соблюдением порядка работы пользователей ИСПДн, на которых проводится обработка ПДн, дополнительно к своим непосредственным обязанностям.

1.4. Ответственный за эксплуатацию ИСПДн непосредственно подчиняется ответственному за организацию обработки ПДн в БУ «Советский комплексный центр социального обслуживания населения».в части, касающейся защиты ПДн в ИСПДн БУ «Советский комплексный центр социального обслуживания населения», и осуществляет контроль за выполнением требований организационно-распорядительных документов по обеспечению безопасности ПДн при их обработке в ИСПДн БУ «Советский комплексный центр социального обслуживания населения».

2. Основные функции ответственного за эксплуатацию информационной системы персональных данных

2.1. Функции ответственного за эксплуатацию ИСПДн:

2.1.1. Осуществление ежедневного контроля над целевым использованием ИСПДн, всех периферийных устройств и технических средств, входящих в состав ИСПДн.

2.1.2. Ежедневный контроль над отсутствием в период обработки защищаемой информации в помещении, где осуществляется обработка, посторонних лиц, не допущенных к обрабатываемой информации.

2.2. Обязанности ответственного за эксплуатацию ИСПДн:

2.2.1. Знать:

− перечень ПДн, обрабатываемых в ИСПДн БУ «Советский комплексный центр социального обслуживания населения»;

− перечень и состав ИСПДн БУ «Советский комплексный центр социального обслуживания населения»;

− перечень должностей сотрудников БУ «Советский комплексный центр социального обслуживания населения», доступ которых к ПДн, в том числе обрабатываемым в ИСПДн, необходим для выполнения ими должностных (трудовых) обязанностей;

− условия и технологический процесс обработки ПДн в ИСПДн.

2.2.2. Знать и выполнять требования действующих нормативных и руководящих документов, а также локальных нормативных актов, регламентирующих порядок действий по защите ПДн.

2.2.3. Осуществлять внутренний контроль за соблюдением сотрудниками ИСПДн требований законодательства Российской Федерации в области ПДн.

2.2.4. Обеспечивать контроль соблюдения сотрудниками локальных документов, регламентирующих порядок работы с программными, техническими средствами ИСПДн и ПДн, машинными носителями ПДн.

2.2.5. Осуществлять контроль за выполнением сотрудниками ИСПДн мероприятий по защите ПДн в ИСПДн.

2.2.6. Осуществлять контроль за хранением документов, содержащих ПДн, и отсутствием несанкционированного доступа к данным документам, их уничтожение по достижению целей обработки либо контроль процедуры их уничтожения.

2.2.7. Участвовать в определении полномочий пользователей ИСПДн (оформлении разрешительной системы доступа), минимально необходимых для выполнения должностных (трудовых) обязанностей.

2.2.8. При появлении новой должности или исключении существующей должности из списка должностей в ИСПДн, которым необходим доступ к ПДн, своевременно предоставить данные ответственному за организацию обработки ПДн для внесения изменений в перечень должностей в БУ «Советский комплексный центр социального обслуживания населения», доступ которых к ПДн, в том числе обрабатываемым в ИСПДн, необходим для выполнения ими должностных (трудовых) обязанностей.

2.2.9. Обеспечивать функционирование ИСПДн в пределах возложенных на него функций.

2.2.10. Своевременно реагировать на попытки несанкционированного доступа к ПДн.

2.2.11. Немедленно сообщить ответственному за организацию обработки ПДн в части, касающейся защиты ПДн, об обнаруженных фактах (попытках) несанкционированного доступа к ПДн и автоматизированным рабочим местам (далее - АРМ), и принимать необходимее меры по пресечению нарушений.

2.2.12. Немедленно прекращать работы на АРМ при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности ПДн.

2.2.13. Блокировать доступ к ПДн при обнаружении нарушений порядка их обработки.

2.2.14. Осуществлять взаимодействие по обеспечению безопасности ПДн с администратором информационной безопасности ИСПДн и ответственным за организацию обработки ПДн.

2.2.15. Вносить свои предложения по совершенствованию мер защиты ПДн в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищённости ПДн вследствие неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

3. Права ответственного за эксплуатацию информационной системы персональных данных

3.1. Ответственный за эксплуатацию ИСПДн имеет право требовать от сотрудников ИСПДн выполнения федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативных правовых актов, а также локальных нормативно-правовых актов в части работы с ПДн.

3.2. Ответственный за эксплуатацию ИСПДн имеет право требовать от пользователей ИСПДн соблюдения установленных технологий обработки информации в соответствии с документом «Описание технологического процесса обработки персональных данных в информационной системе персональных данных» и выполнения инструкций по обеспечению безопасности ПДн в ИСПДн.

3.3. Ответственный за эксплуатацию ИСПДн имеет право инициировать проведение служебных расследований по фактам нарушения требований защиты ПДн, утвержденных соответствующими инструкциями, несанкционированного доступа, утраты, порчи защищаемых ПДн и технических компонентов ИСПДн.

3.3. Ответственный за эксплуатацию ИСПДн имеет право давать свои предложения по совершенствованию организационных и технических мер защиты ПДн.

3.4. Блокировать доступ к ПДн любых пользователей, если это необходимо для предотвращения нарушения режима защиты ПДн.

3.5. Проводить служебные расследования и опрашивать пользователей по фактам несоблюдения условий хранения носителей ПДн, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости

ПДн.

3.6. Иметь доступ к информации, касающейся обработки ПДн в соответствующей ИСПДн и включающей:

- цели обработки ПДн;
- категории обрабатываемых ПДн;
- категории субъектов, ПДн которых обрабатываются;
- правовые основания обработки ПДн;
- перечень действий с ПДн, общее описание используемых в БУ «Советский комплексный центр социального обслуживания населения» способов обработки ПДн;
- дату начала обработки ПДн;
- срок или условия прекращения обработки ПДн;
- сведения о наличии или об отсутствии трансграничной передачи ПДн в процессе их обработки;
- сведения об обеспечении безопасности ПДн в соответствии с требованиями к защите ПДн, установленными Правительством Российской Федерации.

4. Ответственность ответственного за эксплуатацию информационной системы персональных данных

4.1. Ответственный за эксплуатацию ИСПДн несет ответственность за свои действия и действия сотрудников вверенной ИСПДн в соответствии с действующим законодательством РФ.

4.2. На ответственного за эксплуатацию ИСПДн возлагается персональная ответственность за качество проводимых им работ в ИСПДн.

4.3. Ответственный за эксплуатацию ИСПДн несет ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение 18 к приказу
БУ «Советский комплексный
центр социального
обслуживания населения»
от «06» сентября 2023 г. № 167

ИНСТРУКЦИЯ
по организации резервного копирования и восстановления программного обеспечения и баз персональных данных в информационных системах персональных данных

1. Общие положения

1.1. Настоящая инструкция разработана с целью обеспечения возможности оперативного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

1.2. Инструкция определяет правила и объемы резервирования, а также порядок восстановления работоспособности информационных систем персональных данных (далее – ИСПДн).

2. Резервируемое программное обеспечение и базы персональных данных

2.1. В ИСПДн резервированию подлежит:

− общее программное обеспечение (операционная система и программные драйверы устройств (принтера, монитора, видеокарты и т.п.), поставляемые с компонентами автоматизированных рабочих мест (далее – АРМ), входящими в состав ИСПДн);

− прикладное программное обеспечение, используемое для обработки персональных данных (далее - ПДн) (средства обработки текстов и таблиц, специализированные программы и т.п.);

− базы ПДн (текстовые и табличные файлы, а также файлы баз данных специализированных программ);

− программное обеспечение средств защиты информации, в том числе средств антивирусной защиты.

3. Порядок резервирования и хранения резервных копий

3.1. Резервирование общего и прикладного программного обеспечения, программного обеспечения средств защиты информации осуществляется путем создания и хранения резервных копий (дистрибутивов) общего и прикладного программного обеспечения, программного обеспечения средств защиты.

3.2. Резервирование должно осуществляться ежемесячно (полное резервирование информации – резервное копирование всей информации, хранящейся в ИСПДн), еженедельно (неполное резервирование информации – резервное копирование части информации, хранящейся в ИСПДн) Для снижения совокупной нагрузки на информационную систему персональных данных все операции по резервированию информации должны проводиться в ночное время. Резервные копии должны записываться на съемный носитель информации.

3.3. Машинные носители, содержащие обновления общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации, должны храниться у ответственного за обеспечение безопасности ПД в ИСПДн (далее - администратор информационной безопасности ИСПДн).

3.4. Резервные носители ПДн должны храниться в серверной; лицом, ответственным за сохранность резервного носителя ПДн, является администратор информационной безопасности ИСПДн.

3.5. К резервному носителю ПДн может быть приложена учетная карточка, в которой делаются отметки о дате резервирования.

3.6. Копирование информации с резервных носителей ПДн, за исключением случая восстановления работоспособности ИСПДн, запрещается.

4. Порядок восстановления персональных данных из резервных копий и работоспособности информационных систем персональных данных

4.1. Восстановление персональных данных из резервных копий и работоспособности ИСПДн осуществляется в случаях сбоев, отказов и аварий технических средств и систем ИСПДн, а также ее программного обеспечения, администратором информационной безопасности ИСПДн.

4.2. Администратор информационной безопасности ИСПДн обязан срочно уведомить ответственного за организацию обработки персональных данных о факте сбоя в работе ИСПДн, повлёкшего нарушение целостности ПДн.

4.3. Данные работы осуществляются администратором информационной безопасности ИСПДн в соответствии с эксплуатационной документацией на программное обеспечение до полного восстановления работоспособности.

4.4. В случае необходимости привлечения для восстановления работоспособности ИСПДн представителей сторонних организаций, должна быть обеспечена невозможность их ознакомления с ПДн. Ответственность за выполнение данного требования возлагается на администратора информационной безопасности ИСПДн и ответственного за эксплуатацию ИСПДн.

Учетная карточка резервного носителя персональных данных
№ _____

Дата резервного копирования	Объект копирования	Кто производил копирование	Подпись

Приложение 19 к приказу
БУ «Советский комплексный
центр социального
обслуживания населения»
от «06» сентября 2023 г. № 167

ИНСТРУКЦИЯ
по идентификации и аутентификации пользователей информационных систем персональных данных

1. Общие положения

1.1. Настоящая инструкция определяет в БУ «Советский комплексный центр социального обслуживания населения». порядок действий ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных (далее - администратора информационной безопасности ИСПДн) и пользователей информационных систем персональных данных (далее - ИСПДн) при прохождении идентификации и аутентификации пользователями в ИСПДн.

1.2. Настоящая Инструкция разработана на основе следующих нормативных документов:

− Федеральный закон от 27.07.2006 № 149–ФЗ «Об информации, информационных технологиях и защите информации».

− Федеральный закон от 27.07.2006 № 152–ФЗ «О персональных данных».

− Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах 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».

1.3. Пользователи ИСПДн должны быть предупреждены об ответственности за действия с персональными идентификаторами и паролями доступа, нарушающие требования настоящей Инструкции.

1.4. Пользователи ИСПДн должны быть ознакомлены с настоящей Инструкцией до начала работы с ИСПДн под роспись. Обязанность ознакомления пользователей с настоящей инструкцией лежит на ответственном за организацию обработки ПДн.

1.5. Ответственным за создание, присвоение и уничтожение идентификаторов пользователей и устройств, хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в

случае утраты и (или) компрометации средств аутентификации является администратор информационной безопасности ИСПДн.

2. Порядок идентификации и аутентификации внутренних пользователей

2.1. К внутренним пользователям относятся сотрудники БУ «Советский комплексный центр социального обслуживания населения»., допущенные в установленном порядке к работе в ИСПДн, а также должностные лица обладателя информации, заказчика, уполномоченного лица и (или) оператора иной информационной системы, а также лица, привлекаемые на договорной основе для обеспечения функционирования ИСПДн (ремонт, гарантийное обслуживание, регламентные и иные работы) в соответствии с организационно-распорядительными документами БУ «Советский комплексный центр социального обслуживания населения».

2.2. Порядок создания учетной записи пользователя, в том числе привилегированной учетной записи администратора (далее - учетная запись):

2.2.1. В БУ «Советский комплексный центр социального обслуживания населения». применяются следующие типы учетных записей:

- внутренний пользователь;
- системная, приложения;
- временная.

2.2.2. Для создания учетной записи ответственный за эксплуатацию ИСПДн инициирует заявку администратору информационной безопасности ИСПДн о создании учетной записи пользователя, в том числе временной (в виде персональных идентификаторов (логины, имена пользователей). Типовая форма заявки представлена в приложении 1 к настоящей инструкции.

2.2.3. Временная учетная запись заводится для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования ИСПДн, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям с временным доступом к ИСПДн).

2.2.4. Администратор информационной безопасности ИСПДн проверяет права доступа сотрудника к информационным ресурсам, определяет принадлежность к группе и незамедлительно, но в срок не более двух рабочих дней с момента подачи заявки, создает новую учетную запись, с указанными в заявке параметрами.

2.2.5. Создание учетной записи администратором информационной безопасности ИСПДн происходит на контроллере домена: создается логин и генерируется пароль. Созданная учетная запись впоследствии передается пользователю на бумажном носителе, который в дальнейшем уничтожается.

2.2.6. После первой успешной авторизации доменная политика обязывает пользователя сменить выданный ему первичный пароль, согласно

требованиям к сложности пароля, указанными в настоящей Инструкции (п. 2.6.).

2.3. Порядок блокирования учетной записи пользователя:

2.2. Персональные идентификаторы должны быть заблокированы администратором информационной безопасности ИСПДн при превышении времени неиспользования более 90 дней. Учётная запись пользователя должна быть заблокирована администратором информационной безопасности ИСПДн после получения служебной записки об увольнении сотрудника и по окончанию последнего сеанса его работы. Уволенный сотрудник должен быть исключен из числа пользователей ИСПДн.

2.3.4. Разблокировка учетной записи пользователя происходит по устному или письменному обращению ответственного за эксплуатацию ИСПДн.

2.4. Порядок удаления учетной записи пользователя:

2.4.1. Ответственный за эксплуатацию ИСПДн инициирует заявку администратору информационной безопасности ИСПДн об удалении учетной записи увольняющегося пользователя.

2.4.2. Администратор информационной безопасности ИСПДн удаляет учетную запись пользователя ИСПДн при увольнении немедленно по окончании последнего сеанса работы сотрудника, а уволенный сотрудник исключается из числа пользователей ИСПДн. Удаление временных учетных записей производятся, если:

− задача, требующая расширенного полномочия, для которого создавалась временная учетная запись, выполнена;

− произведена настройка и тестирование ИСПДн;

− по достижению даты, которая указывалась в заявке при создании временной учетной записи для организации гостевого доступа.

2.4.3. После удаления учетной записи пользователя администратор информационной безопасности ИСПДн делает отметку об удалении учетной записи в заявке на создание учетной записи.

2.5. Порядок хранения исполненных заявок:

2.5.1. Исполненные заявки подлежат хранению у администратора информационной безопасности ИСПДн, которые могут впоследствии использоваться:

− для восстановления полномочий пользователей после аварий в ИСПДн;

− для контроля правомерности наличия у конкретного пользователя прав доступа к информационному ресурсу;

− тем или иным ресурсам системы при разборе конфликтных ситуаций;

− для проверки правильности настройки средств разграничения доступа к ресурсам ИСПДн.

2.6. Требования к сложности пароля:

− длина пароля должна быть не менее 6 символов;

− алфавит пароля не менее 70 символов (буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

− символы пароля должны вводиться в режиме латинской раскладки клавиатуры;

− пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

− при смене пароля новое значение должно отличаться от предыдущего не менее, чем на 4 символа;

− при создании новых паролей пользователям запрещается использовать 3 последних использованных паролей;

− пароль действует не более 90 дней, по истечении которых пользователь обязан заменить его новым.

2.6. Администратор информационной безопасности ИСПДн осуществляет настройку в ИСПДн параметров количества вводов неправильного пароля. Максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки технического средства или учетной записи пользователя устанавливается равным 5-и попыткам. Время блокировки программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации устанавливается равным 15-и минутам. По истечении установленного времени блокировки пользователь может продолжить процедуру аутентификации.

2.3. Администратор информационной безопасности ИСПДн производит настройку в ИСПДн параметров блокирования сеанса доступа по запросу пользователя.

2.4. Администратором информационной безопасности ИСПДн должно быть исключено повторное использование идентификатора пользователя в течение не менее одного года.

2.5. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение и другие обстоятельства) администратора информационной безопасности ИСПДн.

2.6. Администратору информационной безопасности ИСПДн разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования ИСПДн в случае сбоев в работе или выходе из строя отдельных технических средств (устройств). Пользователям запрещены любые действия в ИСПДн до процедуры идентификации и аутентификации.

3. Действия администратора информационной безопасности ИСПДн при компрометации паролей

3.1. Заблокировать доступ пользователя скомпрометированного пароля к ИСПДн.

3.2. Выявить действия, произведённые в ИСПДн с использованием скомпрометированных персональных идентификаторов и паролей доступа.

3.3. Доложить ответственному за организацию обработки ПДн об инциденте и предоставить результаты анализа инцидента.

3.4. Совместно с ответственным за организацию обработки ПДн определить необходимость расследования инцидента.

3.5. Создать и выдать пользователю новый персональный идентификатор и пароль доступа к ИСПДн.

Приложение 1

Администратору
информационной безопасности
ИСПДн
_____
_____
(должность, ФИО)

от ответственного за
эксплуатацию ИСПДн
_____
_____
(должность, ФИО)

Заявка

Прошу Вас _____
(содержание запрашиваемых изменений)

_____
(должность с указанием отдела, Ф.И.О. сотрудника)

на основании приказа от «___» _____ 20__ г. № ____.

Указанному сотруднику для выполнения должностных обязанностей необходим доступ к следующим ресурсам (нужное отметить):

_____

_____

_____

«____» _____ 20___г.

_____ _____ _____
(должность) (подпись) (расшифровка)

_____ _____ _____
(должность) (подпись) (расшифровка)

Учетная запись создана «____» _____ 20___ г.

Учетная запись удалена «____» _____ 20___ г.

Приложение 20 к приказу
БУ «Советский комплексный
центр социального
обслуживания населения»
от «06» сентября 2023 г. № 167

ИНСТРУКЦИЯ
по организации антивирусной защиты в информационных системах персональных данных

1. Общие требования

1.1. Настоящая инструкция определяет требования к организации антивирусной защиты информационных систем персональных данных (далее – ИСПДн) от разрушающего воздействия вирусов и вредоносных программ и устанавливает ответственность руководства и сотрудников структурных подразделений, эксплуатирующих и сопровождающих ИСПДн, за их выполнение. Инструкция распространяется на все существующие и вновь разрабатываемые ИСПДн.

1.2. К использованию в ИСПДн допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

1.3. Установка и настройка средств антивирусного контроля осуществляется ответственным за обеспечение безопасности персональных данных (далее - ПДн) в ИСПДн (далее - администратор информационной безопасности ИСПДн).

2. Применение средств антивирусного контроля

2.1. При загрузке автоматизированного рабочего места (далее – АРМ) в автоматическом режиме должен проводиться антивирусный контроль служб операционной системы, исполняемых приложений, находящихся в автозагрузке, реестра операционной системы.

2.2. Быстрой и полной антивирусной проверке АРМ и сервера подвергаются один раз в неделю.

2.3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по информационно-телекоммуникационным сетям, а также информация на съемных носителях (магнитных дисках, оптических и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо

проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

2.4. Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

2.5. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов и других вредоносных программ. Непосредственно после установки (изменения) программного обеспечения, администратором информационной безопасности ИСПДн должна быть выполнена антивирусная проверка на защищаемых серверах и пользовательских АРМ.

3. Порядок обновления антивирусных баз

3.1. Обновление антивирусных баз на АРМ, подключенных к локальной сети, осуществляется ежедневно в автоматическом режиме через сервер обновлений.

3.2. Контроль обновления антивирусных баз на АРМ, подключенных к локальной сети, осуществляется администратором информационной безопасности ИСПДн еженедельно. В случае возникновения ошибок при автоматическом обновлении средств антивирусной защиты (появлении диалоговых окон, сообщений об ошибке) необходимо принимать соответствующие меры, обновлять базу вручную в случае необходимости.

4. Действия при обнаружении вирусов

4.1. При возникновении подозрения на наличие вируса либо вредоносной программы (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник БУ «Советский комплексный центр социального обслуживания населения» самостоятельно или вместе с администратором информационной безопасности ИСПДн должен провести внеочередной антивирусный контроль своего АРМ.

4.2. В случае обнаружения при проведении антивирусной проверки зараженных вирусами либо вредоносными программами файлов, необходимо:

- приостановить работу в ИСПДн;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за организацию обработки персональных данных и смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

5. Ответственность

5.1. Ответственность за организацию антивирусной защиты возлагается на администратора информационной безопасности ИСПДн, который один раз в месяц осуществляет контроль за состоянием антивирусной защиты, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками БУ «Советский комплексный центр социального обслуживания населения».

5.2. Ответственность за проведение мероприятий антивирусного контроля в отделах и соблюдение требований настоящей Инструкции возлагается на всех сотрудников, являющихся пользователями ИСПДн.

Приложение 21 к приказу
БУ «Советский комплексный
центр социального
обслуживания населения»
от «06» сентября 2023 г. № 167

ИНСТРУКЦИЯ
по регистрации событий безопасности

1. Общие положения

1.1. Настоящая инструкция разработана в соответствии с п. 8.5 приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.2. Событие безопасности (информационной) – это идентифицированное возникновение состояния информационной системы персональных данных (далее - ИСПДн) (сегмента, компонента информационной системы персональных данных), сервиса или сети, указывающее на возможное нарушение безопасности информации, или сбой средств защиты информации, или ранее неизвестную ситуацию, которая может быть значимой для безопасности информации.

1.3. Отслеживание событий (проверку), происходивших на автоматизированных рабочих местах (далее - АРМ), осуществляет ответственный за обеспечение безопасности персональных данных (далее - ПДн) в информационных системах персональных данных (далее - администратор информационной безопасности ИСПДн).

1.4. Общими задачами проверки являются:

- контролирование состояния защищенности системы;
- выявление причин произошедших изменений;
- определение лиц или процессов, деятельность которых привела к изменению состояния защищенности системы или к НСД;
- установление времени изменений.

2. Определение событий безопасности, подлежащих регистрации, их состава, содержания и сроков хранения

2.1. События, происходящие на АРМ, входящих в состав ИСПДн, регистрируются в журналах, приведенных в п. 3.1. настоящей инструкции.

2.2. Каждому событию соответствует отдельная запись в журнале, содержащая подробную информацию для анализа события.

2.3. В ИСПДн как минимум подлежат регистрации следующие события:

− вход (выход), а также попытки входа субъектов доступа в ИСПДн и загрузки (останова) операционной системы;

− подключение машинных носителей информации и вывод информации на носители информации;

− запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации;

− попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;

− попытки удаленного доступа.

2.4. При регистрации входа (выхода) субъектов доступа в ИСПДн и загрузки (останова) операционной системы состав и содержание информации, как минимум, включают дату и время входа (выхода) в систему (из системы) или загрузки (останова) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.

2.5. При регистрации подключения машинных носителей информации и вывода информации на носители информации состав и содержание регистрационных записей, как минимум, включают дату и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации.

2.6. При регистрации запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации состав и содержание регистрационных записей, как минимум, включают дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).

2.7. При регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам состав и содержание регистрационных записей, как минимум, включают дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип).

2.8. При регистрации попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей) состав и содержание информации, как минимум, включают дату и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта

доступа (устройства), спецификацию защищаемого объекта доступа (логическое имя (номер).

2.9. При регистрации попыток удаленного доступа к ИСПДн состав и содержание информации, как минимум, включают дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе.

2.10. Срок хранения событий безопасности составляет 3 месяца для оперативного доступа, 12 месяцев - архивного хранения.

2.11. События безопасности подлежат защите, реализуемой организационным и техническими мерами, и соответствующим настройкам системы защиты информации на ограничение доступа пользователей к параметрам настройки средств защиты информации.

3. Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них

3.1. События безопасности регистрируются в:

- штатных журналах операционной системы Windows;
- журналах событий средств защиты информации.

3.2. Администратор информационной безопасности ИСПДн производит проверку электронных журналов не реже одного раза в неделю с внесением соответствующей информации в «Журнале учета проверок электронных журналов обращений к информационным системам персональных данных».

3.3. В случае сбоя при регистрации событий безопасности осуществляется предупреждение (сигнализация, индикация) администратора информационной безопасности ИСПДн о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности.

3.4. При обнаружении сбоя при регистрации событий безопасности администратор информационной безопасности ИСПДн обязан реагировать путем изменения параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов ИСПДн, запись поверх устаревших хранимых записей событий безопасности.

3.5. Администратор информационной безопасности ИСПДн совместно с ответственным за организацию обработки ПДн принимают решение об определении события информационной безопасности к относящимся или не относящимся к инцидентам информационной безопасности. Инциденты информационной безопасности могут быть преднамеренными или случайными (например, являться следствием какой-либо человеческой ошибки или природных явлений) и вызваны как техническими, так и нетехническими средствами. Их последствиями могут

быть такие события, как несанкционированные раскрытие или изменение ПДн, ее уничтожение или другие события, которые делают ее недоступной, а также нанесение ущерба активам БУ «Советский комплексный центр социального обслуживания населения» или их хищение.

3.6. В случае обнаружения инцидента информационной безопасности администратор информационной безопасности ИСПДн руководствуется Инструкцией по работе с инцидентами информационной безопасности.

Приложение 22 к приказу
БУ «Советский комплексный
центр социального
обслуживания населения»
от «06» сентября 2023 г. № 167

ИНСТРУКЦИЯ
о пропускном и внутриобъектовом режимах

1. Общие положения

1.1. Данная Инструкция регламентирует условия и порядок осуществления пропускного и внутриобъектового режимов в БУ «Советский комплексный центр социального обслуживания населения», в целях обеспечения предотвращения несанкционированного доступа к персональным данным (далее – ПДн).

1.2. Обеспечение доступа лиц на территорию БУ «Советский комплексный центр социального обслуживания населения» предусматривает комплекс специальных мер, направленных на поддержание и обеспечение установленного порядка деятельности подразделений и определяет порядок пропуска сотрудников БУ «Советский комплексный центр социального обслуживания населения», сотрудников иных организаций и учреждений и граждан.

1.3. Пропускной режим устанавливается в целях:

− исключения фактов хищений собственности БУ «Советский комплексный центр социального обслуживания населения»;

− исключение фактов вандализма со стороны недобросовестных посетителей;

− исключения возможности несанкционированного доступа персонала и посетителей в помещения БУ «Советский комплексный центр социального обслуживания населения».

1.4. Внутриобъектовый режим устанавливается в целях:

− соблюдения сотрудниками и посетителями правил внутреннего распорядка и пожарной безопасности;

− установления порядка допуска сотрудников в помещения ограниченного доступа БУ «Советский комплексный центр социального обслуживания населения»;

− исключения возможности бесконтрольного передвижения посетителей по территории БУ «Советский комплексный центр социального обслуживания населения».

1.5. Ответственным за организацию пропускного и внутриобъектового режимов в БУ «Советский комплексный центр социального обслуживания населения» является заместитель директора БУ «Советский комплексный центр социального обслуживания населения».

1.6. Ответственным за соблюдение правил внутреннего трудового распорядка, установленного режима функционирования, порядка содержания служебных помещений и мер противопожарной безопасности на объекте является ответственный за организацию обработки ПДн.

1.7. Ответственным за реализацию организационно-технических мероприятий, связанных с осуществлением пропускного и внутриобъектового режимов в БУ «Советский комплексный центр социального обслуживания населения» является администратор информационной безопасности ИСПДн.

2. На территории БУ «Советский комплексный центр социального обслуживания населения» запрещено

2.1. На территории БУ «Советский комплексный центр социального обслуживания населения» запрещается:

- проводить без разрешения руководства фото-, кино-, видеосъемки, в том числе с использованием мобильных телефонов;
- пользоваться неисправными или самодельными электронагревательными и другими электробытовыми приборами;
- загромождать территорию, основные и запасные входы (выходы), лестничные площадки материалами и предметами, которые создают помехи для системы видеонаблюдения, затрудняют эвакуацию людей, материальных ценностей, препятствуют ликвидации очагов возгорания;
- совершать действия, нарушающие установленные режимы функционирования технических средств охраны и пожарной сигнализации;
- заниматься торговой деятельностью.
- вносить химические, взрывчатые и легковоспламеняющиеся вещества и иные предметы и средства, наличие либо применение (использования) которых может представлять угрозу для безопасности окружающих;
- вносить боеприпасы, оружие всех видов и патроны к нему (кроме лиц, которым законодательством Российской Федерации разрешено ношение, хранение и применение оружия для исполнения возложенных на них обязанностей);
- иметь при себе крупногабаритные предметы, в том числе хозяйственные сумки, рюкзаки, вещевые мешки, чемоданы (за исключением папок, портфелей, кейсов для документов).

3. Порядок входа на территорию БУ «Советский комплексный центр социального обслуживания населения».

3.1. Для обеспечения пропускного режима на территорию устанавливаются следующие виды документов:

Заявка на вход на территорию для работы в выходные (праздничные) дни (приложение 1);

Заявка на внос (вынос) материальных ценностей на (с) территорию (ии) (приложение 2).

3.2. Вход на территорию для сотрудников разрешается с 8:00 до 21:00 в рабочие дни, в субботу с 8:00 до 21:00, воскресенье выходной.

3.3. Вход на территорию посетителей разрешается с 8:00 до 20:00 в рабочие дни, в субботу с 8:00 до 20:00, в предпраздничные дни на один час короче.

3.4. Вход на территорию разрешается круглосуточно в рабочие, выходные и праздничные дни:

— Директору;
— Заместителям директора;
— Главному бухгалтеру.
— Начальникам отделов.

3.5.Вход на территорию для работы в выходные (праздничные) дни осуществляется на основании заявки сотрудника, которая согласовывается с ответственным за реализацию организационно-технических мероприятий. При выполнении строительно-ремонтных работ на территории в заявке обязательно указывается фамилия, имя и отчество, должность, рабочий телефон ответственного должностного лица, который будет присутствовать при проведении этих работ и осуществлять контроль над их проведением, в соответствии с законом от 17.12.1994 № 67-ФЗ «О федеральной фельдъегерской связи» без оформления заявки.

Приложение 1

Директору БУ «Советский
комплексный центр
социального обслуживания
населения».
_____

З А Я В К А

на вход на территорию БУ «Советский комплексный центр социального обслуживания населения» **в выходные (праздничные) дни**

Прошу Вашего разрешения пропустить меня на территорию БУ «Советский комплексный центр социального обслуживания населения» для работы в выходные (праздничные) дни в связи с _____

_____
(Обоснование необходимости выполнения работы или наименование мероприятия)

с ___ часов ___ минут «___» _____ 20 __ г. до ___ часов ___ минут «___» _____ 20 __ г.

Должность_____

И.О. Фамилия_____

Подпись_____

« ___ » _____ 20 __ г.

Приложение 2

Директору БУ «Советский
комплексный центр
социального обслуживания
населения»
_____

З А Я В К А

на внос (вынос) материальных ценностей на (с) территорию (ии)

БУ «Советский комплексный центр социального обслуживания населения»

Прошу разрешить _____
(полное наименование организации, должность, фамилия, имя, отчество)

внос (вынос) «___» _____ 20 __ г.
в связи _____
(указать цель вноса (выноса)

следующих материальных ценностей:

1._____
(наименование материальных ценностей, серийный номер изделия (если таковой имеется) или инвентарный номер)

_____

Всего в заявку внесено _____ (_____) наименований.

Должность_____
И.О. Фамилия_____
Подпись_____

« ___ » _____ 20 __ г.

Отметка сотрудника

«___»_____ 20__г. в __ час. ___мин. внос (вынос), ввоз (вывоз) осуществлен

_____ _____
(подпись) (расшифровка подписи)

Приложение 23 к приказу
БУ «Советский комплексный
центр социального
обслуживания населения»
от «06» сентября 2023 г. № 167

ИНСТРУКЦИЯ
по обработке персональных данных без использования средств автоматизации

1. Общие положения

1.1. Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому гражданину, обратившемуся в БУ «Советский комплексный центр социального обслуживания населения», или сотруднику (далее – субъекту персональных данных) БУ «Советский комплексный центр социального обслуживания населения».

1.2. Обработка персональных данных, содержащихся в информационных системах персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

1.3. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационных системах персональных данных либо были извлечены из нее.

1.4. Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установленные настоящим Положением, должны применяться с учетом требований Постановления Правительства Российской Федерации «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15 сентября 2008 г. № 687, а также требований нормативных правовых актов федеральных органов исполнительной власти.

2. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации

2.1. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной

информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее – материальные носители), в специальных разделах или на полях форм (бланков).

2.2. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

2.3. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники БУ «Советский комплексный центр социального обслуживания населения» или лица, осуществляющие такую обработку по договору с БУ «Советский комплексный центр социального обслуживания населения».), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется БУ «Советский комплексный центр социального обслуживания населения». без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти, а также локальными правовыми актами БУ «Советский комплексный центр социального обслуживания населения».

2.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовая форма), должны соблюдаться следующие условия:

− типовая форма или связанные с ней документы должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование и адрес БУ «Советский комплексный центр социального обслуживания населения» фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых БУ «Советский комплексный центр социального обслуживания населения». способов обработки персональных данных;

− типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации,– при необходимости получения письменного согласия на обработку персональных данных;

− типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными,

содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных.

2.5. При ведении журналов (журналов регистрации, журналов посещений), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных в помещения БУ «Советский комплексный центр социального обслуживания населения» или в иных аналогичных целях, должны соблюдаться следующие условия:

− необходимость ведения такого журнала должна быть предусмотрена актом БУ «Советский комплексный центр социального обслуживания населения», содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способах фиксации и составе информации, запрашиваемой у субъектов персональных данных, перечне лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроках обработки персональных данных;

− копирование содержащейся в таких журналах информации не допускается;

− персональные данные каждого субъекта персональных данных могут заноситься в такой журнал не более одного раза в каждом случае пропуска субъекта персональных данных.

2.6. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, зачеркивание, стирание).

2.7. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

3. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

3.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

3.2. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

3.3. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

3.4. Перечень мест хранения материальных носителей ПДн приведен в приложении к настоящей инструкции.

Приложение
к Инструкции по обработке персональных данных
без использования средств автоматизации

ПЕРЕЧЕНЬ МЕСТ ХРАНЕНИЯ,
материальных носителей персональных данных

№ п/п	Тип материального носителя	Ответственное лицо	Расположение хранилища	Тип хранилища	Регистрационный (учетный) номер хранилища
1.					
2.					
3.					
4.					
5.					
6.					

Приложение 24 к приказу
БУ «Советский комплексный
центр социального
обслуживания населения»
от «06» сентября 2023 г. № 167

ИНСТРУКЦИЯ
по работе с инцидентами информационной безопасности

1. Общие положения

1.1. Настоящая инструкция устанавливает порядок действий по управлению инцидентами информационной безопасности (далее - ИБ) в БУ «Советский комплексный центр социального обслуживания населения».

1.2. Ответственность за выявление инцидентов ИБ и реагирование на них в БУ «Советский комплексный центр социального обслуживания населения» возлагается на ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных (далее - ИСПДн) (далее - администратор информационной безопасности ИСПДн).

1.3. В случае обнаружения инцидента ИБ администратор информационной безопасности ИСПДн руководствуется настоящей Инструкцией.

2. Порядок выявления инцидентов информационной безопасности

2.1. Администратор информационной безопасности ИСПДн совместно с ответственным за организацию обработки персональных данных (далее - ПДн) принимают решение об определении события информационной безопасности к относящимся или не относящимся к инцидентам информационной безопасности (далее - ИБ).

2.2. Инциденты информационной безопасности могут быть преднамеренными или случайными (например, являться следствием какой-либо человеческой ошибки или природных явлений) и вызваны как техническими, так и нетехническими средствами. Их последствиями могут быть такие события, как несанкционированные раскрытие или изменение ПДн, ее уничтожение или другие события, которые делают ее недоступной, а также нанесение ущерба активам БУ «Советский комплексный центр социального обслуживания населения» или их хищение.

2.3. Внутренний инцидент – инцидент, источником которого является нарушитель, связанный с пострадавшей стороной непосредственным образом (трудовым договором или иным способом). Среди инцидентов такого типа можно выделить следующие наиболее распространенные:

- утечка ПДн;

- неправомерный доступ к ПДн;
- удаление ПДн;
- компрометация ПДн;
- саботаж;
- мошенничество;
- использование ПДн в личных целях или в мошеннических операциях.

2.4. Внешний инцидент – инцидент, источником которого является нарушитель, не связанный с пострадавшей стороной непосредственным образом. Среди инцидентов такого типа можно выделить следующие наиболее распространенные:

- атаки типа «отказ в обслуживании» (DoS), в том числе распределенные (DDoS);
- перехват и подмена трафика;
- фишинг;
- размещение конфиденциальной/провокационной информации в сети Интернет;
- взлом, попытка взлома, сканирование портала;
- сканирование сети, попытка взлома сетевых узлов;
- вирусные атаки;
- неправомерный доступ к ПДн.

2.5. Данный перечень не является исчерпывающим. В общем случае инцидентом является единичное, нежелательное или неожиданное событие информационной безопасности (или совокупность таких событий), которое угрожает информационной безопасности ИСПДн.

3. Анализ исходной информации и принятие решения о проведении разбирательства инцидента информационной безопасности

3.1. Администратор информационной безопасности ИСПДн совместно с ответственным за организацию обработки ПДн проводят анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценку их последствий. Источниками и причинами возникновения инцидентов в ИСПДн могут являться:

- действия организаций и отдельных лиц враждебные интересам БУ «Советский комплексный центр социального обслуживания населения»;
- отсутствие персональной ответственности сотрудников оператора и их руководителей за обеспечение ИБ, в том числе ПДн;
- недостаточная работа с персоналом по обеспечению необходимого режима соблюдения конфиденциальности, в том числе ПДн;
- отсутствие моральной и материальной стимуляции за соблюдение правил и требований ИБ;
- недостаточная техническая оснащённость подразделений, ответственных за обеспечение ИБ;

− совмещение функций по разработке и сопровождению или сопровождению и контролю за ИСПДн;

− наличие привилегированных бесконтрольных пользователей в ИСПДн;

− пренебрежение правилами и требованиями ИБ сотрудниками БУ «Советский комплексный центр социального обслуживания населения»;

− другие причины.

3.2. По усмотрению директора БУ «Советский комплексный центр социального обслуживания населения» инцидент ИБ, не приведший к негативным последствиям и совершенный впервые, фиксируется администратором информационной безопасности ИСПДн в «Журнале учета выявленных инцидентов информационной безопасности» (приложение 7) с присвоением статуса «Разбирательство не требуется».

3.3. В случае нарушения прав субъекта персональных данных разбирательство инцидента и реагирование на него происходит в порядке и сроки, предусмотренном в документе БУ «Советский комплексный центр социального обслуживания населения». Правила рассмотрения запросов субъектов персональных данных».

3.4. В случае наличия признаков инцидента ИБ в полученной информации, администратор информационной безопасности ИСПДн определяет предварительную степень важности инцидента ИБ и принимает решение о необходимости проведения разбирательства, информирует директора БУ «Советский комплексный центр социального обслуживания населения» об инциденте ИБ, производит запись в «Журнале учета выявленных инцидентов информационной безопасности» с присвоением ему статуса «В процессе разбирательства».

3.5. В срок не более 3 (трех) рабочих дней с момента поступления информации об инциденте ИБ, администратор информационной безопасности ИСПДн, по согласованию с ответственным за организацию обработки ПДн, определяет и инициирует первоочередные меры, направленные на локализацию инцидента ИБ и на минимизацию его последствий.

4. Разбирательство инцидента информационной безопасности

4.1. Цели и этапы разбирательства инцидента ИБ:

4.1.1. Целями разбирательства инцидента ИБ являются:

− выработка организационных и технических решений, направленных на снижение рисков нарушения информационной безопасности, предотвращение и минимизацию подобных нарушений в будущем;

− защита репутации БУ «Советский комплексный центр социального обслуживания населения» и его ресурсов;

− обеспечение безопасности ПДн;

− обеспечение прав субъектов ПДн на обеспечение безопасности и конфиденциальности их ПДн, обрабатываемых БУ «Советский комплексный центр социального обслуживания населения»;

− предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации.

4.1.2. Разбирательство инцидента ИБ, состоит из следующих этапов:

− подтверждение/опровержение факта возникновения инцидента ИБ;

− подтверждение/корректировка уровня значимости инцидента ИБ;

− уточнение дополнительных обстоятельств (деталей) инцидента ИБ;

− получение (сбор) доказательств возникновения инцидента ИБ, обеспечение их сохранности и целостности;

− минимизация последствий инцидента ИБ;

− информирование и консультирование сотрудников БУ «Советский комплексный центр социального обслуживания населения». по действиям обнаружения, устранения последствий и предотвращения инцидентов ИБ;

− разработка мероприятий по обнаружению и/или предупреждению инцидентов ИБ.

4.2. Порядок проведения разбирательства инцидента ИБ:

4.2.1. В процессе проведения разбирательства инцидента ИБ обязательными для установления являются:

− дата и время совершения инцидента ИБ;

− Ф.И.О, должность и подразделение Нарушителя ИБ (для внутреннего инцидента);

− уровень критичности инцидента ИБ;

− обстоятельства и мотивы совершения инцидента ИБ;

− информационные ресурсы, затронутые инцидентом ИБ;

− характер и размер реального и потенциального ущерба;

− обстоятельства, способствовавшие совершению инцидента ИБ.

4.3.1. Администратор информационной безопасности ИСПДн в процессе проведения расследования инцидента ИБ, при необходимости, запрашивает информацию в отделах БУ «Советский комплексный центр социального обслуживания населения». Запрос направляется на имя начальника отдела с обязательным указанием сроков предоставления информации (с учетом необходимости ее анализа, сбора и подготовки).

4.3.2. После получения необходимой информации по инциденту ИБ администратор информационной безопасности ИСПДн проводит анализ полученных данных.

4.3.3. В течение 5 (пяти) рабочих дней администратор информационной безопасности ИСПДн запрашивает у начальника отдела объяснительную записку Нарушителя ИБ. Объяснительная записка должна быть составлена, подписана Нарушителем ИБ в течение 2 (двух) рабочих дней и представлена его непосредственным руководителем администратору информационной безопасности ИСПДн в течение 3 (трех) рабочих дней с момента поступления запроса. В случае отказа Нарушителя ИБ предоставить

объяснительную записку администратору информационной безопасности ИСПДн, составляется акт в соответствии с установленным в БУ «Советский комплексный центр социального обслуживания населения» порядке.

4.2.8. Администратор информационной безопасности ИСПДн проводит оценку негативных последствий от реализации инцидента ИБ. В ходе данной оценки учитываются:

- прямой финансовый ущерб;
- репутационный ущерб;
- потенциальный ущерб;
- косвенные потери, связанные с недоступностью сервисов, потерей информации;
- другие виды ущерба или аспекты негативных последствий для БУ «Советский комплексный центр социального обслуживания населения». или субъектов ПДн.

4.2.9. С целью минимизации последствий инцидента ИБ возможно временное отключение прав доступа Нарушителя ИБ к информационным ресурсам (далее - ИР) на время проведения расследования, предварительно сделав заявку. Подобное отключение инициируется администратором информационной безопасности ИСПДн с обязательным предварительным устным согласованием с руководителем Нарушителя ИБ.

4.2.10. В случае, если у Нарушителя ИБ были отключены права доступа к ИР на время проведения разбирательства, то по его результатам администратор информационной безопасности ИСПДн по согласованию с руководителем Нарушителя ИБ принимает решение и инициирует возвращение в полном или ограниченном объеме ранее имевшихся у Нарушителя ИБ прав доступа к ИР либо инициирует официальную процедуру отмены (изменения) прав доступа к ИР в соответствии с установленным порядком в БУ «Советский комплексный центр социального обслуживания населения». Если нарушение ИБ было вызвано незнанием Нарушителем ИБ правил (технологии) работы с ИР высокого уровня безопасности, то основанием для возврата прав доступа является успешное прохождение повторного инструктажа ответственным за организацию обработки персональных данных, ознакомлением с положениями должностной инструкции, иными локальными нормативными актами БУ «Советский комплексный центр социального обслуживания населения».

4.2.11. Восстановление временно отключенных у Нарушителя ИБ прав доступа к ИР (разблокировка пользователя) может производиться только по заявке руководителя Нарушителя ИБ.

5. Оформление результатов проведенного разбирательства

5.1. Собранная в процессе разбирательства инцидента ИБ информация фиксируется администратором информационной безопасности ИСПДн в «Журнале учета выявленных инцидентов информационной

безопасности» и учитывается при подготовке итогового заключения по инциденту ИБ (Приложение 7).

5.2. Администратор информационной безопасности ИСПДн формирует, согласовывает со всеми участниками разбирательства и подписывает итоговое заключение по расследованию инцидента ИБ.

5.3. Итоговое заключение по инциденту ИБ администратор информационной безопасности ИСПДн направляет директору, начальникам отделов, затронутых инцидентом ИБ, и ответственному за организацию обработки ПДн.

5.4. Администратор информационной безопасности ИСПДн фиксирует завершение разбирательства в «Журнале учета выявленных инцидентов информационной безопасности» и присваивает инциденту статус «Разбирательство завершено».

6. Завершение разбирательства инцидента информационной безопасности

6.1. По завершению разбирательства инцидента ИБ, администратор информационной безопасности ИСПДн передает имеющиеся материалы в объеме, достаточном для принятия решения, ответственному за организацию обработки ПДн для решения вопроса о целесообразности привлечения Нарушителя ИБ к дисциплинарной ответственности.

6.2. На основании полученных результатов разбирательства ответственный за организацию обработки персональных данных в срок не более 3 (трех) рабочих дней организовывает проведение одного или нескольких мероприятий, направленных на снижение рисков ИБ в будущем:

- повторное ознакомление Нарушителя ИБ с правилами по обеспечению безопасности ПДн;
- просмотр и анализ имеющихся прав доступа к ИР у Нарушителя ИБ;
- доведение до всех сотрудников внутренних нормативных документов;
- обсуждение инцидента ИБ на совещании руководителей;
- отмена неактуальных прав доступа к ИР;
- проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- и другие обоснованные мероприятия.

6.3. О результатах проведенного разбирательства инцидента ИБ ответственный за организацию обработки ПДн по необходимости инициирует подготовку сообщения об инциденте ИБ в адрес директора БУ «Советский комплексный центр социального обслуживания населения».

7. Обязанности и права участников разбирательства инцидента информационной безопасности

7.1. Администратор информационной безопасности ИСПДн обязан:

− объективно и основательно проводить разбирательство каждого инцидента ИБ;

− определять первоочередные меры, направленные на локализацию инцидента ИБ и минимизацию негативных последствий;

− фиксировать в «Журнале учета выявленных инцидентов информационной безопасности» всю исходную информацию об инциденте ИБ и результаты его расследования;

− предоставлять отчеты и рекомендации по проведенным разбирательствам ответственному за организацию обработки ПДн и директору БУ «Советский комплексный центр социального обслуживания населения»;

− проводить анализ обстоятельств, способствовавших совершению каждого инцидента ИБ, и на его основе, совместно с ответственным за организацию обработки ПДн, разрабатывать рекомендации и предложения по снижению ущерба от подобных инцидентов ИБ и минимизации возможности их повторения в будущем.

7.2. Администратор информационной безопасности ИСПДн имеет право:

− по согласованию с непосредственным руководителем Нарушителя ИБ требовать предоставлений письменных объяснений по обстоятельствам инцидента ИБ у Нарушителя ИБ;

− запрашивать и получать от руководителей и сотрудников, в рамках их компетенций, устные и письменные разъяснения и иную информацию, необходимую для проведения разбирательства инцидента ИБ;

− инициировать отключение от ИР сотрудников, нарушивших правила или требования ИБ, на период проведений расследования инцидента ИБ, в случае если имеется существенный риск того, что продолжение работы сотрудника с ИР может повлечь значительное увеличение ущерба или новые инциденты ИБ;

− по результатам расследования инцидента ИБ инициировать изменения ИР с целью повышения их защищенности и снижения рисков инцидентов ИБ;

− инициировать процедуры привлечения Нарушителя ИБ к дисциплинарной или материальной ответственности, согласно внутренним нормативным документам БУ «Советский комплексный центр социального обслуживания населения».

7.3. Начальники отделов и сотрудники обязаны:

− предоставлять по запросам администратора информационной безопасности ИСПДн устные и письменные разъяснения и иную информацию в рамках своей компетенции, необходимую для проведения разбирательства инцидента ИБ;

− информировать администратора информационной безопасности ИСПДн о выявленных инцидентах ИБ.

Приложение 25 к приказу
БУ «Советский комплексный
центр социального
обслуживания населения»
от «06» сентября 2023 г. № 167

ИНСТРУКЦИЯ
по обращению со средствами криптографической защиты информации

1. Общие положения

1.1. Настоящая инструкция регламентирует порядок обращения с шифровальными средствами (средствами криптографической защиты информации, СКЗИ), предназначенными для защиты информации, не содержащей сведений, составляющих государственную тайну, в процессе их получения, транспортировки, учета, хранения, уничтожения, встраивания в прикладные системы, тестирования, а также порядок допуска к работам с шифровальными средствами.

1.2. Перечень должностей, допущенных к работе с СКЗИ, приведен в приложении 1 к настоящей инструкции.

1.3. Ответственным за эксплуатацию СКЗИ является ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных (далее - администратор информационной безопасности ИСПДн).

1.4. Работы с СКЗИ должны проводиться с учетом приказа ФСБ от 09.02.2005 г. № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» и приказом ФСБ России от 10 июля 2014 года № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», а также эксплуатационной и технической документации к ним.

2. Ответственные лица

2.1. В БУ «Советский комплексный центр социального обслуживания населения», эксплуатирующей сертифицированные СКЗИ, контроль за обеспечением безопасности при работе с СКЗИ осуществляется администратором информационной безопасности ИСПДн.

2.2. Основные обязанности администратора информационной безопасности ИСПДн:

- обеспечение корректного и безопасного функционирования СКЗИ;
- обеспечение корректной и безопасной эксплуатации СКЗИ;
- ознакомление пользователей с настоящей инструкцией;
- контроль работоспособности и соблюдения правил эксплуатации СКЗИ.

2.3. Основные обязанности пользователей СКЗИ:

- ознакомиться с данной инструкцией под подпись и строго выполнять требования настоящей инструкции в части, их касающейся, а также строго выполнять требования нормативных правовых актов Российской Федерации, относящихся к деятельности с СКЗИ, нормативных и методических документов лицензирующего органа
- соблюдение правил корректной и безопасной эксплуатации СКЗИ;
- обеспечение режима сохранности СКЗИ, ЭТД и ключевых документов, переданных им.

2.4. Администратор информационной безопасности ИСПДн и Пользователи СКЗИ допускаются к работе с СКЗИ только после инструктажа и обучения правилам работы с СКЗИ. Для администратора информационной безопасности ИСПДн инструктаж и обучение проводит Лицензиат. Пользователей инструктирует и обучает администратор информационной безопасности ИСПДн.

3. Требования по размещению, оборудованию и охране помещений

3.1. Размещение, оборудование, охрана и режим в помещениях, в которых проводятся работы с СКЗИ (далее – помещения), должны обеспечивать безопасность СКЗИ, сведение к минимуму возможности неконтролируемого доступа посторонних лиц. Доступ сотрудников в эти помещения должен быть ограничен в соответствии со служебной необходимостью и определяться перечнем должностей, представленном в приложении 1 к настоящему приказу.

3.2. Обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода и оборудование помещений пожарной сигнализацией и соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений.

3.3. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Окна помещений должны быть защищены от НСД посторонних лиц (в случае, если окна на первом этаже, либо рядом с пожарными лестницами) металлическими решетками, а также от визуального просмотра извне окна помещений работ (жалюзи, шторы и т.п.).

4. Порядок обращения с СКЗИ

4.1. Пользователи криптосредств обязаны:

− не разглашать информацию о ключевых документах;

− не допускать вывод ключевых документов на дисплей (монитор) или принтер;

− не допускать установки ключевых документов в другие ПЭВМ.

4.2. Все поступающие СКЗИ, инсталлирующие СКЗИ носители, эксплуатационная и техническая документация (при наличии) к ним должны браться на поэкземплярный учет в «Журнале учета средств криптографической защиты информации». Ведет журналы администратор информационной безопасности ИСПДн.

4.3. Единицей поэкземплярного учета СКЗИ является:

− для аппаратных и программно-аппаратных СКЗИ - конструктивно законченное техническое устройство;

− для программных СКЗИ – инсталлирующий СКЗИ носитель (дискета, компакт-диск (CD-ROM) и т.п.).

4.4.Должны быть приняты организационные меры с целью исключения возможности несанкционированного копирования СКЗИ.

4.5. Хранение съемных машинных носителей должно осуществляется в сейфах (металлических шкафах – при наличии), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками. В случае если на съемном машинном носителе хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне сейфов (металлических шкафов).

4.6. Хранение инсталлирующих СКЗИ носителей допускается в одном хранилище с другими документами при условиях, исключающих непреднамеренное их уничтожение или иное, не предусмотренное правилами пользования СКЗИ применение.

4.7. В случае отсутствия у сотрудника индивидуального хранилища инсталлирующие СКЗИ носители по окончании рабочего дня должны сдаваться администратору информационной безопасности ИСПДн.

4.8. В случае утери носителя СКЗИ или вероятном копировании сотрудник обязан немедленно сообщить об этом администратору информационной безопасности ИСПДн.

4.9. Администратор информационной безопасности ИСПДн должен проводить контроль сохранности и работоспособности установленного СКЗИ, а также всего используемого совместно с СКЗИ программного обеспечения для предотвращения внесения программно-аппаратных закладок и вирусов с периодичностью раз в месяц.

4.10. Используемые СКЗИ должны иметь сертификат соответствия ФСБ и должны быть класса КС1 и выше.

5. Ответственность за нарушение требований Инструкции

5.1. За нарушение требований настоящей Инструкции виновные лица несут дисциплинарную либо материальную ответственность в зависимости от характера нарушения и тяжести наступивших отрицательных последствий.

Приложение 1

Перечень должностей, допущенных к работе с СКЗИ

№ п/п	Должность
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	
11.	
12.	
13.	

Приложение 26 к приказу
БУ «Советский комплексный
центр социального
обслуживания населения»
от «06» сентября 2023 г. № 167

ПРАВИЛА
рассмотрения запросов субъектов персональных данных или их представителей

1. Общие положения

1.1. Настоящие Правила рассмотрения запросов субъектов персональных данных или их представителей (далее - Правила) в БУ «Советский комплексный центр социального обслуживания населения» разработана в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» и определяют сроки и последовательность действий сотрудников БУ «Советский комплексный центр социального обслуживания населения» при рассмотрении запросов субъектов персональных данных или их представителей.

1.2. Представитель субъекта персональных данных – лицо, действующее от имени субъекта персональных данных в силу полномочий, основанных на доверенности, указании закона, либо акте уполномоченного на то государственного органа или органа местного самоуправления. При обращении представителя субъекта персональных данных в БУ «Советский комплексный центр социального обслуживания населения» представляется документ, подтверждающий полномочия законного представителя.

2. Порядок рассмотрения запросов субъектов персональных данных или их представителей или уполномоченного органа по защите прав субъектов персональных данных

2.1.Действия БУ «Советский комплексный центр социального обслуживания населения» при обращении субъекта:

− в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - № 152-ФЗ) при личном устном приеме субъект ПДн предъявляет документ, удостоверяющий его личность;

− в случае, если при личном приеме от имени субъекта ПДн действует его законный представитель, сотрудник БУ «Советский комплексный центр социального обслуживания населения» обязан удостовериться в наличии у такого лица законных полномочий;

− содержание устного обращения регистрируется в «Журнал учета обращений субъектов персональных данных по вопросам обработки персональных данных». Ответ на обращение с согласия субъекта ПДн может быть дан устно в ходе личного приема, а также субъекту ПДн

предоставляется возможность ознакомления с его ПДн, о чем делается запись в «Журнал учета обращений субъектов персональных данных по вопросам обработки персональных данных». При отсутствии возможности ознакомления субъекта с его ПДн немедленно при его личном обращении, такая возможность должна быть предоставлена субъекту ПДн в течение 10 (десяти) рабочих дней с даты обращения;

− в том случае, когда при личном приеме субъект ПДн изъявил желание получить ответ в письменной форме, сотрудник, ведущий прием, предлагает субъекту ПДн БУ «Советский комплексный центр социального обслуживания населения» обязано дать ответ на такой запрос в соответствии с № 152-ФЗ;

− если при рассмотрении обращения субъекта ПДн будет установлено, что предоставление ПДн нарушает права и законные интересы третьих лиц, сотрудник, осуществляющий личный прием субъекта ПДн, сообщает ему об отказе в предоставлении информации о ПДн, о чем делается запись в «Журнал учета обращений субъектов персональных данных по вопросам обработки персональных данных». Также в срок, не превышающий 10 (десяти) рабочих дней со дня обращения субъекта ПДн или его представителя либо с даты получения запроса субъекта ПДн или его представителя, сотрудник направляет в адрес субъекта ПДн мотивированный ответ в письменной форме, содержащий ссылку на положение п. 4 ч. 8 ст. 14 № 152-ФЗ.

2.2. Действия БУ «Советский комплексный центр социального обслуживания населения» при получении запроса субъекта ПДн:

2.2.1. В соответствии с ч. 3 ст. 14 № 152-ФЗ запрос должен содержать:

− сведения о номере основного документа, удостоверяющего личность субъекта персональных данных или его представителя;

− сведения о дате выдачи указанного документа и выдавшем его органе;

− сведения, подтверждающие участие субъекта персональных данных в отношениях с БУ «Советский комплексный центр социального обслуживания населения» (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения) либо сведения, иным образом подтверждающие факт обработки персональных данных БУ «Советский комплексный центр социального обслуживания населения»;

− подпись субъекта персональных данных или его представителя.

2.2.2. Регистрация запросов субъектов ПДн, а также регистрация ответов, направляемых субъектам ПДн, осуществляется в «Журнал учета обращений субъектов персональных данных по вопросам обработки персональных данных».

2.2.3. Сотрудником БУ «Советский комплексный центр социального обслуживания населения», осуществляющим прием обращений субъектов ПДн и регистрацию запросов субъектов ПДн и уполномоченного органа по

защите прав субъектов ПДн (далее - сотрудник), является _____.

2.2.4. Сотрудником БУ «Советский комплексный центр социального обслуживания населения», осуществляющим рассмотрение запросов субъектов ПДн и контроль за подготовкой ответов на них, является ответственный за организацию обработки персональных данных.

2.2.5. При получении запроса субъекта ПДн, сотрудник БУ «Советский комплексный центр социального обслуживания населения» непосредственно в день получения проверяет соответствие запроса требованиям к письменному обращению, установленным ст. 7 Федерального закона «О порядке рассмотрения обращений граждан Российской Федерации» от 02.05.2006 г. № 59-ФЗ (далее - № 59-ФЗ), а именно:

− наименование государственного органа, в который направлено письменное обращение, либо фамилию, имя, отчество соответствующего должностного лица, либо должность соответствующего лица;

− наличие фамилии, имени, отчества (последнее - при наличии) субъекта ПДн;

− наличие почтового адреса, по которому должен быть направлен ответ;

− наличие личной подписи и даты;

− наличие сведений о документе, удостоверяющем личность субъекта ПДн (номер документа, сведения о дате выдачи указанного документа и выдавшем его органе).

2.2.6. В случае соответствия запроса субъекта ПДн требованиям, перечисленным в п. 5.2.5. настоящего Порядка, такой запрос подлежит приему и регистрации в «Журнал учета обращений субъектов персональных данных по вопросам обработки персональных данных».

2.2.7. В случае если в запросе субъекта ПДн не указаны фамилия гражданина, направившего обращение, и почтовый адрес, по которому должен быть направлен ответ, в соответствии с ч. 1 ст. 11 № 59-ФЗ, ответ на такой запрос не дается, о чем делается отметка в «Журнал учета обращений субъектов персональных данных по вопросам обработки персональных данных».

2.2.8. В случае не соответствия запроса субъекта ПДн требованиям, перечисленным в п. 5.2.1. настоящего порядка, такой запрос подлежит приему и регистрации в «Журнал учета обращений субъектов персональных данных по вопросам обработки персональных данных» в тот же день. Также в срок, не превышающий 10 (десяти) рабочих дней со дня обращения субъекта ПДн или его представителя либо с даты получения запроса субъекта ПДн или его представителя, сотрудник направляет в адрес субъекта ПДн мотивированный ответ в письменной форме о том, что сведения не могут быть предоставлены.

2.2.9. Зарегистрированные запросы субъектов ПДн в день регистрации подлежат передаче ответственному за организацию обработки персональных данных.

2.2.10. Ответственный за организацию обработки ПДн обязан рассмотреть запрос субъекта ПДн и поручить подготовку ответа на него в письменной форме ответственному сотруднику БУ «Советский комплексный центр социального обслуживания населения». Ответ на запрос должен быть подготовлен в течение 10 (десяти) рабочих дней со дня обращения субъекта ПДн или его представителя либо с даты получения запроса субъекта ПДн или его представителя. Указанный срок может быть продлен, но не более чем на 5 рабочих дней в случае направления оператором в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

2.2.11. В случае, если в запросе субъект ПДн изъявил желание ознакомиться со своими ПДн, возможность такого ознакомления должна быть предоставлена субъекту ПДн в течение 10 (десяти) рабочих дней со дня обращения субъекта ПДн или его представителя либо с даты получения запроса субъекта ПДн или его представителя. Указанный срок может быть продлен, но не более чем на 5 рабочих дней в случае направления оператором в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

2.2.12. Письменный ответ на запрос субъекта ПДн должен быть направлен по его адресу заказным письмом с уведомлением о вручении с соблюдением сроков, предусмотренных законодательством (приложение 1).

2.2.13. Если при рассмотрении запроса субъекта ПДн будет установлено, что предоставление ПДн нарушает права и законные интересы третьих лиц, БУ «Советский комплексный центр социального обслуживания населения» сообщает ему об отказе в предоставлении информации о ПДн, о чем в срок, не превышающий 7 (семи) рабочих дней со дня получения запроса субъекта ПДн, в адрес субъекта ПДн направляется мотивированный ответ в письменной форме, содержащий ссылку на положение п. 4 ч. 8 ст. 14 № 152-ФЗ.

2.2.14. Для обработки ПДн, содержащихся в обращении в письменной форме субъекта ПДн, дополнительного его согласия не требуется.

2.3. Действия БУ «Советский комплексный центр социального обслуживания населения» при получении запроса субъекта ПДн в электронной форме:

2.3.1. Согласно п. 3 ст. 7 № 59-ФЗ обращение, поступившее в государственный орган в форме электронного документа, подлежит рассмотрению в соответствии с порядком, установленным ст. 10 указанного закона.

2.3.2. В обращении субъект ПДн в обязательном порядке указывает свои фамилию, имя, отчество (последнее - при наличии), адрес электронной

почты, если ответ должен быть направлен в форме электронного документа, и почтовый адрес, если ответ должен быть направлен в письменной форме. Субъект ПДн вправе приложить к такому обращению необходимые документы и материалы в электронной форме либо направить указанные документы и материалы или их копии в письменной форме.

2.3.3. Прием и регистрация запросов субъектов ПДн в электронной форме подлежат регистрации в «Журнал учета обращений субъектов персональных данных по вопросам обработки персональных данных».

2.4. Действия БУ «Советский комплексный центр социального обслуживания населения» при получении запроса уполномоченного органа по защите прав субъектов ПДн:

2.4.1. Прием и регистрация запросов уполномоченного органа по защите прав субъектов подлежат регистрации в «Журнал учета обращений субъектов персональных данных по вопросам обработки персональных данных».

2.4.2. При получении запроса уполномоченного органа по защите прав субъектов ПДн сотрудник БУ «Советский комплексный центр социального обслуживания населения», ответственный за прием и регистрацию входящей корреспонденции, в тот же день осуществляет регистрацию такого запроса и передает его ответственному за организацию обработки персональных данных.

2.4.3. БУ «Советский комплексный центр социального обслуживания населения», в лице ответственного за организацию обработки персональных данных, сообщает в уполномоченный орган по защите прав субъектов ПДн по его запросу информацию, необходимую для осуществления деятельности указанного органа, а также направляет запрошенные им документы в течение 10 (десяти) рабочих дней с даты получения такого запроса. Указанный срок может быть продлен, но не более чем на 5 рабочих дней в случае направления БУ «Советский комплексный центр социального обслуживания населения» в адрес уполномоченного органа по защите прав субъектов ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

2.4.4. В случае выявления уполномоченным органом по защите прав субъектов ПДн фактов недостоверности ПДн или неправомерных действий с ними, уточнение, блокирование или уничтожение таких ПДн осуществляется в порядке и сроки, предусмотренные законодательством (приложение 1) для соответствующих действий (операций) в отношении ПДн.

2.4.5. Формы ответов на запросы субъектов персональных данных или их представителей и уполномоченного органа по защите прав субъектов персональных данных представлены в приложении 2 к настоящим Правилам.

Приложение 1
к Правилам рассмотрения запросов
субъектов персональных данных или
их представителей

Сводная таблица
действий БУ «Советский комплексный центр социального обслуживания населения» в ответ на запросы субъекта персональных данных или его представителя

№ п/п	Запрос	Действия	Срок	Ответ
1. Запрос субъекта персональных данных или его представителя				
1.1.	Наличие персональных данных	Подтверждение обработки персональных данных	10 рабочих дней (согласно п. 1 ст. 20 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – 152-ФЗ)	Подтверждение обработки персональных данных
		Отказ подтверждения обработки персональных данных	10 рабочих дней (согласно п. 2 ст. 20 152-ФЗ)	Уведомление об отказе подтверждения обработки персональных данных
1.2.	Ознакомление с персональными данными	Предоставление информации по персональным данным	10 рабочих дней (согласно п. 1 ст. 20 152-ФЗ)	Подтверждение обработки персональных данных, а также правовые основания и цели такой обработки
				Способы обработки персональных данных
				Сведения о лицах, которые имеют доступ к персональным данным
				Перечень обрабатываемых

				персональных данных и источник их получения
				Сроки обработки персональных данных, в том числе сроки их хранения
				Информация об осуществленной или о предполагаемой трансграничной передаче
				Сведения о лицах, осуществляющих обработку ПДн по поручению оператора, если обработка поручена или будет поручена такому лицу
				Информация о способах исполнения БУ «Советский комплексный центр социального обслуживания населения» обязанностей, установленных статьей 18.1 152-ФЗ
		Отказ предоставления информации по персональным данным	10 рабочих дней (согласно п. 2 ст. 20 152-ФЗ)	Уведомление об отказе предоставления информации по персональным данным
1.3.	Уточнение персональных данных	Изменение персональных данных	7 рабочих дней со дня предоставления уточняющих сведений (согласно п. 3 ст. 20 152-ФЗ)	Уведомление о внесенных изменениях
		Отказ изменения персональных данных	10 рабочих дней	Уведомление об отказе изменений персональных данных
1.4.	Уничтожение персональных данных	Уничтожение персональных данных	7 рабочих дней со дня предоставления сведений, подтверждающих, что такие персональные данные являются незаконно	Уведомление об уничтожении персональных данных

			полученными или не являются необходимыми для заявленной цели обработки (согласно п. 3 ст. 20 152-ФЗ)	
		Отказ уничтожения персональных данных	10 рабочих дней	Уведомление об отказе уничтожения персональных данных
1.5.	Отзыв согласия на обработку персональных данных	Прекращение обработки и уничтожение персональных данных	10 рабочих дней (согласно п. 5.1. ст. 21 152-ФЗ)	Уведомление о прекращении обработки и уничтожении персональных данных
		Отказ прекращения обработки и уничтожения персональных данных	10 рабочих дней	Уведомление об отказе прекращения обработки и уничтожения персональных данных
1.6.	Недостоверность персональных данных Субъекта	Блокирование персональных данных	с момента получения запроса на период проверки (согласно п. 1 ст. 21 152-ФЗ)	Уведомление о внесенных изменениях
		Изменение персональных данных	7 рабочих дней со дня предоставления уточненных сведений (согласно п. 2 ст. 21 152-ФЗ)	
		Снятие блокировки персональных данных		Уведомление об отказе изменения персональных данных
		Отказ изменения персональных данных	10 рабочих дней	
1.7.	Неправомерность действий с персональными данными Субъекта	Прекращение неправомерной обработки персональных данных	3 рабочих дня (согласно п. 3 ст. 21 152-ФЗ)	Уведомление об устранении нарушений
		Уничтожение персональных данных в случае невозможности обеспечения правомерности обработки	10 рабочих дней (согласно п. 3 ст. 21 152-ФЗ)	Уведомление об уничтожении персональных данных
1.8.	Достижение целей обработки персональных	Прекращение обработки персональных данных	30 дней (согласно п. 4 ст. 21 152-ФЗ)	Уведомление об уничтожении персональных данных

	данных Субъекта	Уничтожение персональных данных		
2. Запрос Уполномоченного органа по защите прав субъектов персональных данных				
2.1.	Информация для осуществления деятельности уполномоченного органа	Предоставление затребованной информации по персональным данным	10 рабочих дней (согласно п. 4 ст. 20 152-ФЗ)	Предоставление затребованной информации по персональным данным
2.2.	Неточность персональных данных Субъекта	Блокирование персональных данных	с момента получения запроса на период проверки (согласно п. 1 ст. 21 152-ФЗ)	Уведомление о внесенных изменениях
		Изменение персональных данных	7 рабочих дней со дня предоставления уточненных сведений (согласно п. 2 ст. 21 152-ФЗ)	
		Снятие блокировки персональных данных		Уведомление об отказе изменения персональных данных
		Отказ изменения персональных данных	10 рабочих дней	
2.3.	Неправомерность действий с персональными данными Субъекта	Прекращение неправомерной обработки персональных данных	3 рабочих дня (согласно п. 3 ст. 21 152-ФЗ)	Уведомление об устранении нарушений
		Уничтожение персональных данных в случае невозможности обеспечения правомерности обработки	10 рабочих дней (согласно п. 3 ст. 21 152-ФЗ)	Уведомление об уничтожении персональных данных
2.4.	Достижение целей обработки персональных данных Субъекта	Прекращение обработки персональных данных	30 дней с даты достижения цели обработки персональных данных (согласно п.4 ст. 21 152-ФЗ)	Уведомление об уничтожении персональных данных
		Уничтожение персональных данных		

Приложение 2

Форма ответа на запрос субъекта персональных данных о наличии и ознакомлении с ПДн

Г-ну/Г-ке_____

На Ваш запрос от «___» _____ 20___ г. относительно обработки Ваших персональных данных могу сообщить следующее.

БУ «Советский комплексный центр социального обслуживания населения» в период с «___» _____ 20___ г. по настоящее время с целью _____
_____
обрабатывает в рамках договора № _____ от «___» _____ 20___ г. следующие полученные от Вас персональные данные: _____ _____
_____

Эта информация обрабатывается в соответствии с законодательством РФ о персональных данных, в Ваших интересах и с Вашего согласия. Обработка данных включает хранение, использование и, в случае необходимости, передачу данных третьим лицам. Обработкой Ваших персональных данных занимаются сотрудники БУ «Советский комплексный центр социального обслуживания населения», ознакомленные с обязанностями, возложенными на них в связи с обработкой Ваших персональных данных, и давшие подписку об их неразглашении. Никто другой к обработке Ваших персональных данных не допускается. Ваши персональные данные будут обрабатываться вплоть до достижения указанных целей, но не позже _____ лет с момента Вашего последнего обращения в БУ «Советский комплексный центр социального обслуживания населения» («_____» _____ 20___ г.).

Если у Вас возникнут еще какие-либо вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением, _____ _____ _____
(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г

Г-ну/Г-ке_____

На Ваш запрос от «____» _____ 20____ г. относительно обработки Ваших персональных данных могу сообщить следующее.

БУ «Советский комплексный центр социального обслуживания населения» не осуществляет обработки Ваших персональных данных.

С уважением, _____ _____ _____
(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Форма ответа на запрос субъекта персональных данных на уточнение ПДн

Г-ну/Г-ке_____

На Ваш запрос от «___» _____ 20__ г. относительно уточнения Ваших персональных данных могу сообщить следующее.

БУ «Советский комплексный центр социального обслуживания населения» были внесены изменения в Ваши персональные данные:

_____

_____

Если у Вас возникнут еще какие-либо вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением, _____ М.П. _____ _____

(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Г-ну/Г-ке_____

На Ваш запрос от «__» _____ 20__ г. относительно уточнения Ваших персональных данных могу сообщить следующее.

БУ «Советский комплексный центр социального обслуживания населения» не может внести изменения в Ваши персональные данные, так как Вами не было предоставлено необходимых документов, подтверждающих запрашиваемые Вами изменения.

Если у Вас возникнут еще какие-либо вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением, _____ _____ _____

(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Форма ответа на запрос субъекта персональных данных на уничтожение ПДн

Г-ну/Г-ке_____

На Ваш запрос от «___» _____ 20__ г. относительно уничтожения Ваших персональных данных могу сообщить следующее.

БУ «Советский комплексный центр социального обслуживания населения». были уничтожены Ваши персональные данные: _____

_____

Если у Вас возникнут еще какие-либо вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением, _____ _____ _____
(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Г-ну/Г-ке_____

На Ваш запрос от «___» _____ 20__ г. относительно уничтожения Ваших персональных данных могу сообщить следующее.

БУ «Советский комплексный центр социального обслуживания населения». не может уничтожить Ваши персональные данные, так как их обработка осуществляется согласно _____

_____

Если у Вас возникнут еще какие-либо вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением, _____ _____ _____
(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Форма ответа на запрос субъекта персональных данных с отзывом согласия на обработку ПДн

Г-ну/Г-ке_____

На Ваш запрос от «___» _____ 20__ г. относительно отзыва согласия на обработку Ваших персональных данных могу сообщить следующее.

БУ «Советский комплексный центр социального обслуживания населения» была прекращена обработка и уничтожены Ваши персональные данные: ____

_____

Если у Вас возникнут еще какие-либо вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением, _____ _____ _____
(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Г-ну/Г-ке_____

На Ваш запрос от «___» _____ 20__ г. относительно отзыва согласия на обработку Ваших персональных данных могу сообщить следующее.

БУ «Советский комплексный центр социального обслуживания населения». не может прекратить обработку и уничтожить Ваши персональные данные, так как их обработка осуществляется согласно

_____

_____

Если у Вас возникнут еще какие-либо вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением, _____ _____ _____
(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Форма уведомления субъекта персональных данных, его законного представителя или уполномоченного органа по защите прав субъектов персональных данных при выявлении недостоверности ПД

Г-ну/Г-же_____

В связи с выявлением недостоверности Ваших персональных данных могу сообщить следующее.

БУ «Советский комплексный центр социального обслуживания населения» были внесены изменения в Ваши персональные данные:

_____
_____

Если у Вас есть вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением, _____ _____ _____
(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Законному представителю г-на/г-ки
(Уполномоченному органу по защите прав
субъектов персональных данных)
(выбрать необходимое)

В связи с выявлением недостоверности персональных данных г-на/г-ки _____ могу сообщить следующее.

БУ «Советский комплексный центр социального обслуживания населения» были внесены изменения в персональные данные г- на/г-ки _____:
_____

Если у Вас есть вопросы, связанные с обработкой персональных данных г-на/г-ки _____, пожалуйста, обращайтесь.

С уважением, _____ _____ _____
(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Г-ну/Г-ке_____

На Ваш запрос от «___» _____ 20___ г., относительно обработки Ваших персональных данных могу сообщить следующее.

БУ «Советский комплексный центр социального обслуживания населения» не может внести изменения в Ваши персональные данные, так как факт недостоверности не подтвержден и не были предоставлены необходимые документы, подтверждающие недостоверность ПДн.

Если у Вас есть вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением, _____ _____ _____
(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Законному представителю г-на/г-ки
(Уполномоченному органу по защите прав
субъектов персональных данных)
(выбрать необходимое)

На Ваш запрос от «___» _____ 20___ г., относительно недостоверности обработки персональных данных г-на/г-ки _____ могу сообщить следующее.

БУ «Советский комплексный центр социального обслуживания населения». не может внести изменения в персональные данные г-на/г-ки _____, так как факт недостоверности не подтвержден и не были предоставлены необходимые документы, подтверждающие недостоверность ПДн.

Если у Вас есть вопросы, связанные с обработкой персональных данных г-на/г-ки _____, пожалуйста, обращайтесь.

С уважением, _____ _____ _____
(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Формы уведомления субъекта персональных данных, его законного представителя или уполномоченного органа по защите прав субъектов персональных данных при выявлении неправомерности действий с ПДн

Г-ну/Г-ке___

В связи с выявлением неправомерности действий с Вашими персональными данными могу сообщить следующее.

БУ «Советский комплексный центр социального обслуживания населения». были уничтожены Ваши персональные данные:

_____

_____

Если у Вас есть вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением, _____ _____ _____
(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Законному представителю г-на/г-ки
(Уполномоченному органу по защите прав
субъектов персональных данных)
(выбрать необходимое)

В связи с выявлением неправомерности действий с персональных данными г-на/г-ки _____ могу сообщить следующее.

БУ «Советский комплексный центр социального обслуживания населения». были уничтожены персональные данные г-на/г-ки _____:

_____

Если у Вас есть вопросы, связанные с обработкой персональных данных г-на/г-ки _____, пожалуйста, обращайтесь.

С уважением, _____ _____ _____
(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Г-ну/Г-ке_____

На Ваш запрос от «____» _____ 20___ г., относительно неправомерности обработки Ваших персональных данных могу сообщить следующее.

БУ «Советский комплексный центр социального обслуживания населения».не может уничтожить Ваши персональные данные, так как факт неправомерности действий с Вашими персональными данными не подтвержден и Вами не были предоставлены необходимые документы, подтверждающие неправомерность действий с Вашими персональными данными.

БУ «Советский комплексный центр социального обслуживания населения». осуществляет обработку Ваших персональных данных согласно требованиям следующих законодательных актов: _____

Если у Вас есть вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением, _____ _____ _____
(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Законному представителю г-на/г-ки
(Уполномоченному органу по защите прав
субъектов персональных данных)
(выбрать необходимое)

На Ваш запрос от «____» _____ 20___ г., относительно неправомерности действий с персональными данными г-на/г-ки _____ могу сообщить следующее.

БУ «Советский комплексный центр социального обслуживания населения». не может уничтожить персональные данные г-на/г- ки _____, так как факт неправомерности действий с персональными данными г-на/г-ки _____ не подтвержден и Вами не были предоставлены необходимые документы, подтверждающие неправомерность действий с персональными данными г-на/г-ки _____.

БУ «Советский комплексный центр социального обслуживания населения». осуществляет обработку Ваших персональных данных согласно требованиям следующих законодательных актов: _____

Если у Вас есть вопросы, связанные с обработкой персональных данных г-на/г-ки _____, пожалуйста, обращайтесь.

С уважением, _____ _____ _____
(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Форма уведомления субъекта персональных данных, его законного представителя или уполномоченного органа по защите прав субъектов персональных данных при достижении целей обработки ПДн

Г-ну/Г-ке_____

В связи с достижением целей обработки Ваших персональных данных могу сообщить следующее.

БУ «Советский комплексный центр социального обслуживания населения». была прекращена обработка и уничтожены Ваши персональные данные: _____

Если у Вас есть вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением, _____ _____ _____
(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Законному представителю г-на/г-ки
(Уполномоченному органу по защите прав
субъектов персональных данных)
(выбрать необходимое)

В связи с достижением целей обработки персональных данных г-на/г-ки _____ могу сообщить следующее.

БУ «Советский комплексный центр социального обслуживания населения». была прекращена обработка и уничтожены персональные данные г-на/г-ки _____:
_____

Если у Вас есть вопросы, связанные с обработкой персональных данных г-на/г-ки _____, пожалуйста, обращайтесь.

С уважением, _____ _____ _____
(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Г-ну/Г-ке_____

На Ваш запрос от «___» _____ 20___ г. относительно достижения целей обработки Ваших персональных данных могу сообщить следующее.

БУ «Советский комплексный центр социального обслуживания населения». не может прекратить обработку и уничтожить Ваши персональные данные, так как их обработка осуществляется согласно _____

Если у Вас есть вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением, _____ _____ _____
(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Законному представителю г-на/г-ки
(Уполномоченному органу по защите прав
субъектов персональных данных)
(выбрать необходимое)

На Ваш запрос от «___» _____ 20___ г., относительно достижения целей обработки персональных данных г-на/г-ки _____ могу сообщить следующее.

БУ «Советский комплексный центр социального обслуживания населения». не может прекратить обработку и уничтожить персональные данные г-на/г-ки _____, так как их обработка осуществляется согласно _____

Если у Вас есть вопросы, связанные с обработкой персональных данных г-на/г-ки _____, пожалуйста, обращайтесь.

С уважением, _____ _____ _____
(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Приложение 27 к приказу
БУ «Советский комплексный
центр социального
обслуживания населения»
от «06» сентября 2023 г. № 167

Правила работы лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими должностных (трудовых) обязанностей

1. Общие положения

1.1. Лицами, участвующими в рамках своих функциональных обязанностей в процессах обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным информационных систем персональных данных (далее - ИСПДн) являются сотрудники БУ «Советский комплексный центр социального обслуживания населения» в соответствии с утвержденным Перечнем должностей в БУ «Советский комплексный центр социального обслуживания населения»., доступ которых к персональным данным, в том числе обрабатываемым в ИСПДн, необходим для выполнения ими должностных (трудовых) обязанностей (далее - Пользователи).

1.2. Пользователи должны принимать все необходимые меры по защите персональных данных (далее - ПДн) и контролю за соблюдением прав доступа к ней.

1.3. Пользователи ИСПДн в своих должностных (трудовых) обязанностях обязаны руководствоваться настоящей Инструкцией и должны быть ознакомлены под роспись с настоящим документом и предупреждены об индивидуальной ответственности за его нарушение.

1.4. Основными задачами при обработке ПДн в ИСПДн являются:

- обеспечение исполнения требований нормативных правовых актов, руководящих документов, регламентирующих защиту ПДн в Российской Федерации в процессе создания, хранения, передачи и удаления документов, содержащих ПДн в ИСПДн БУ «Советский комплексный центр социального обслуживания населения»;
- обеспечение в ИСПДн необходимого уровня безопасности обработки, хранения и передачи ПДн;
- обеспечение необходимого уровня безопасности носителей ПДн;
- обеспечение безопасности ПДн при ее копировании, размножении.

2. Обязанности лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими должностных (трудовых) обязанностей

2.1. При первичном допуске к работе в ИСПДн пользователь изучает требования настоящего документа, разрешительную систему доступа к ИСПДн, технологический процесс обработки информации в ИСПДн, руководящие, нормативно-методические и организационно-распорядительные документы по вопросам обеспечения безопасности ПДн.

2.2. Каждый пользователь ИСПДн, имеющий доступ к автоматизированному рабочему месту (далее - АРМ), программному обеспечению (далее - ПО) и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

- строго соблюдать установленные правила обеспечения безопасности ПДн при работе с программными и техническими средствами ИСПДн, в том числе положения настоящего документа;
- знать и строго выполнять правила работы со средствами защиты информации, установленными на АРМ;
- при работе в ИСПДн выполнять только те обязанности, которые прописаны в должностной инструкции;
- не разглашать известные им ПДн лицам, не имеющим допуска к этим ПДн;
- располагать во время работы экран монитора в помещении так, чтобы исключалась возможность ознакомления с отображаемой на нем информацией посторонними лицами, и основные технические средства и системы (далее – ОТСС) в соответствии с Техническим паспортом на ИСПДн;
- помнить свой идентификатор и пароль;
- держать свой пароль в тайне, а именно не сообщать, не разглашать и любым другим способом не доводить до чьего-либо сведения (в том числе других сотрудников БУ «Советский комплексный центр социального обслуживания населения», в т.ч. руководителей) личный пароль;
- осуществлять ввод пароля только в условиях, исключающих его просмотр;
- не хранить записки-памятки с личным паролем на видном и/или в легко доступном месте: на столе, на мониторе, под клавиатурой, в верхнем ящике стола и т.п.;
- своевременно сообщать ответственному за обеспечение безопасности ПДн в ИСПДн (далее - администратор информационной безопасности ИСПДн) о фактах компрометации пароля (когда пароль стал или может быть известен ещё кому - либо кроме его владельца), об утере или повреждении аппаратного идентификатора и в этих случаях не использовать ИСПДн до специального разрешения администратора информационной безопасности ИСПДн;
- немедленно известить администратора информационной безопасности ИСПДн в случае утери электронного идентификатора или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации АРМ;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования компонентов АРМ, а также перебоев в системе электроснабжения;
- некорректного функционирования установленных на АРМ технических средств защиты;
- непредусмотренных отводов кабелей и подключенных устройств.

− при работе в ИСПДн использовать только учтенные съемные машинные носители ПДн, при обоснованной необходимости использования неучтённых носителей согласовывать использование с администратором информационной безопасности ИСПДн. После того как цель переноса информации на носители достигнута (переданы третьим лицам и т.п.) информация незамедлительно удаляется с носителей;

− при работе со съемными машинными носителями ПДн каждый раз перед началом работы обязан проверить их на отсутствие вирусов и иных вредоносных программ с использованием штатных антивирусных средств, установленных на АРМ. В случае обнаружения вирусов либо вредоносных программ пользователь ИСПДн обязан немедленно прекратить их использование и действовать в соответствии с требованиями Инструкции по организации антивирусной защиты в ИСПДн;

− выполнять требования Инструкции по организации антивирусной защиты в ИСПДн в полном объеме;

− осуществлять установленным порядком уничтожение ПДн с машинных носителей ПДн (с помощью средства защиты информации от несанкционированного доступа (далее - НСД));

− немедленно выполнять предписания администратора информационной безопасности ИСПДн в части обеспечения безопасности ПДн;

− соблюдать установленный режим разграничения доступа к информационным ресурсам;

− все изменения конфигурации технических и программных средств ИСПДн, ремонт, модификация и техническое обслуживание технических средств и систем, входящих в состав ИСПДн, производить только по согласованию с администратором информационной безопасности ИСПДн;

− обеспечить сохранность оборудования и физической целостности системных блоков компьютеров;

− при отсутствии необходимости работы компьютера выключить (блокировать нажатием клавиш Windows+L) его.

3. Права лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими должностных (трудовых) обязанностей

3.1. Пользователь ИСПДн имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. При этом для обработки, хранения и транспортировки ПДн разрешается использовать в ИСПДн только те машинные носители ПДн, которые учтены в «Журнале учета машинных носителей персональных данных».

3.2. Пользователь ИСПДн имеет право участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи ПДн и технических компонентов ИСПДн, если данное нарушение произошло под его идентификационными данными.

3.3. Своевременно получать доступ к информационным ресурсам ИСПДн, необходимым ему для выполнения своих должностных обязанностей.

3.4. Требовать от администратора информационной безопасности ИСПДн смены идентификационных данных в случае появления сведений или подозрений на то, что эти данные стали известны третьим лицам.

4. Лицам, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими должностных (трудовых) обязанностей, запрещается

4.1. Пользователю ИСПДн категорически запрещается:

− самостоятельно устанавливать, тиражировать или модифицировать ПО, изменять установленный алгоритм функционирования технических и программных средств, устанавливать или удалять установленные администратором информационной безопасности ИСПДн сетевые программы на компьютерах, вскрывать компьютер, сетевое и периферийное оборудование, подключать к компьютеру дополнительное оборудование;

− запускать любые системные или прикладные программы, не входящие в состав ПО;

− использовать компоненты программного и аппаратного обеспечения АРМ в личных целях;

− самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного ПО АРМ;

− записывать и хранить ПДн на неучтенных машинных носителях ПДн (гибких магнитных дисках, флэш-накопителях и т.п.);

− оставлять включенным без присмотра АРМ, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

− оставлять без личного присмотра на рабочем месте или в ином месте свой электронный идентификатор, машинные носители ПДн и распечатки, содержащие ПДн;

− умышленно использовать недокументированные свойства и ошибки в ПО или в настройках средств защиты ПДн;

− размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации, содержащей ПДн;

− осуществлять попытки НСД к ресурсам ИСПДн, проводить или участвовать в сетевых атаках и сетевом взломе;

− производить действия, направленные на взлом (несанкционированное получение привилегированного доступа) рабочих станций и серверов;

− привлекать посторонних лиц для производства ремонта ОТСС без письменной заявки и согласования с администратором информационной безопасности ИСПДн;

− отключать (блокировать) средства защиты информации;

− сообщать (или передавать) посторонним лицам личные атрибуты доступа к ресурсам ИСПДн;

− хранить на учтенных носителях программы и данные, не относящиеся к рабочей информации;

− выполнять работы с документами, содержащими ПДн, на дому, выносить их за пределы контролируемой зоны;

− вводить в ОТСС ПДн под диктовку или с микрофона;

− закрывать доступ к информации паролями без согласования с администратором информационной безопасности ИСПДн;

− передавать свои учетные носители кому-либо;

− запускать файлы-вложения, которые содержатся в спам-письмах.

5. Действия при обнаружении попыток несанкционированного доступа

5.1. К попыткам НСД относятся:

− сеансы работы с ПДн незарегистрированных пользователей, или пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истёк, или превышающих свои полномочия по доступу к ПДн;

− действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учётной записи администратора информационной безопасности ИСПДн или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашённого владельцем учётной записи или любым другим методом.

5.2. При выявлении факта несанкционированного доступа (далее - НСД) лицо, выявившее факт НСД (пользователь, ответственный за организацию обработки ПДн, ответственный за эксплуатацию ИСПДн, администратор информационной безопасности ИСПДн) обязан:

− законными способами прекратить НСД к ПДн;

− известить администратора информационной безопасности ИСПДн о факте НСД;

− известить руководителя пользователя, от имени учетной записи которого была осуществлена попытка НСД, о факте НСД;

− известить директора БУ «Советский комплексный центр социального обслуживания населения».

6. Порядок модификации конфигураций технических и программных средств ИСПДн

6.1. Право внесения изменений в конфигурацию аппаратно-программных средств защиты ИСПДн предоставляется администратору информационной безопасности ИСПДн:

– в отношении системных и прикладных программных средств - по согласованию (в случае, если проводилась аттестация) с аттестационной комиссией, проводившей аттестацию данной ИСПДн;

– в отношении аппаратных средств, а также в отношении программно-аппаратных средств защиты - по согласованию (в случае, если проводилась аттестация) с аттестационной комиссией, проводившей аттестацию данной ИСПДн.

6.2. Изменение конфигурации аппаратно-программных средств ИСПДн кем-либо, кроме вышеперечисленного уполномоченного сотрудника, запрещено.

6.3. Процедура внесения изменений в конфигурацию системных и прикладных программных средств ИСПДн, а также средств защиты информации инициируется заявкой ответственного за эксплуатацию ИСПДн.

6.4. В заявке могут указываться следующие виды необходимых изменений в составе аппаратных и программных средств ИСПДн:

– установка (развертывание) на компьютер(ы) программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи в данной ИСПДн;

– обновление (замена) на компьютере(ах) программных средств, необходимых для решения определенной задачи (обновление версий используемых для решения определенной задачи программ);

– изменение настроек средств защиты информации;

– удаление с компьютера программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на данном компьютере).

6.5. Также в заявке указывается условное наименование ИСПДн. Наименования задач указываются в соответствии с перечнем задач архива дистрибутивов установленного ПО, которые можно решать с использованием указанного компьютера.

6.6. Заявку ответственного за эксплуатацию ИСПДн, в которой требуется произвести изменения конфигурации, рассматривает директор,

визирует ее, утверждая тем самым производственную необходимость проведения указанных в заявке изменений.

6.7. После чего заявка передается администратору информационной безопасности ИСПДн для непосредственного исполнения работ по внесению изменений в конфигурацию компьютера, указанного в заявке ИСПДн.

6.8. Подготовка обновления, модификации общесистемного и прикладного ПО ИСПДн, тестирование, стендовые испытания (при необходимости) и передача исходных текстов, документации и дистрибутивных носителей программ в архив дистрибутивов установленного ПО, внесение необходимых изменений в настройки системы защиты информации от НСД и средств контроля целостности файлов на компьютерах, (обновление) и удаление системных и прикладных программных средств производится администратором информационной безопасности ИСПДн по согласованию с аттестационной комиссией (в случае, если проводилась аттестация), проводившей аттестацию данной ИСПДн. Работы производятся в присутствии ответственного за эксплуатацию ИСПДн.

6.9. Установка и обновление ПО (системного, тестового и т.д.) на компьютерах производится только с оригинальных лицензионных дистрибутивных носителей, полученных установленным порядком, прикладного ПО - с эталонных копий программных средств, полученных из архива дистрибутивов установленного ПО.

6.11. Все добавляемые программные и аппаратные компоненты должны быть предварительно установленным порядком проверены на работоспособность, а также отсутствие опасных функций.

6.12. После установки (обновления) ПО, администратор информационной безопасности ИСПДн должен произвести требуемые настройки средств управления доступом к компонентам компьютера и проверить работоспособность ПО, правильность их настройки и произвести соответствующую запись в «Журнале учета выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн», делает отметку о выполнении (на обратной стороне заявки) и в Техническом паспорте на ИСПДн.

6.13. При возникновении ситуаций, требующих передачи технических средств в сервисный центр с целью ремонта, ответственный за эксплуатацию ИСПДн докладывает об этом администратору информационной безопасности ИСПДн, который в свою очередь связывается с аттестационной комиссией (в случае, если проводилась аттестация) и в дальнейшем действует согласно их инструкций. В данном случае администратор информационной безопасности ИСПДн обязан предпринять необходимые меры для удаления ПДн с помощью средства защиты информации от НСД, которые хранились на компьютере. Оригиналы заявок (документов), на основании которых производились изменения в составе программных средств компьютеров, с отметками о внесении изменений в состав программных средств, должны

храниться вместе с Техническим паспортом на ИСПДн и «Журналом учета выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн» у администратор информационной безопасности ИСПДн для:

– восстановления конфигурации ИСПДн после аварий;

– контроля правомерности установки на ИСПДн средств для решения соответствующих задач при разборе конфликтных ситуаций;

– проверки правильности установки и настройки средств защиты информации, факта уничтожения ПДн, находившихся на компьютере, который оформляется актом и подписывается администратором информационной безопасности ИСПДн и ответственным за эксплуатацию ИСПДн.

7. Порядок учета, хранения и выдачи машинных носителей персональных данных

7.1. Порядок хранения и учета машинных носителей ПДн:

− машинные носители, содержащие ПДн, подлежат обязательному учёту администратором информационной безопасности ИСПДн. Учёт осуществляется с помощью «Журнала учёта машинных носителей ПДн» (форма указанного журнала приведена в приложении 7 к данному приказу);

− учёт машинных носителей ПДн включает присвоение регистрационных (учетных) номеров носителям. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей, номер инвентарного учета и иные номера;

− носители должны храниться в сейфе, расположенном в помещении БУ «Советский комплексный центр социального обслуживания населения», и изыматься только для выполнения должностных обязанностей;

− при поступлении нового машинного носителя, который будет использоваться для хранения или передачи ПДн, администратор информационной безопасности ИСПДн регистрирует его в «Журнале учёта машинных носителей ПДн».

7.2. Порядок регистрации выдачи машинных носителей ПДн:

− учет выдачи машинных носителей ПДн ведётся в «Журнале учёта машинных носителей ПДн», в котором указывается регистрационный (учетный) номер машинного носителя ПДн, дата, время, фамилия, имя и отчество должностного лица, получившего машинный носитель ПДн, его роспись;

− в случае возврата должностным лицом машинного носителя ПДн в «Журнале учёта машинных носителей ПДн» администратором информационной безопасности ИСПДн проставляется отметка о возврате с указанием даты, времени возврата, личных подписей передающей и принимающей стороны.

7.3. Доступ к машинным носителям ПДн осуществляется в соответствии с перечнем должностей, физический доступ которых к ПДн необходим для выполнения ими должностных обязанностей, который представлен в приложении 1 к настоящему приказу.

8. Порядок работы с файлами документов, внесение корректировок, уничтожение, хранение документов

№ п.п.	Этап	Описание этапа
Подготовка к обработке информации		
1	Получение допуска к работе	Допуск сотрудников к ИСПДн осуществляется в соответствии с Перечнем должностей в БУ «Советский комплексный центр социального обслуживания населения», доступ которых к ПДн, в том числе обрабатываемым в ИСПДн, необходим для выполнения ими должностных (трудовых) обязанностей и Разрешительной системе доступа пользователей к сведениям конфиденциального характера ИСПДн. Для работы в ИСПДн каждый пользователь должен получить соответствующий допуск, сведения о котором фиксируются в «Журнале учета лиц, допущенных к работе с ПДн в ИСПДн». Права по доступу к информационным ресурсам должны быть определенны утверждённой Разрешительной системой доступа пользователей к сведениям конфиденциального характера ИСПДн.
2	Получение исходной информации для обработки в системе	Исходная информация, обработка которой осуществляется в ИСПДн, может находиться на бумажных носителях.
3	Вход пользователя в систему	Авторизация пользователя осуществляется средствами защиты информации от несанкционированного доступа по имени и с использованием его персонального пароля длиной не менее 6 символов.
Обработка информации		
1	Регистрация времени начала работы	Осуществляется штатными средствами прикладного ПО и средствами защиты информации от несанкционированного доступа.
2	Ввод обрабатываемых исходных данных в систему	Ввод в систему обрабатываемых ПДн производится вручную с клавиатуры.

№ п.п.	Этап	Описание этапа
3	Обработка текстовой информации	Пользователь обязан принять меры по исключению возможности просмотра обрабатываемых ПДн с экрана монитора и с бумажных носителей (в том числе распечатываемых материалов) лицами, не допущенными к ПДн.
4	Временное хранение обрабатываемой информации между сеансами работы пользователя в системе	Хранение ПДн между сеансами работы в ИСПДн осуществляется в каталогах на жестком диске ПЭВМ, выделенных в ИСПДн для ПДн. Контроль доступа к ним осуществляется соответствующими средствами защиты информации.
Сохранение результатов обработки информации		
1	Распечатка документов	Распечатка документов (данных) производится на принтере, входящем в состав ОТСС объекта информатизации, при этом не ведется учет распечатанных документов.
2	Сохранение окончательных результатов работы	Готовые данные в электронном виде хранятся на АРМ пользователя и на учтенном съемном носителе ПДн. Готовые данные в бумажном виде хранятся в кабинетах здания.
3	Передача носителей ПДн и распечатанных документов	В соответствии с требованиями организационно-распорядительных документов.
4	Очистка остаточной (удаленной) информации	Гарантированная очистка удаляемых ПДн с машинных носителей ПДн (без возможности ее восстановления) осуществляется средствами системы защиты информации от НСД.
5	Регистрация времени работы и действий пользователя в системе	Осуществляется штатными средствами прикладного ПО.
6	Завершение работы	После окончания работы с ИСПДн пользователь обязан на своем рабочем месте завершить работу всех программ, входящих в состав специализированного ПО и выключить компьютер (перегрузить). При необходимости оставить свое рабочее место на непродолжительное время

№ п.п.	Этап	Описание этапа
		пользователь обязан его заблокировать (дальнейшая работа может быть продолжена пользователем только после ввода его логина и пароля). После окончания рабочего дня необходимо закрыть окна и форточки, выключать электроприборы и запереть и опечатать дверь.

9. Ответственность лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими должностных (трудовых) обязанностей

9.1. Персональную ответственность за соблюдение установленных требований настоящего положения несут пользователи ИСПДн и администратор информационной безопасности ИСПДн.

9.2. За разглашение ПДн и нарушение порядка обращения с машинными носителями ПДн администратор информационной безопасности ИСПДн, а также пользователи ИСПДн, работающие с этими машинными носителями ПДн, могут быть привлечены к дисциплинарной и иной, предусмотренной законодательством Российской Федерации, ответственности.

9.3. Пользователи несут персональную ответственность за все действия, совершенные от имени его учётной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

9.4. Пользователь несет ответственность за правильность включения и выключения АРМ, входа и выхода в систему и за все свои действия при работе в ИСПДн.

9.5. Нарушение данной инструкции, повлекшее уничтожение, блокирование, модификацию либо копирование ПДн, нарушение работы компьютеров пользователей ИСПДн или ИСПДн в целом, может повлечь ответственность в соответствии с действующим законодательством.

Приложение 28 к приказу
БУ «Советский комплексный
центр социального
обслуживания населения»
от «06» сентября 2023 г. № 167

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

1. Общие положения

1.1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных в БУ «Советский комплексный центр социального обслуживания населения» требованиям к защите персональных данных, установленным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Правила), разработаны в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» и устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере обработки персональных данных, а также определяют основания, порядок и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям законодательства Российской Федерации.

2. Порядок осуществления внутреннего контроля соответствия обработки персональных данных к требованиям защиты персональных данных

2.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных в БУ «Советский комплексный центр социального обслуживания населения» организовывается проведение ежегодных проверок.

2.2. Проверки проводятся ответственным за организацию обработки персональных данных совместно с ответственным за обеспечение безопасности персональных данных в информационных системах персональных данных и ответственным за эксплуатацию информационной системы персональных данных.

2.3. Плановые проверки условий обработки персональных данных проводятся на основании утвержденного руководителем БУ «Советский комплексный центр социального обслуживания населения» ежегодного плана внутренних проверок режима защиты персональных данных (плановые проверки).

2.4. Внеплановые проверки проводятся на основании поступившей информации о нарушениях правил обработки персональных данных, по инициативе ответственного за организацию обработки персональных данных, либо ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных. Проведение внеплановой проверки организуется в течение 10 (десяти) рабочих дней со дня поступления информации о нарушениях правил обработки персональных данных.

2.5. В проведении проверки условий обработки персональных данных не могут участвовать сотрудники БУ «Советский комплексный центр социального обслуживания населения», прямо или косвенно заинтересованные в ее результате.

2.6. Проверки условий обработки персональных данных осуществляются непосредственно на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра служебных мест сотрудников БУ «Советский комплексный центр социального обслуживания населения», участвующих в процессе обработки персональных данных.

2.7. При проведении проверки должны быть полностью, объективно и всесторонне, установлены:

- соответствие целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям БУ «Советский комплексный центр социального обслуживания населения»;
- соответствие объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достаточность (избыточность) персональных данных для целей обработки персональных данных, заявленных при сборе персональных данных;
- отсутствие (наличие) объединения, созданных для несовместимых между собой целей, баз данных информационных систем персональных данных;
- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
- порядок и условия соблюдения парольной защиты;
- порядок и условия соблюдения антивирусной защиты;
- порядок и условия обеспечения резервного копирования;
- эффективность принимаемых мер по обеспечению безопасности персональных данных до их ввода в ИСПДн;
- условия соблюдения режима защиты при подключении к информационно-телекоммуникационным сетям;

− порядок и условия обновления программного обеспечения и единообразия применяемого программного обеспечения на всех элементах ИСПДн;

− порядок и условия применения средств защиты информации;

− соблюдение учета носителей персональных данных;

− соблюдение правил доступа к персональным данным;

− соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных;

− наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

− мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

2.8. Ответственный за организацию обработки персональных данных и ответственный за обеспечение безопасности персональных данных в ИСПДн, а также ответственный за эксплуатацию ИСПДн в ходе проверки имеют право:

− запрашивать у сотрудников информацию, необходимую для реализации своих полномочий;

− требовать от уполномоченных на обработку персональных данных сотрудников уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

− принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

− вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

− вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

2.9. Проверка условий обработки персональных данных должна быть завершена не позднее чем через тридцать календарных дней со дня принятия решения о ее проведении.

2.10. По результатам проведенной проверки условий обработки персональных данных ответственный за организацию обработки персональных данных предоставляет руководителю БУ «Советский комплексный центр социального обслуживания населения» письменное заключение с указанием мер, необходимых для устранения выявленных нарушений.

Приложение 29 к приказу
БУ «Советский комплексный
центр социального
обслуживания населения»
от «06» сентября 2023 г. № 167

ПОРЯДОК
уничтожения персональных данных при достижении целей обработки и (или) при наступлении иных законных оснований

1. Общие положения

1.1. Настоящий документ устанавливает порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

2 Порядок уничтожения персональных данных при достижении целей обработки и (или) при наступлении иных законных оснований

2.1. Документы, дела, книги и журналы учета, содержащие персональные данные, при достижении целей обработки или при наступлении иных законных оснований, (например, утратившие практическое значение, а также с истекшим сроком хранения), подлежат уничтожению.

2.2. Вопрос об уничтожении документов, содержащих персональные данные, рассматривается на заседании Комиссии по защите информации.

2.3. Уничтожение документов производится в присутствии ответственного за организацию обработки персональных данных, который несет персональную ответственность за правильность и полноту уничтожения перечисленных данных. Результаты уничтожения документов оформляются актом (акт составляется в свободной форме).

2.4. Отобранные к уничтожению материалы измельчаются механическим способом до степени, исключающей возможность прочтения текста, или сжигаются.

2.5. После уничтожения материальных носителей ответственный за организацию обработки персональных данных подписывает акт в двух экземплярах, также в номенклатурах и описях дел проставляется отметка «Уничтожено. Акт №__(дата)».

2.6. Уничтожение информации на носителях необходимо осуществлять путем стирания информации с помощью средства защиты информации от несанкционированного доступа с гарантированной очисткой информации, установленной на АРМ.

2.7. Информация, содержащая персональные данные, при достижении целей обработки или при наступлении иных законных оснований (например, утратившие практическое значение, с истекшим сроком хранения) в электронном виде, подлежит уничтожению.