ГОСУДАРСТВЕННОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ НОВОСИБИРСКОЙ ОБЛАСТИ

«ЦЕНТР СОЦИАЛЬНОЙ ПОДДЕРЖКИ НАСЕЛЕНИЯ СЕВЕРНОГО РАЙОНА»

ПРИКАЗ

30.04.2025 № 157

с.Северное

Об утверждении документов, определяющих политику ГКУ НСО ЦСПН Северного района в отношении обработки персональных данных

В целях исполнения Федеральных законов от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и от 27.07.2006 № 152-ФЗ «О персональных данных», постановлений Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», главы 14 Трудового кодекса Российской Федерации, пункта 8 Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 № 21, пункта 20 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 № 17, приказа Роскомнадзора от 24.02.2021 № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения»

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемые:

1) инструкцию идентификации и аутентификации субъектов доступа и объектов доступа;

2) инструкцию по управлению доступом субъектов доступа к объектам доступа;

3) инструкцию по ограничению программной среды;

4) инструкцию по защите машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;

5) инструкцию по регистрации событий безопасности;

6) инструкцию по организации антивирусной защиты;

7) инструкцию по организации системы обнаружения вторжений;

8) инструкцию по контролю (анализу) защищенности персональных данных;

9) инструкцию по обеспечению целостности информации;

10) инструкцию по обеспечению доступности персональных данных;

11) инструкцию по защите технических средств;

12) инструкцию по выявлению компьютерных инцидентов и реагированию на них;

13) инструкцию по управлению конфигурацией;

14) инструкцию пользователя информационных систем;

15) инструкцию администратора безопасности информационных систем;

16) инструкцию ответственного за защиту информации в информационных системах;

17) инструкцию ответственного за организацию обработки персональных данных;

18) инструкцию ответственного по обеспечению безопасности персональных данных;

19) правила обработки персональных данных, осуществляемой без использования средств автоматизации;

20) правила работы с обезличенными данными;

21) правила рассмотрения запросов субъектов персональных данных или их представителей;

22) правила обработки персональных данных;

23) правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных;

24) регламент защиты информационной системы, ее средств, систем связи и передачи данных;

25) типовое обязательство сотрудника ГКУ НСО ЦСПН Северного района, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта (трудового договора) прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей;

26) типовая форма согласия на обработку персональных данных;

27) типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные.

28) положение об обработке и защите персональных данных в ГКУ НСО ЦСПН Северного района.

29) политика в отношении обработки персональных данных ГКУ НСО ЦСПН Северного района.

30) порядок доступа работников, в помещения ГКУ НСО ЦСПН Северного района, в которых ведется обработка персональных данных.

2. Контроль за исполнением настоящего приказа оставляю за собой.

Директор А.И.Сандзюк

УТВЕРЖДЕНА
приказом ГКУ НСО ЦСПН Северного района
от «30» апреля 2025 г. № 157

Инструкция идентификации и аутентификации субъектов доступа и объектов доступа

1. Общие положения

1.1. Настоящая Инструкция разработана в целях реализации мер по идентификации и аутентификации субъектов доступа и объектов доступа, которые должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности) в информационных системах (далее – ИС) ГКУ НСО ЦСПН Северного района.

Настоящая Инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в ИС, а также контроль за действиями пользователей при работе с паролями.

1.2. Организационное и техническое обеспечение смены, прекращения действия паролей в ИС, процессов генерации и использования возлагается на администратора безопасности ИС, сопровождающих механизмы идентификации и аутентификации (подтверждения подлинности) пользователей.

2. Требования к паролям

2.1. Требования к паролям в операционных системам, установленных в ИС, функциональным приложениям и средствам защиты информации обеспечиваются организационно-техническими мерами и реализуются посредством настроек механизмов парольной политики операционных систем или средствами защиты информации от несанкционированного доступа, установленными в ИС.

2.2. Пароли должны меняться пользователями самостоятельно с учетом следующих требований:

– минимальная длина пароля – 10 символов;

– максимальный срок действия пароля – 90 дней;

– при назначении нового пароля он должен быть уникальным (не повторяющимся), не допускается использования любого из пяти предыдущих;

– пароль не должен совпадать с именем пользователя, а также включать в себя легко вычисляемые сочетания символов, общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.) и не должен содержать:

– месяцы года, дни недели и т.п.;

– фамилии, инициалы и регистрационные номера автомобилей;

– номера телефонов или группы символов, состоящие из одних цифр (12345678 и т.п.).

2.3. Пароль должен быть задан набором на клавиатуре буквенно-цифровых символов, которые будут заменяться специальными символами, и не будут видны пользователям или посторонним лицам.

2.4. После 3 неудачных попыток ввода пароля в систему, учетная запись соответствующего пользователя блокируется. Снятие блокировки происходит автоматически через 15 минут, так же блокировка может быть снята принудительно администратором безопасности ИС.

2.5. Настройки операционной системы со встроенными средствами защиты информации и средства защиты информации от несанкционированного доступа должны позволять:

– оповещать пользователя об истечения срока действия пароля;

– блокировать доступ в случае истечения срока действия пароля;

– проверять длину и сложность пароля в соответствии с требованиями настоящей Инструкции;

– регистрировать события, связанные с любым из нарушений настоящей Инструкции;

– исключать возможность несанкционированного изменения регистрационных записей пользователями.

2.6. Напоминание (предупреждение) пользователю о приближении окончания срока действия пароля учетной записи должно производиться не менее чем за 5 дней, по истечении которых текущее значение пароля прекратит действие.

2.7. Временный пароль должен иметь минимальную длину – 6 символов. Временный пароль должен быть сменен пользователем при его первом обращении к соответствующему информационному ресурсу.

2.8. Последние 24 пароля, введенные пользователем при попытке его замены должны быть не допущены к применению как аутентификационная информация.

3. Порядок работы с паролями

3.1. При заведении новой учетной записи пользователя, администратором безопасности ИС назначается временный пароль. Временный пароль сообщается пользователю в устной или письменной (электронной) форме и должен быть сменен пользователем при первом входе в систему. Смена временного пароля осуществляется в соответствии с требованиями к паролям, изложенными в разделе 2 настоящей Инструкции.

3.2. При работе с паролями пользователям ЗАПРЕЩАЕТСЯ:

– передавать (сообщать) личный пароль кому-либо;

– проводить какие-либо действия с паролем, которые могут повлечь за

собой разглашение пароля (записи паролей на бумаге, ящике стола, клавиатуре, мониторе и т.п.);

– набирать пароль в присутствии постороннего лица.

3.3. Пароли подлежат обязательной смене в следующих случаях:

– при запросе системы на смену пароля;
– в случае компрометации действующего пароля;
– по истечении максимального срока действия пароля;
– по требованию администратора безопасности ИС.

3.4. В случаях компрометации (разглашения) пароля, пользователь обязан немедленно заменить пароль, не дожидаясь запроса на его принудительную смену и сообщить о факте компрометации администратору безопасности ИС.

3.5. Хранение пользователем значений своих паролей допускается только на бумажном носителе в личном сейфе, либо в сейфе администратора безопасности ИС.

3.6. Событие блокировки учетной записи по причине ошибочного ввода пароля в обязательном порядке регистрируется в соответствующем журнале безопасности операционной системой или средством защиты информации от несанкционированного доступа.

3.7. Пользователи не должны вносить изменения в настройки функционирования операционной системы и средств защиты информации.

3.8. Парольная информация относится к защищаемой (конфиденциальной) информации. Пользователи несут дисциплинарную и административную ответственность за разглашение парольной информации (в зависимости от последствий такого разглашения).

3.9. Идентификатор пользователя в ИС должен однозначно идентифицировать пользователя (содержать его фамилию в обязательном порядке).

4. Идентификация и аутентификация устройств

4.1. Идентификации и аутентификации подлежат следующие виды устройств, используемые в ГКУ НСО ЦСПН Северного района:

– серверы;
– автоматизированные рабочие места.

4.2. Идентификация устройств в информационных системах обеспечивается по комбинации логического имени (имени устройства), логическому адресу (IP-адресу) и физическому адресу (MAC-адресу).

4.2. Аутентификация осуществляется встроенными механизмы обеспечения информационной безопасности используемых операционных систем или с использованием средств защиты информации от несанкционированного доступа.

5. Ответственность при организации правил и процедур идентификации и аутентификации

5.1. Ответственность за организацию правил и процедур идентификации и аутентификации ИС в соответствии с требованиями настоящей Инструкции возлагается на администратора безопасности ИС.

5.2. Ответственность за соблюдение требований настоящей Инструкции возлагается на всех сотрудников, эксплуатирующих ИС.

УТВЕРЖДЕНА
приказом ГКУ НСО ЦСПН Северного района
от «30» апреля 2025 г. № 157

Инструкция по управлению доступом субъектов доступа к объектам доступа

1. Общие положения

1.1. Настоящая Инструкция разработана в целях реализации мер по управлению доступом субъектов доступа к объектам доступа, которые должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационных системах (далее – ИС) ГКУ НСО ЦСПН Северного района.

Настоящая инструкция предназначена для обеспечения защиты информации, содержащейся в ИС при разграничении доступа пользователей к ресурсам и информации ИС.

1.2. Настоящая инструкция определяет порядок действий администратора безопасности и пользователей ИС при разграничении доступа пользователей к защищаемым ресурсам ИС.

1.3. Права на администрирование средств защиты информации также имеют сотрудники государственного казенного учреждения Новосибирской области «Соцтехсервис», согласно устава от 12.10.2022 № 1378, и сотрудники государственного бюджетного учреждения Новосибирской области «Центр защиты информации Новосибирской области».

2. Порядок предоставления пользователям доступа к ресурсам и информации ИС

2.1. Разграничение доступа к ресурсам и информации осуществляет и контролирует администратор безопасности ИС путем настройки операционных систем или средств защиты информации от несанкционированного доступа на основании разрешительной системы доступа, утвержденной в ГКУ НСО ЦСПН Северного района на ИС.

2.2. Вход в ИС и действия с ресурсами ИС до прохождения процедур идентификации и аутентификации разрешен администратору безопасности ИС для восстановления работоспособности ИС после сбоев и отказов технических средств ИС.

2.3. В ИС назначение прав и привилегий пользователям и запускаемым от их имени процессам, производится администратором безопасности ИС.

2.4. Назначаются минимально необходимые для выполнения пользователями и запускаемым от их имени процессам своих должностных обязанностей (функций) и санкционированного доступа к объектам доступа в соответствии с минимально необходимыми правами и привилегиями.

2.5. События неправомерного доступа пользователя к информационным

ресурсам, не имеющим на это права, в обязательном порядке регистрируется в журнале безопасности с указанием ресурса к которому пытались получить неправомерный доступ.

2.6. Блокировка передачи защищаемой информации через сеть Интернет (или другие информационно-телекоммуникационные сети международного информационного обмена) по незащищенным линиям связи, сетевые запросы и трафик, несанкционированно исходящие из ИС и (или) входящие в ИС осуществляется с использование сертифицированных межсетевых экранов.

3. Процедура ограничения прав доступа к защищаемым ресурсам ИС

3.1. Администратор безопасности ИС с использованием механизмов операционных систем или средств защиты информации от несанкционированного доступа, разграничивает права доступа конкретного пользователя к защищаемому ресурсу (папка с персональными данными) путем выставления галочек для разрешающего действия в соответствии с разрешительной системой доступа, утвержденной в ГКУ НСО ЦСПН Северного района для ИС.

3.2. Настройки производятся согласно разделу «Настройки средств защиты информации» инструкции администратора безопасности ИС.

3.3. Для учетной записи администратора безопасности ИС также меняются права доступа к защищаемому ресурсу в соответствии с разрешительной системой доступа, утвержденной в ГКУ НСО ЦСПН Северного района для ИС.

3.4. Механизмами операционной системы или средствами защиты информации от несанкционированного доступа, производится ограничение на доступ к защищаемой информации других учетных записей или групп.

3.5. В случае внесения необходимых изменений в права доступа к защищаемым ресурсам, это возможно сделать с помощью учетной записи администратора безопасности ИС, путем внесения изменений в разрешительную систему доступа, утвержденную в ГКУ НСО ЦСПН Северного района для ИС. Настройка производится аналогично первичной настройки операционной системы или средства защиты информации от несанкционированного доступа.

3.6. Разграничение прав к папкам, в которых располагаются средства защиты информации или программные средства производится механизмами операционной системы или средством защиты информации от несанкционированного доступа по умолчанию и не требует внесения дополнительных изменений в настройку.

3.7 В ИС должно осуществляться ограничение количества неуспешных попыток входа в ИС (доступа к ИС), а также обеспечиваться блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в ИС (доступа к ИС) на установленный период времени.

3.7 В ИС должно обеспечиваться блокирование сеанса доступа

пользователя после установленного времени его бездействия (неактивности) в ИС или по запросу пользователя ИС.

3.9 Блокирование сеанса доступа пользователя в ИС обеспечивает временное приостановление работы пользователя со средством вычислительной техники, с которого осуществляется доступ к ИС (без выхода из ИС).

3.10 В ИС на устройстве отображения (мониторе) после блокировки сеанса не должна отображаться информация сеанса пользователя (в том числе использование «хранителя экрана», гашение экрана или иные способы).

3.11 Для заблокированного сеанса должно осуществляться блокирование любых действий по доступу к информации и устройствам отображения, кроме необходимых для разблокирования сеанса.

3.12 Блокирование сеанса доступа пользователя в ИС должно сохраняться до прохождения им повторной идентификации.

3.13 Пользователям ИС запрещены любые действия до прохождения ими процедур идентификации и аутентификации (кроме необходимых для прохождения процедур идентификации и аутентификации).

4. Управление информационными потоками

4.1 В ИС должно осуществляться управление информационными потоками, обеспечивающее разрешенный (установленный) маршрут прохождения информации между пользователями, устройствами, сегментами в рамках ИС, а также между ИС или при взаимодействии с сетью «Интернет» (или другими информационно-телекоммуникационными сетями международного информационного обмена) на основе правил управления информационными потоками, включающих контроль конфигурации ИС, источника и получателя передаваемой информации, структуры передаваемой информации, характеристик информационных потоков и (или) канала связи (без анализа содержания информации).

4.2 Управление информационными потоками должно блокировать передачу защищаемой информации через сеть «Интернет» (или другие информационно-телекоммуникационные сети международного информационного обмена) по незащищенным линиям связи, сетевые запросы и трафик, несанкционированно исходящие из ИС и (или) входящие в ИС.

5. Правила удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети

5.1 В ИС должна обеспечиваться защита информации при доступе пользователей (процессов запускаемых от имени пользователей) и (или) иных субъектов доступа к объектам доступа ИС через информационно-телекоммуникационные сети, в том числе сети связи общего пользования, с использованием стационарных и (или) мобильных технических средств (защита удаленного доступа).

5.2 Защита удаленного доступа должна обеспечиваться для всех видов

доступа и включает:

– ограничение на использование удаленного доступа в соответствии с задачами (функциями) ИС, для решения которых такой доступ необходим;

– предоставление удаленного доступа только тем лицам, которым он необходим для осуществления технической поддержки на основании договора;

– мониторинг и контроль удаленного доступа на предмет выявления несанкционированного удаленного доступа к объектам доступа ИС;

– контроль удаленного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа ИС до начала информационного взаимодействия с ИС (передачи защищаемой информации);

– использование ограниченного (минимально необходимого) количества точек подключения к ИС при организации удаленного доступа к объектам доступа ИС;

– исключение удаленного доступа от имени привилегированных учетных записей (администраторов) для администрирования ИС и ее системы защиты информации.

6. Управление взаимодействием с информационными системами сторонних организаций (внешними ИС)

6.1 Управление взаимодействием ИС с внешними ИС должно включать в себя определение порядка обработки, хранения и передачи информации с использованием внешних ИС.

6.2 Оператор разрешает обработку, хранение и передачу информации с использованием внешней ИС при выполнении следующих условий:

– при наличии договора (соглашения) об информационном взаимодействии с оператором (обладателем, владельцем) внешней информационной системы;

– при наличии подтверждения выполнения во внешней ИС предъявленных к ней требований о защите информации (наличие аттестата соответствия требованиям по безопасности информации или иного подтверждения).

7. Ответственность при управлении правилами и процедурами управления доступом к информационным ресурсам

7.1. Ответственность по управлению правилами и процедурами управления доступом к информационным ресурсам в соответствии с требованиями настоящей Инструкции возлагается на администратора безопасности ИС.

7.2. Ответственность за соблюдение требований настоящей Инструкции возлагается на всех сотрудников, эксплуатирующих ИС.

УТВЕРЖДЕНА
приказом ГКУ НСО ЦСПН Северного района
от «30» 04 2025 г. № 157

Инструкция по ограничению программной среды

1. Общие положения

1.1. Настоящая Инструкция разработана в целях реализации мер по ограничению программной среды, которые должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационных системах (далее – ИС) ГКУ НСО ЦСПН Северного района программного обеспечения или исключать возможность установки и (или) запуска, запрещенного к использованию в ИС, программного обеспечения.

1.2. Настоящая Инструкция предназначена для обеспечения защиты информации, обрабатываемой в ИС, при установке и обновлении программного обеспечения, в том числе средств защиты информации и определяет порядок действий администратора безопасности ИС при установке и обновлении.

2. Порядок установки и обновления программного обеспечения

2.1. Для ИС определено программное обеспечение, разрешенное к установке (приложение 1 к настоящей Инструкции).

2.2. Программное обеспечение, устанавливаемое и применяемое на серверах государственных информационных систем Новосибирской области, Оператором которых выступает ГКУ НСО ЦСПН Северного района, определяется в контрактах на создание данных систем и в контрактах на оказание услуг по сопровождению, технической поддержке и сервисному обслуживанию.

2.3. В ИС ГКУ НСО ЦСПН Северного района может быть установлено лицензионное программное обеспечение, свободно распространяемое программное обеспечение и драйверы для функционирования периферийных устройств.

2.4. Установка стороннего программного обеспечения, не представленного в перечне программного обеспечения, разрешенного к установке, ЗАПРЕЩЕНО.

2.5. Устанавливаемое программное обеспечение должно быть предварительно проверено (протестировано) администратором безопасности ИС на работоспособность, а также на совместимость с установленными в ИС программными и техническими средствами, в том числе средствами защиты информации.

2.6. Установку (обновление) средств защиты информации организовывает администратор безопасности ИС.

2.7. Установка средств защиты информации производится с оригинальных лицензионных дистрибутивных носителей, полученных законным порядком (путем). Устанавливаемые средства защиты информации

должны иметь необходимую эксплуатационную документацию, формуляр и руководство пользователя.

2.8. После установки (обновления) программного обеспечения администратор безопасности ИС выполняет необходимые настройки, выполняет тестирование работоспособности и вносит необходимые изменения в эксплуатационную документацию (при необходимости).

2.9. В случае необходимости расширения перечня программного обеспечения, разрешенного к установке (приложение 1 к настоящей Инструкции) администратор безопасности ИС проверяет правовое обоснование установки программного обеспечение (наличие его лицензий или относится ли оно к свободно распространяемому программному обеспечению), необходимость данного программного обеспечения пользователю в работе для выполнения его функций данного программного обеспечения, а также проверяет программное обеспечение на наличие в нем уязвимостей по банку уязвимостей ФСТЭК России https://bdu.fstec.ru/vul, а после инициирует внесение изменений в перечень.

3. Ответственность при ограничении программной среды и контролю обновлений программного обеспечения

3.1. Ответственность установку обновлений программного обеспечения, его состава в ИС в соответствии с требованиями настоящей Инструкции возлагается на администратора безопасности ИС.

3.2. Ответственность за соблюдение требований настоящей Инструкции возлагается на всех сотрудников, эксплуатирующих ИС.

Приложение № 1 к Инструкции по ограничению программной среды

ПЕРЕЧЕНЬ
программного обеспечения, разрешенного к установке в информационных системах ГКУ НСО ЦСПН Северного района

№ п/п	Программное обеспечение, разрешенное к установке в информационных системах ГКУ НСО ЦСПН Северного района
	На автоматизированных рабочих местах под управлением ОС Windows
1.	Архиватор 7-zip
2.	Редактор PDF Adobe Acrobat
3.	Офисный мессенджер BeeBEEP
4.	Браузер Chromium-Gost
5.	Браузер Google Chrome
6.	Браузер Mozilla Firefox
7.	Браузер Microsoft Edge
8.	Программное обеспечение управления электронной подписью и шифрованием (Crypto+ DE)
9.	Криптопровайдер КриптоПро CSP
10.	Программное обеспечение для создания и проверки электронной подписи (ЭП) на веб-страницах КриптоПро ЭЦП Browser plug-in
11.	Офисный пакет Microsoft Office
12.	Офисный пакет Р7-Офис. Профессиональный
13.	Специальное программное обеспечение АИС «ИСКО»
14.	Специальное программное обеспечение Сводная установка ПК Катарсис 8, Новосибирск - 1
15.	Специальное программное обеспечение СФР АРМ СЗН
16.	СЗИ от НСД Dallas Lock 8.0-K
17.	Средство антивирусной защиты Kaspersky Endpoint Security для Windows
18.	Агент администрирования Kaspersky Security Center
19.	VPN-клиент ViPNet Client 4
20.	Необходимые библиотеки и драйвера для функционирования технических средств и операционной системы
	На автоматизированных рабочих местах под управлением ОС Альт 8 СП
21.	Офисный пакет LibreOffice
22.	Офисный пакет Р7-Офис
23.	Редактор PDF Master PDF Editor
24.	Браузер Chromium-Gost
25.	Браузер Chromium
26.	Браузер Mozilla Firefox
27.	Браузер Yandex
28.	Специальное программное обеспечение Сводная установка ПК Катарсис 8, Новосибирск - 1
29.	Средство антивирусной защиты Kaspersky Endpoint Security для Linux
30.	Агент администрирования Kaspersky Security Center
31.	VPN-клиент ViPNet Client 4U для Linux
32.	Агент системы комплексной защиты ViPNet EndPoint Protection Agent
33.	Стандартное программное обеспечение операционной системы
34.	Необходимые библиотеки и драйвера для функционирования технических средств и операционной системы

УТВЕРЖДЕНА
приказом ГКУ НСО ЦСПН Северного района
от «30» 04 2025 г. № 157

Инструкция по защите машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные

1. Общие положения

1.1. Настоящая Инструкция разработана в целях реализации мер по защите машинных носителей информации (средств обработки (хранения) информации), которые должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них информации в информационных системах (далее – ИС) ГКУ НСО ЦСПН Северного района.

1.2. Настоящая Инструкция определяет порядок работы с машинными носителями информации в ИС, которые входят в состав автоматизированных рабочих мест в составе ИС, а также съемных машинных носителей информации, которые применяются в ИС.

2. Порядок работы с машинными носителями информации ИС

2.1. Машинные носители информации ИС учитываются администратором безопасности ИС.

2.2. Право на перемещение машинных носителей информации ИС за пределы территории, на которой осуществляется обработка не допускается без предварительного форматирования или переноса информации на резервные машинные носители.

2.3. Использование неучтённых машинных носителей информации ИС фиксируется как несанкционированное, а администратор безопасности ИС инициирует служебную проверку. По факту выясненных обстоятельств составляется Акт проведения расследования инцидента.

2.4. Пользователи, в случаях утраты или кражи машинных носителей информации ИС, сообщают об этом администратору безопасности ИС.

2.5. Машинные носители информации ИС, пришедшие в негодность, или отслужившие в установленный срок, подлежат уничтожению. По результатам уничтожения составляется Акт уничтожения машинных носителей информации.

2.6. При передаче машинных носителей информации между пользователями, в сторонние организации для ремонта или утилизации информации на таких носителях подлежат уничтожению (стиранию) штатными средствами операционной системы и (или) форматирование машинного носителя информации штатными средствами операционной системы.

3. Порядок организации машинных носителей информации ИС

3.1. Администратор безопасности ИС вносит в Журнал учета машинных носителей информации сведения о машинных носителях информации:

- дата регистрации (в графе проставляется дата постановки носителя на учет);
- вид носителя (вид учтенного носителя (USB-носитель, оптический диск и т.д.);
- серийный/инвентарный номер:
  - USB - носителя (порядковый номер, зафиксированный на носителе);
  - жесткого диска (заводской/инвентарный номер системного блока);
  - оптический носитель (зафиксированный на носителе, согласно внутреннему конфиденциальному делопроизводству);
- подпись (подпись должностного лица, передавшего/получившего носитель);
- дата и номер акта уничтожения (указывается дата и номер акта уничтожения).

3.2. В случае применения в ИС съемных машинных носителей информации обеспечивается их хранение в запираемых шкафах или сейфах (металлических шкафах) ГКУ НСО ЦСПН Северного района.

4. Защита применяемых в информационной системе мобильных технических средств

4.1 В ИС запрещен беспроводной доступ к объектам доступа с использованием имеющих проводной сетевой интерфейс портативных вычислительных устройств, входящих в состав ИС.

4.2 Защита мобильных технических средств включает реализацию следующих мер:

- реализацию в зависимости от мобильного технического средства (типа мобильного технического средства) мер по идентификации и аутентификации, управлению доступом, ограничению программной среды, защите машинных носителей информации, регистрации событий безопасности, антивирусной защите, контролю (анализу) защищенности, обеспечению целостности;
- уничтожение съемных машинных носителей информации, которые не подлежат очистке;
- выборочные проверки съемных машинных носителей информации (на предмет их наличия) и хранящейся на них информации (например, на предмет отсутствия информации, не соответствующей маркировке носителя информации);
- запрет возможности автоматического запуска (без команды пользователя) в ИС программного обеспечения на съемных машинных носителей информации;
- контроль использования в ИС съемных машинных носителей информации.

4.3 Контроль использования мобильных технических средств в ИС включает:

– использование в составе ИС для доступа к объектам доступа мобильных технических средств (служебных мобильных технических средств), в которых реализованы меры защиты информации в соответствии с требованиями по защите информации;

– ограничение на использование мобильных технических средств в соответствии с задачами (функциями) ИС, для решения которых использование таких средств необходимо, и предоставление доступа с использованием мобильных технических средств;

– мониторинг и контроль применения мобильных технических средств на предмет выявления несанкционированного использования мобильных технических средств для доступа к объектам доступа ИС.

5. Ответственность при организации защиты машинных носителей информации

5.1. Ответственность по защите и учету машинных носителей информации в соответствии с требованиями настоящей Инструкции возлагается на администратора безопасности ИС.

5.2. Пользователи несут ответственность за исполнение правил и требований, изложенным в настоящей Инструкции.

УТВЕРЖДЕНА
приказом ГКУ НСО ЦСПН Северного района
от «30» 04 2025 г. № 157

Инструкция по регистрации событий безопасности

1. Общие положения

1.1. Настоящая Инструкция разработана в целях реализации мер по регистрации событий безопасности, по обеспечению сбора, записи, хранения и защиты информации о событиях безопасности в информационных системах (далее – ИС) ГКУ НСО ЦСПН Северного района, а также возможности просмотра и анализа информации о таких событиях и реагирования на них.

1.2. Настоящая Инструкция определяет:

– порядок составления и утверждения перечня событий безопасности, подлежащих регистрации и сроки их хранения;

– порядок определения состава и содержания информации о событиях безопасности, подлежащих регистрации;

– порядок сбора, записи и хранения информации о событиях безопасности в течение определённого времени хранения;

– порядок мониторинга (просмотра, анализа) результатов регистрации событий безопасности и реагирования на них;

– порядок защиты информации о событиях безопасности.

2 Перечень событий безопасности подлежащих регистрации

2.1. Перечень событий безопасности, подлежащих регистрации в ИС, составляет администратор безопасности ИС.

2.2 Администратор безопасности ИС обеспечивает средствами защиты информации, установленными в ИС регистрацию следующих событий:

– вход (выход), а также попытки входа субъектов доступа в ИС 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 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.

2.3 Администратор безопасности ИС отслеживает, чтобы записи событий содержали в себе:

– дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная);
– идентификатор субъекта доступа (устройства);
– спецификация защищаемого файла (логическое имя, тип);
– используемый интерфейс доступа;
– и (или) иную информацию о попытках доступа к информационным ресурсам ИС.

3 Порядок сбора, записи, хранения и мониторинга информации о событиях безопасности

3.1. Настройку журналов регистрации событий информационной безопасности в средствах защиты информации ИС осуществляет администратор безопасности ИС.

3.2. Сведения о настройке средств защиты информации в рамках сбора и регистрации событий информационной безопасности в ИС представлены в разделе «Настройка средств защиты информации» инструкции администратора безопасности ИС.

3.3. Администратор безопасности ИС должен **не реже 1 раза в неделю** просматривать журналы регистрации событий безопасности на предмет возможны инцидентов безопасности.

3.4. В случае выявления признаков инцидентов безопасности администратором безопасности ИС осуществляется планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности в соответствии с Инструкцией по выявлению инцидентов и реагированию на них.

3.5. Настройки журналов регистрации событий информационной безопасности должны обеспечивать запись информации о поступающих событиях безопасности без переполнения памяти **в течение 1 месяца**.

3.6. Информация о событиях безопасности в ИС, не подлежащая автоматической регистрации (нерегистрируемые программно-аппаратные сбои и неисправности, нарушения организационно-правового плана) должна фиксироваться администратором безопасности ИС при её обнаружении в журнале событий безопасности самостоятельно.

3.7. Доступ к записям аудита и функциям управления механизмами регистрации (аудита) предоставляется только администратору безопасности ИС.

3.8 В ИС должно осуществляться генерирование надежных меток времени и (или) синхронизация системного времени.

3.9 Получение меток времени, включающих дату и время, используемых при генерации записей регистрации (аудита) событий безопасности в ИС достигается посредством применения внутренних системных часов ИС.

4. Ответственность при управлении событиями информационной безопасности

4.1. Ответственность при управлении событиями информационной безопасности в соответствии с требованиями настоящей Инструкции возлагается на администратора безопасности ИС.

4.2. Ответственность за соблюдение требований настоящей Инструкции возлагается на всех сотрудников, эксплуатирующих ИС.

УТВЕРЖДЕНА
приказом ГКУ НСО ЦСПН Северного района
от «30» 04 2025 г. № 157

Инструкция по организации антивирусной защиты

1. Общие положения

1.1. Настоящая Инструкция разработана в целях реализации мер по антивирусной защите, которые должны обеспечивать обнаружение в информационных системах (далее – ИС) ГКУ НСО ЦСПН Северного района компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

1.2. Контроль за исполнением настоящей Инструкции осуществляет администратор безопасности ИС.

1.3. Права на администрирование средств защиты информации также имеют сотрудники государственного казенного учреждения Новосибирской области «Соцтехсервис», согласно устава от 12.10.2022 № 1378, и сотрудники государственного бюджетного учреждения Новосибирской области «Центр защиты информации Новосибирской области».

2. Порядок организации антивирусной защиты

2.1. Для антивирусной защиты ИС допускаются к использованию только сертифицированные ФСТЭК России лицензионные антивирусные средства.

2.2. Права по администрированию средств антивирусной защиты предоставлены только администратору безопасности ИС.

2.3. При загрузке, открытии или исполнении объектов (файлов) из внешних источников средствами антивирусной защиты проводится автоматическая проверка объектов (файлов).

2.4. Расширенный антивирусный контроль проводится администратором безопасности ИС при необходимости в случае заражения или подозрения в заражении ИС вирусной программой.

3. Организация обновления сигнатурных баз антивирусной защиты

3.1. Для обновления антивирусных баз в ИС программного изделия «Kaspersky Endpoint Security для Windows» и «Kaspersky Endpoint Security для Linux» используются серверы компании Лаборатория Касперского.

3.2. Настройки обновления вирусных баз программного изделия «Kaspersky Endpoint Security для Windows» и «Kaspersky Endpoint Security для

Linux», производятся через Центр управления Kaspersky, который развернут либо на ресурсах ГКУ НСО ЦСПН Северного района, либо на ресурсах государственного бюджетного учреждения Новосибирской области «Центр защиты информации Новосибирской области».

3.3. Параметры настройки обновления антивирусных баз программного изделия «Kaspersky Endpoint Security для Windows» и «Kaspersky Endpoint Security для Linux» в ИС определяются и устанавливаются государственным бюджетным учреждением Новосибирской области «Центр защиты информации Новосибирской области».

4. Порядок проведения антивирусного контроля

4.1. При установке/обновлении программного обеспечения на ИС установочные пакеты проверяются администратором безопасности ИС на наличие вирусов.

4.2. При загрузке компьютера средствами антивирусной защиты проводится антивирусный контроль в автоматическом режиме.

4.3. При подключении внешнего носителя информации средствами антивирусной защиты проводится антивирусный контроль подключенного носителя в автоматическом режиме.

4.4. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов, пользователю необходимо:

- приостановить работу с файлами документов:
- дождаться завершения антивирусной проверки;
- в случае успешного устранения угрозы (по отчету антивирусной программы) повторно запустить проверку объекта на вирусы;
- в случае невозможности автоматического устранения угрозы (по отчету антивирусной программы) немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности ИС, не производить никаких действий на ИС до прихода администратора безопасности ИС (не останавливать работу антивирусных средств, не отключать внешний носитель, не закрывать информационные сообщения и т.д.).

4.5. При получении сообщения пользователя об обнаружении вируса в случае невозможности лечения зараженных файлов администратор безопасности обязан:

- запретить использование внешнего носителя (если зараженные файлы находились на подключенном носителе) либо временно запретить использовать ИС;
- определить возможный источник заражения;
- в случае подозрения на заражение из внешних источников принять меры к нейтрализации возможности повторного заражения из этих источников;

– при необходимости проверить сохранность конфиденциальной информации при повреждении обеспечить их восстановление из резервных копий.

5. Ответственность при организации антивирусной защиты

5.1. Ответственность за организацию антивирусной защиты ИС в соответствии с требованиями настоящей Инструкции возлагается на администратора безопасности ИС.

5.2. Ответственность за соблюдение требований настоящей Инструкции возлагается на всех сотрудников, эксплуатирующих ИС.

УТВЕРЖДЕНА
приказом ГКУ НСО ЦСПН Северного района
от «30» 04 2025 г. № 157

Инструкция по организации системы обнаружения вторжений

1. Общие положения

1.1. Настоящая Инструкция разработана в целях реализации мер по обнаружению вторжений, которые должны обеспечивать обнаружение (предотвращение) вторжений (компьютерных атак), направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней, в информационных системах (далее – ИС) ГКУ НСО ЦСПН Северного района.

1.2. Контроль за исполнением настоящей Инструкции осуществляет администратор безопасности ИС.

1.3. Права на администрирование средств защиты информации также имеют сотрудники государственного казенного учреждения Новосибирской области «Соцтехсервис», согласно устава от 12.10.2022 № 1378, и сотрудники государственного бюджетного учреждения Новосибирской области «Центр защиты информации Новосибирской области».

2. Обнаружение вторжений

2.1. В ИС обеспечивается обнаружение вторжений, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней, с использованием систем обнаружения вторжений хоста, а именно с помощью следующих средств:

- Система обнаружения и предотвращения вторжений Dallas Lock;
- Система обнаружения вторжений ViPNet EndPoint Protection.

2.2. Применяемые системы обнаружения вторжений имеют компоненты регистрации событий безопасности (датчики), компоненты анализа событий безопасности и распознавания компьютерных атак (анализаторы) и базу решающих правил, содержащую информацию о характерных признаках компьютерных атак.

2.3. Права по администрированию системы обнаружения вторжений предоставлены только администратору безопасности ИС.

2.4. Факт сетевой атаки является инцидентом информационной безопасности. Обработка данного инцидента осуществляется согласно Инструкции по выявлению инцидентов и реагированию на них.

2.5. В качестве меры по реагированию может быть предпринято изменение конфигурации средств защиты информации (например, межсетевого экрана) с целью блокирования трафика от источника атаки или блокирования сетевых пакетов, в которых были обнаружены сигнатуры атак.

3. Обновление базы данных признаков вредоносных компьютерных программ

3.1. Должно обеспечиваться обновление базы решающих правил системы обнаружения вторжений из доверенных источников и установку обновлений базы решающих правил.

3.2. Контроль за загрузкой обновлений и корректностью их установки осуществляет администратор безопасности ИС.

4. Ответственность при организации системы обнаружения вторжений

4.1. Ответственность за организацию системы обнаружения вторжений в ИС в соответствии с требованиями настоящей Инструкции возлагается на администратора безопасности ИС.

4.2. Ответственность за соблюдение требований настоящей Инструкции возлагается на всех сотрудников, эксплуатирующих ИС.

УТВЕРЖДЕНА
приказом ГКУ НСО ЦСПН Северного района
от «30» 04 2025 г. № 157

Инструкция по контролю (анализу) защищенности персональных данных

1. Общие положения

1.1. Настоящая Инструкция разработана в целях реализации мер по контролю (анализу) защищенности информации в информационных системах (далее – ИС) ГКУ НСО ЦСПН Северного района, которые должны обеспечивать контроль уровня защищенности информации, обрабатываемых в ИС, путем проведения систематических мероприятий по анализу защищенности ИС и тестированию работоспособности системы защиты информации ИС.

1.2. Настоящая Инструкция предназначена для обеспечения защиты информации, обрабатываемой в ИС, при функционировании ИС и определяет порядок действий администратора безопасности ИС при эксплуатации ИС.

1.3. Мероприятия по контролю защищенности информации в ИС и тестированию работоспособности системы защиты информации проводятся в пределах своих полномочий администратором безопасности ИС, системным администратором ИС и лицами, ответственными за безопасность персональных данных в ИС, содержащих персональные данные, используемые в ГКУ НСО ЦСПН (наименование) района.

2. Выявление, анализ уязвимостей ИС и оперативное устранение вновь выявленных уязвимостей

2.1. В ИС при выявлении (поиске), анализе и устранении уязвимостей проводятся:

– выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении средств защиты информации, правильностью установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректностью работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;

– разработка по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению;

– анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации;

– устранение выявленных уязвимостей, в том числе путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств;

– информирование должностных лиц Министерства (пользователей, администраторов) о результатах поиска уязвимостей и оценки достаточности реализованных мер защиты информации.

2.2. Выявление (поиск), анализ и устранение уязвимостей проводится на этапах создания и эксплуатации ИС. На этапе эксплуатации поиск и анализ уязвимостей проводится не реже одного раза в год. При этом в обязательном порядке для критических уязвимостей проводится поиск и анализ уязвимостей в случае опубликования в общедоступных источниках информации о новых уязвимостях в средствах защиты информации, технических средствах и программном обеспечении, применяемом в ИС.

2.3. Ответственное лицо за обеспечение безопасности персональных данных в информационных системах, содержащих персональные данные, используемые в ГКУ НСО ЦСПН Северного района или администратор безопасности ИС согласно полученных сведений оформляют сведения о выявленных уязвимостях в ИС по форме, представленной в приложении № 1 к настоящей Инструкции и администратор безопасности ИС производит действия по устранению критических уязвимостей с учетом, представленных на сайте ФСТЭК России (https://bdu.fstec.ru/vul) рекомендаций по их устранению (рисунок 1).

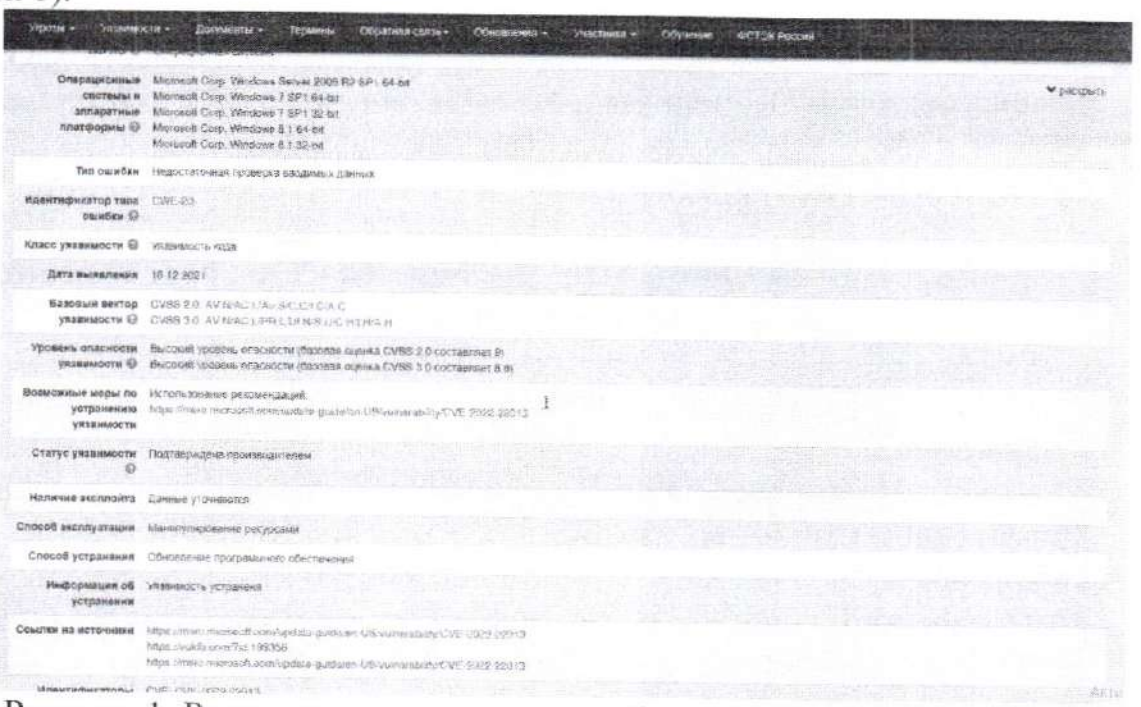

Рисунок 1. Расположение рекомендаций по устранению уязвимостей.

2.4. Необходимо обеспечить устранение критических уязвимостей в прикладном и системном программном обеспечении ИС из представленных на сайте ФСТЭК России (https://bdu.fstec.ru/vul) уязвимостей.

2.5. В случае невозможности устранения выявленных уязвимостей путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств необходимо предпринять действия (настройки средств защиты

информации, изменение режима и порядка использования ИС), направленные на устранение возможности использования выявленных уязвимостей.

2.6. Контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации ИС производится администратором безопасности ИС в соответствии с Инструкцией по ограничению программной среды.

2.7. При контроле состава технических средств, программного обеспечения и средств защиты информации ИС администратором безопасности ИС осуществляется:

– контроль соответствия состава технических средств, программного обеспечения и средств защиты информации приведенному в техническом паспорте ИС с целью поддержания актуальной конфигурации ИС и принятие мер, направленных на устранение выявленных недостатков;

– контроль состава технических средств, программного обеспечения и средств защиты информации ИС на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков;

– контроль выполнения условий и сроков действия сертификатов средств защиты информации ИС соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;

– исключение (восстановление) из состава ИС несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

2.8. Работы из пункта 2.7 проводятся администратором безопасности ИС проводятся администратором безопасности **не реже 1 раза в квартал.**

2.9. При контроле работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации ИС осуществляется:

– контроль работоспособности (неотключения) программного обеспечения и средств защиты информации; проверка правильности функционирования программного обеспечения и средств защиты информации ИС;

– контроль соответствия настроек программного обеспечения и средств защиты информации ИС параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации ИС;

– восстановление работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации ИС, в том числе с использованием резервных копий и (или) дистрибутивов (в случае необходимости и выявлении нарушения функционирования).

2.10. Работы из пункта 2.9 проводятся администратором безопасности ИС **не реже 1 раза в квартал.**

2.11. При контроле правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил

разграничения доступом, полномочий пользователей в ИС ГКУ НСО ЦСПН Северного района:

- контроль правил генерации и смены паролей пользователей;
- контроль заведения и удаления учетных записей пользователей;
- контроль реализации правил разграничения доступом;
- контроль реализации полномочий пользователей;
- контроль наличия документов, подтверждающих разрешение изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей, предусмотренных организационно-распорядительными документами по защите информации в ГКУ НСО ЦСПН Северного района;
- устранение нарушений, связанных с генерацией и сменой паролей пользователей, заведением и удалением учетных записей пользователей, реализацией правил разграничения доступом, установлением полномочий пользователей.

2.12. Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИС ГКУ НСО ЦСПН Северного района проводится в пределах своей компетенции администратором безопасности ИС, системным администратор ИС и лицами, ответственными за безопасность персональных данных в информационных системах, содержащих персональные данные, используемые в ГКУ НСО ЦСПН Северного района, не реже одного раза в 2 года.

2.13. Серверные сегменты государственных информационных систем Новосибирской области, размещенные в центре обработки данных Правительства Новосибирской области, сканируются и обслуживаются ГБУ НСО «ЦЗИ НСО». В случае выявленных уязвимостей и необходимости проведения дополнительных работ ГБУ НСО «ЦЗИ НСО» уведомляет об этом ГКУ НСО ЦСПН Северного района.

3. Ответственность при контроле (анализе) защищенности информации

3.1. Ответственность при контроле (анализе) защищенности информации в соответствии с требованиями настоящей Инструкции возлагается на администратора безопасности ИС.

3.2. Ответственность за соблюдение требований настоящей Инструкции возлагается на всех сотрудников, эксплуатирующих ИС.

Приложение № 1 к Инструкции
по контролю (анализу) защищенности
персональных данных

Форма

Акт о проведении анализа уязвимости с использованием средств контроля эффективности защиты информации от несанкционированного доступа, обрабатываемой в _____

1. Объект информатизации: _____.
2. ИС в своем составе _____ АРМ, _____ серверов.
3. Вид работ: полный.
4. Цель работ: обнаружение уязвимостей средств защиты информации, технических средств и программного обеспечения.
5. Метод проведения работы: инструментальный.
6. Средства контроля: _____.
(наименование и сертификат ФСТЭК России)
7. Контроль осуществлен с АРМ (кабинет № _____) из состава ЛВС (IP-адрес узла:_____).

Определение доступности улов из числа заявленных к проверке приведено в таблице № 1:

Таблица № 1

IP-адрес узла	Расположение	Назначение узла

8. Результаты контроля:

В ходе сканирования системы на _____ узла выявлено_____ уязвимостей. Наименование, уровень критичности, описание, способ устранения приведен в таблице № 2:

Таблица 2

№ п/п	Наименование уязвимости	Количество уязвимостей	Уровень критичности	Описание	Способ устранения

9. Вывод: в ходе сканирования узлов, проверка показала, что выявленные уязвимости влияют/не влияют на работу системы _____.

При проведении работ присутствовал:
(должность) ФИО
(должность) ФИО
Дата проведения работ «_____» _____ 20_____ года.

УТВЕРЖДЕНА
приказом ГКУ НСО ЦСПН Северного района
от «30» 04 2025 г. № 157

Инструкция по обеспечению целостности информации

1. Общие положения

1.1. Настоящая Инструкция разработана в целях реализации мер по обеспечению целостности информации в информационных системах (далее – ИС) ГКУ НСО ЦСПН Северного района, которые должны обеспечивать:

– обнаружение фактов несанкционированного нарушения целостности ИС и содержащейся в ней информации, а также возможность восстановления ИС и содержащейся в ней информации.

– авторизованный доступ пользователей, имеющих права по такому доступу, к информации, содержащейся в ИС, в штатном режиме функционирования ИС.

1.2. Настоящая Инструкция предназначена для обеспечения защиты информации, обрабатываемой в ИС, при функционировании ИС и определяет порядок действий администратора безопасности ИС при эксплуатации ИС.

2. Действия администратора безопасности ИС по контролю целостности программного обеспечения, включая программное обеспечение средств защиты информации

2.1. Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации (далее – ПО), должен предусматривать:

– контроль целостности ПО, включая его обновления, по наличию имен (идентификаторов) и (или) по контрольным суммам компонентов средств защиты информации в процессе загрузки и (или) динамически в процессе работы ИС;

– контроль целостности компонентов ПО (за исключением средств защиты информации), определяемого администратором безопасности ИС исходя из возможности реализации угроз безопасности информации, по наличию имен (идентификаторов) компонентов ПО и (или) по контрольным суммам в процессе загрузки и (или) динамически в процессе работы ИС;

– контроль применения средств разработки и отладки программ в составе ПО ИС;

– тестирование с периодичностью установленной администратором безопасности ИС функций безопасности средств защиты информации, в том числе с помощью тест-программ, имитирующих попытки несанкционированного доступа, и (или) специальных программных средств, в соответствии с АН3.1 и АН3.2;

– обеспечение физической защиты технических средств ИС в соответствии с ЗТС.2 и ЗТС.3.

2.2. В случае если функциональные возможности ИС должны предусматривать применение в составе ее ПО средств разработки и отладки программ, администратором безопасности ИС обеспечивается выполнение процедур контроля целостности ПО после завершения каждого процесса функционирования средств разработки и отладки программ.

2.3. Настройку механизма целостности в средствах защиты информации производить:

– для средства защиты информации от несанкционированного доступа Dallas Lock 8.0-К согласно таблицы 5 «Рекомендаций по настройке для соответствия требованиям о защите информации Dallas Lock 8.0-К» и разделом 9 Руководства по эксплуатации RU.48957919.501410-01 92;

– для ОС Альт 8 СП согласно разделам 3, 11 Руководства администратора ЛКНВ.11100-01 90 02. Операционная система АЛЬТ 8 СП (ОС Альт 8 СП).

3. Действия администратора безопасности ИС по обеспечению возможности восстановления ПО при возникновении нештатных ситуаций

3.1. Возможность восстановления ПО при возникновении нештатных ситуаций предусматривает следующие действия администратора безопасности ИС:

– восстановление ПО из резервных копий (дистрибутивов) ПО;

– восстановление и проверка работоспособности системы защиты информации, обеспечивающие необходимый уровень защищенности информации в ИС;

– возврат ИС в начальное состояние (до возникновения нештатной ситуации), обеспечивающее ее штатное функционирование, или восстановление отдельных функциональных возможностей ИС, позволяющих решать задачи по обработке информации.

3.2. Администратор безопасности ИС совместно с государственным бюджетным учреждением Новосибирской области «Центр защиты информации Новосибирской области» должен обеспечивать хранение дистрибутивов в заранее определенном месте недоступным для несанкционированного доступа лиц, не имеющих прав доступа для выполнения ими их служебных обязанностей.

3.3. В случае обновления дистрибутивов с личных кабинетов производителя/сайтов/регуляторов администратор безопасности ИС должен обеспечить своевременную запись обновленных дистрибутивов на оптический носитель или специальной выделенный для данных целей съемный машинный носитель.

4. Ответственность при обеспечении целостности информации в ИС

4.1. Ответственность при обеспечении целостности и доступности информации в соответствии с требованиями настоящей Инструкции возлагается на администратора безопасности ИС.

4.2. Ответственность за соблюдение требований настоящей Инструкции возлагается на всех сотрудников, эксплуатирующих ИС.

УТВЕРЖДЕНА
приказом ГКУ НСО ЦСПН Северного района
от «30» 04 2025 г.№ 157

Инструкция по обеспечению доступности персональных данных

1. Общие положения

1.1. Настоящая инструкция разработана в целях реализации мер по обеспечению авторизованного доступа пользователей, имеющих права по такому доступу, к информации, содержащейся в информационных системах (далее – ИС) ГКУ НСО ЦСПН Северного района, в штатном режиме функционирования ИС.

1.2. Назначение и область применения.

1.2.1. Данная инструкция определяет порядок обеспечения доступности в ИС.

1.2.2. Требования настоящей инструкции реализуются средствами ИС или сертифицированными средствами защиты информации с применением организационных мер защиты информации.

1.2.3. Серверный сегмент государственных информационных систем Новосибирской области, размещенный в центре обработки данных Новосибирской области, относится к зоне ответственности государственного бюджетного учреждения Новосибирской области «Центр защиты информации Новосибирской области» (далее – ГБУ НСО «ЦЗИ НСО») и государственного бюджетного учреждения Новосибирской области «Центр информационных технологий Новосибирской области» (далее – ГБУ НСО «ЦИТ НСО») каждого в своей зоне ответственного согласно определенных их функциональных обязанностей.

1.3. Права на администрирование средств защиты информации также имеют сотрудники государственного казенного учреждения Новосибирской области «Соцтехсервис», согласно устава от 12.10.2022 № 1378, и сотрудники государственного бюджетного учреждения Новосибирской области «Центр защиты информации Новосибирской области».

2. Действия администратора безопасности ИС по периодическому резервному копированию информации на резервные машинные носители

3.

2.1. В ИС должно обеспечиваться периодическое резервное копирование информации на резервные машинные носители информации, предусматривающее:

– резервное копирование информации на резервные машинные носители информации при изменении конфигурации системы и во время технологических пауз;

– разработку перечня информации, подлежащих периодическому резервному копированию на резервные машинные носители информации;

– регистрацию событий, связанных с резервным копированием информации на резервные машинные носители информации;

– принятие мер для защиты резервируемых информации, обеспечивающих ее доступность, целостность и конфиденциальность.

2.2. В ИС должна осуществляться периодическая проверка работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий.

2.3. Резервное копирование информации серверных сегментов, а также средств защиты информации относится к зоне ответственности ГБУ НСО «ЦЗИ НСО» и ГБУ НСО «ЦИТ НСО».

2.4. Периодичность организации работ по резервному копированию информации устанавливается в обязательном порядке: внутренними документами ГБУ НСО «ЦЗИ НСО» и ГБУ НСО «ЦИТ НСО».

2.5. Администратор безопасности ИС ГКУ НСО ЦСПН Северного района проводит работы по резервному копированию средств защиты информации и прочих конфигурационных файлов, входящих в его зону ответственности.

2.6. Пользователи ИС самостоятельно могу производить работы по сохранению необходимой информации при производственной необходимости на учетные съемные носители информации.

3. Действия администратора безопасности ИС по обеспечению возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала

3.1. В ИС должна быть обеспечена возможность восстановления информации с резервных машинных носителей информации (резервных копий).

3.2. Восстановление информации в ГКУ НСО ЦСПН Северного района с резервных машинных носителей информации (резервных копий) производится администратором безопасности ИС при выявленной производственной необходимости и(или) после устранения компьютерных инцидентов.

4. Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование

4.1. В ИС ГКУ НСО ЦСПН Северного района должен осуществляться контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование.

4.2. Контроль безотказного функционирования проводится в отношении серверного и телекоммуникационного оборудования, каналов связи, средств обеспечения функционирования ИС путем периодической проверки работоспособности в соответствии с эксплуатационной документацией (в том числе путем посылки тестовых сообщений и принятия «ответов», визуального контроля, контроля трафика, контроля «поведения» системы или иными методами).

4.3. При обнаружении отказов функционирования осуществляется их локализация и принятие мер по восстановлению отказавших средств в соответствии с настоящей Инструкцией, их тестирование в соответствии с эксплуатационной документацией, а также регистрация событий, связанных с отказами функционирования.

5. Ответственность при обеспечении доступности информации в ИС

5.1. Ответственность при обеспечении доступности информации в соответствии с требованиями настоящей Инструкции возлагается на администратора безопасности ИС.

5.2. Ответственность за соблюдение требований настоящей Инструкции возлагается на всех сотрудников, эксплуатирующих ИС.

УТВЕРЖДЕНА
приказом ГКУ НСО ЦСПН Северного района
от «30» 04 2025 г. № 157

Инструкция по защите технических средств

1. Общие положения

1.1. Настоящая Инструкция разработана в целях реализации мер по защите технических средств, которые должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию в информационных системах (далее – ИС) ГКУ НСО ЦСПН Северного района, средствам, обеспечивающим функционирование ИС, и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленных в виде информативных электрических сигналов и физических полей.

1.2. Контроль за исполнением настоящей Инструкции осуществляет администратор безопасности ИС.

2. Определение границ контролируемой зоны

2.1. Технические средства ИС должны быть размещены внутри контролируемой зоны.

2.2. Границы контролируемой зоны ИС определены соответствующим документом ГКУ НСО ЦСПН Северного района.

2.3. Перемещение стационарного оборудования ИС за границу контролируемой зоны без согласования с администратором безопасности ИС не допускается.

3. Правила контроля физического доступа в контролируемую зону.

3.1. На период обработки защищаемой информации в помещениях, где размещено оборудование ИС, могут находиться только пользователи, допущенные в помещения.

3.2. Нахождение в помещениях контролируемой зоны других лиц (например, для проведения необходимых профилактических или ремонтных работ, посетителей) возможно только в присутствии пользователя ИС.

3.3. Контроль физического доступа в помещение контролируемой зоны осуществляет администратор безопасности ИС.

4. Правила размещения устройств вывода информации.

4.1. При размещении в контролируемой зоне технических средств отображения информации должен быть исключен несанкционированный просмотр выводимой на них информации.

4.2. Выполнение требований к размещению устройств вывода информации в контролируемой зоне проверяет администратор безопасности ИС.

5. Защита каналов связи, выходящих за пределы контролируемой зоны.

5.1. Расположение указанных технических средств и физический доступ к ним контролирует администратор безопасности ИС.

6. Порядок применения специальных защитных знаков в ИС

6.1. Установку специальных защитных знаков на ИС осуществляет администратор безопасности ИС в соответствии со своей компетенцией и согласно их описанию, изложенному в Приложении № 2 к настоящей Инструкции.

6.2. Установка специальных защитных знаков производится путем наклеивания специальных защитных знаков на поверхность технического средства ИС. Место установки специальных защитных знаков должно исключать несанкционированный доступ к защищаемому объекту без изменения целостности специальных защитных знаков.

6.3. Установке специальных защитных знаков на объект защиты ИС предшествует проставление на специальный защитный знак даты установки, номера специального защитного знака и росписи ответственного за установку лица.

6.4. Санкционированное вскрытие установленного специального защитного знака на объекте защиты ИС может осуществлять администратор безопасности ИС с целью модернизации и (или) ремонта объекта защиты.

6.5. Вскрытие установленного специального защитного знака на объекте защиты ИС предусматривает составление акта вскрытия специального защитного знака по форме, изложенной в Приложении № 1 к настоящей Инструкции.

6.6. В акте отражаются:

– фамилия, имя, отчество работников ГКУ НСО ЦСПН Северного района, осуществивших вскрытие специального защитного знака;

– причины вскрытия специального защитного знака;

– состояние защитного знака до вскрытия.

6.7. В случае обнаружения нарушения целостности или возникновения сомнения в подлинности специального защитного знака, установленного на

объекте защиты ИС, незамедлительно информируется администратор безопасности ИС.

6.8. По факту обнаружения нарушения целостности или возникновения сомнения в подлинности специального защитного знака, установленного на объекте защиты ИС, проводится служебная проверка в порядке и в сроки, установленные в ГКУ НСО ЦСПН Северного района.

6.9. Результаты служебной проверки комиссия оформляется актом служебной проверки.

6.10. Образец и описание специального защитного знака приведены в Приложении № 4 к настоящей Инструкции.

6.11. Номер специального защитного знака фиксируется в соответствующем журнале по форме, представленной в Приложении № 3 к настоящей Инструкции.

7. Ответственность при организации защиты технических средств, входящих в состав ИС

7.1. Ответственность за защиту технических средств, входящих в состав ИС, в соответствии с требованиями настоящей Инструкции возлагается на администратора безопасности ИС.

7.2. Ответственность за соблюдение требований настоящей Инструкции возлагается на всех сотрудников, эксплуатирующих ИС.

Приложение № 1
к инструкции по защите технических средств

ФОРМА

Акт № _____ от _____ 20___года
вскрытия специального защитного знака в ИС ГКУ НСО ЦСПН Северного района

Мы,_____
(фамилия, имя, отчество работника подразделения организации, администратора безопасности ИС)

_____

произвели _____ 20_____года вскрытие технических средств информационных систем ГКУ НСО ЦСПН Северного района _____.
(наименование ИС)

ГКУ НСО ЦСПН Северного района, опечатанной специальным защитным знаком с целью _____.
(цель вскрытия)

Установлено:

1. Целостность и подлинность специального защитного знака соответствует Инструкции по защите технических средств, входящих в состав ИС ГКУ НСО ЦСПН Северного района.

2. В ходе вскрытия технических средств ИС ГКУ НСО ЦСПН Северного района уничтожен специальный защитный знак под регистрационным номером № _____.
(номер СЗЗ)

3. На вскрытый элемент технических средств ИС ГКУ НСО ЦСПН Северного района по завершению работ установлен новый специальный защитный знак установленного образца № _____.
(номер СЗЗ)

.

_____
(подпись, инициалы, фамилия)

_____
(подпись, инициалы, фамилия)

Приложение № 2
к инструкции по защите технических средств

ОПИСАНИЕ
специального защитного знака

1. Специальный защитный знак (разработанный) реализован в виде полосы бумаги размером:

– ширина – 14 см;
– длина – 6 см.

ГКУ НСО ЦСПН Северного района

СЗЗ № _____
О П Е Ч А Т А Н О

Вскрывать в соответствии с инструкцией

_____ (дата)

_____ (подпись)

номер специального защитного знака. В центре специального защитного знака, непосредственно под порядковым номером специального защитного знака, представлена надпись: ОПЕЧАТАНО.

В центральной части поля специального защитного знака отведено место для нанесения даты установки и подписи лица, установившего специальный защитный знак.

2. Стандартный специальный защитный знак (приобретенный):

В центре специального защитного знака располагается надпись: ОПЛОМБИРОВАНО НЕ ВСКРЫВАТЬ. Под ней идет соответствующее сообщение, содержащее сведения, что факт вскрытия будет отображен на специальном защитном знаке.

Под соответствующими надписями ставится дата и указывается фамилия, имя и отчество лица, ответственного за установку на объекте защиты специального защитного знака.

В левом поле специального защитного знака указывается порядковый номер специального защитного знака.

В правом поле специального защитного знака может быть указан тип «Тип-ПС».

Приложение № 3
к инструкции по защите технических средств

ФОРМА

Журнал учета специальных защитных знаков
ГКУ НСО ЦСПН Северного района

№ п/п	Номер СЗЗ	Номер кабинета	Место установки (инвентарный номер АРМ)	Дата и подпись лица, установившего СЗЗ	Основание для снятия СЗЗ, дата и подпись лица, снявшего СЗЗ	Отметка об уничтожении СЗЗ

УТВЕРЖДЕНА
приказом ГКУ НСО ЦСПН Северного района
от «30» 04 2025 г. № 157

Инструкция по выявлению компьютерных инцидентов и реагированию на них

1. Общие положения

1.1. Настоящая Инструкция разработана в целях реализации мер по выявлению компьютерных инцидентов и реагирование на них, которые должны обеспечивать обнаружение в информационных системах (далее – ИС) ГКУ НСО ЦСПН Северного района.

1.2. Контроль за исполнением настоящей Инструкции осуществляет администратор безопасности ИС.

1.3. Серверный сегмент государственных информационных систем Новосибирской области, размещенных в центре обработки данных Новосибирской области, относится к зоне ответственности государственного бюджетного учреждения Новосибирской области «Центр защиты информации Новосибирской области» (ГБУ НСО «ЦЗИ НСО») и государственного бюджетного учреждения Новосибирской области «Центр информационных технологий Новосибирской области» (ГБУ НСО «ЦИТ НСО») каждого в своей зоне ответственного согласно определенных их функциональных обязанностей. В случае выявления инцидентов на стороне ГКУ НСО ЦСПН Северного района вышеуказанные организации обязуются уведомить ГКУ НСО ЦСПН Северного района и при необходимости принять участие в проведении расследований по результатам.

1.4. Анализ инцидентов в ГКУ НСО ЦСПН Северного района производится с применением следующих средств:

- Система обнаружения и предотвращения вторжений и журналы Dallas Lock;
- Система обнаружения вторжений ViPNet EndPoint Protection;
- Журналы ОС Альт 8 СП;
- Журналы Kaspersky Endpoint Security для Windows и Kaspersky Endpoint Security для Linux.

2. Категории инцидентов информационной безопасности

К инцидентам информационной безопасности в ИС (далее – инциденты ИБ) относятся:

- заражение вредоносным программным обеспечением;
- распространение вредоносного программного обеспечения;
- нарушение или замедление работы ИС;

– несанкционированный доступ в систему;
– нарушение целостности информации, обрабатываемой в ИС.

Инциденты ИБ подразделяются на категории, определенные в таблице 1.

Таблица 1 – Сведения о категориях инцидента ИБ

№	Наименование категории	Описание категории
1.	Атаки на веб-сервисы	Сценарии, связанные с атаками на веб-сервисы
2.	Контроль активности процессов\служб	Сценарии, связанные с работой служб\сервисов\приложений и т.д.
3.	Контроль антивирусной защиты	Сценарии, связанные с обнаружением вирусов средствами антивирусной защиты и их работоспособности
4.	Контроль утечек	Сценарии, связанные с фактами утечек информации
5.	Контроль изменений - конфигурация	Сценарии, связанные с фактами изменения конфигурации систем и сервисов
6.	Контроль изменений - критичные файлы	Сценарии, связанные с фактами изменения и доступа к файлам\каталогам
7.	Контроль сетевого доступа	Сценарии, связанные с сетевыми средствами защиты информации (межсетевые экраны, системы обнаружения вторжений и т.д.)
8.	Контроль удаленного доступа (VPN)	Сценарии, связанные с работой VPN-решений
9.	Сетевые атаки	Сценарии, связанные с различными сетевыми атаками на инфраструктуру
10.	Контроль идентификации и аутентификации	Сценарии, связанные с идентификацией и аутентификацией пользователей в системах
11.	Контроль управления доступа	Сценарии, связанные с фактами изменения\удаления\создания учетных записей
12.	Контроль уязвимостей	Сценарии, связанные с попытками эксплуатации уязвимостей
13.	Другое	Все, что не предусмотрено предыдущими категориями

3. Правила и процедуры мониторинга инцидентов ИБ

3.1. В рамках мониторинга событий администратор безопасности ИС должен осуществлять:

а) наблюдение за событиями ИБ, в т.ч. наблюдение и оценка статистической информации:

– возникновение событий ИБ с высокой важностью;
– возникновение определенных категорий/типов событий ИБ;
– возникновение событий ИБ на определенных сегментах ИС;
– возникновение событий ИБ в определенные промежутки времени;
– отсутствие событий ИБ от источников событий ИБ.

б) выявление отклонений как в большую, так и в меньшую сторону (аномалий), а также достижений пороговых значений и/или возникновений отдельно взятых событий ИБ;

в) формирование уведомлений.

3.2. Должно осуществляться реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти.

3.3. Реагирование на сбои при регистрации событий безопасности должно предусматривать:

– предупреждение (сигнализация, индикация) администратора безопасности ИС о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности;

– реагирование на сбои при регистрации событий безопасности путем изменения администратором безопасности ИС параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов систем, запись поверх устаревших хранимых записей событий безопасности.

3.4. Защита информации о событиях безопасности должна обеспечиваться применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования и в том числе включает защиту средств ведения регистрации и настроек механизмов регистрации событий.

3.5. Доступ к записям аудита и функциям управления механизмами регистрации предоставляться только администратору безопасности ИС.

4. Порядок реагирования на инциденты ИБ

4.1. Выявление инцидентов ИБ

Выявление инцидента ИБ возможно получением информации из следующих источников:

– события ИБ, поступившие с используемых средств защиты информации;
– иная информация о состоянии защищенности;
– обращения работников ГКУ НСО ЦСПН Северного района;
– обращения представителей сторонней организации или лица.

После получения информации об инциденте должен зарегистрировать ее в формате карточки инцидента ИБ, включающей:

– уникальный идентификатор;

– название (имя) инцидента ИБ;

– дату и время регистрации инцидента ИБ;

– сведения о том, каким образом обнаружен инцидент ИБ (обращение работника, обращение другая информация о состоянии или техническим средством);

– дополнительную информацию (если она доступна на данный момент (примечания/комментарии)).

Допускается ведение карточки инцидента ИБ в электронном виде.

Далее администратор безопасности ИС должен получить сведения об источнике активности и ее цели (узле, системе, сегменте сети и т.п.), путем анализа событий ИБ, связанных с указанным инцидентом ИБ, и иной информации о состоянии защищенности на предмет наличия в них соответствующих идентификаторов (IP-адрес, имя учетной записи и т.п.) и сопоставления их со справочными данными (диапазоны подсетей, группы пользователей и т.п.). На данном этапе должно происходить дополнение карточки инцидента ИБ сведениями об источнике активности (IP-адрес, сведения о пользователе и т.п.) и сведениями о цели (IP-адрес (диапазон IP-адресов) и т.п.).

Далее должен производиться анализ событий ИБ, действий, произошедших на источнике активности и цели в течение ближайшего времени, поиск признаков, подтверждающих несанкционированность действий, проверка отсутствия отказов/сбоев при регистрации событий ИБ, связанных с указанным инцидентом ИБ, и иной информации о состоянии защищенности. В случае принятия решения о ложном срабатывании должно происходить закрытие инцидента ИБ со статусом «Ложное срабатывание». В ином случае идет процесс реагирование на инцидент ИБ.

4.2. Реагирование на инцидент ИБ

Администратор безопасности ИС обязан принять меры, сдерживающие дальнейшее распространение инцидента. В числе таких мер может быть изоляция скомпрометированных устройств.

Также в ходе сдерживания дальнейшего развития инцидента ИБ необходимо принять меры по фиксированию возможных доказательств для дальнейшего расследования.

4.3. Устранение последствий инцидента ИБ

Обязанности по устранению последствий инцидента ИБ возлагаются на администратора безопасности ИС. Не позднее одного дня с момента наступления инцидента ИБ администратора безопасности ИС должен составить план устранения последствий инцидента ИБ. В данный план необходимо включить:

– общую информацию о произошедшем инциденте ИБ;

– анализ ситуации, оперативные контрмеры, примененные для локализации инцидента ИБ;

– меры, которые необходимо применить для устранения последствий инцидента и восстановления штатной работы ИС;

– определение лиц, ответственных за расследование и установление причин, по которым стало возможным наступление инцидента ИБ;

– определение лиц, ответственных за проведение профилактических мероприятий, разработку и внедрение мер по недопущению повторного наступления инцидента ИБ.

Ответственность за реализацию плана устранения последствий и причин наступления инцидента ИБ лежит на администраторе безопасности ИС. В ходе реализации Плана должны быть приняты меры по устранению последствий инцидента ИБ и восстановление ИС до исходного состояния способами, определяемыми в Плане.

К реализации плана могут привлекаться специалисты ГКУ НСО ЦСПН Северного района, ответственные за поддержание технических средств и систем в рабочем состоянии (системные администраторы).

4.4. Проведение расследования инцидента ИБ

Разбирательство и составление заключений в обязательном порядке должны проводиться в случае выявления следующих фактов:

– нарушение конфиденциальности, целостности и доступности информации;

– халатность и несоблюдение требований по обеспечению безопасности информации;

– несоблюдение условий хранения носителей информации.

Расследование инцидента ИБ может производиться работниками ГКУ НСО ЦСПН Северного района (внутреннее расследование) или с привлечением независимых организаций (Лицензиатов ФСТЭК) на основании оформленных договоров.

Задачами расследования являются:

– установление обстоятельств нарушений, приведших к возникновению инцидента ИБ, в том числе времени, места и способа их совершения;

– установление лиц, непосредственно виновных в данных нарушениях;

– выявление причин и условий, способствовавших развитию инцидента.

Обязанность проведения внутреннего расследования возлагается на администратора безопасности ИС. Администратор безопасности ИС должен приступить к работе по расследованию инцидента ИБ не позднее следующего дня после даты выявления инцидента ИБ.

Общая продолжительность внутреннего расследования не должна превышать одного месяца.

Расследование инцидента ИБ должны включать в себя:

– восстановление хронологии событий при инциденте;

– выявление задействованного оборудования, программного обеспечения и инструментов, которые могли использоваться для реализации инцидента ИБ;

– сбор доказательной базы по инциденту;

– установление источника инцидента;

– оценку последствий инцидента ИБ;

– выдачу рекомендаций по предотвращению аналогичных инцидентов ИБ.

Все полученные в ходе расследования материалы подлежат письменному оформлению.

По окончании расследования администратор безопасности ИС должен предоставить директору ГКУ НСО ЦСПН Северного района заключение, в котором излагаются:

– основания и время проведения расследования;

– проделанная работа (кратко);

– выявленные нарушения, приведшие к реализации инцидента;

– причины и условия совершения нарушений;

– виновные лица и степень их вины;

– наличие умысла в действиях виновных лиц;

– предложения по возмещению ущерба;

– рекомендации по предотвращению повторного возникновения инцидентов;

– другие вопросы (об актуальности конфиденциальной информации, о размерах ущерба и т.д.).

Материалы расследования подлежат хранению не менее 1 года.

5. Информирование о компьютерных инцидентах уполномоченных органов

5.1. Уведомление о компьютерных атаках на информационные ресурсы Российской Федерации, являющиеся ИС.

5.1.1. Уведомление о компьютерных атаках на информационные ресурсы Российской Федерации, включая информирование о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных (далее – инцидент) производится в соответствии с пунктом 12 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ).

5.1.2. Руководствуясь положениями пункта 3 статьи 21 Федерального закона № 152-ФЗ в случае выявления такого инцидента предпринимаются следующие действия:

5.1.2.1. В течение 24 часов уведомляется уполномоченный орган по защите прав субъектов персональных данных через сервис https://pd.rkn.gov.ru/incidents/form/ с передачей следующих сведений:

— произошедший инцидент,

— предполагаемые причины, повлекшие нарушение прав субъектов персональных данных;

— предполагаемый вред, нанесенный правам субъектов персональных данных;

— о принятых мерах по устранению последствий соответствующего инцидента;

— сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом.

5.1.2.2. В течение 72 часов направляется посредством сервиса https://pd.rkn.gov.ru/incidents/form/ информация о результатах внутреннего расследования выявленного инцидента, а также предоставляются сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

5.1.2.3. Направление сведений о расследовании производится с указанием полученного номера и ключа уведомления при регистрации инцидента.

5.1.2.4. Проверить состояние своего уведомления об инциденте можно посредством сервиса https://pd.rkn.gov.ru/incidents/notification_check/.

6. Ответственность при организации мероприятий по выявлению компьютерных инцидентов и реагированию на них

6.1. Ответственность за организацию мероприятий по выявлению компьютерных инцидентов и реагированию на них в соответствии с требованиями настоящей Инструкции возлагается на администратора безопасности ИС.

6.2. Ответственность за соблюдение требований настоящей Инструкции возлагается на всех сотрудников, эксплуатирующих ИС

УТВЕРЖДЕНА
приказом ГКУ НСО ЦСПН Северного района
от «30» 04 2025 г. № 157

Инструкция по управлению конфигурацией

1. Общие положения

1.1. Настоящая Инструкция разработана в целях реализации мер по управлению конфигурацией информационных систем (далее – ИС) ГКУ НСО ЦСПН Северного района и системы защиты информации, которые должны обеспечивать управление изменениями конфигурации ИС и системы защиты информации, анализ потенциального воздействия планируемых изменений на обеспечение безопасности информации, а также документирование этих изменений.

1.2. Контроль за исполнением настоящей Инструкции осуществляет администратор безопасности ИС.

2. Управление изменениями конфигурации ИС

2.1. Лицом, которому разрешены действия по внесению изменений в конфигурацию ИС и системы защиты информации является администратор безопасности ИС.

2.2. Администратор безопасности ИС должен производить анализ потенциального воздействия планируемых изменений в конфигурации ИС и системы защиты информации на обеспечение защиты информации. В случае принятия решения об изменении конфигурации администратор безопасности ИС должен проверять в банке уязвимостей ФСТЭК России (https://bdu.fstec.ru/vul) наличие уязвимых версий планируемого к использованию в ИС программного обеспечения при изменении конфигурации ИС.

2.3. В случае принятия положительного решения об изменении конфигурации администратором безопасности ИС производится согласование изменений в конфигурации ИС с должностным лицом (работником), ответственным за обеспечение безопасности информации.

2.4. При анализе администратором безопасности ИС возможных изменений в конфигурацию ИС и системы защиты информации ИС учитываются следующие факторы:

– в случае развития (модернизации) ИС, в ходе которого изменена конфигурация (параметры настройки) средств защиты информации, исключены программные, программно-технические средства и средства защиты информации, дополнительно включены аналогичные средства или заменены на аналогичные средства, производится внесение изменений в проектную и рабочую документацию;

– в случае развития (модернизации) ИС, приводящего к повышению уровня защищенности ИС и (или) к изменению архитектуры подсистемы безопасности информации ИС в части изменения видов и типов программных, программно-технических средств и средств защиты информации, изменения структуры системы защиты информации, состава и мест расположения ИС и его компонентов, организуется проведение повторной оценки эффективности ИС.

3. Правила документирования информации (данных) об изменениях в конфигурации ИС и системы защиты информации ИС.

3.1. Сведения о применяемых технических и программных средствах в составе ИС фиксируются в техническом паспорте ИС.

3.2. В техническом паспорте ИС должен быть предусмотрен раздел, фиксирующий сведения об изменении состава применяемых технических и программных средствах в составе ИС.

3.3. В случае необходимости внесения изменений конфигурации ИС и системы защиты информации ИС инициатором такого изменения разрабатывается заявка на внесение изменений (Приложение № 1 к настоящей Инструкции) и передается администратору безопасности ИС, который в свою очередь, опираясь на положения раздела 2 настоящей Инструкции принимает решение об изменении конфигурации.

3.4. Отметка о принятом решении проставляется в соответствующей заявке. При необходимости вносятся изменения в технический паспорт ИС.

3.5. В случае необходимости изменения конфигурации с учетом пункта 2.4. настоящей Инструкции могут быть привлечены организации – лицензиаты ФСТЭК России.

4. Ответственность при управлении конфигурацией ИС и системы защиты информации в ИС

4.1. Ответственность за управление конфигурацией ИС и системы защиты информации в ИС в соответствии с требованиями настоящей Инструкции возлагается на администратора безопасности ИС.

4.2. Ответственность за соблюдение требований настоящей Инструкции возлагается на всех сотрудников ГКУ НСО ЦСПН Северного района, эксплуатирующих ИС.

Приложение № 1
к инструкции по управлению
конфигурацией

ФОРМА

Заявка № _____
на внесение изменений в конфигурацию информационных систем
ГКУ НСО ЦСПН Северного района

1. Прошу внести изменение в конфигурацию информационной системы

Автор запроса (Ф.И.О. работника ГКУ НСО ЦСПН (наименование) района): _____

Должность: _____

Наименование структурного подразделения: _____

_____

Краткое описание предлагаемого изменения: _____

Обоснование необходимости внесения изменения: _____

_____

(должность)

_____ _____ «_____» _____ _____г.
(Ф.И.О) *(Подпись)* *(Дата)*

2. Возможность внести изменение в конфигурацию информационных систем ГКУ НСО ЦСПН Северного района в указанных целях согласую / не согласую
(нужное подчеркнуть)

_____

(должность)

_____ «_____» _____ _____г.
(Ф.И.О) *(Подпись)* *(Дата)*

в связи с

_____

(указывается причина не согласования изменений в случае наличия таковых)

3. Возможность внести изменение в конфигурацию информационных систем ГКУ НСО ЦСПН Северного района в указанных целях подтверждаю

_____

(должность)

_____ _____ «_____» _____ _____г.
(Ф.И.О) *(Подпись)* *(Дата)*

4. Отметка исполнителя

Выполненные действия

_____

_____

_____

(должность)

_____ _____ «_____» _____ _____г.
(Ф.И.О) *(Подпись)* *(Дата)*

УТВЕРЖДЕНА
приказом ГКУ НСО ЦСПН Северного района
от «30» 04 2025 г. № 157

Инструкция пользователя информационных систем

1. Общие положения

1.1. Настоящая инструкция определяет функции, права и ответственность пользователя информационных систем (далее – ИС) ГКУ НСО ЦСПН Северного района.

1.2. ГКУ НСО ЦСПН Северного района назначает пользователей ИС соответствующими внутренними документами ГКУ НСО ЦСПН Северного района.

1.3. Пользователями ИС, являются работники ГКУ НСО ЦСПН Северного района, которым это необходимо и предусмотрено в процессе исполнения их функциональных обязанностей. Лица допускаются к работе в ИС в установленном в ГКУ НСО ЦСПН Северного района порядке.

1.4. Ознакомление пользователей ИС с настоящей инструкцией осуществляется под подпись.

2. Обязанности пользователя

2.1. Знать и выполнять требования законодательства Российской Федерации и локальных актов ГКУ НСО ЦСПН Северного района, устанавливающих правила обработки и защиты информации.

2.2. При эксплуатации ИС с целью защиты информации, пользователь обязан:

– руководствоваться требованиями настоящей инструкции, а также других локальных нормативных правовых актов в отношении обработки информации.

– соблюдать установленную технологию обработки информации, в том числе технологию обработки информации.

2.3. Пользователь должен свести к минимуму возможность неконтролируемого доступа к средствам вычислительной техники (далее – СВТ) посторонних лиц, а также возможность просмотра посторонними лицами ведущихся на СВТ работ. В случаях кратковременного отсутствия (перерыв, обед) при выходе в течение рабочего дня из помещения, в котором размещаются СВТ, пользователь обязан блокировать ввод-вывод информации на своем рабочем месте или выключить СВТ.

2.4. Пользователь самостоятельно следит за состоянием специального защитного знака, расположенного на СВТ.

2.5. Докладывать администратору безопасности ИС и своему непосредственному руководителю:

– о фактах имевшегося или предполагаемого несанкционированного доступа к информации, носителям информации, СВТ, помещениям, в которых располагаются СВТ;

– об утрате носителей информации, паролей и идентификаторов, ключей от помещений, где ведется обработка информации;

– об обнаружении вредоносного программного обеспечения или нетипичного поведения ИС;

– о попытках получения информации лицами, не имеющими к ней допуска.

– об иных внештатных ситуациях, связанных с угрозой безопасности ИС.

2.6. Пользователю запрещается:

– подключать к СВТ нештатные устройства;

– самостоятельно вносить изменения в состав, конфигурацию и размещение СВТ;

– самостоятельно вносить изменения в состав, конфигурацию и настройку программного обеспечения, установленного в ИС;

– самостоятельно вносить изменения в размещение, состав и настройку средств защиты информации (СЗИ) ИС;

– сообщать устно, письменно или иным способом (показ и т.п.) другим лицам идентификаторы и пароли, передавать ключи от хранилищ и помещений и другие реквизиты доступа к ИС;

– разрешать работу с СВТ ИС лицам, не допущенным к обработке информации в установленном порядке.

3. Права пользователя ИС

3.1. Пользователь ИС имеет право:

– обращаться к администратору безопасности ИС по любым вопросам, касающихся обработки и защиты информации в ИС (выполнение режимных мер, установленной технологии обработки информации, инструкций и других документов по обеспечению безопасности информации ИС);

– обращаться к администратору безопасности ИС с просьбой об оказании консультаций и технической помощи по обеспечению безопасности обрабатываемой в ИС информации, а также по вопросам эксплуатации установленных СЗИ;

– обращаться к администратору безопасности ИС с просьбой об оказании консультаций и технической помощи по использованию установленных программных и технических средств ИС.

4. Ответственность

4.1. На пользователя возлагается персональная ответственность:

– за соблюдение установленной технологии обработки информации в ИС;

– за соблюдение режима конфиденциальности информации в ИС;

– за правильность понимания и полноту выполнения задач, функций, прав и обязанностей, возложенных на него при работе в ИС;

– за соблюдение требований локальных актов по вопросам обработки и защиты информации в ИС.

УТВЕРЖДЕНА
приказом ГКУ НСО ЦСПН Северного района
от «30» 04 2025 г. № 157

Инструкция администратора безопасности информационных систем

1. Общие положения

1.1. Настоящая инструкция определяет функции, права и ответственность лица, ответственного за обеспечение безопасности информационных систем (далее – ИС) ГКУ НСО ЦСПН Северного района, определенного администратором безопасности ИС ГКУ НСО ЦСПН Северного района.

1.2. ГКУ НСО ЦСПН Северного района назначает администратора безопасности ИС соответствующим внутренним документом ГКУ НСО ЦСПН Северного района.

1.3. Администратор безопасности ИС в своей деятельности руководствуется Федеральными законами от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и от 27.07.2006 № 152-ФЗ «О персональных данных», постановлениями Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», главой 14 Трудового кодекса Российской Федерации, пунктом 8 Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 № 21, пунктом 20 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 № 17, иными нормативными правовыми актами Российской Федерации в области защиты информации, в том числе персональных данных, настоящей инструкцией и иными нормативными правовыми актами ГКУ НСО ЦСПН Северного района в области защиты информации, в том числе персональных данных.

1.4. Администратор безопасности ИС знакомится с настоящей инструкцией под роспись.

2. Обязанности администратора безопасности ИС

2.1. Администратор безопасности ИС обязан:

– применять технические меры защиты информации;

– обеспечивать функционирование и безопасность средств защиты информации;

– обучать пользователей работе на персональных компьютерах с установленными средствами защиты информации;

– контролировать выполнение установленных правил обеспечения защиты информации лицами, допущенными к обработке информации соответствующим внутренним документом ГКУ НСО ЦСПН Северного района;

– инициировать проведение служебных расследований по фактам нарушения установленных правил обеспечения защиты информации, несанкционированного доступа к информации;

– разъяснять пользователям порядок использования машинных носителей информации и контролировать заполнение соответствующего журнала;

– информировать ответственного за организацию обработки информации об инцидентах и попытках несанкционированного доступа к защищаемой информации, элементам систем и средствам защиты информации;

– организовывать антивирусную защиту в соответствии с соответствующей Инструкцией;

– предоставлять доступ к ИС новым пользователям, предоставлять им возможность задать пароль, соответствующий требованиям «Инструкции по управлению правилами и процедурами идентификации и аутентификации»;

– производить мероприятия по внеплановой смене паролей;

– осуществлять периодическое резервное копирование баз информации и сопутствующей защищаемой информации, а также осуществлять внеплановое создание резервных копий по запросу пользователей ИС и/или в иных случаях, когда это необходимо для обеспечения сохранности информации;

– осуществлять восстановление информации из резервных копий по запросу пользователей ИС и/или в иных случаях, когда это необходимо для восстановления утраченных сведений;

– хранить дистрибутивы программного обеспечения, установленного в ИС, в том числе дистрибутивы средств защиты информации, в месте, исключающем несанкционированный доступ к ним третьих лиц;

– реализовывать контроль (анализ) защищенности информации ИС;

– осуществлять выявление компьютерных инцидентов, реагирование на них и проведение расследований;

– обеспечивать управление конфигурацией ИС и системы защиты информации ИС;

– вносить свои предложения по совершенствованию мер защиты информации в ИС, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня

защищённости информации.

2.2. Администратор безопасности ИС может выполнять свои обязанности с привлечением сотрудников иных организаций на основании заключенных соглашений.

3. Действия администратора безопасности ИС при обнаружении попыток несанкционированного доступа

3.1. К попыткам несанкционированного доступа относятся:

– действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к ИС, при использовании учётной записи администратора или другого пользователя ИС, методом подбора пароля, использования пароля, разглашённого владельцем учётной записи или любым другим методом;

– сеансы работы с ИС незарегистрированных пользователей, или пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истёк, или превышающих свои полномочия по доступу к данным.

3.2. При выявлении факта несанкционированного доступа администратор безопасности ИС обязан действовать в соответствии с Инструкцией по выявлению компьютерных инцидентов и реагированию на них.

4. Настройка средств защиты информации ИС

4.1. Администратор безопасности ИС при настройке и администрировании средств защиты информации ИС руководствуется нормативно-правовыми актами Российской Федерации в области обработки персональных данных и защиты информации.

4.2. Действия администратора безопасности ИС по параметрам настройки средств защиты информации при необходимости согласовываются с государственным бюджетным учреждением Новосибирской области «Центр защиты информации Новосибирской области» (далее – ГБУ НСО «ЦЗИ НСО») и производятся согласно внутренних документов ГБУ НСО «ЦЗИ НСО».

5. Права администратора безопасности

Администратор безопасности ИС имеет право:

– требовать от работников выполнения установленных правил обеспечения защиты информации;

– требовать от работников прекращения обработки информации в случаях их неправомерного использования и нарушения правил обеспечения защиты информации;

– вносить предложения по совершенствованию технических мер по защите информации.

6. Ответственность

4.1. Администратор безопасности ИС несёт персональную ответственность за качество проводимых им работ по обеспечению безопасности информации.

4.2. Администратор безопасности ИС несёт ответственность за разглашение информации ограниченного доступа, ставшей известной ему по роду работы, в соответствии с законодательством Российской Федерации.

УТВЕРЖДЕНА
приказом ГКУ НСО
ЦСПН Северного района
от 30.04.25 № 157

Инструкция
ответственного за защиту информации в информационных системах

1. Общие положения

1.1. Настоящая Инструкция ответственного за защиту информации в информационных системах ГКУ НСО ЦСПН Северного района (далее – Инструкция) определяет функции, права и обязанности ответственного за защиту информации в информационных системах ГКУ НСО ЦСПН Северного района.

1.2. Ответственный за защиту информации в информационных системах ГКУ НСО ЦСПН Северного района назначается из числа заместителя директора ГКУ НСО ЦСПН Северного района или сотрудника, исполняющего обязанности директора ГКУ НСО ЦСПН Северного района в его отсутствие.

2. Обязанности ответственного за защиту информации

2.1. Ответственный за защиту информации в информационных системах ГКУ НСО ЦСПН Северного района обязан:

– осуществлять контроль за выполнением требований, действующих нормативных правовых актов по вопросам обеспечения защиту информации в информационных системах в ГКУ НСО ЦСПН Северного района;

– обеспечивать эксплуатацию информационных систем ГКУ НСО ЦСПН Северного района в соответствии с их назначением;

– организовать порядок доступа в информационные системы ГКУ НСО ЦСПН Северного района;

– осуществлять взаимодействие с администратором безопасности информационных систем ГКУ НСО ЦСПН Северного района в целях контроля состояния защищенности персональных данных в ГКУ НСО ЦСПН Северного района;

– контролировать качество и своевременность выполнения должностными лицами установленных требований по обеспечению безопасности персональных данных;

– контролировать соблюдение правил допуска сотрудников в помещения, в которых находятся компоненты информационных систем ГКУ НСО ЦСПН Северного района;

– контролировать проведение технического обслуживания информационных систем ГКУ НСО ЦСПН Северного района;

– принимать участие в организации и проведении расследований по фактам нарушений в области защиты персональных данных (далее – ПДн) и разработке предложений по устранению недостатков и предупреждению подобного рода нарушений.

3. Права ответственного за защиту информации

3.1. Ответственный за защиту информации в информационных системах ГКУ НСО ЦСПН Северного района имеет право:

– требовать от сотрудников выполнение инструкций по обеспечению безопасности ПДн при их обработке в информационных системах ГКУ НСО ЦСПН Северного района;

– инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения безопасности ПДн, несанкционированного доступа, утраты, модификации, порчи ПДн и технических средств информационных систем ГКУ НСО ЦСПН Северного района;

– требовать прекращения обработки ПДн в случае нарушения установленного порядка работ или нарушения функционирования средств защиты информации;

– участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа;

– участвовать в мероприятиях по осуществлению контроля обеспечения безопасности ПДн. Одной из форм контроля защиты ПДн является периодическая проверка информационных систем ГКУ НСО ЦСПН Северного района, проводимая не реже одного раза в три года. Указанный контроль можно проводить самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации;

– участвовать в расследовании возникающих инцидентов безопасности ПДн в информационных системах ГКУ НСО ЦСПН Северного района. По каждой предпосылке к утечке ПДн для выяснения обстоятельств и причин невыполнения установленных требований проводится расследование. Для проведения расследования назначается специальная комиссия. Комиссия обязана установить, имела ли место утечка ПДн, и обстоятельства ей сопутствующие, установить лиц, виновных в нарушении предписанных мероприятий по обеспечению безопасности ПДн, установить причины и условия, способствовавшие нарушению, и выработать рекомендации по их устранению. После окончания расследования директор ГКУ НСО ЦСПН Северного района принимает решение о наказании виновных лиц и необходимых мероприятиях по устранению недостатков.

4. Ответственность ответственного за защиту информации

Ответственный за защиту информации в информационных системах ГКУ НСО ЦСПН Северного района несет персональную ответственность за:

– неисполнение, несвоевременное или некачественное выполнение возложенных на него обязанностей по защите информации в информационных системах ГКУ НСО ЦСПН Северного района;

– достоверность отчетных данных и других подготавливаемых материалов;

– качество работ по защите информации в соответствии с функциональными обязанностями;

– соблюдение режима конфиденциальности ПДн при их обработке и хранении в информационных системах ГКУ НСО ЦСПН Северного района;

– соблюдение требований нормативных правовых актов, приказов, распоряжений и инструкций, определяющих порядок организации работ по обеспечению безопасности ПДн.

дм. СД, Сердакова ю.в. 30.04.2025

УТВЕРЖДЕНА
приказом ГКУ НСО ЦСПН
Северного района
от 30. 04. 15 № 157

Инструкция
ответственного за организацию обработки персональных данных

1. Общие положения

1.1. Инструкция ответственного за организацию обработки персональных данных в ГКУ НСО ЦСПН Северного района (далее – Инструкция) разработана в целях обеспечения безопасности персональных данных (далее - ПДн) при их обработке в информационных системах ГКУ НСО ЦСПН Северного района.

1.2. Ответственный за организацию обработки ПДн в ГКУ НСО ЦСПН Северного района назначается приказом директора ГКУ НСО ЦСПН Северного района.

1.3. Ответственный за организацию обработки ПДн в своей работе руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», иными нормативными правовыми актами, настоящей Инструкцией, а также иными нормативными правовыми актами ГКУ НСО ЦСПН Северного района, регламентирующими вопросы обработки ПДн и несет персональную ответственность за свои действия.

2. Обязанности ответственного за организацию обработки ПДн

2.1. Осуществлять внутренний контроль за соблюдением сотрудниками ГКУ НСО ЦСПН Северного района законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн.

2.2. Доводить до сведения сотрудников ГКУ НСО ЦСПН Северного района положения законодательства Российской Федерации о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн.

2.3. Организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и осуществлять контроль за приемом и обработкой указанных обращений и запросов.

3. Основные функции ответственного за организацию обработки ПДн

3.1. Проведение единой политики ГКУ НСО ЦСПН Северного района и координация работ по организации обработки ПДн.

3.2. Контроль за исполнением организационных и распорядительных документов по организации обработки ПДн в ГКУ НСО ЦСПН Северного района.

3.3. Проведение периодического контроля эффективности мер защиты ПДн в ГКУ НСО ЦСПН Северного района. Анализ результатов контроля.

3.4. Рассмотрение и утверждение предложений по совершенствованию системы защиты ПДн в ГКУ НСО ЦСПН Северного района.

3.5. Осуществление непосредственного контроля за соблюдением установленного законодательством порядка рассмотрения запросов субъектов ПДн.

3.6. Организация повышения квалификации сотрудников в области защиты ПДн.

3.7. Организация повышения информированности сотрудников по вопросам обеспечения безопасности ПДн.

4. Права ответственного за организацию обработки ПДн

Ответственный за организацию обработки ПДн имеет право:

4.1. Запрашивать и получать необходимые материалы для организации и проведения работ по вопросам организации обработки ПДн.

4.2. Осуществлять контроль за реализацией требований организационных и распорядительных документов по организации обработки ПДн, а также предписаний государственных органов контроля.

5. Ответственность ответственного за организацию обработки ПДн

Ответственный за организацию обработки ПДн несет персональную ответственность за:

- правильность и объективность принимаемых решений по вопросам обработки ПДн;
- правильное и своевременное выполнение требований организационных и распорядительных документов, принятых в ГКУ НСО ЦСПН Северного района по вопросам обработки ПДн;
- выполнение возложенных на него обязанностей, предусмотренных настоящей Инструкцией;
- соблюдение трудовой дисциплины, охраны труда.
-

озн. Сф. Сердакова 10.11. 30.04.25г.

УТВЕРЖДЕНА
приказом ГКУ НСО ЦСПН
Северного района
от 30.04.25 № 157

Инструкция
ответственного по обеспечению безопасности персональных данных

1. Общие положения

1.1. Инструкция ответственного по обеспечению безопасности персональных данных в ГКУ НСО ЦСПН Северного района (далее – Инструкция) разработана в целях обеспечения безопасности персональных данных (далее - ПДн) при их обработке в ГКУ НСО ЦСПН Северного района.

1.2. Ответственный по обеспечению безопасности ПДн в ГКУ НСО ЦСПН Северного района назначается приказом директора ГКУ НСО ЦСПН Северного района.

1.3. Ответственный по обеспечению безопасности ПДн в своей работе руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», иными нормативными правовыми актами, настоящей Инструкцией, а также иными нормативными правовыми актами ГКУ НСО ЦСПН Северного района, регламентирующими вопросы обработки ПДн и несет персональную ответственность за свои действия.

2. Обязанности ответственного по обеспечению безопасности ПДн

2.1. Осуществлять внутренний контроль за соблюдением сотрудниками ГКУ НСО ЦСПН Северного района законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн.

2.2. Доводить до сведения сотрудников ГКУ НСО ЦСПН Северного района положения законодательства Российской Федерации о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн.

3. Основные функции ответственного по обеспечению безопасности ПДн

3.1. Проведение единой политики ГКУ НСО ЦСПН Северного района и координация работ по обеспечению безопасности ПДн.

3.2. Планирование мероприятий по организации обеспечения безопасности ПДн.

3.3. Организация мероприятий по техническому обеспечению безопасности ПДн.

3.4. Организация мероприятий, направленных на предотвращение несанкционированного доступа к ПДн или передачи их лицам, не имеющим права доступа к такой информации.

3.5. Организация постоянного контроля за обеспечением уровня защищенности ПДн.

3.6. Координация действий по подготовке информационных систем к аттестации по выполнению требований по обеспечению безопасности ПДн.

3.7. Контроль за исполнением организационных и распорядительных документов по обеспечению безопасности ПДн в ГКУ НСО ЦСПН Северного района.

3.8. Рассмотрение предложений по устранению недостатков и предупреждению нарушений в части обеспечения безопасности ПДн, осуществление контроля за устранением нарушений.

3.9. Организация повышения информированности сотрудников по вопросам обеспечения безопасности ПДн.

3.10. Изучение отчетов о состоянии работ по обеспечению безопасности ПДн в ГКУ НСО ЦСПН Северного района.

4. Права ответственного по обеспечению безопасности ПДн

Ответственный по обеспечению безопасности ПДн имеет право:

4.1. Запрашивать и получать необходимые материалы для организации и проведения работ по вопросам обеспечения безопасности ПДн.

4.2. Осуществлять контроль за реализацией требований организационных и распорядительных документов по обеспечению безопасности ПДн, а также предписаний государственных органов контроля.

4.3. Контролировать деятельность сотрудников ГКУ НСО ЦСПН Северного района в части выполнения ими требований по обеспечению безопасности ПДн.

4.4. Принимать решение о приостановке работ в случае обнаружения несанкционированного доступа, утечки (или предпосылок для утечки) ПДн.

4.5. Привлекать в установленном порядке необходимых специалистов из числа сотрудников ГКУ НСО ЦСПН Северного района для проведения исследований, разработки решений, мероприятий и организационно-распорядительных документов по вопросам обеспечения безопасности ПДн.

5. Ответственность ответственного по обеспечению безопасности ПДн

Ответственный по обеспечению безопасности ПДн несет персональную ответственность за:

- правильность и объективность принимаемых решений по вопросам защиты ПДн;
- правильное и своевременное выполнение требований организационных и распорядительных документов, принятых в ГКУ НСО ЦСПН Северного района по вопросам защиты ПДн;
- выполнение возложенных на него обязанностей, предусмотренных настоящей Инструкцией;
- качество проводимых работ по обеспечению безопасности ПДн в соответствии с функциональными обязанностями;
- соблюдение трудовой дисциплины, охраны труда.

Сф - Сергеева Ю.И. 30.04.2025.

УТВЕРЖДЕНЫ
приказом ГКУ НСО ЦСПН
Северного района
от 30.04.25 № 157

Правила
обработки персональных данных, осуществляемой без использования средств автоматизации

1. Общие положения

1.1. Настоящие правила определяют порядок обработки персональных данных без использования средств вычислительной техники в ГКУ НСО ЦСПН Северного района, являются обязательными для исполнения его сотрудниками и должны доводиться под роспись.

1.2. Правила разработаны в соответствии с требованиями постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и распространяются на документы, исполненные на бумажных носителях, в том числе полученные путем извлечения из информационных систем персональных данных (вывода на печать).

1.3. К документам на бумажных носителях, содержащим персональные данные (далее – документы), относятся:

типовые формы документов (бланки);

журналы (реестры, книги);

иные документы.

1.4. Не допускается в одном документе фиксация персональных данных, цели обработки которых заведомо не совместимы.

2. Порядок обращения с документами, содержащими персональные данные

2.1. Прием и учет (регистрация) документов, осуществляются специалистом, которому поручен приём и учет несекретной документации.

2.2. Все документы подлежат обязательному учету в соответствии с правилами ведения делопроизводства.

Их подготовка, движение и уничтожение должны осуществляться в соответствии с требованиями, предусмотренными для документов, содержащих служебную информацию ограниченного распространения.

При этом в отношении каждого документа в любой момент времени должно быть документально установлено его местонахождение, а именно – сотрудник, у которого находится документ.

2.3. Документы передаются сотрудникам под роспись. Документы хранятся сотрудниками в порядке, предусмотренном для документов, содержащих служебную информацию ограниченного распространения.

Передача документов от одного работника к другому осуществляется с разрешения директора ГКУ НСО ЦСПН Северного района, в котором находится документ на момент возникновения необходимости его передачи, или по согласованному решению директора ГКУ НСО ЦСПН Северного района, между сотрудниками которых осуществляется передача.

2.4. Размножение (тиражирование) документов осуществляется только с письменного разрешения директора ГКУ НСО ЦСПН Северного района.

2.6. О фактах утраты документа ставится в известность директора ГКУ НСО ЦСПН Северного района, который принимает решение о необходимости и порядке расследования обстоятельств его утраты.

3. Особенности работы с типовыми формами и журналами

3.1. При использовании типовых форм документов, должны соблюдаться следующие условия:

типовая форма или связанные с ней документы должны содержать сведения о цели обработки персональных данных, реквизиты ГКУ НСО ЦСПН Северного района, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных;

типовая форма должна предусматривать раздел, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных (если согласие не предусмотрено законодательством Российской Федерации, то типовая форма должна содержать ссылку на Федеральный закон Российской Федерации с указанием статей);

типовая форма должна разрабатываться с учетом необходимости ознакомления субъектов персональных данных таким образом, чтобы не были нарушены права и интересы иных субъектов персональных данных.

3.2. При ведении журналов (реестров, книг), содержащих персональные данные, должны соблюдаться следующие условия:

необходимость ведения журнала должна быть предусмотрена нормативными правовыми актами Российской Федерации, ведомственными нормативными актами или локальными нормативными актами ГКУ НСО ЦСПН Северного района;

определение круга лиц, которые имеют доступ к журналу, отвечают за его ведение и сохранность;

определение сроков хранения заполненных журналов.

Копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается.

УТВЕРЖДЕНЫ
приказом ГКУ НСО ЦСПН
Северного района
от 30.04.25 № 157

Правила
работы с обезличенными данными

1. В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» обрабатываемые персональные данные подлежат обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей.

2. Директор ГКУ НСО ЦСПН Северного района принимает решение о необходимости обезличивания персональных данных.

3. Специалисты, непосредственно осуществляющие обработку персональных данных, готовят предложения по обезличиванию персональных данных, включающие обоснование такой необходимости и способы обезличивания.

4. Специалисты, обслуживающие базы данных с персональными данными, совместно с ответственным за организацию обработки персональных данных, осуществляют непосредственное обезличивание выбранным способом.

5. В ГКУ НСО ЦСПН Северного района применяются следующие способы обезличивания:

1) метод введения идентификаторов – замена части сведений (значений персональных данных) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным;

2) метод изменения состава или семантики – изменение состава или семантики персональных данных путем замены результатами статистической обработки, преобразования, обобщения или удаления части сведений;

3) метод декомпозиции – разделение множества (массива) персональных данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств;

4) метод перемешивания – перестановка отдельных значений или групп значений атрибутов персональных данных в массиве персональных данных.

6. Выбор и применение конкретного метода осуществляется в соответствии с Методическими рекомендациями по применению приказа Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

7. Обезличивание персональных данных осуществляют сотрудники, ответственные за проведение мероприятий по обезличиванию обрабатываемых персональных данных.

8. Обезличенные персональные данные не подлежат разглашению.

9. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

10. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

1) парольной политики;

2) антивирусной политики;

3) правил работы со съемными носителями (если они используются);

4) правил резервного копирования;

5) правил доступа в помещения, где расположены элементы информационных систем.

11. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

1) правил хранения бумажных носителей;

2) правил доступа к обезличенным персональным данным и в помещения, где они хранятся.

УТВЕРЖДЕНЫ
приказом ГКУ НСО ЦСПН
Северного района
от 30.04.25 № 157

Правила
рассмотрения запросов субъектов персональных данных или их представителей

1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных ГКУ НСО ЦСПН Северного района;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые ГКУ НСО ЦСПН Северного района способы обработки персональных данных;

4) наименование и место нахождения ГКУ НСО ЦСПН Северного района, сведения о лицах (за исключением работников ГКУ НСО ЦСПН Северного района), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с ГКУ НСО ЦСПН Северного района или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;

8) наименование должности, фамилию, имя, отчество и местонахождение лица, осуществляющего обработку персональных данных по поручению ГКУ НСО ЦСПН Северного района, если обработка поручена или будет поручена такому лицу;

9) иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

2. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами.

3. Сведения, указанные в пункте 1 настоящих Правил, должны быть предоставлены субъекту персональных данных ГКУ НСО ЦСПН Северного района в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

4. Сведения, указанные в пункте 1 настоящих Правил, предоставляются субъекту персональных данных или его представителю ГКУ НСО ЦСПН Северного района при обращении либо при получении запроса субъекта персональных данных или его представителя по форме согласно приложению 1 к настоящим Правилам.

Запрос должен содержать номер 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 ГКУ НСО ЦСПН Северного района (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных ГКУ НСО ЦСПН Северного района, подпись субъекта персональных данных или его представителя.

Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

5. В случае, если сведения, указанные в пункте 1 настоящих Правил, а также обрабатываемые персональные данные, были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в ГКУ НСО ЦСПН Северного района или направить повторный запрос в целях получения сведений, указанных в пункте 1 настоящих Правил, и ознакомления с такими персональными данными не ранее чем через тридцать 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 персональных данных.

6. Субъект персональных данных вправе обратиться повторно в ГКУ НСО ЦСПН Северного района или направить повторный запрос в целях получения сведений, указанных в пункте 1 настоящих Правил, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 5 настоящих Правил, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 4 настоящих Правил, должен содержать обоснование направления повторного запроса.

7. ГКУ НСО ЦСПН Северного района вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 5 и 6 настоящих Правил. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на ГКУ НСО ЦСПН Северного района.

8. Обязанности ГКУ НСО ЦСПН Северного района при обращении субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя:

1) ГКУ НСО ЦСПН Северного района обязано сообщить в порядке, предусмотренном пунктами 1-7 настоящих Правил, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональных данных при обращении субъекта персональных данных или его представителя либо в течение десяти рабочих дней с даты получения запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления ГКУ НСО ЦСПН Северного района в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации;

2) в случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя ГКУ НСО ЦСПН Северного района обязано дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона от 27.07.2006 № 152-ФЗ или иного федерального закона, являющегося основанием для такого отказа, в срок, не превышающий десяти рабочих дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления ГКУ НСО ЦСПН Северного района в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации;

3) ГКУ НСО ЦСПН Северного района обязано предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных;

4) в срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, ГКУ НСО ЦСПН (наименование) района обязано внести в них необходимые изменения;

5) в срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, ГКУ НСО ЦСПН Северного района обязано уничтожить такие персональные данные;

6) ГКУ НСО ЦСПН Северного района обязано уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

9. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, ГКУ НСО ЦСПН Северного района обязано с момента выявления такого инцидента оператором, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных:

1) в течение 24 часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, 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).

10. В случае обращения субъекта персональных данных в ГКУ НСО ЦСПН Северного района с требованием о прекращении обработки персональных данных ГКУ НСО ЦСПН Северного района обязано в срок, не превышающий десяти рабочих дней с даты получения ГКУ НСО ЦСПН Северного района соответствующего требования, прекратить их обработку или обеспечить прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку персональных данных), за исключением случаев, предусмотренных пунктами 2-11 части 1 статьи 6, частью 2 статьи 10 и частью 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления ГКУ НСО ЦСПН Северного района в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

ПРИЛОЖЕНИЕ № 1
к Правилам рассмотрения
запросов субъектов персональных
данных или их представителей

ФОРМА

Директору
ГКУ НСО ЦСПН
Северного района
А.И.Сандзюку

от _____
фамилия, имя, отчество (последнее – при наличии)

_____

_____

_____
почтовый адрес или адрес электронной почты

_____

_____

_____
паспортные данные

ЗАПРОС
о предоставлении персональных данных субъекта персональных данных

Мной _____,
(фамилия, имя, отчество (последнее – при наличии)

«____» _____ 202__ г. в связи с осуществлением
дата предоставления персональных данных

_____

_____
сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором

в ГКУ НСО ЦСПН Северного района предоставлены следующие персональные данные:

_____

_____
указать, какие сведения были предоставлены

В соответствии со статьей 14 Федерального закона от 27.07.2006 № 152- ФЗ «О персональных данных» я имею право получить от Вас информацию, касающуюся обработки моих персональных данных.

Прошу Вас предоставить мне следующие сведения: _____

_____

_____

_____

указать сведения, которые необходимо предоставить

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

_____ _____ _____

(фамилия, имя, отчество (последнее – при наличии) подпись дата

_____

УТВЕРЖДЕНЫ
приказом ГКУ НСО ЦСПН
Северного района
от 30.04.25 № 157

Правила
обработки персональных данных

1. Общие положения

1.1. Настоящие Правила обработки персональных данных в ГКУ НСО ЦСПН Северно района (далее - Правила) направлены на предотвращение нарушений законодательства Российской Федерации, регулирующего обработку персональных данных (далее - ПДн) и определяют политику в ГКУ НСО ЦСПН Северного района как оператора, осуществляющего обработку ПДн, устанавливающую цели обработки ПДн и содержание обрабатываемых данных, категории субъектов, ПДн которых обрабатываются, сроки их обработки и хранения, совершаемые действия (операции), порядок уничтожения ПДн при достижении целей обработки ПДн и др.

1.2. Правила разработаны в соответствии с федеральными законами от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Федеральный закон от 27.07.2006 № 152-ФЗ), Трудовым кодексом Российской Федерации, постановлениями Правительства Российской Федерации от 21 03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», нормативными и методическими документами по технической защите информации ФСТЭК России и ФСБ России.

1.3. Содержание обрабатываемых в ГКУ НСО ЦСПН Северного района ПДн определяется, исходя из требований нормативных правовых актов Российской Федерации и нормативных правовых актов Новосибирской области, в том числе Устава ГКУ НСО ЦСПН Северного района, утвержденного приказом министерства труда и социального развития Новосибирской области от 05.12.2018 № 1308, и целей обработки ПДн.

2. Категории субъектов ПДн

В ГКУ НСО ЦСПН Северного района осуществляется обработка ПДн следующих субъектов ПДн:

1) сотрудников ГКУ НСО ЦСПН Северного района;

2) кандидатов, претендующих на замещение вакантных должностей ГКУ НСО ЦСПН Северного района;

3) граждан, обратившихся в ГКУ НСО ЦСПН Северного района в связи с предоставлением государственных услуг, исполнением государственных функций.

3. Принципы обработки ПДн

3.1. Обработка ПДн в ГКУ НСО ЦСПН Северного района осуществляется на законной и справедливой основе и ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн.

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

3.3. Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.

3.4. При обработке ПДн должны быть обеспечены точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. Должны приниматься необходимые меры по удалению или уточнению неполных, или неточных данных.

3.5. Хранение ПДн должно осуществляться в форме, позволяющей определить субъект ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен нормативными правовыми актами Российской Федерации, нормативными правовыми актами Новосибирской области. Обрабатываемые в ГКУ НСО ЦСПН Северного района ПДн подлежат уничтожению, либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено нормативными правовыми актами Российской Федерации, нормативными правовыми актами Новосибирской области.

4. Цели обработки ПДн

4.1. Цели обработки ПДн должны быть четко определены и соответствовать: заявленным в Уставе ГКУ НСО ЦСПН Северного района основным полномочиям и правам; задачам и функциям ГКУ НСО ЦСПН Северного района.

4.2. Цели обработки ПДн определяют:

содержание и объем обрабатываемых ПДн;

категории субъектов ПДн;

сроки их обработки и хранения;

порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

4.3. Цели обработки ПДн должны быть конкретны, заранее определены, законны и заявлены.

4.4. Обработка ПДн в ГКУ НСО ЦСПН Северного района осуществляется для исполнения наделенных полномочий, организации кадровой работы, финансовой деятельности в соответствии с действующим Уставом ГКУ НСО ЦСПН Северного района.

5. Способы и правила обработки ПДн

5.1. В ГКУ НСО ЦСПН Северного района применяется два способа обработки ПДн:

обработка ПДн без использования средств автоматизации;

обработка ПДн с использованием средств автоматизации.

5.2. Обработка ПДн с использованием средств автоматизации в ГКУ НСО ЦСПН Северного района допускается в следующих случаях:

обработка ПДн осуществляется с согласия субъекта ПДн на обработку его ПДн;

обработка ПДн необходима для достижения целей, предусмотренных законодательством, при осуществлении и выполнении возложенных на ГКУ НСО ЦСПН Северного района полномочий и обязанностей;

обработка ПДн необходима для исполнения договора, стороной которого является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн;

обработка ПДн необходима для предоставления государственных услуг гражданам и организациям;

обработка ПДн необходима для осуществления прав и законных интересов ГКУ НСО ЦСПН Северного района или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;

осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законодательством.

5.3. Обработка ПДн средствами автоматизации осуществляется на основании правил, инструкций, руководств, регламентов и иных документов, определяющих технологический процесс обработки информации, содержащей такие данные.

6. Обработка ПДн с согласия субъекта ПДн

6.1. ГКУ НСО ЦСПН Северного района, как оператор, перед обработкой ПДн получает у субъектов ПДн согласие на обработку ПДн.

6.2. Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем только в письменной форме. Равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с действующим законодательством электронной подписью.

6.3. Получение согласия субъекта ПДн в форме электронного документа на обработку его ПДн в целях предоставления государственных услуг осуществляется в порядке, установленном Правительством Российской Федерации.

6.4. В случае получения согласия на обработку ПДн от законного представителя субъекта ПДн полномочия данного представителя на дачу согласия от имени субъекта ПДн проверяются оператором.

6.5. Допускается включение согласия в типовые формы (бланки) материальных носителей ПДн и в договор с субъектом ПДн.

6.6. Согласие на обработку ПДн может быть отозвано субъектом ПДн путем направления запроса в ГКУ НСО ЦСПН Северного района.

7. Обработка ПДн без согласия субъекта ПДн

Обработка ПДн без получения согласия на такую обработку от субъекта ПДн в ГКУ НСО ЦСПН Северного района может осуществляться при наличии оснований, предусмотренных пунктами 2-11 части 1 статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ.

8. Порядок обработки ПДн в связи с реализацией служебных или трудовых отношений

8.1. ПДн субъектов ПДн, указанных в подпунктах 1, 2 пункта 2 настоящих Правил, обрабатываются в целях обеспечения кадровой работы, формирования кадрового резерва, обучения и должностного роста, учета результатов исполнения сотрудниками ГКУ НСО ЦСПН Северного района должностных обязанностей, обеспечения личной безопасности сотрудников и руководителей, членов их семей, обеспечения установленных

законодательством Российской Федерации условий труда, гарантий и компенсаций, сохранности принадлежащего им имущества, а также в целях противодействия коррупции.

8.2. В целях, указанных в пункте 8.1 настоящих Правил, обрабатываются следующие категории ПДн:

1) фамилия, имя, отчество (при наличии) (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);

2) число, месяц, год рождения;

3) место рождения;

4) сведения о гражданстве (в том числе предыдущие гражданства, иные гражданства);

5) вид, серия, номер документа, удостоверяющего личность, дата выдачи, наименование органа, выдавшего его;

6) адрес и дата регистрации по месту жительства (месту пребывания), адрес фактического проживания;

7) номер контактного телефона или сведения о других способах связи;

8) реквизиты страхового свидетельства обязательного пенсионного страхования;

9) идентификационный номер налогоплательщика;

10) реквизиты страхового медицинского полиса обязательного медицинского страхования;

11) реквизиты свидетельства государственной регистрации актов гражданского состояния;

12) сведения о семейном положении, составе семьи и о близких родственниках (в том числе бывших);

13) сведения о трудовой деятельности;

14) сведения о воинском учете и реквизиты документов воинского учета;

15) сведения об образовании (когда и какие образовательные, научные и иные организации окончил, номера документов об образовании, направление подготовки или специальность по документу об образовании, квалификация);

16) сведения об ученой степени;

17) сведения о владении иностранными языками, уровень владения;

18) фотография;

19) сведения, содержащиеся в служебном контракте, дополнительных соглашениях к служебному контракту;

20) сведения о пребывании за границей;

21) сведения о наличии или отсутствии судимости;

22) сведения об оформленных допусках к государственной тайне;

26) сведения о государственных наградах, иных наградах и знаках отличия;

27) сведения о профессиональной переподготовке и (или) повышении квалификации;

28) сведения о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания;

29) сведения о доходах, расходах, об имуществе и обязательствах имущественного характера;

30) номер расчетного счета;

31) номер банковской карты;

32) иные персональные данные, необходимые для достижения целей, предусмотренных пунктом 8.1 настоящих Правил.

8.3. Обработка ПДн и биометрических ПДн субъектов ПДн, указанных в подпунктах 1, 2 пункта 2. настоящих Правил осуществляется без согласия указанных граждан в рамках целей, предусмотренных пунктом 8.1. настоящих Правил, в

соответствии с пунктом 2 части 1 статьи 6 и частью 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ и Трудовым кодексом Российской Федерации.

8.4. Обработка специальных категорий ПДн субъектов ПДн, указанных в подпунктах 1, 2 пункта 2. настоящих Правил осуществляется без согласия указанных граждан в рамках целей, предусмотренных пунктом 8.1. настоящих Правил, в соответствии с подпунктом 2.3 пункта 2 части 2 статьи 10 Федерального закона от 27.07.2006 № 152-ФЗ и положениями Трудового кодекса Российской Федерации, за исключением случаев получения ПДн субъекта ПДн у третьей стороны (в соответствии с пунктом 3 статьи 86 Трудового кодекса Российской Федерации требуется письменное согласие руководителей подведомственных организаций и граждан, претендующих на замещение указанной должности).

8.5. Обработка ПДн субъектов, указанных в подпунктах 1, 2 пункта 8.2. настоящих Правил, осуществляется при условии получения согласия указанных граждан в следующих случаях:

1) при передаче (распространении, предоставлении) ПДн третьим лицам в случаях, не предусмотренных действующим законодательством Российской Федерации о государственной гражданской службе;

2) при трансграничной передаче ПДн;

3) при принятии решений, порождающих юридические последствия в отношении указанных граждан или иным образом затрагивающих их права и законные интересы, на основании исключительно автоматизированной обработки их ПДн.

8.6. В случаях, предусмотренных пунктом 8.5. настоящих Правил, согласие субъекта ПДн оформляется в письменной форме, если иное не установлено федеральным законодательством.

8.7. Обработка ПДн субъектов, указанных в подпунктах 1, 2 пункта 2. настоящих Правил, осуществляется отделом кадровой и мобилизационной работы ГКУ НСО ЦСПН Северного района и включает в себя следующие действия:

сбор,
запись,
систематизацию,
накопление,
хранение,
уточнение (обновление, изменение),
извлечение,
использование,
передачу (распространение, предоставление, доступ),
обезличивание,
блокирование,
удаление,
уничтожение.

8.8. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) ПДн осуществляется путем:

1) непосредственного получения оригиналов необходимых документов (заявление, трудовая книжка, анкета, иные документы, предоставляемые в отдел кадровой и мобилизационной работы);

2) копирования оригиналов документов;

3) внесения сведений в учетные формы (на бумажных и электронных носителях);

4) формирования ПДн в ходе реализации функций кадровой работы;

5) внесения ПДн в информационные системы, используемые отделом кадровой и мобилизационной работы.

8.9. В случае возникновения необходимости получения ПДн у третьей стороны следует известить об этом субъектов ПДн заранее, получить их письменное согласие и сообщить им о целях, предполагаемых источниках и способах получения ПДн.

8.10. Запрещается получать, обрабатывать и приобщать к личному делу ПДн, не предусмотренные пунктом 8.2. настоящих Правил, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

8.11. При сборе ПДн сотрудник отдела кадровой и мобилизационной работы разъясняет субъектам ПДн юридические последствия отказа предоставить ПДн.

8.12. Передача (распространение, предоставление) и использование ПДн осуществляется лишь в случаях и порядке, предусмотренных законодательством Российской Федерации.

9. Порядок обработки ПДн, необходимых в связи с предоставлением государственных услуг и исполнением государственных функций

9.1. Обработка ПДн граждан, обратившихся в ГКУ НСО ЦСПН Северного района, осуществляется в том числе в целях предоставления государственных услуг и исполнения государственных функций.

9.2. ПДн граждан, обратившихся в ГКУ НСО ЦСПН Северного района лично, а также направивших индивидуальные или коллективные письменные обращения или обращения в форме электронного документа, обрабатываются в целях рассмотрения указанных обращений с последующим уведомлением граждан о результатах рассмотрения.

В соответствии с законодательством Российской Федерации в ГКУ НСО ЦСПН Северного района подлежат рассмотрению обращения граждан Российской Федерации, иностранных граждан, лиц без гражданства, а также обращения организаций.

9.3. Категории ПДн, обрабатываемых в ГКУ НСО ЦСПН Северного района в связи с оказанием государственных услуг и осуществлением государственных функций:

1) сведения, содержащиеся в документах, удостоверяющих личность граждан Российской Федерации, иностранных граждан, лиц без гражданства или беженцев;

2) сведения, содержащиеся в документах, подтверждающих проживание на территории Новосибирской области, место жительства, пребывания, фактического проживания;

3) контактные телефоны;

4) сведения, содержащиеся в документах, подтверждающих правовые основания владения, пользования жилым помещением;

5) сведения, содержащиеся в документах с места жительства о совместном проживании;

6) сведения, содержащиеся в документах, подтверждающих родственные отношения, факт нахождения на иждивении;

7) сведения, содержащиеся в документах, подтверждающих доходы гражданина за 3, 6, 9, 12 месяцев;

8) сведения, содержащиеся в документах, подтверждающих факт нахождения в местах лишения свободы или принудительного лечения;

9) сведения, содержащиеся в документах, подтверждающих факт установления инвалидности, заболевания, подтверждающих факт утраты трудоспособности (без установления инвалидности);

10) сведения, содержащиеся в документах, подтверждающих получение пенсии и ее размер (пенсионное удостоверение, справка о назначении пенсии);

11) сведения, содержащиеся в документах, подтверждающих отсутствие трудовой деятельности;

12) сведения, содержащиеся в документах, подтверждающих наличие трудового стажа, необходимого для назначения трудовой (страховой) пенсии по старости или пенсии за выслугу лет, или основания для получения удостоверения «Ветеран труда»;

13) сведения, содержащиеся в документах, подтверждающих право на меры социальной поддержки отдельным категориям граждан, проживающих на территории Новосибирской области;

14) сведения, содержащиеся в документах, подтверждающих государственную регистрацию факта рождения ребенка;

15) сведения, содержащиеся в документах, подтверждающих установление опеки над ребенком или подтверждающий факт назначения опекуна (попечителя) над недееспособным или ограниченно дееспособным гражданином;

16) сведения, содержащиеся в документах, подтверждающих утрату гражданином в несовершеннолетнем возрасте родительского попечения;

17) иные сведения согласно утвержденным нормативными правовыми актами, административными регламентами предоставления государственных услуг.

9.4. При рассмотрении обращений граждан Российской Федерации, иностранных граждан, лиц без гражданства подлежат обработке их следующие ПДн:

1) фамилия, имя, отчество (последнее при наличии);

2) почтовый адрес;

3) адрес электронной почты;

4) указанный в обращении контактный телефон;

5) иные ПДн, указанные в обращении, а также ставшие известными в ходе личного приема граждан или в процессе рассмотрения обращения.

9.5. При обращении юридических лиц (индивидуальных предпринимателей), осуществляется обработка следующих ПДн их представителей:

1) фамилия, имя, отчество (последнее при наличии);

2) документ, удостоверяющий личность (вид, серия, номер, дата выдачи, наименование органа, выдавшего его);

3) адрес места жительства;

4) номер контактного телефона и, при наличии, адрес электронной почты;

5) идентификационный номер налогоплательщика.

9.6. Обработка ПДн, необходимых в связи с предоставлением государственных услуг и исполнением государственных функций, осуществляется без согласия субъектов ПДн в соответствии с пунктом 4 части 1 статьи 6 Федерального закона от 27.07.2006 № 152 - ФЗ, Федеральным законом 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» и иными нормативными правовыми актами, определяющими предоставление государственных услуг и исполнение государственных функций в установленной сфере деятельности ГКУ НСО ЦСПН (наименование) района.

9.7. Обработка ПДн, необходимых в связи с предоставлением государственных услуг и исполнением государственных функций, осуществляется специалистами ГКУ НСО ЦСПН Северного района, ответственными за предоставление соответствующих государственных услуг и (или) исполняющих государственные функции, и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

9.8. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) ПДн, необходимых в связи с предоставлением государственных услуг или исполнением государственных функций, осуществляется непосредственно от субъектов ПДн путем:

1) получения подлинников документов, необходимых для предоставления государственных услуг или исполнения государственных функций, в том числе заявления;

2) заверения необходимых копий документов;

3) внесения сведений в учетные формы (на бумажных и электронных носителях);

4) внесения ПДн в прикладные программные подсистемы информационных систем ГКУ НСО ЦСПН Северного района.

9.9. При обработке ПДн, необходимых в связи с предоставлением государственных услуг и исполнением государственных функций, запрещается запрашивать у субъектов ПДн и третьих лиц ПДн в случаях, не предусмотренных законодательством.

9.10. При сборе ПДн сотрудник ГКУ НСО ЦСПН Северного района, осуществляющий получение ПДн непосредственно от субъектов ПДн, обратившихся за предоставлением государственной услуги или в связи с исполнением государственной функции, разъясняет указанным субъектам ПДн юридические последствия отказа предоставить ПДн.

9.11. Передача (распространение, предоставление) и использование ПДн субъектов ПДн (заявителей), необходимых в связи с предоставлением государственных услуг и исполнением государственных функций, осуществляется в случаях и порядке, предусмотренных федеральным законодательством.

10. Правила обработки ПДн при поручении обработки ПДн другому лицу

10.1. ГКУ НСО ЦСПН Северного района вправе поручить обработку ПДн другому лицу:

с согласия субъекта ПДн, если иное не предусмотрено федеральным законодательством;

на основании заключаемого с этим лицом договора;

путем принятия соответствующего акта (далее - поручение).

10.2. Лицо, осуществляющее обработку ПДн по поручению ГКУ НСО ЦСПН Северного района, обязано соблюдать принципы и правила обработки ПДн.

10.3. В случае, если ГКУ НСО ЦСПН Северного района поручит обработку ПДн другому лицу, ответственность перед субъектом ПДн за действия указанного лица несет ГКУ НСО ЦСПН Северного района. Лицо, осуществляющее обработку ПДн по поручению ГКУ НСО ЦСПН Северного района, несет ответственность перед ГКУ НСО ЦСПН Северного района.

10.4. В случае необходимости получения согласия на обработку ПДн от субъекта ПДн обязанность получения такого согласия возлагается на ГКУ НСО ЦСПН Северного района.

11. Правила обработки общедоступных ПДн

11.1. Общедоступные ПДн физических лиц, полученные из сторонних общедоступных источников ПДн, обрабатываются в исключительных случаях в сроки, не превышающие необходимые для их использования. При этом совместно с такими данными должны собираться реквизиты их источника и подтверждение согласия субъекта ПДн на включение такой информации в общедоступные источники ПДн, так как в случае обработки общедоступных ПДн обязанность доказывания того, что обрабатываемые ПДн являются общедоступными, возлагается на ГКУ НСО ЦСПН Северного района.

По достижению целей обработки общедоступных ПДн они подлежат немедленному уничтожению.

С целью информационного обеспечения и осуществления взаимодействия со сторонними физическими и юридическими лицами в ГКУ НСО ЦСПН Северного района

могут создаваться общедоступные источники ПДн. Создание общедоступного источника ПДн осуществляется по решению директора ГКУ НСО ЦСПН Северного района.

В общедоступный источник ПДн с письменного согласия (при наличии) субъекта ПДн могут включаться: должность, фамилия, имя, отчество, абонентский номер рабочего телефона, место получения образования, достигнутые результаты и другая информация.

Включение в общедоступные источники ПДн субъекта ПДн допускается только на основании его письменного согласия.

Исключение ПДн из указанного общедоступного источника осуществляется при утрате необходимости в обработке таких данных, либо на основании заявления субъекта ПДн в соответствии с действующим законодательством Российской Федерации.

11.2. Особенности обработки ПДн, разрешенных субъектом ПДн для распространения.

11.1.1. Согласие на обработку ПДн, разрешенных субъектом ПДн для распространения, оформляется отдельно от иных согласий субъекта ПДн на обработку его ПДн. ГКУ НСО ЦСПН Северного района обязано обеспечить субъекту ПДн возможность определить перечень ПДн по каждой категории ПДн, указанной в согласии на обработку ПДн, разрешенных субъектом ПДн для распространения.

11.1.2. В случае раскрытия ПДн неопределенному кругу лиц самим субъектом ПДн без предоставления ГКУ НСО ЦСПН Северного района согласия, предусмотренного настоящей статьей, обязанность предоставить доказательства законности последующего распространения или иной обработки таких ПДн лежит на каждом лице, осуществившем их распространение или иную обработку.

11.1.3. В случае, если ПДн оказались раскрытыми неопределенному кругу лиц вследствие правонарушения, преступления или обстоятельств непреодолимой силы, обязанность предоставить доказательства законности последующего распространения или иной обработки таких ПДн лежит на каждом лице, осуществившем их распространение или иную обработку.

11.1.4. В случае, если из предоставленного субъектом ПДн согласия на обработку ПДн, разрешенных субъектом ПДн для распространения, не следует, что субъект ПДн согласился с распространением ПДн, такие ПДн обрабатываются оператором, которому они предоставлены субъектом ПДн, без права распространения.

11.1.5. В случае, если из предоставленного субъектом ПДн согласия на обработку ПДн, разрешенных субъектом ПДн для распространения, не следует, что субъект ПДн не установил запреты и условия на обработку ПДн, предусмотренные подпунктом 11.1.9. настоящего пункта, или если в предоставленном субъектом ПДн таком согласии не указаны категории и перечень ПДн, для обработки которых субъект ПДн устанавливает условия и запреты в соответствии с подпунктом 11.1.9. настоящего пункта, такие ПДн обрабатываются оператором, которому они предоставлены субъектом ПДн, без передачи (распространения, предоставления, доступа) и возможности осуществления иных действий с ПДн неограниченному кругу лиц.

11.1.6. Согласие на обработку ПДн, разрешенных субъектом ПДн для распространения, может быть предоставлено ГКУ НСО ЦСПН Северного района:

1) непосредственно;

2) с использованием информационной системы уполномоченного органа по защите прав субъектов ПДн.

11.1.7. Правила использования информационной системы уполномоченного органа по защите прав субъектов ПДн, в том числе порядок взаимодействия субъекта ПДн с ГКУ НСО ЦСПН Северного района, определяются уполномоченным органом по защите прав субъектов ПДн.

11.1.8. Молчание или бездействие субъекта ПДн ни при каких обстоятельствах не может считаться согласием на обработку ПДн, разрешенных субъектом ПДн для распространения.

11.1.9. В согласии на обработку ПДн, разрешенных субъектом ПДн для распространения, субъект ПДн вправе установить запреты на передачу (кроме предоставления доступа) этих ПДн ГКУ НСО ЦСПН Северного района неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих ПДн неограниченным кругом лиц. Отказ ГКУ НСО ЦСПН Северного района в установлении субъектом ПДн запретов и условий, предусмотренных настоящей статьей, не допускается.

11.1.10. ГКУ НСО ЦСПН Северного района обязано в срок не позднее трех 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.

11.1.11. Установленные субъектом ПДн запреты на передачу (кроме предоставления доступа), а также на обработку или условия обработки (кроме получения доступа) ПДн, разрешенных субъектом ПДн для распространения, не распространяются на случаи обработки ПДн в государственных, общественных и иных публичных интересах, определенных законодательством Российской Федерации.

11.1.12. Передача (распространение, предоставление, доступ) ПДн, разрешенных субъектом ПДн для распространения, должна быть прекращена в любое время по требованию субъекта ПДн. Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) субъекта ПДн, а также перечень ПДн, обработка которых подлежит прекращению. Указанные в данном требовании ПДн могут обрабатываться только оператором, которому оно направлено.

11.1.13. Действие согласия субъекта ПДн на обработку ПДн, разрешенных субъектом ПДн для распространения, прекращается с момента поступления ГКУ НСО ЦСПН Северного района требования, указанного в подпункте 11.1.12. настоящего пункта.

11.1.14. Субъект ПДн вправе обратиться с требованием прекратить передачу (распространение, предоставление, доступ) своих ПДн, ранее разрешенных субъектом ПДн для распространения, к любому лицу, обрабатывающему его ПДн, в случае несоблюдения положений настоящей статьи или обратиться с таким требованием в суд. Данное лицо обязано прекратить передачу (распространение, предоставление, доступ) ПДн в течение трех рабочих дней с момента получения требования субъекта ПДн или в срок, указанный во вступившем в законную силу решении суда, а если такой срок в решении суда не указан, то в течение трех рабочих дней с момента вступления решения суда в законную силу.

12. Правовое основание обработки ПДн

12.1. Правовое основание обработки ПДн в ГКУ НСО ЦСПН Северного района включает в себя:

определение законности целей обработки ПДн;

оценку вреда, который может быть причинен субъекту ПДн в случае нарушения требований по обработке и обеспечению безопасности ПДн; определение заданных характеристик безопасности ПДн;

определение сроков обработки, в т.ч. хранения ПДн, осуществление контроля за соблюдением сроков обработки ПДн и фактов достижения целей обработки ПДн.

12.2. Определение законности целей обработки ПДн.

При определении правовых оснований обработки ПДн должны определяться реквизиты федеральных законов, а также иных подзаконных нормативных правовых актов и документов, которые требуют обработки ПДн или иных документов, являющихся такими основаниями.

Обработка ПДн без документально определенного и оформленного правового основания обработки ПДн в ГКУ НСО ЦСПН Северного района не допускается.

12.3. Оценка вреда, который может быть причинен субъектам ПДн в случае нарушения требований по обработке и обеспечению безопасности ПДн.

Оценкой вреда, который может быть причинен субъекту ПДн в случае нарушения требований по обработке и обеспечению безопасности ПДн, является определение юридических или иным образом затрагивающих права и законные интересы последствий в отношении субъекта ПДн, которые могут возникнуть в случае нарушения требований по обработке и обеспечению безопасности ПДн.

Определение таких юридических последствий необходимо для недопущения нарушения и обеспечения защиты прав и свобод человека и гражданина при обработке его ПДн, в т.ч. защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также определения соотношения вреда, который может быть причинен субъектам ПДн в случае нарушения требований по обработке и обеспечению безопасности ПДн и принимаемых мер.

Обработка ПДн в ГКУ НСО ЦСПН Северного района без принятия мер по обеспечению безопасности ПДн не допускается.

12.4. Заданные характеристики безопасности ПДн.

Всеми специалистами ГКУ НСО ЦСПН Северного района, получающими доступ к ПДн, должна обеспечиваться конфиденциальность таких данных: обязательное для соблюдения требование не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законодательством.

Вне зависимости от необходимости обеспечения конфиденциальности ПДн, при обработке ПДн должно определяться наличие требований по обеспечению защищенности от уничтожения ПДн; обеспечению защищенности от изменения ПДн; обеспечению защищенности от блокирования ПДн; обеспечению защищенности от иных несанкционированных действий.

Обеспечение указанных характеристик безопасности ПДн устанавливается нормативными правовыми актами Российской Федерации и нормативными правовыми актами Новосибирской области.

12.5. Определение сроков обработки, в т.ч. хранения ПДн, осуществление контроля за соблюдением сроков обработки ПДн и фактов достижения целей обработки ПДн.

На основании определенных целей обработки ПДн, способов обработки и образующихся в процессе такой обработки различных видов документов устанавливаются сроки обработки и хранения ПДн.

Определение сроков хранения осуществляется в соответствии с требованиями законодательства Российской Федерации, в т.ч. в соответствии с перечнями типовых архивных документов с указанием сроков их хранения.

При использовании документов, содержащих ПДн, в различных целях, определение сроков обработки, в т.ч. хранения, таких документов устанавливается по максимальному сроку, предусмотренному федеральным законодательством.

При этом в случае наличия ПДн в документах, обработка которых более не требуется, производятся действия по уничтожению ПДн.

Обработка ПДн без документально определенных и оформленных сроков обработки, в том числе хранения ПДн, не допускается.

С целью выполнения требования по уничтожению, либо обезличиванию ПДн по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законодательством, в ГКУ НСО ЦСПН Северного района может создаваться комиссия, определяющая факт достижения целей обработки ПДн и достижение предельных сроков хранения документов, содержащих ПДн.

13. Действия (операции) с ПДн

Обработкой ПДн называется любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств, включая: сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу, обезличивание, блокирование, удаление, уничтожение персональных данных.

Обработка ПДн без определенных и документально оформленных действий (операций), совершаемых с ПДн, не допускается.

14. Осуществление сбора ПДн

14.1. Способы сбора ПДн и источники их получения.

В ГКУ НСО ЦСПН (наименование) района применяются следующие способы получения ПДн субъектов ПДн:

заполнение субъектом ПДн соответствующих форм;

получение ПДн от третьих лиц;

получение данных на основании запроса третьим лицам;

сбор данных из общедоступных источников.

14.2. Правила сбора ПДн.

Если предоставление ПДн является обязательным в соответствии с федеральным законодательством, иными нормативными правовыми документами, ГКУ НСО ЦСПН Северного района обязано разъяснить субъекту ПДн юридические последствия отказа предоставить его ПДн.

Если основания на обработку ПДн без согласия отсутствуют, то необходимо получение согласия субъекта ПДн на обработку его ПДн. Обработка ПДн без получения такого согласия запрещается.

Если ПДн получены не от субъекта ПДн, ГКУ НСО ЦСПН Северного района до начала обработки таких ПДн обязано предоставить субъекту ПДн следующую информацию: наименование оператора или его представителя; сведения о цели обработки ПДн и ее правовое основание; сведения о предполагаемых пользователях ПДн; сведения об установленных правах субъекта ПДн; сведения об источниках получения ПДн.

ГКУ НСО ЦСПН Северного района освобождается от обязанности предоставлять субъекту ПДн информацию в случаях, если:

субъект ПДн уведомлен об осуществлении обработки его ПДн соответствующим оператором;

ПДн получены на основании федерального законодательства или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект ПДн;

ПДн сделаны общедоступными субъектом ПДн или получены из общедоступного источника;

предоставление субъекту ПДн сведений нарушает права и законные интересы третьих лиц.

15. Осуществление систематизации, накопления, уточнения и использования ПДн

Систематизация, накопление, уточнение, использование ПДн в ГКУ НСО ЦСПН Северного района осуществляются законными способами в соответствии с правилами, инструкциями, руководствами, регламентами и иными документами, определяющими технологический процесс обработки информации.

Уточнение ПДн в ГКУ НСО ЦСПН Северного района производится только на основании законно полученной в установленном порядке информации. Решение об уточнении ПДн субъекта ПДн принимается лицом, ответственным за организацию обработки ПДн.

Использование ПДн в ГКУ НСО ЦСПН Северного района осуществляется исключительно в заявленных целях. Использование ПДн в заранее не определенных и не оформленных установленным образом целях не допускается.

16. Осуществление передачи ПДн

Передача персональных данных в ГКУ НСО ЦСПН Северного района осуществляется с соблюдением настоящих Правил и действующего законодательства Российской Федерации.

В ГКУ НСО ЦСПН Северного района приняты следующие способы передачи ПДн субъектов ПДн:

передача ПДн на электронных и бумажных носителях информации нарочно;

передача ПДн на электронных и бумажных носителях посредством почтовой связи;

передача ПДн по электронным каналам с использованием средств криптографической защиты информации.

Перед осуществлением передачи ПДн проверяется основание на осуществление такой передачи и наличие согласия на передачу ПДн в согласии субъекта ПДн на обработку ПДн или наличие иных законных оснований.

Передача ПДн должна осуществляться на основании:

договора с третьей стороной, которой осуществляется передача ПДн; запроса, полученного от третьей стороны, которой осуществляется передача ПДн;

исполнения возложенных законодательством Российской Федерации на ГКУ НСО ЦСПН Северного района функций, полномочий и обязанностей.

17. Осуществление хранения ПДн

Хранение ПДн в ГКУ НСО ЦСПНСеверного района осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен нормативными правовыми актами Российской Федерации, нормативными правовыми актами Новосибирской области.

Хранение ПДн в ГКУ НСО ЦСПН Северного района осуществляется на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного: доступа к ним; их уничтожения; изменения; блокирования; копирования; предоставления; распространения.

18. Осуществление блокирования ПДн

Блокированием ПДн называется временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

Блокирование ПДн осуществляется:

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 с момента такого обращения или получения указанного запроса на период проверки;

в случае отсутствия возможности уничтожения ПДн в установленные сроки до их уничтожения.

После устранения выявленной неправомерной обработки ПДн ГКУ НСО ЦСПН Северного района осуществляет снятие блокирования ПДн.

Решение о блокировании и снятии блокирования ПДн субъекта ПДн принимается лицом, ответственным за организацию обработки ПДн.

19. Осуществление обезличивания ПДн

Обезличивание ПДн при обработке ПДн с использованием средств автоматизации осуществляется на основании нормативных правовых актов, правил, инструкций, руководств, регламентов и иных документов для достижения заранее определенных и заявленных целей.

Допускается обезличивание ПДн при обработке ПДн без использования средств автоматизации производить способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

20. Осуществление уничтожения ПДн

ГКУ НСО ЦСПН Северного района обязано уничтожить или обеспечить уничтожение ПДн (если обработка ПДн осуществляется другим лицом, действующим по поручению ГКУ НСО ЦСПН Северного района) в следующих случаях:

при достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом (в срок, не превышающий тридцати 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 оператором и субъектом ПДн либо если оператор не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ или другими федеральными законами);

персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки (в срок, не превышающий семи рабочих дней);

в случае выявления неправомерной обработки ПДн, если обеспечить правомерность обработки ПДн невозможно (в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн);

в случае отзыва субъектом ПДн согласия на обработку его ПДн и в случае, если сохранение ПДн более не требуется для целей обработки ПДн (в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между оператором и субъектом ПДн либо если оператор не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ или другими федеральными законами);

в случае обращения субъекта ПДн к оператору с требованием о прекращении обработки ПДн (в срок, не превышающий десяти рабочих дней с даты получения оператором соответствующего требования, за исключением случаев, предусмотренных пунктами 2 - 11 части 1 статьи 6, частью 2 статьи 10 и частью 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации).

В случае отсутствия возможности уничтожения ПДн в течение сроков, указанных в абзацах втором – шестом настоящего Порядка, осуществляется блокирование таких ПДн или обеспечивается их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению министерства) и обеспечивается уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

При уничтожении ПДн необходимо:

убедиться в необходимости уничтожения ПДн;

убедиться в том, что уничтожаются те персональные данные, которые предназначены для уничтожения;

уничтожить персональные данные подходящим способом в соответствии с нижеследующими требованиями или способом, указанным в соответствующем распорядительном документе или технологической инструкции;

при необходимости уведомить об уничтожении ПДн требуемых лиц.

При необходимости уничтожения ПДн следует руководствоваться следующими требованиями:

бумажные носители, содержащие персональные данные, должны уничтожаться при помощи специального оборудования (уничтожителей (измельчителей) бумаги);

после окончания процедуры уничтожения ПДн и (или) материальных носителей ПДн должен быть составлен соответствующий акт уничтожения;

контроль за своевременным уничтожением ПДн осуществляют ответственные за организацию обработки ПДн;

осуществлять подтверждение факта уничтожения ПДн в соответствии с Требованиями к подтверждению уничтожения персональных данных, утвержденными приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 179 «Об утверждении требований к подтверждению уничтожению персональных данных».

Уничтожение части ПДн (обрабатываемых с использованием и без использования средств автоматизации), если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, зачеркивание, стирание).

При необходимости уничтожения части ПДн допускается уничтожать материальный носитель одним из указанных в настоящих Правилах способов, с предварительным копированием сведений, не подлежащих уничтожению, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению.

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

Уничтожение документов, содержащих персональные данные, утративших свое практическое значение и не подлежащих архивному хранению, производится на основании акта уничтожения ПДн:

в случае уничтожения ПДн по заявлению гражданина либо в случае неправомерного осуществления обработки ПДн – по форме согласно приложению № 1 к Правилам;

в других случаях – по форме согласно приложению № 2 к Правилам.

Акт об уничтожении ПДн должен содержать:

наименование и адрес оператора;

наименование или фамилию, имя, отчество (последнее - при наличии), адрес лица (лиц), осуществляющего (осуществляющих) обработку ПДн субъекта (субъектов) ПДн по поручению оператора (если обработка была поручена такому (таким) лицу (лицам);

фамилию, имя, отчество (последнее - при наличии) субъекта (субъектов) или иную информацию, относящуюся к определенному (определенным) физическому (физическим) лицу (лицам), чьи ПДн были уничтожены;

фамилию, имя, отчество (последнее - при наличии), должность лиц (лица), уничтоживших ПДн субъекта ПДн, а также их (его) подпись;

перечень категорий, уничтоженных ПДн субъекта (субъектов) ПДн;

наименование уничтоженного материального (материальных) носителя (носителей), содержащего (содержащих) ПДн субъекта (субъектов) ПДн, с указанием количества листов в отношении каждого материального носителя (в случае обработки ПДн без использования средств автоматизации);

наименование информационной (информационных) системы (систем) ПДн, из которой (которых) были уничтожены ПДн субъекта (субъектов) ПДн (в случае обработки ПДн с использованием средств автоматизации);

способ уничтожения ПДн;

причину уничтожения ПДн;

дату уничтожения ПДн субъекта (субъектов) ПДн.

Хранение актов об уничтожении ПДн и (или) материальных носителей ПДн осуществляется в течение срока исковой давности, если иное не установлено нормативными правовыми актами Российской Федерации.

21. Права и обязанности субъекта ПДн и ГКУ НСО ЦСПН (наименование) района при обработке ПДн

21.1. Права субъекта ПДн

Субъект персональных данных, чьи ПДн обрабатываются в ГКУ НСО ЦСПН Северного района, имеет право:

на получение сведений о подтверждении факта обработки ПДн в ГКУ НСО ЦСПН Северного района;

на получение сведений о правовых основаниях и целях обработки ПДн; на получение сведений о лицах (за исключением сведений о государственных служащих и сотрудниках ГКУ НСО ЦСПН Северного района), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании служебного контракта (трудового договора) или на основании федерального законодательства;

на получение сведений об обрабатываемых ПДн, относящихся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законодательством; на получение сведений о сроках обработки ПДн, в т.ч. сроках их хранения; на получение сведений о порядке осуществления субъектом ПДн своих прав, предусмотренных законодательством в области ПДн;

на получение информации об осуществленной или о предполагаемой трансграничной передаче данных;

на получение сведений о наименовании и адресе лица, осуществляющего обработку ПДн по поручению ГКУ НСО ЦСПН Северного района, если обработка поручена или будет поручена такому лицу;

на получение иных сведений, предусмотренных законодательством в области ПДн и другими федеральными законами;

требовать от ГКУ НСО ЦСПН Северного района 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;

принимать предусмотренные законом меры по защите своих прав; требовать от ГКУ НСО ЦСПН Северного района предоставления ему ПДн в доступной форме; повторного обращения и запроса в целях получения сведений и ознакомления с его ПДн;

заявить возражение против принятия решения на обработку ПДн, порождающего юридические последствия в отношении субъекта ПДн или иным образом затрагивающего его права и законные интересы;

обжаловать действия или бездействие ГКУ НСО ЦСПН Северного района в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке, если субъект ПДн считает, что ГКУ НСО ЦСПН Северного района осуществляет обработку его ПДн с нарушением требований федерального законодательства или иным образом нарушает его права и свободы;

на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке;

требовать предоставления безвозмездно субъекту ПДн или его представителю возможности ознакомления с ПДн, относящимися к этому субъекту ПДн;

принимать решение о предоставлении его ПДн и давать согласие на их обработку свободно, своей волей и в своем интересе; отзывать согласие на обработку ПДн;

на прекращение обработки ПДн в срок, не превышающий десяти рабочих дней с даты получения за исключением случаев, предусмотренных пунктами 2-11 части 1 статьи 6, частью 2 статьи 10 и частью 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае уведомления с указанием причин продления срока предоставления запрашиваемой информации.

21.2. Обязанности субъекта ПДн

Субъект ПДн, чьи ПДн обрабатываются в ГКУ НСО ЦСПН Северного района, обязан:

предоставлять свои ПДн в случаях, когда федеральным законодательством предусматриваются случаи обязательного предоставления субъектом ПДн своих ПДн;

с целью соблюдения его законных прав и интересов подавать только достоверные ПДн.

Кроме указанных обязанностей в вопросах обработки его ПДн на субъект ПДн налагаются иные обязанности, предусмотренные действующим законодательством Российской Федерации.

21.3. Права ГКУ НСО ЦСПН Северного района при обработке ПДн субъектов ПДн ГКУ НСО ЦСПН Северного района при обработке ПДн субъектов ПДн имеет право:

обрабатывать ПДн в соответствии с действующим законодательством Российской Федерации;

поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законодательством, на основании заключаемого с этим лицом договора, в том числе государственного контракта, либо путем принятия соответствующего акта;

мотивированно отказать субъекту ПДн в выполнении повторного запроса в целях получения сведений, касающихся обработки его ПДн, при нарушении субъектом ПДн своих обязанностей по подаче такого запроса;

ограничить право субъекта ПДн на доступ к его ПДн в соответствии с федеральным законодательством, в т.ч. если обработка ПДн осуществляется в соответствии с законодательством о противодействии легализации доходов, полученных преступным путем, и финансированию терроризма;

ограничить право субъекта ПДн на доступ к его ПДн в соответствии с федеральным законодательством, в т.ч. если доступ субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц;

самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных действующим законодательством в области ПДн, если иное не предусмотрено федеральным законодательством;

осуществлять или обеспечивать блокирование, или уничтожение ПДн, если обеспечить правомерность обработки ПДн невозможно; осуществлять или обеспечивать уничтожение ПДн;

в случае достижения цели обработки ПДн продолжить обработку ПДн, если обработка ПДн осуществляется без согласия субъекта ПДн на основании пункта 4 статьи 21 Федерального закона от 27.07.2006 № 152-ФЗ;

в случае отзыва субъектом ПДн согласия на обработку его ПДн продолжить обработку ПДн, если обработка ПДн осуществляется без согласия субъекта ПДн на основании пункта 5 статьи 21 Федерального закона от 27.07.2006 № 152-ФЗ;

в случае отсутствия возможности уничтожения ПДн осуществить блокирование таких ПДн и обеспечить уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен федеральным законодательством;

осуществлять без уведомления уполномоченного органа по защите прав субъектов ПДн обработку ПДн, указанных в пункте 2 статьи 22 Федерального закона от 27.07.2006 № 152-ФЗ.

21.4. Обязанности ГКУ НСО ЦСПН Северного района при обработке ПДн субъектов ПДн

ГКУ НСО ЦСПН Северного района при обработке ПДн субъектов ПДн обязано:

строго соблюдать принципы и правила обработки ПДн; в случае, если обработка ПДн осуществляется по поручению оператора, строго соблюдать и выполнять требования оператора;

не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законодательством;

по требованию субъекта ПДн либо по решению суда или иных уполномоченных государственных органов исключить из общедоступных источников ПДн сведения о субъекте ПДн;

обеспечить конкретность и информированность согласия на обработку ПДн;

получать согласие на обработку ПДн, если иное не предусмотрено действующим законодательством;

в случае получения согласия на обработку ПДн от представителя субъекта ПДн проверять полномочия данного представителя на дачу согласия от имени субъекта ПДн;

представить доказательство получения согласия субъекта ПДн на обработку его ПДн или доказательство наличия оснований обработки ПДн без получения согласия;

строго соблюдать требования к содержанию согласия в письменной форме субъекта ПДн на обработку его ПДн;

предоставить субъекту ПДн сведения по запросу субъекта ПДн в доступной форме, в которых не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн;

мотивировать и представить доказательства обоснованности отказа в выполнении повторного запроса субъекта ПДн;

разъяснить субъекту ПДн порядок принятия решения на обработку его ПДн и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом ПДн своих прав и законных интересов;

предоставить субъекту ПДн по его просьбе информацию, касающуюся обработки его ПДн;

разъяснить субъекту ПДн юридические последствия отказа предоставить его ПДн, если предоставление ПДн является обязательным в соответствии с федеральным законодательством;

принимать меры, необходимые и достаточные для обеспечения выполнения своих обязанностей в области ПДн, если иное не предусмотрено федеральным законодательством;

опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн;

по запросу уполномоченного органа по защите прав субъектов ПДн представить документы, определяющие политику в отношении обработки ПДн, и сведения о реализуемых требованиях к защите ПДн;

принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн;

сообщить 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 при получении запроса субъекта ПДн или его представителя; 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;

предоставить безвозмездно субъекту ПДн или его представителю возможность ознакомления с ПДн, относящимися к этому субъекту ПДн;

внести в ПДн необходимые изменения или уничтожить такие ПДн в случае предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными; строго соблюдать сроки по уведомлениям, блокированию и уничтожению 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;

сообщить в уполномоченный орган по защите прав субъектов ПДн по запросу этого органа необходимую информацию;

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 оператор обязан осуществить блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту ПДн, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора) 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 оператор обязан осуществить блокирование ПДн, относящихся к этому субъекту ПДн, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора) 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;

уточнить ПДн, либо обеспечить их уточнение (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора) и снять блокирование ПДн 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;

прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению оператора в случае выявления неправомерной обработки ПДн, осуществляемой оператором или лицом, действующим по поручению оператора;

уничтожить ПДн или обеспечить их уничтожение в случае, если обеспечить правомерность обработки ПДн невозможно;

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 об устранении допущенных нарушений или об уничтожении ПДн;

прекратить обработку ПДн или обеспечить ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора) и уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора):

в случае достижения цели обработки ПДн, если обработка ПДн осуществляется без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ;

в случае отзыва субъектом ПДн согласия на обработку его ПДн, если обработка ПДн осуществляется без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ;

уведомить уполномоченный орган по защите прав субъектов ПДн о своем намерении осуществлять обработку ПДн;

уведомить уполномоченный орган по защите прав субъектов ПДн в случае изменения сведений, указанных в уведомлении о своем намерении осуществлять обработку ПДн;

назначить лицо, ответственное за организацию обработки ПДн; предоставлять лицу, ответственному за организацию обработки ПДн, необходимые сведения;

неукоснительно соблюдать все требования настоящих Правил;

ознакомить сотрудников ГКУ НСО ЦСПН Северного района, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в т.ч. требованиями к защите ПДн, документами, определяющими политику в отношении обработки ПДн, и организовать их обучение;

в случае обращения субъекта ПДн к ГКУ НСО ЦСПН Северного района с требованием о прекращении обработки ПДн ГКУ НСО ЦСПН Северного района обязано в срок, не превышающий десяти рабочих дней с даты получения ГКУ НСО ЦСПН Северного района 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 Федерального закона от 27.07.2006 № 152-ФЗ. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления ГКУ НСО ЦСПН Северного района в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации;

в случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) ПДн, повлекшей нарушение прав субъектов ПДн, ГКУ НСО ЦСПН Северного района обязано с момента выявления такого инцидента оператором, уполномоченным органом по защите прав субъектов ПДн или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов ПДн:

1) в течение двадцати четырех 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 оператором на взаимодействие с уполномоченным органом по защите прав субъектов ПДн, по вопросам, связанным с выявленным инцидентом;

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

22. Требования к сотрудникам ГКУ НСО ЦСПН (наименование) района, осуществляющим доступ к ПДн или их обработку

Лицо, ответственное за организацию обработки ПДн в ГКУ НСО ЦСПН Северного района, организует ознакомление сотрудников, непосредственно осуществляющих обработку ПДн или доступ к ним, с положениями законодательства Российской Федерации о ПДн (в т.ч. с требованиями к защите ПДн), нормативных правовых актов ГКУ НСО ЦСПН Северного района по вопросам обработки ПДн, включая настоящие Правила:

при оформлении служебного контракта (трудового договора); при первоначальном допуске к обработке ПДн;

при назначении на должность, связанную с обработкой ПДн или доступом к ним;

после внесения изменений в действующее законодательство Российской Федерации о ПДн, нормативные правовые акты ГКУ НСО ЦСПН Северного района по вопросам обработки ПДн.

Сотрудники ГКУ НСО ЦСПН Северного района, непосредственно осуществляющие обработку ПДн или доступ к ним, обязаны:

неукоснительно следовать принципам обработки ПДн;

знать и строго соблюдать положения действующего законодательства Российской Федерации в области ПДн;

знать и строго соблюдать положения нормативных правовых актов ГКУ НСО ЦСПН Северного района в области обработки и обеспечения безопасности ПДн;

знать и строго соблюдать инструкции, руководства и иные эксплуатационные документы на применяемые средства автоматизации, в том числе программное обеспечение, и средства защиты информации;

соблюдать конфиденциальность ПДн, не предоставлять третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законодательством;

не допускать нарушений требований и правил обработки и обеспечения безопасности ПДн.

Сотрудники ГКУ НСО ЦСПН Северного района несут личную ответственность за соблюдение требований действующего законодательства Российской Федерации, настоящих Правил.

23. Обеспечение безопасности ПДн при их обработке

В соответствии с требованиями действующего законодательства в области ПДн при обработке ПДн ГКУ НСО ЦСПН Северного района принимает необходимые правовые, организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий.

24. Мероприятия при возникновении обстоятельств непреодолимой силы (форс-мажор)

В случае обстоятельств непреодолимой силы, возникших в результате событий чрезвычайного характера, повлекших нарушения прав субъектов ПДн, ГКУ НСО ЦСПН Северного района освобождается от ответственности при наличии доказательств указанных выше обстоятельств.

В случае возникновения обстоятельств непреодолимой силы и нарушения прав субъектов ПДн, связанных с такими обстоятельствами, ГКУ НСО ЦСПН Северного района принимает все меры для извещения субъекта ПДн.

ПРИЛОЖЕНИЕ № 1
к Правилам обработки
персональных данных

ФОРМА

Акт
об уничтожении персональных данных, обрабатываемых без(с) использования(ем) средств автоматизации

Уважаемый (ая) _____

ГКУ НСО ЦСПН Северного района (ИНН 5435102102, юридический адрес 632080, область Новосибирская, село Северное, улица Ленина, дом 14) уведомляет Вас, что в связи с _____

(указать причины уничтожения персональных данных)

Ваши персональные данные, а именно: _____

_____

являющиеся персональными данными _____

_____ категории, уничтожены

(указать категорию уничтоженных персональных данных субъекта персональных данных)

Нижеследующие бумажные носители (электронные образцы) уничтожены путем

_____

(указать способ уничтожения персональных данных, наименование информационной системы)

№ п/п	Наименование бумажного носителя	Количество листов (цифрами и прописью)

Если выбран ответственный

_____ _____ _____

(должность) *(подпись)* *(расшифровка подписи)*

Если выбрана Комиссия:

Председатель комиссии: _____

Члены комиссии: _____

_____

_____

_____

«___»_____20___г.

ПРИЛОЖЕНИЕ № 2
к Правилам обработки
персональных данных

ФОРМА

Акт
об уничтожении персональных данных, обрабатываемых без(с) использования(ем) средств автоматизации

_____
(фамилия, имя, отчество (последнее – при наличии) субъекта персональных данных)

_____
(фамилия, имя, отчество (последнее – при наличии) субъекта персональных данных)

ГКУ НСО ЦСПН Северного района (ИНН 5435102102, юридический адрес 632080, область Новосибирская, село Северное, улица Ленина, дом 14) уведомляет Вас, что в связи с _____
(указать причины уничтожения персональных данных)
Ваши персональные данные, а именно: _____
_____
являющиеся персональными данными_____
_____ категории,
уничтожены.
(указать категорию уничтоженных персональных данных субъекта персональных данных)
Нижеследующие бумажные носители (электронные образцы) уничтожены путем
_____
(указать способ уничтожения персональных данных, наименование информационной системы)

№ п/п	Наименование бумажного носителя	Количество листов (цифрами и прописью)

Если выбран ответственный

_____ _____ _____
(должность) *(подпись)* *(расшифровка подписи)*

Если выбрана Комиссия:

Председатель комиссии: _____

Члены комиссии: _____
_____
_____

«___»_____20___г.

УТВЕРЖДЕНЫ
приказом ГКУ НСО
ЦСПН Северного
района
от 30.04.25 № 157

Правила
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

1. Настоящими Правилами определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных (далее - ПДн), основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн.

2. В целях осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям в ГКУ НСО ЦСПН Северного района проводятся периодические проверки условий обработки ПДн.

3. Проверки осуществляются лицом, ответственным за защиту информации, в том числе за обеспечение безопасности ПДн, в ГКУ НСО ЦСПН Северного района.

4. Проверки соответствия обработки ПДн установленным требованиям проводятся на основании утвержденного директором ГКУ НСО ЦСПН Северного района ежегодного плана осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям или на основании поступившего в ГКУ НСО ЦСПН Северного района письменного заявления о нарушениях правил обработки ПДн (внеплановые проверки).

Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления.

5. При проведении проверки соответствия порядка обработки ПДн установленным требованиям должны быть полностью, объективно и всесторонне установлены:

1) порядок и условия применения организационных и технических мер по обеспечению безопасности ПДн при их обработке;

2) порядок и условия применения средств защиты информации;

3) эффективность принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию информационной системы ПДн;

4) состояние учета машинных носителей;

5) соблюдение правил обработки ПДн в ГКУ НСО ЦСПН Северного района;

6) наличие (отсутствие) фактов несанкционированного доступа к ПДн и принятие необходимых мер;

7) мероприятия по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) осуществление мероприятий по обеспечению целостности ПДн;

9) соответствие информационной системы, обрабатывающей ПДн, эксплуатационной, проектной и аттестационной документации.

6. Лицо, ответственное за организацию обработки ПДн в ГКУ НСО ЦСПН Северного района, при проведении проверки соответствия обработки ПДн имеет право:

1) запрашивать у сотрудников ГКУ НСО ЦСПН Северного района информацию, необходимую для реализации полномочий;

2) требовать от уполномоченных на обработку ПДн лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем ПДн;

3) принимать меры по приостановлению или прекращению обработки ПДн, осуществляемой с нарушением требований законодательства Российской Федерации;

4) вносить директору ГКУ НСО ЦСПН Северного района предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности ПДн при их обработке;

5) вносить директору ГКУ НСО ЦСПН Северного района предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки ПДн.

7. В отношении ПДн, ставших известными лицу, ответственному за организацию обработки ПДн в ГКУ НСО ЦСПН Северного района при проведении проверки соответствия обработки ПДн в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность.

8. Своевременность и правильность проведения проверки контролируется ответственным за организацию обработки ПДн.

9. Проверка должна быть завершена не позднее чем через 30 календарных дней со дня принятия решения о её проведении.

О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, директору ГКУ НСО ЦСПН Северного района докладывает ответственный за организацию обработки ПДн в форме письменного заключения (докладной записки).

УТВЕРЖДЕН
приказом ГКУ НСО ЦСПН Северного района
от «30» 04 2025 г. № 157

Регламент
защиты информационной системы, ее средств, систем связи и передачи данных

1. Общие положения

1.1 Настоящий Регламент разработан в целях реализации мер по защите периметра (физических и (или) логических границ) информационных систем (далее – ИС) ГКУ НСО ЦСПН Северного района с установленным **2-м классом защищенности** при их взаимодействии с иными ИС и информационно-телекоммуникационными сетями, предусматривающий:

- управление (контроль) входящими в ИС и исходящими из ИС информационными потоками на физической и (или) логической границе;
- обеспечение взаимодействия ИС с иными информационными системами и сетями только через сетевые интерфейсы, которые обеспечивают управление (контроль) информационными потоками с использованием средств защиты информации (управляемые (контролируемые) сетевые интерфейсы), установленных на физическом и (или) логическом периметре ИС (маршрутизаторов, межсетевых экранов, коммутаторов, прокси-серверов, шлюзов безопасности, средств построения виртуальных частных сетей и иных средств защиты информации).

1.2 Количество точек доступа в ИС определяется администратором безопасности ИС с учетом функций ИС, при этом количество точек должно быть минимальным и должен обеспечиваться постоянный и всесторонний контроль входящих и исходящих информационных потоков.

1.3 Настоящий Регламент предназначена для обеспечения защиты информации, обрабатываемой в ИС, при функционировании ИС и определяет порядок действий администратора безопасности ИС при эксплуатации ИС.

2. Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода

2.1 В ИС осуществляется контроль санкционированного и исключение несанкционированного использования технологий мобильного кода (активного контента), в том числе регистрация событий, связанных с использованием технологии мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологии мобильного кода. Технология мобильного кода включает, в том числе использование Java, JavaScript, ActiveX, PDF, Postscript, Flash-анимация и VBScript и иных технологий.

2.2 При контроле использования технологий мобильного кода обеспечивается:

- определение перечня мобильного кода и технологий мобильного кода разрешенных и (или) запрещенных для использования в ИС;
- определение разрешенных мест распространения (серверы информационной системы) и использования мобильного кода;
- (автоматизированные рабочие места, мобильные технические средства информационной системы) и функций ИС, для которых необходимо применение технологии мобильного кода;
- регистрация и анализ событий, связанных с разработкой, приобретением или внедрением технологии мобильного кода;
- исключение возможности использования запрещенного мобильного кода в ИС, а также внедрение мобильного кода в местах, не разрешенных для его установки.

2.3 В ИС определены механизмы обнаружения и анализа мобильного кода для выявления фактов несанкционированного использования мобильного кода и выполнения действий по реагированию (оповещение администраторов, изоляция мобильного кода (перемещение в карантин), блокирование мобильного кода, удаление мобильного кода).

3. Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов

В ИС осуществляется обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов (защита от атак типа «человек посередине»).

Для подтверждения подлинности сторон сетевого соединения (сеанса взаимодействия) и защиты сетевых устройств и сервисов от подмены осуществляться их аутентификация в соответствии с Инструкцией идентификации и аутентификации субъектов доступа и объектов доступа.

4. Исключение возможности отрицания пользователем факта отправки/получения информации другому пользователю

В ИС обеспечивается исключение возможности отрицания пользователем факта отправки/получения информации другому пользователю.

Для исключения возможности отрицания пользователем факта отправки/получения информации другому пользователю осуществляется:

- определение объектов или типов информации, для которых требуется обеспечение неотказуемости отправки/получения (например, сообщения электронной почты);
- обеспечение целостности информации при ее подготовке к передаче и непосредственной ее передаче по каналам связи в соответствии с п.2 настоящего Регламента;

– регистрация событий, связанных с отправкой/получением информации другому пользователю в соответствии с Инструкцией регистрации событий безопасности.

5. Исключение возможности отрицания пользователем факта получения информации от другого пользователя

В ИС обеспечивается исключение возможности отрицания пользователем факта получения информации от другого пользователя.

Для исключения возможности отрицания пользователем факта получения информации осуществляется:

– определение объектов или типов информации, для которых требуется обеспечение неотказуемости получения (сообщения электронной почты);

– обеспечение целостности полученной информации в соответствии с п.3 настоящего Регламента;

– регистрация событий, связанных с получением информации от другого пользователя в соответствии с Инструкцией регистрации событий безопасности.

6. Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации

В ИС обеспечивается защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения, иных данных, не подлежащих изменению в процессе обработки информации.

Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации, обеспечивается принятием мер защиты информации, направленных на обеспечение их конфиденциальности и целостности.

Защита данных, не подлежащих изменению в процессе обработки информации, обеспечивается в отношении информации, хранящейся на жестких магнитных дисках, дисковых накопителях и иных накопителях в информационной системе.

7. Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании этой информационной системы

В ИС обеспечивается защита от угроз безопасности информации, направленных на отказ в обслуживании этой системы.

Защита от угроз безопасности информации, направленных на отказ в обслуживании, осуществляется посредством реализации в ИС мер защиты информационной системы в соответствии с настоящим Регламентом и повышенными характеристиками производительности

телекоммуникационного оборудования и каналов передачи совместно с резервированием информации и технических средств, программного обеспечения, каналов передачи информации в соответствии с Инструкцией обеспечения доступности.

8. Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями

В ИС осуществляется защита периметра (физических и (или) логических границ) ИС при ее взаимодействии с иными ИС и информационно-телекоммуникационными сетями, предусматривающая:

- управление (контроль) входящими в ИС и исходящими из ИС информационными потоками на физической и (или) логической границе ИС (сегментов ИС);
- обеспечение взаимодействия ИС и (или) ее сегментов с иными ИС и сетями только через сетевые интерфейсы, которые обеспечивают управление (контроль) информационными потоками с использованием средств защиты информации (управляемые (контролируемые) сетевые интерфейсы), установленных на физическом и (или) логическом периметре ИС или ее отдельных сегментов (маршрутизаторов, межсетевых экранов, коммутаторов, прокси-серверов, шлюзов безопасности, средств построения виртуальных частных сетей и иных средств защиты информации).

В ИС обеспечена возможность размещения публичных общедоступных ресурсов (в частности, общедоступный веб-сервер), взаимодействующих с ИС через отдельные физические управляемые (контролируемые) сетевые интерфейсы.

Предоставление доступа во внутренние сегменты ИС (демилитаризованную зону) из внешних ИС и сетей возможно только через средства защиты периметра (за исключением внутренних сегментов, которые специально выделены для такого взаимодействия).

В ИС ограничено количество точек доступа в ИС из внешних ИС и сетей до минимально необходимого числа для решения постановленных задач, а также обеспечивающего постоянный и всесторонний контроль входящих и исходящих информационных потоков.

В ИС применяется отдельный физический управляемый (контролируемый) сетевой интерфейс для каждого внешнего телекоммуникационного сервиса.

В ИС установлены правила управления информационными потоками для каждого физического управляемого (контролируемого) сетевого интерфейса.

В ИС обеспечивается защита информации при ее передаче по каналам связи, имеющим выход за пределы контролируемой зоны (при необходимости), путем применения организационно-технических мер или

криптографических методов в соответствии с законодательством Российской Федерации.

В ИС обеспечивается удаление введенных исключений из правил управления информационными потоками после истечения установленного времени.

В ИС исключен выход (вход) через управляемые (контролируемые) сетевые интерфейсы информационных потоков по умолчанию (реализация принципа «запрещено все, что не разрешено»).

9. Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения

В ИС осуществляется завершение сетевых соединений (например, открепление пары порт/адрес (TCP/IP)) по их завершении и (или) по истечении заданного оператором временного интервала неактивности сетевого соединения.

10. Защита мобильных технических средств, применяемых в ИС

К мобильным техническим средствам в ИС относятся:

- съемные машинные носители информации,
- портативные вычислительные устройства и устройства связи с возможностью обработки информации.

Защита мобильных технических средств включает:

- реализацию в зависимости от мобильного технического средства (типа мобильного технического средства) мер по:
  - идентификации и аутентификации в соответствии с Инструкцией идентификации и аутентификации субъектов доступа и объектов доступа,
  - управлению доступом в соответствии с Инструкцией управления доступом субъектов доступа к объектам доступа;
  - ограничению программной среды в соответствии с Инструкцией ограничения программной среды;
  - защите машинных носителей информации в соответствии с настоящим Регламентом;
  - регистрации событий безопасности в соответствии с Инструкцией регистрации событий безопасности;
  - антивирусной защите в соответствии с Инструкцией антивирусной защиты и обнаружения вторжений;
  - контролю (анализу) защищенности в соответствии с Инструкцией контроля защищенности информации.
- очистку (удаление) информации в мобильном техническом средстве после завершения сеанса удаленного доступа к защищаемой

информации или принятие иных мер, исключающих несанкционированный доступ к хранимой защищаемой информации;

– уничтожение съемных машинных носителей информации, которые не подлежат очистке;

– выборочные проверки мобильных технических средств (на предмет их наличия) и хранящейся на них информации (например, на предмет отсутствия информации, не соответствующей маркировке носителя информации);

– запрет возможности автоматического запуска (без команды пользователя) в ИС программного обеспечения на мобильных технических средствах;

– контроль использования в ИС мобильных технических средств.

В ИС допускаются проводные (коммутируемые), беспроводные и широкополосные доступы к объектам доступа ИС с использованием мобильных технических средств: съемных машинных носителей информации (флэш-накопители, внешние накопители на жестких дисках), портативных вычислительных устройств и устройств связи с возможностью обработки информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства).

Контроль использования мобильных технических средств в ИС включает:

– использование в составе ИС для доступа к объектам доступа мобильных технических средств (служебных мобильных технических средств), в которых реализованы меры защиты информации в соответствии с Инструкцией обращения с машинными носителями информации и мобильными техническими средствами в ИС ГКУ НСО ЦСПН (наименование) района;

– ограничение на использование мобильных технических средств в соответствии с задачами (функциями) ИС для решения которых использование таких средств необходимо, и предоставление доступа с использованием мобильных технических средств;

– мониторинг и контроль применения мобильных технических средств на предмет выявления несанкционированного использования мобильных технических средств для доступа к объектам доступа ИС;

– запрет возможности запуска без команды пользователя в информационной системе ПО (программного кода), используемого для взаимодействия с мобильным техническим средством;

– применение мобильных технических средств, включая процедуры выдачи и возврата мобильных технических средств, а также их передачи на техническое обслуживание (процедура должна обеспечивать удаление или недоступность информации), в соответствии с требованиями Инструкцией обращения с машинными носителями информации и мобильными техническими средствами.

В ИС обеспечивается запрет использования в ИС не входящих в ее состав (находящихся в личном использовании) съемных машинных носителей информации.

В ИС обеспечивается запрет использования в ИС съемных машинных носителей информации, для которых не определен владелец (пользователь, организация, ответственные за принятие мер защиты информации).

УТВЕРЖДЕНО
приказом ГКУ НСО ЦСПН
Северного района
от 30.04.25 № 157

Типовое обязательство
сотрудника ГКУ НСО ЦСПН Северного района, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта (трудового договора) прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей

Обязательство о соблюдении конфиденциальности персональных данных

Я, _____

_____

(фамилия, имя, отчество (последнее - при наличии), должность)

непосредственно осуществляя обработку персональных данных при выполнении своих должностных обязанностей, ознакомлен (а) с требованиями по соблюдению конфиденциальности обрабатываемых мною персональных данных субъектов персональных данных и обязуюсь в случае расторжения со мной служебного контракта (трудового договора) прекратить обработку персональных данных, ставших мне известными в связи с исполнением должностных обязанностей.

Я ознакомлен (а) с предусмотренной действующим законодательством Российской Федерации ответственностью за нарушения неприкосновенности частной жизни и установленного порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).

_____

(фамилия, имя, отчество (последнее – при наличии))

_____

(паспортные данные)

_____

(подпись)

_____

(дата)

УТВЕРЖДЕНА
приказом ГКУ НСО ЦСПН
Северного района
от 30.04.25 № 157

Типовая форма согласия на обработку персональных данных

Я,_____
_____
(фамилия, имя, отчество (последнее - при наличии), должность)
документ, удостоверяющий личность: серия_____№_____выдан_____
(дата выдачи)
_____
(кем выдан)
зарегистрированный(ая) по адресу:_____
_____

даю ГКУ НСО ЦСПН Северного района (ОГРН 1185476101491, ИНН 5435102102), находящемуся по адресу: 632080, с.Северное, ул. Ленина, д. 14, (далее - оператор) согласие на обработку своих персональных данных.

В лице представителя субъекта персональных данных (заполняется в случае получения согласия от представителя субъекта персональных данных)

_____
(фамилия, имя, отчество (последнее - при наличии) полностью)
документ, удостоверяющий личность: серия_____№_____выдан_____
(дата выдачи)
_____
(кем выдан)
зарегистрированный(ая) по адресу:_____
_____
действующий от имени субъекта персональных данных на основании_____
_____
(реквизиты доверенности или иного документа, подтверждающего полномочия представителя)

Цель обработки персональных данных:

- обеспечение соблюдения требований законодательства Российской Федерации;
- оформление и регулирование трудовых отношений;
- отражение информации в кадровых документах;
- начисление заработной платы;
- исчисление и уплата налоговых платежей, предусмотренных законодательством Российской Федерации;
- представление законодательно установленной отчетности в отношении физических лиц в ИФНС и внебюджетные фонды;
- подача сведений в банк для оформления банковской карты и последующего перечисления на нее заработной платы;
- предоставление налоговых вычетов;
- обеспечение безопасных условий труда;
- исполнение обязательств, предусмотренных договорами_____
_____
(указать какими)
_____
(указать иные цели (при наличии)

Перечень персональных данных, на обработку которых дается согласие:

- фамилия, имя, отчество (при наличии);
- год, месяц, дата и место рождения;
- свидетельство о гражданстве (при необходимости);
- реквизиты документа, удостоверяющего личность;
- идентификационный номер налогоплательщика, дата постановки его на учет, реквизиты свидетельства постановки на учет в налоговом органе;
- номер свидетельства обязательного пенсионного страхования, дата регистрации в системе обязательного пенсионного страхования;
- номер полиса обязательного медицинского страхования;
- адрес фактического места проживания и регистрации по месту жительства и (или) по месту пребывания;
- почтовый и электронный адреса;
- номера телефонов;
- фотографии;
- сведения об образовании, профессии, специальности и квалификации, реквизиты документов об образовании;
- сведения о семейном положении и составе семьи;
- сведения об имущественном положении, доходах, задолженности;
- сведения о занимаемых ранее должностях и стаже работы, воинской обязанности, воинском учете;

_____

_____

(указать иные категории персональных данных, в случае их обработки)

Наименование или фамилия, имя, отчество (последнее - при наличии) и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу_____

_____

_____

(указать полное наименование юридического лица, фамилия, имя, отчество (последнее - при наличии) и адрес физического лица, осуществляющего обработку персональных данных по поручению оператора, которому будет поручена обработка)

Перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных:

Обработка вышеуказанных персональных данных будет осуществляться путем смешанной (автоматизированной, не автоматизированной) обработки персональных данных.

Сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (только те, которые применяются реально)

Обработка вышеуказанных персональных данных будет осуществляться путем_____

(указать способ обработки (смешанной, автоматизированной, неавтоматизированной)

обработки персональных данных.

Даю согласие на передачу (предоставление) оператором моих данных: _____

_____

(указать полное наименование юридического лица; фамилия, имя, отчество (последнее – при наличии) и адрес физического лица, передачу которым дается согласие)

путем_____

(предоставления, допуска, предоставления)

Срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом:

Настоящее согласие на обработку персональных данных действует с момента его представления оператору до «____»_____20____г. или на период действия_____и может быть отозвано мной в любое время путем подачи оператору заявления в простой письменной форме.

Персональные данные субъекта подлежат хранению в течение сроков, установленных законодательством Российской Федерации. Персональные данные уничтожаются: по достижению целей обработки персональных данных; при ликвидации или реорганизации оператора; на основании письменного обращения субъекта персональных данных с требованием о прекращении обработки его персональных данных (оператор прекратит обработку таких персональных данных в течение 3 (трех) рабочих дней, о чем будет направлено письменное уведомление субъекту персональных данных в течение 10 (десяти) рабочих дней.

_____/_____/ «____»_____20____г.

(подпись) (фамилия, имя, отчество (последнее - при наличии)) (дата)

УТВЕРЖДЕНА
приказом ГКУ НСО ЦСПН
Северного района
от 30.04.25 № 157

Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные

В соответствии со статьями 65, 86 Трудового кодекса Российской Федерации ГКУ НСО ЦСПН Северного района определен перечень персональных данных, которые субъект персональных данных обязан предоставить ГКУ НСО ЦСПН Северного района в связи с поступлением на работу.

Без представления субъектом персональных данных обязательных для заключения служебного контракта (трудового договора) сведений, служебный контракт (трудовой договор) не может быть заключен.

В соответствии с действующим законодательством Российской Федерации в области персональных данных субъект персональных данных имеет право:

на получение сведений о ГКУ НСО ЦСПН Северного района как операторе, осуществляющем обработку его персональных данных (в объеме, необходимом для защиты своих прав и законных интересов по вопросам обработки своих персональных данных), о месте нахождения ГКУ НСО ЦСПН Северного района, о наличии у оператора своих персональных данных, а также на ознакомление с такими персональными данными; подавать запрос на доступ к своим персональным данным; требовать безвозмездного предоставления возможности ознакомления со своими персональными данными, а также внесения в них необходимых изменений, их уничтожения или блокирования при предоставлении сведений, подтверждающих, что такие персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

получать уведомления по вопросам обработки персональных данных в установленных действующим законодательством Российской Федерации случаях и сроки;

требовать от оператора разъяснения порядка защиты субъектом персональных данных своих прав и законных интересов;

обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке;

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

Мне, _____
(фамилия, имя, отчество (последнее - при наличии))

разъяснены юридические последствия отказа предоставить свои персональные данные ГКУ НСО ЦСПН Северного района.

_____ _____
(число, месяц.год) (подпись)