Муниципальное автономное учреждение города Новосибирска
«Новосибирский Центр Высшего Спортивного Мастерства»

П Р И К А З

От 30.12.2021 № 01-02-144

«Об оптимизации и совершенствовании работы по защите персональных данных в МАУ «НЦВСМ»

В целях совершенствования системы защиты персональных данных в МАУ «НЦВСМ» и во исполнение требований Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие с 01.01.2022 Положение о защите персональных данных работников муниципального автономного учреждения города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства» (Приложение 1).
2. Утвердить и ввести в действие с 01.01.2022 Политику оператора в отношении обработки персональных данных в МАУ «НЦВСМ» (Приложение 2).
3. Утвердить и ввести в действие с 01.01.2022 Положение о порядке работы с конфиденциальной информацией в муниципальном автономном учреждении города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства» (Приложение 3).
4. Утвердить и ввести в действие с 01.01.2022 Перечень сведений конфиденциального характера в муниципальном автономном учреждении города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства» (Приложение 4).
5. Утвердить и ввести в действие с 01.01.2022 Положение о внутреннем контроле соответствия обработки ПДн в ИСПДн требованиям к защите персональных данных МАУ «НЦВСМ» (Приложение 5).
6. Утвердить и ввести в действие с 01.01.2022 Положение об ответственности работников, допущенных к обработке персональных данных и иной конфиденциальной информации в МАУ «НЦВСМ» (Приложение 6).
7. Утвердить и ввести в действие с 01.01.2022 Положение об обработке и обеспечении безопасности персональных данных, обрабатываемых в информационных системах персональных данных муниципального автономного учреждения города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства» (Приложение 7).
8. Утвердить и ввести в действие с 01.01.2022 Положение о службе (ответственном лице) информационной безопасности муниципального автономного учреждения города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства» (Приложение 8).
9. Утвердить и ввести в действие с 01.01.2022 Положение о разграничении прав доступа к обрабатываемым персональным данным в информационных системах персональных данных муниципального автономного учреждения города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства» (Приложение 9).
10. Утвердить и ввести в действие с 01.01.2022 Порядок доступа сотрудников в помещения, в которых ведется обработка персональных данных, хранилища для бумажных и машинных носителей ПДн в ИСПДн (Приложение 10).

11. Утвердить и ввести в действие с 01.01.2022 Требования к оборудованию помещений и размещению технических средств, используемых для обработки персональных данных в муниципальном автономном учреждении города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства» (Приложение 11).

12. Утвердить и ввести в действие с 01.01.2022 Правила рассмотрения запросов субъектов персональных данных или их представителей (Приложение 12).

13. Утвердить и ввести в действие с 01.01.2022 Типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные (Приложение 13).

14. Утвердить и ввести в действие с 01.01.2022 Перечень персональных данных, обрабатываемых в муниципальном автономном учреждении города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства» (Приложение 14).

15. Утвердить и ввести в действие с 01.01.2022 Перечень должностей муниципального автономного учреждения города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства», допущенных к обработке персональных данных, обрабатываемых в ИСПДн (Приложение 15).

16. Утвердить и ввести в действие с 01.01.2022 Порядок уничтожения и обезличивания персональных данных после достижения цели их обработки (Приложение 16).

17. Утвердить и ввести в действие с 01.01.2022 Инструкцию о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и средств защиты информации в информационных системах муниципального автономного учреждения города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства» (Приложение 17).

18. Утвердить и ввести в действие с 01.01.2022 Инструкцию по обращению с сертифицированными ФСБ России средствами криптографической защиты информации (Приложение 18).

19. Утвердить и ввести в действие с 01.01.2022 Инструкцию о порядке учета и выдачи средств криптографической защиты информации, электронной подписи, эксплуатационно-технической документации и ключевых документов (Приложение 19).

20. Утвердить и ввести в действие с 01.01.2022 Инструкцию о порядке допуска сотрудников МАУ «НЦВСМ» к самостоятельной работе со средствами криптографической защиты информации (Приложение 20).

21. Утвердить и ввести в действие с 01.01.2022 Политику «чистого стола» и «чистого экрана» в муниципальном автономном учреждении города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства» (Приложение 21).

22. Утвердить и ввести в действие с 01.01.2022 Регламент использования электронной почты в муниципальном автономном учреждении города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства» (Приложение 22).

23. Утвердить и ввести в действие с 01.01.2022 Регламент использования ресурсов сети Интернет работниками муниципального автономного учреждения города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства» (Приложение 23).

24. Утвердить и ввести в действие с 01.01.2022 Инструкцию ответственного за доступ к сети Интернет в муниципальном автономном учреждении города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства» (Приложение 24).

25. Утвердить и ввести в действие с 01.01.2022 форму заявления и согласий на обработку персональных данных получателей стипендии мэрии города Новосибирска одаренным детям в области физической культуры и спорта/ единовременного вознаграждения спортсменам и тренерам города Новосибирска, добившимся высоких спортивных результатов (Приложение 25).

26. Утвердить и ввести в действие с 01.01.2022 Журнал обучения сотрудников в

области защиты персональных данных (Приложение 26).

27. Утвердить и ввести в действие с 01.01.2022 Журнал проверок осведомленности сотрудников в области защиты персональных данных (Приложение 27).

28. Утвердить и ввести в действие с 01.01.2022 План мероприятий по защите персональных данных на 2022 (Приложение 28).

29. Утвердить и ввести в действие с 01.01.2022 Положение об обеспечении безопасности автоматизированной информационной системы МАУ «НЦВСМ» (Приложение 29).

30. Признать утратившим силу пункт 9 приказа МАУ «НЦВСМ» от 18.03.2020 № 01-02-17 «Об утверждении инструкций и ознакомлении с ними ответственных лиц».

31. Признать утратившим силу пункты 1,2,3,4,6 приказа МАУ «НЦВСМ» от 18.03.2020 № 01-02-18 «Об утверждении организационно-распорядительных документов по защите персональных данных в МАУ «НЦВСМ».

32. Признать утратившим силу приказ МАУ «НЦВСМ» от 29.11.2013 № 01-02-61/3 «Об утверждении и введении в действие Положения о защите персональных данных работников МАУ «НЦВСМ».

33. Признать утратившим силу приказ МАУ «НЦВСМ» от 16.07.2019 № 01-02-42 «О мерах по совершенствованию в МАУ «НЦВСМ работы по защите персональных данных».

34. Признать утратившим силу приказ МАУ «НЦВСМ» от 18.03.2020 № 01-02-19 «О внесении изменений в приказ от 16.07.2019 № 01-02-42 в редакции приказа от 26.07.2019 № 01-02-43».

35. Признать утратившим силу приказ МАУ «НЦВСМ» от 30.09.2021 № 01-02-90 «Об оптимизации и совершенствовании работы по защите персональных данных в МАУ «НЦВСМ».

36. Назначить с 01.01.2022 ответственного за организацию обработки персональных данных в МАУ «НЦВСМ» заместителя генерального директора по неолимпийским видам спорта Кабанова П.Г.

37. Назначить с 01.01.2022 ответственного за работу с персональными данными работников и их хранение начальника отдела кадров Шаповалову Е.М.

38. Назначить с 01.01.2022 администратором безопасности информационных систем МАУ «НЦВСМ» системного администратора Петрущенкова М. Ю.

39. Назначить с 01.01.2022 ответственного за защиту информации, в том числе за обеспечение безопасности ПДн в информационных системах МАУ «НЦВСМ» системного администратора Петрущенкова М. Ю.

40. Назначить с 01.01.2022 ответственного за работу в сети Интернет и ограничение доступа к информационным Интернет-ресурсам системного администратора Петрущенкова М. Ю.

41. Начальникам отделов МАУ «НЦВСМ» и директору обособленного структурного подразделения «Спортивный комплекс «Фламинго» обеспечить:

- ознакомление с изложенными в прилагаемых документах по обработке и защите персональных данных под подпись работников, участвующих в обработке персональных данных;

- организовать и вести работу по обеспечению обработки и защиты персональных данных в соответствии с нормами, изложенными в прилагаемых документах.

42. Контроль за исполнением настоящего приказа возложить на ответственного за организацию обработки персональных данных в МАУ «НЦВСМ» заместителя генерального директора по неолимпийским видам спорта Кабанова П.Г.

Генеральный директор С. В. Даниленко

Ю.Д. Вейбер

Приложение 1 к приказу от
«30» декабря 2021 г. № 01-02-144

Положение
о защите персональных данных работников муниципального автономного учреждения города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства»

1. Общие положения

1.1. Настоящее положение о защите персональных данных работников МАУ «НЦВСМ» (далее по тексту - Положение) определяет понятия, общие требования при обработке, порядок получения, обработки, передачи, хранения и использование персональных данных лиц, состоящих в трудовых отношениях с муниципальным автономным учреждением города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства» (МАУ «НЦВСМ»), (далее по тексту – Учреждение), а также гарантии их защиты.

1.2. Положение разработано на основании Конституции Российской Федерации, Трудового кодекса РФ (далее – ТК РФ), Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и иных федеральных законов и нормативных актов, регулирующих трудовые правоотношения в Российской Федерации.

1.3. Целью данного Положения является защита персональных данных работников от несанкционированного доступа, неправомерного их использования или утраты, а также обеспечение соблюдения законных прав и интересов Учреждения и ее работников в связи с необходимостью получения (сбора), систематизации (комбинирования), хранения и передачи сведений, составляющих персональные данные.

2. Основные понятия. Состав персональных данных Работников

2.1. Для целей настоящего Положения используются следующие основные понятия:

Работник – лицо, состоящее в трудовых отношениях с МАУ «НЦВСМ»;

Оператор – МАУ «НЦВСМ» (далее по тексту – Работодатель);

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

Персональные данные Работника – любая информация, необходимая Работодателю и касающаяся конкретного Работника в связи с возникшими трудовыми отношениями;

Должностное лицо Работодателя – Работник, состоящий в трудовых отношениях с Работодателем и имеющий право на получение, обработку, передачу в процессе работы персональных данных;

Личное дело Работника – это ряд документов, содержащих сведения о сотруднике, его работе, персональные данные Работника;

Обработка персональных данных Работника — любое действие или совокупность действий, совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

Распространение персональных данных — действия, направленные на раскрытие персональных данных Работников неопределенному кругу лиц;

Предоставление персональных данных — действия, направленные на раскрытие персональных данных работников определенному лицу или определенному кругу лиц;

Уничтожение персональных данных — действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных работников и (или) в результате которых уничтожаются материальные носители персональных данных работников;

Информация — сведения (сообщения, данные) независимо от формы их представления;

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

2.2. Информация, представляемая Работником при поступлении на работу в Учреждение, должна иметь документальную форму. При заключении трудового договора лицо, поступающее на работу, предъявляет документы, содержащие персональные данные, к которым относятся:

- фамилия, имя, отчество;
- дата и место его рождения;
- гражданство;
- сведения о состоянии в браке и о составе семьи;
- паспортные данные: номер, серия, дата выдачи;
- сведения о регистрации по месту жительства или по месту пребывания;
- адрес места жительства фактический;
- номер страхового свидетельства государственного пенсионного страхования;
- идентификационный номер налогоплательщика;

- сведения о воинском учете;

- сведения о предыдущих местах работы и основаниях увольнения;

- сведения о трудовом и общем стаже;

- сведения об образовании, квалификации или наличии специальных знаний;

- сведения о заработной плате;

- содержание декларации, подаваемой в налоговую инспекцию;

- сведения о социальных льготах;

- подлинники и копии приказов по личному составу;

- основания к приказам по личному составу;

- сведения о содержании трудового договора, изменений трудового договора, договоров о материальной ответственности;

- документы по оценке деловых и профессиональных качеств Работника при приеме на работу;

- документы, отражающие деятельность конкурсных и аттестационных комиссий;

- документы о результатах служебных расследований;

- подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству предприятия, руководителям структурных подразделений и служб;

- копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения;

- документы бухгалтерского учета, содержащие информацию о расчетах с работником;

- сведения о наличии судимости;

- номер телефона;

- фото;

- трудовая книжка;

- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;

- характеристики;

- рекомендательные письма;

- справки, подтверждающие период работы у работодателя и размер заработной платы;

- наградные документы;

- листки нетрудоспособности;

- медицинские справки;

- иные сведения, относящиеся к персональным данным Работника;

- иные документы, содержащие персональные сведения о работнике.

2.3. Указанные пунктом 2.2. Положения документы являются конфиденциальными. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом. Кроме того, режим конфиденциальности персональных данных снимается по истечении срока хранения, если иное не установлено законом.

3. Сбор и обработка персональных данных Работника

3.1. Работник предоставляет в кадровый отдел свои персональные данные и достоверные сведения о себе, в пределах необходимых при трудоустройстве и для выполнения конкретных трудовых функций (формы согласий Приложение 1,2,3).

Работник по своему желанию может предоставлять Работодателю иные персональные данные оценочного характера (характеристики, аттестации, докладные записки, оценки, сделанные в других формах), а также дополнять такие данные заявлением, выражающим его собственную точку зрения.

3.2. Обработка персональных данных Работника осуществляется в следующих целях:

- обеспечения соблюдения законов и иных нормативных правовых актов;

- содействия Работникам в трудоустройстве, обучении и продвижении по службе;

- обеспечения личной безопасности Работников;

- контроля количества и качества выполняемой работы.

3.3. Источником информации обо всех персональных данных Работника является непосредственно Работник. Персональные данные Работника следует получать у него самого. Если персональные данные Работника возможно получить только у третьей стороны, то Работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить Работнику о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

3.4. Работодателю не допускается получать и обрабатывать персональные данные Работника без его согласия:

- о его политических, религиозных, философских убеждениях, расовой, национальной принадлежности и частной жизни;

- о состоянии здоровья, интимной жизни;

- о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами;

- запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции (например, при решении вопроса о переводе Работника на другую должность (работу) по производственной необходимости либо наличии медицинского заключения, дающего основания полагать о невозможности выполнения Работником трудовой функции на условиях, предусмотренных трудовым договором);

3.5. Работодателю запрещено сообщать персональные данные Работника:

- третьей стороне без письменного согласия самого Работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровья Работника, а также в случаях, установленных федеральным законом;

- в коммерческих целях без письменного согласия Работника;

- передача информации, содержащей сведения о персональных данных Работника без его письменного согласия, по телефону, факсу, электронной почте запрещается.

3.6. Работодатель имеет право:

- запрашивать сведения о состоянии здоровья Работника, для определения возможности выполнения им трудовой функции;

- с письменного согласия Работника получать дополнительную информацию о профессиональной подготовке Работника в другой организации;

3.7. Обработка персональных данных Работников Работодателем возможна без их согласия в следующих случаях:

- персональные данные являются общедоступными;

- обработка персональных данных осуществляется на основании Трудового кодекса РФ или иного федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определенного полномочия Работодателя;

- обработка персональных данных в целях исполнения трудового договора;

- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов Работника, если получение его согласия невозможно.

- персональные данные относятся к состоянию здоровья Работника, и их обработка необходима — по требованию полномочных государственных органов — в случаях, предусмотренных федеральным законом.

3.8. Работодатель вправе обрабатывать персональные данные Работников только с их письменного согласия, которое включает в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

- наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;

- цель обработки персональных данных;

- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

- срок, в течение которого действует согласие, а также порядок его отзыва.

3.9. Требования Работника об исключении или исправлении неверных или неполных персональных данных предъявляются им Работодателю в письменном виде с приложением документов, подтверждающих обоснованность таких требований.

3.10. Должностные лица Работодателя не имеют права сообщать персональные данные Работника третьей стороне без письменного согласия Работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью Работника, а также, в случаях, установленных федеральными законами (Трудовым кодексом РФ, Налоговым кодексом РФ, Федеральными законами «О милиции», «О федеральной службе безопасности», «О прокуратуре Российской Федерации»), предусматривающими право должностных лиц контролирующих и правоохранительных органов запрашивать документы, содержащие персональные данные Работника.

4. Доступ к персональным данным работников

4.1. Право доступа к персональным данным работников имеют:

- генеральный директор Учреждения;

- заместители генерального директора;

- работники отдела кадров;

- работники отдела по олимпийским видам спорта;

- работники отдела по неолимпийским видам спорта;

- работники бухгалтерии (к тем данным, которые необходимы для выполнения конкретных функций);

- начальник отдела по связям с общественностью (информация о фактическом месте проживания и контактные телефоны, дни рождения Работников);

- директор обособленного структурного подразделения (доступ к персональным данным только Работников своего подразделения);

- работники юридического отдела (к тем данным, которые необходимы для выполнения конкретных функций);

- специалист по охране труда (в части соблюдения трудового режима Работника, а также отражения необходимой информации в трудовом договоре, ознакомление с результатами медицинских осмотров, подготовка списков Работников к плановым медосмотрам);

- сам Работник, носитель данных.

4.2. Право доступа к персональным данным Работника имеют так же следующие юридические лица:

4.2.1. Государственные и негосударственные функциональные структуры:

- налоговые инспекции;

- правоохранительные органы;

- органы статистики;

- страховые агентства;

- военкоматы;

- органы социального страхования;

- пенсионные фонды;

- подразделения муниципальных органов управления.

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

4.2.3. Родственники и члены семей.

Персональные данные Работника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого Работника.

В случае развода бывшая супруга (супруг) имеют право обратиться к Работодателю с письменным запросом о размере заработной платы Работника без его согласия.

5. Права и обязанности Работника

5.1. Работник имеет право на:

- полную информацию о своих персональных данных и обработку этих данных;

- свободный бесплатный доступ к своим персональным данным, ознакомление с ними включая право на безвозмездное получение копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных федеральным законом РФ;

- определение своих представителей для защиты своих персональных данных;

- доступ к относящимся к нему медицинским данным с помощью медицинского специалиста по своему выбору;

- требование об исключении или исправлении неверных или неполных своих персональных данных, путем предъявления им в письменном виде заявления на имя директора Учреждения с приложением документов, подтверждающих обоснованность таких требований;

- дополнить заявлением персональные данные оценочного характера, выражающим его собственную точку зрения;

- обжалование в суд любых неправомерных действий или бездействия Работодателя при обработке и защите его персональных данных;

- требование от Работодателя уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для Работодателя персональных данных;

- требование извещения Работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;

- обжалование в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия Работодателя при обработке и защите его персональных данных;

- передачу информации третьей стороне возможна только при письменном согласии Работника;

- получение сведений о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

- получение сведений о сроках обработки персональных данных, в том числе сроках их хранения.

5.2. Работник обязан:

- предоставлять Работодателю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ. Предоставление Работником подложных документов или ложных сведений при поступлении на работу является основанием для расторжения трудового договора в соответствии с п. 11 ст. 81 Трудового кодекса РФ;

- незамедлительно письменно уведомлять Работодателя об изменении любого из следующих данных: паспорта и/или имени, фамилии, отчества, постоянного места жительства (места пребывания) — указанных им при заключении трудового договора.

В случае неисполнения данной обязанности риск неблагоприятных последствий несет Работник.

6. Формирование и ведение личных дел, документов, содержащих персональные данные

6.1. При оформлении Работника специалистом по кадрам заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные работника:

- общие сведения (Ф.И.О., дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные);

- сведения о воинском учете;

- данные о приеме на работу;

- сведения об аттестации;

- сведения о повышенной квалификации;

- сведения о профессиональной переподготовке;

- сведения о наградах (поощрениях), почетных званиях;

- сведения об отпусках;

- сведения о социальных гарантиях;

- сведения о месте жительства и о контактных телефонах.

6.2. Личное дело Работника формируется после издания приказа о его приеме на работу.

Первоначально в личное дело группируются документы, содержащие персональные данные Работника, в порядке, отражающем процесс приема на работу:

- заявление Работника о приеме на работу;

- анкета;

- медицинское заключение о годности Работника к работе в Учреждении;

- трудовой договор;

- копия паспорта или иного документа, удостоверяющего личность;

- копия страхового свидетельства государственного пенсионного страхования;

- копия свидетельства идентификационного номера налогоплательщика;

- копия документа воинского учета;

- документы об образовании, о квалификации или наличии специальных знаний, требующую специальных знаний или специальной подготовки, имеющихся как при поступлении на работу, так и приобретенных в процессе работы;

- уведомление Работника в ведении в учреждении видеосъемки;

- согласие работника на сбор, хранение и использование персональных данных.

У Работников, не достигших возраста 16 и/или 18 лет, личное дело, помимо указанных выше документов, содержит:

- письменное согласие органа опеки и попечительства администрации района по месту жительства;

- письменное согласие одного из родителей (попечителя);

- справка с места учебы.

Личному делу присваивается номер, который фиксируется в журнале учета личных дел.

К каждому личному делу прилагается фотография Работника (без головного убора) формата не более 35х45мм.

Все документы, поступающие в личное дело, располагаются в хронологическом порядке.

7. Учет, хранение, передача и защита персональных данных Работника

7.1. Персональные данные на бумажных носителях и трудовые книжки Работников хранятся в отделе кадров в металлических шкафах, сейфах, имеющих надежные запоры, ключ от кабинета опечатывается. Персональные данные в электронном виде хранятся на сервере, персональных компьютерах.

7.2. Персональные данные предоставляются в распоряжение должностных лиц Работодателя лишь в следующих случаях:

- необходимости оформления наградных документов;

- формирования статистических данных;

- подготовки характеристики;

- необходимости оформления субсидий;

- при наличии соответствующей резолюции руководителя Работодателя на служебной записке соответствующей формы.

7.3. Трудовые книжки Работников могут предоставляться Работниками отдела кадров лишь Работникам бухгалтерии и членам комиссии по социальному страхованию, при необходимости проверки данных о непрерывном трудовом стаже Работников, для решения вопросов о начислении и выплате пособий по государственному социальному страхованию.

7.4. В целях обеспечения сохранности и конфиденциальности персональных данных Работников, все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться только Работниками, осуществляющими данную работу в соответствии со своими служебными обязанностями, зафиксированными в их трудовых договорах.

7.5. Ответственным за работу с персональными данными Работников и их хранение является начальник отдела кадров.

7.6. Персональные компьютеры Работников, содержащие персональные данные Работников, защищены паролями доступа.

Личные дела, в которых хранятся персональные данные Работников, являются документами «Для внутреннего пользования».

Личное дело регистрируется, о чем вносится запись в «Журнал учета личных дел». Журнал содержит следующие графы:

- порядковый номер личного дела;

- фамилия, имя, отчество сотрудника;

- дата постановки дела на учет;

- дата снятия дела с учета.

После увольнения Работника в личное дело вносятся соответствующие документы, составляется окончательная опись, само личное дело оформляется и передается для хранения.

7.7. Персональные данные на бумажных носителях хранятся в отделах по олимпийским и неолимпийским видам спорта в шкафах, дверь и ключ от кабинета опечатываются. Персональные данные в электронном виде хранятся на сервере, персональных компьютерах.

Персональные данные предоставляются в распоряжение должностных лиц отделов по олимпийским и неолимпийским видам спорта для следующих задач:

- для организации и обеспечения подготовки спортивного резерва и оказания услуг по спортивной подготовке;

- для направления работников и лиц, проходящих спортивную подготовку, в служебные командировки, служебные поездки, направление указанных лиц для участия в тренировочных и спортивных мероприятиях, также для прохождения УМО.

7.8. Защита персональных данных работников от неправомерного их использования или утраты обеспечивается Учреждением за счет собственных средств в порядке, установленным Трудовым кодексом РФ и иными федеральными законами.

7.9. Передача информации, содержащей сведения о персональных данных работников организации, по телефону, электронной почте без письменного согласия работника запрещается.

8. Ответственность за нарушение норм, регулирующих обработку персональных данных

8.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных Работника, несут дисциплинарную и материальную ответственность, установленном Трудовым кодексом РФ и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

9. Заключительные положения

9.1. Иные вопросы, не отражённые в настоящем положении, подлежат разрешению в соответствии с действующим законодательством РФ и другими локальными актами Учреждения.

9.2. Сведения о персональных данных Работников всегда являются конфиденциальной и охраняемой информацией. Работники, указанные в пункте 5.1. настоящего Положения, имеющие доступ к персональным данным Работника, обязаны соблюдать режим секретности (конфиденциальности). Данное Положение не распространяется на обмен персональными данными Работников в порядке, установленном федеральными законами.

Режим конфиденциальности в отношении персональных данных снимается:

- в случае их обезличивания;

- по истечении 75 лет срока их хранения;

- в других случаях, предусмотренных федеральными законами.

9.3. Работодатель должен ознакомить под роспись с данным Положением всех Работников Учреждения, и вновь поступающих на работу, при заключении трудового договора.

Приложение 2 к приказу от
«30» декабря 2021 г. №01-02-144

ПОЛИТИКА ОПЕРАТОРА В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В МАУ «НЦВСМ»

1. Общие положения

1.1. Политика оператора в отношении обработки персональных данных в МАУ «НЦВСМ» (далее – Политика, Оператор) разработана в целях обеспечения защиты прав и свобод субъекта персональных данных при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.2. Политика разработана в соответствии с положениями Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных" (далее - Федеральный закон "О персональных данных") и рекомендациями Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 31 июля 2017 г. "Рекомендации по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном Федеральным законом от 27 июля 2006 года № 152-ФЗ "О персональных данных".

1.3. Основные понятия, используемые в Политике:

1.3.1. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (далее - субъект персональных данных) (фамилия, имя, отчество, год, месяц, дата рождения, место рождения, адрес, семейное положение, социальное положение, имущественное положение, образование, профессия, доходы, другая информация, относящаяся к субъекту персональных данных).

1.3.2. Специальные категории персональных данных (расовая, национальная принадлежности, политические взгляды, религиозные или философские убеждения, состояния здоровья, интимной жизни).

1.3.3. Биометрические персональные данные (сведения, которые характеризуют физиологические и биологические особенности человека, на основе которых можно установить его личность (биометрические персональные данные) и которые используются Оператором для установления личности субъекта персональных данных.

1.3.4. Обработка персональных данных - любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя в том числе: сбор; запись; систематизацию; накопление; хранение; уточнение (обновление, изменение); извлечение; использование; передачу (распространение, предоставление, доступ); обезличивание; блокирование; удаление; уничтожение.

1.3.5. Автоматизированная обработка персональных данных - обработка

персональных данных с помощью средств вычислительной техники.

Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что эти данные содержались в информационной системе персональных данных либо были извлечены из нее.

1.3.6. Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

1.3.7. Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

1.3.8. Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

1.3.9. Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

1.3.10. Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

1.3.11. Оператор персональных данных (оператор) - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

1.4. Оператор, получив доступ к персональным данным, обязан соблюдать конфиденциальность персональных данных - не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

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

подтверждение факта обработки персональных данных Оператором;

правовые основания и цели обработки персональных данных;

цели и применяемые Оператором способы обработки персональных данных;

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

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

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

порядок осуществления субъектом персональных данных прав, предусмотренных федеральным законом;

информацию об осуществленной или о предполагаемой трансграничной передаче данных;

наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу;

иные сведения, предусмотренные Федеральным законом "О персональных данных" или другими федеральными законами.

1.6. Субъект персональных данных вправе требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

1.8. Оператор персональных данных вправе:

отстаивать свои интересы в суде;

предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.);

отказывать в предоставлении персональных данных в случаях, предусмотренных законодательством;

использовать персональные данные субъекта без его согласия в случаях, предусмотренных законодательством.

1.9. При сборе персональных данных Оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 7 статьи 14 Федерального закона "О персональных данных".

1.10. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", Оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 Федерального закона "О персональных данных".

2. Цели сбора персональных данных

2.1. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка

персональных данных, несовместимая с целями сбора персональных данных.

2.2. Цели обработки персональных данных определены правовыми актами, регламентирующими деятельность Оператора.

2.3. К целям обработки персональных данных Оператором относятся:

обеспечение соблюдения Конституции Российской Федерации, законодательных и нормативных правовых актов Российской Федерации, содействие работнику НЦВСМ в выполнении трудовых обязанностей, обучении и должностном росте, в росте спортивных результатов;

учет результатов исполнения работником должностных обязанностей и обеспечение сохранности имущества Оператора;

исполнение требований налогового законодательства по вопросам исчисления и уплаты налога на доходы физических лиц и единого социального налога, пенсионного законодательства при формировании и передаче в ПФР персонифицированных данных о каждом получателе доходов, которые учитываются при начислении взносов на обязательное пенсионное страхование, трудового законодательства при заключении договоров страхования жизни и здоровья спортсменов- инструкторов Оператора;

заполнение первичной статистической документации в соответствии с трудовым, налоговым законодательством и иными федеральными законами;

формирование кадрового резерва Оператора;

учет работников Оператора, награжденных государственными наградами Российской Федерации, представленных к награждению; имеющих спортивные звания и почетные звания и представленных к присвоению спортивных и почетных званий; представление работников Оператора к поощрению муниципальными и государственными органами власти, к присвоению спортивных и почетных званий;

осуществление полномочий мэрии города Новосибирска по исполнению публичных обязательств перед физическими лицами, подлежащих исполнению в денежной форме, переданных Оператору.

3. Передача персональных данных третьим лицам

Оператор персональных данных может передавать обрабатываемые персональные данные третьим лицам, если передача необходима в рамках процедуры, установленной законодательством Российской Федерации.

4. Правовые основания обработки персональных данных

4.1. Правовым основанием обработки персональных данных является совокупность правовых актов, во исполнение которых и в соответствии с которыми Оператор осуществляет обработку персональных данных: Конституция Российской Федерации; статьи 86 - 90 Трудового кодекса Российской Федерации; Федеральный закон от 12.01.1996 № 7-ФЗ «О некоммерческих организациях»; Федеральный закон от 03.11.2006 № 174-ФЗ "Об автономных учреждениях"; Федеральный закон от 04.12.2007 № 329-ФЗ "О физической культуре и спорте в Российской Федерации"; Федеральный закон от 26.07.2006 № 135-ФЗ «О защите конкуренции»; Федеральный закон от 18.07.2011 № 223-ФЗ "О закупках товаров,

работ, услуг отдельными видами юридических лиц"; Федеральный закон от 25.12.2008 № 273-ФЗ «О противодействии коррупции»; постановление мэрии города Новосибирска от 03.04.2017 № 1356 "Об осуществлении муниципальным автономным учреждением города Новосибирска "Новосибирский центр высшего спортивного мастерства" полномочий мэрии города Новосибирска по исполнению публичных обязательств перед физическими лицами, подлежащих исполнению в денежной форме";

договоры, заключаемые между Оператором и субъектом персональных данных;

согласие на обработку персональных данных (в случаях, прямо непредусмотренных законодательством Российской Федерации, и соответствующих полномочиям Оператора).

5. Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных

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

5.2. Обработка персональных данных допускается в следующих случаях:

- обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

- обработка персональных данных необходима для осуществления прав и законных интересов Оператора или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

- обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

- обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 Федерального закона "О персональных данных", при условии обязательного обезличивания персональных данных;

- осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных);

- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

5.3. К категориям субъектов персональных данных относятся:

5.3.1. Работники Оператора, бывшие работники, кандидаты на замещение вакантных должностей, а также родственники работников.

В данной категории субъектов Оператором обрабатываются персональные данные в связи с реализацией трудовых отношений:

- фамилия, имя, отчество;
- пол;
- гражданство;
- национальность;
- дата (число, месяц, год) и место рождения (страна, республика, край, область, район, город, поселок, деревня, иной населенный пункт);
- адрес места проживания (почтовый индекс, страна, республика, край, область, район, город, поселок, деревня, иной населенный пункт, улица, дом, корпус, квартира);
- сведения о регистрации по месту жительства или пребывания (почтовый индекс, страна, республика, край, область, район, город, поселок, деревня, иной населенный пункт, улица, дом, корпус, квартира);
- номера телефонов (домашний, мобильный, рабочий), адрес электронной почты;
- замещаемая должность;
- сведения о трудовой деятельности (наименования организаций (органов) и занимаемых должностей, продолжительность работы (службы) в этих организациях (органах));
- сведения об инвалидности;
- идентификационный номер налогоплательщика (дата (число, месяц, год) и место постановки на учет, дата (число, месяц, год) выдачи свидетельства);
- данные страхового свидетельства обязательного пенсионного страхования;
- данные полиса обязательного медицинского страхования;
- данные паспорта или иного удостоверяющего личность документа;
- данные паспорта, удостоверяющего личность гражданина Российской Федерации за пределами территории Российской Федерации;
- данные трудовой книжки, вкладыша в трудовую книжку;
- сведения о воинском учете (серия, номер, дата (число, месяц, год) выдачи, наименование органа, выдавшего военный билет, военно-учетная специальность,

воинское звание, данные о принятии/снятии на (с) учет(а), о прохождении военной службы, о пребывании в запасе, о медицинском освидетельствовании и прививках);

- сведения об образовании (наименование образовательной организации, дата (число, месяц, год) окончания, специальность и квалификация, ученая степень, звание, реквизиты документа об образовании и о квалификации);

- сведения о получении дополнительного профессионального образования (дата (число, месяц, год), место, программа, реквизиты документов, выданных по результатам);

- сведения о владении иностранными языками (иностранный язык, уровень владения);

- сведения о спортивных званиях, дата (число, месяц, год) присвоения, и спортивных достижениях;

- сведения о дееспособности (реквизиты документа, устанавливающие опеку (попечительство), основания ограничения в дееспособности, реквизиты решения суда);

- сведения о наградах, иных поощрениях и знаках отличия (название награды, поощрения, знака отличия, дата (число, месяц, год) присвоения, реквизиты документа о награждении или поощрении);

- сведения о дисциплинарных взысканиях;

- сведения, содержащиеся в материалах служебных проверок;

- сведения о семейном положении (состояние в браке (холост (не замужем), женат (замужем), повторно женат (замужем), разведен(а), вдовец (вдова), с какого времени в браке, с какого времени в разводе, количество браков, состав семьи, реквизиты свидетельства о заключении брака);

- сведения о близких родственниках, свойственниках (степень родства, фамилия, имя, отчество, дата (число, месяц, год) и место рождения, место и адрес работы (службы), адрес места жительства, сведения о регистрации по месту жительства или пребывания);

- сведения, содержащиеся в документах о заработной плате, доходах, расходах, об имуществе и обязательствах имущественного характера;

- номер расчетного счета;

- информация об оформленных допусках к государственной тайне;

- фотографии.

5.3.2. Клиенты и контрагенты Оператора (физические лица);

В данной категории субъектов Оператором обрабатываются персональные данные, полученные Оператором в связи с заключением договора, стороной которого является субъект персональных данных, и используемые Оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных:

- фамилия, имя, отчество;

- пол;

- гражданство;

- дата (число, месяц, год) и место рождения (страна, республика, край, область, район, город, поселок, деревня, иной населенный пункт);

- адрес места проживания (почтовый индекс, страна, республика, край, область, район, город, поселок, деревня, иной населенный пункт, улица, дом, корпус, квартира);

- сведения о регистрации по месту жительства или пребывания (почтовый индекс, страна, республика, край, область, район, город, поселок, деревня, иной населенный пункт, улица, дом, корпус, квартира);

- номера телефонов (домашний, мобильный, рабочий), адрес электронной почты;

- замещаемая должность;

- идентификационный номер налогоплательщика (дата (число, месяц, год) и место постановки на учет, дата (число, месяц, год) выдачи свидетельства);

- данные паспорта или иного удостоверяющего личность документа;

- сведения об участии в управлении хозяйствующим субъектом (за исключением жилищного, жилищно-строительного, гаражного кооперативов, садоводческого, огороднического, дачного потребительских кооперативов, товарищества собственников недвижимости и профсоюза, зарегистрированного в установленном порядке), занятии предпринимательской деятельностью;

- номер расчетного счета;

- сведения о доходах, полученных в рамках исполнения договоров с Оператором.

5.3.3. Представители/работники клиентов и контрагентов Оператора (юридических лиц).

В данной категории субъектов Оператором обрабатываются персональные данные, полученные Оператором в связи с заключением договора, стороной которого является клиент/контрагент (юридическое лицо), и используемые Оператором исключительно для исполнения указанного договора:

- фамилия, имя, отчество;

- пол;

- номера телефонов (домашний, мобильный, рабочий), адрес электронной почты;

- замещаемая должность;

- данные паспорта или иного удостоверяющего личность документа;

- сведения об участии в управлении хозяйствующим субъектом (за исключением жилищного, жилищно-строительного, гаражного кооперативов, садоводческого, огороднического, дачного потребительских кооперативов, товарищества собственников недвижимости и профсоюза, зарегистрированного в установленном порядке), занятии предпринимательской деятельностью.

5.4. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, допускается:

- в случае, если субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

- в соответствии с законодательством о государственной социальной помощи, трудовым и пенсионным законодательством Российской Федерации.

5.5. Обработка биометрических персональных данных может осуществляться только при наличии согласия в письменной форме субъекта персональных данных.

6. Порядок и условия обработки персональных данных

6.1. Оператор осуществляет обработку персональных данных - операции, совершаемые с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

6.2. Обработка персональных данных осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законом "О персональных данных".

6.3. Обработка персональных данных Оператором ограничивается достижением конкретных, заранее определенных и законных целей. Обработке подлежат только персональные данные, которые отвечают целям их обработки. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки.

6.4. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

6.5. При осуществлении хранения персональных данных Оператор персональных данных обязан использовать базы данных, находящиеся на территории Российской Федерации, в соответствии с ч. 5 ст. 18 Федерального закона "О персональных данных".

Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только 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.

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков). При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

6.6. Условием прекращения обработки персональных данных может являться достижение целей обработки персональных данных, истечение срока действия согласия или отзыв согласия субъекта персональных данных на обработку его персональных данных, а также выявление неправомерной обработки персональных данных.

6.7. Оператор вправе поручить обработку персональных данных другому лицу на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта.

Лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Федеральным законом "О персональных данных".

Кроме того, Оператор вправе передавать персональные данные органам дознания и следствия, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством Российской Федерации.

6.8. Оператор и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

6.9. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами. Состав и перечень мер Оператор определяет самостоятельно.

6.10. Оператор при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

7. Актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным

7.1. Оператор обязан сообщить в порядке, предусмотренном статьей 14 Федерального закона "О персональных данных", субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

7.2. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. 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, Оператор обязан внести в них необходимые изменения. 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, Оператор обязан уничтожить такие персональные данные. Оператор обязан 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.

7.3. В случае подтверждения факта неточности персональных данных Оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

7.4. Оператор обязан прекратить обработку персональных данных или обеспечить прекращение обработки персональных данных лицом, действующим по поручению Оператора:

в случае выявления неправомерной обработки персональных данных, осуществляемой Оператором или лицом, действующим по поручению Оператора, в срок, не превышающий трех рабочих дней с даты этого выявления;

в случае отзыва субъектом персональных данных согласия на обработку его персональных данных Оператором.

7.5. При достижении цели обработки персональных данных Оператор обязан уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению

Оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных. В случае отсутствия возможности уничтожения персональных данных в течение указанного срока Оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

Приложение 3 к приказу от
«30» декабря 2021 г. №01-02-144

Положение о порядке работы с конфиденциальной информацией в муниципальном автономном учреждении города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства»

1. Термины и определения

Для целей настоящего Положения используются следующие термины и определения.

Конфиденциальная информация – любые сведения, составляющие служебную, коммерческую тайну, включая персональные данные работников.

Обладатель конфиденциальной информации - лицо, которое владеет информацией, составляющей конфиденциальную информацию, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим конфиденциальной информации. Обладателем информации, составляющей конфиденциальную информацию, является муниципальное автономное учреждение города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства» (далее по тексту – Учреждение).

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

Служебная тайна – научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау)), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании, и в отношении которой обладателем такой информации введен режим коммерческой тайны. Информация может быть отнесена к служебной тайне в том, случае, если она получена, разработана в процессе осуществления трудовых правоотношений и не влечет (не может повлечь) получения прибыли обладателем такой информации. Служебную тайну организации составляют любые сведения, в том числе сведения, содержащиеся в служебной переписке, телефонных переговорах, почтовых отправлениях, телеграфных и иных сообщениях, передаваемых по сетям электрической и почтовой связи, которые стали известны работнику организации в связи с исполнением им возложенных на него трудовых обязанностей.

К служебной тайне не относится информация, разглашенная учреждением самостоятельно или с его согласия, а также иная информация, ограничения доступ к которой не допускаются в соответствии с законодательством РФ.

Коммерческая тайна - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду; научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау)), которая имеет действительную или потенциальную коммерческую ценность в силу

неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны. Информация может быть отнесена к коммерческой тайне в том, случае, если она получена, разработана в процессе осуществления трудовых правоотношений, либо в результате гражданско-правовых отношений, влекущая или могущая повлечь получение прибыли обладателем такой информации.

Врачебная тайна - информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении.

Персональные данные работника – любая информация, относящаяся к работнику как субъекту персональных данных, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.

Доступ к конфиденциальной информации - ознакомление определенных лиц с информацией, составляющей тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.

Передача конфиденциальной информации - передача информации, составляющей тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности.

Предоставление информации, составляющей тайну, - передача информации, составляющей тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций.

Разглашение конфиденциальной информации - действие или бездействие, в результате которых информация, составляющая тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

2. Общие положения

2.1. Руководитель учреждения осуществляет общее управление обеспечением режима безопасности сведений, содержащих конфиденциальную информацию.

2.2. Лица, допущенные к конфиденциальной информации, должны быть ознакомлены с настоящим Положением под роспись.

2.3. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не предусмотрено законодательством РФ.

2.4. Настоящее Положение утверждается и вводится в действие приказом Руководителя учреждения и является обязательным для исполнения всеми работниками, имеющими доступ к конфиденциальной информации учреждения.

2.5. Работники учреждения должны быть ознакомлены под роспись с документами учреждения, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

2.6. В установленном законом порядке субъект персональных данных даёт письменное согласие на обработку своих персональных данных.

2.7. В целях защиты персональных данных работник (его законный представитель) имеет право:

- требовать исключения или исправления неверных или неполных персональных данных;

- на свободный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;

- определять своих представителей для защиты своих персональных данных;

- на сохранение и защиту своей личной и семейной тайны;

- право обжаловать действия учреждения, в случае нарушения законодательства о персональных данных.

2.8. Работник (его законный представитель) обязан:

- в установленном законодательством порядке предоставлять учреждению комплекс достоверных, документированных персональных данных;

- своевременно сообщать об изменении своих персональных данных (ставить учреждение в известность об изменении фамилии, имени, отчества, даты рождения, смены паспорта, что получает отражение в информационной базе данных, а также в документах, содержащих персональные данные).

3. Информация, являющаяся конфиденциальной, и доступ к ней

3.1. Перечень конфиденциальной информации учреждения утверждается приказом Руководителя.

3.2. Каждый работник, получающий доступ к конфиденциальной информации, в том числе к персональным данным, подписывает обязательство о неразглашении конфиденциальной информации, в том числе сведений о персональных данных, а также уведомление об ответственности в случае нарушения требований действующего законодательства в сфере обработки персональных данных, которое хранится в личной карточке работника (Приложение 1).

3.3. Список работников, допущенных к работе с конфиденциальной информацией, утверждается приказом Руководителя. Каждый работник, имеющим доступ к конфиденциальной информации, подписывает обязательство о неразглашении конфиденциальной информации.

3.4. В состав персональных данных входят:

- фамилия, имя, отчество;

- дата и место его рождения;

- гражданство;

- сведения о состоянии в браке и о составе семьи;

- паспортные данные: номер, серия, дата выдачи;

- сведения о регистрации по месту жительства или по месту пребывания;

- адрес места жительства фактический;

- номер страхового свидетельства государственного пенсионного страхования;

- идентификационный номер налогоплательщика;

- сведения о воинском учете;

- сведения о предыдущих местах работы и основаниях увольнения;

- сведения о трудовом и общем стаже;

- сведения об образовании, квалификации или наличии специальных знаний;

- сведения о заработной плате;

- содержание декларации, подаваемой в налоговую инспекцию;

- сведения о социальных льготах;

- подлинники и копии приказов по личному составу;

- основания к приказам по личному составу;

- сведения о содержании трудового договора, изменений трудового договора, договоров о материальной ответственности;

- документы по оценке деловых и профессиональных качеств Работника при приеме на работу;

- документы, отражающие деятельность конкурсных и аттестационных комиссий;

- документы о результатах служебных расследований;

- подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству предприятия, руководителям структурных подразделений и служб;

- копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения;

- документы бухгалтерского учета, содержащие информацию о расчетах с работником;

- сведения о наличии судимости;

- номер телефона;

- фото;

- трудовая книжка;

- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;

- характеристики;

- рекомендательные письма;

- справки, подтверждающие период работы у работодателя и размер заработной платы;

- наградные документы;

- листки нетрудоспособности;

- медицинские справки;

- иные сведения, относящиеся к персональным данным Работника;

- иные документы, содержащие персональные сведения о работнике.

4. Порядок обращения конфиденциальной информации

4.1. Сведения, составляющие конфиденциальную информацию, могут быть выражены в письменной, устной и иных формах. Конфиденциальная информация, ставшая известной работнику из письменных, устных и иных источников, охраняется равным образом.

4.2. Конфиденциальная информация, ставшая известной работнику из устных источников, не должна быть им разглашена. В случае разглашения данной информации работник несёт ответственность в установленном законодательством порядке.

4.3. Письменные и машинные источники информации, содержащие служебную и коммерческую тайну, полежат учёту и специальному обозначению.

4.4. В случае необходимости оперативного доведения до заинтересованных лиц сведений, составляющих тайну, Руководителем ставится резолюция на самом документе, содержащем служебную или коммерческую тайну. Такое разрешение должно содержать перечень фамилий работников, обязанных ознакомиться с документами или их исполнить, срок исполнения, другие указания, подпись руководителя и дату. Руководитель может при необходимости предусмотреть ограничения в доступе конкретных работников к определенным сведениям.

4.5. Не допускается разглашение сведений, составляющих врачебную тайну лицами, которым они стали известны при обучении, исполнении профессиональных, служебных и иных обязанностей, кроме случаев, установленных в настоящем Положении.

4.6. С согласия гражданина или его законного (уполномоченного) представителя допускается передача сведений, составляющих врачебную

тайну, другим гражданам, в том числе должностным лицам, в интересах обследования и лечения гражданина, для проведения научных исследований, публикации в научной литературе, использования этих сведений в учебном процессе и в иных целях.

4.7. Законными представителями являются родители, усыновители или попечители лица.

4.8. Полномочия законного представителя подтверждаются следующими документами:

- родители – паспорт, свидетельство о рождении ребенка;

- опекуны – паспорт (иной документ, удостоверяющий личность), решение органа опеки и попечительства, либо решение суда об установлении опеки над лицом и назначении опекуна;

- попечители - паспорт (иной документ, удостоверяющий личность), решение органа опеки и попечительства, либо решение суда об установлении попечительства над лицом и назначении попечителя.

4.9. Уполномоченными представителями являются лица, действующие на основании нотариально удостоверенной доверенности.

4.10. Полномочия представителя подтверждаются нотариально удостоверенной доверенностью.

4.11. Под обработкой персональных данных понимается сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных и любое другое использование персональных данных.

4.12. В целях обеспечения прав и свобод человека и гражданина работники учреждения при обработке персональных данных обязаны соблюдать следующие общие требования:

4.12.1. Обработка персональных данных может осуществляться исключительно в целях оказания услуг по спортивной подготовке надлежащего качества и объёма, в целях выполнения условий трудового договора, в иных предусмотренных законодательством случаях;

4.12.2. При определении объема и содержания обрабатываемых персональных данных работники учреждения, должны руководствоваться Конституцией Российской Федерации и федеральными законами.

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

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

4.15. Передача персональных данных возможна только с согласия субъекта персональных данных или его законных представителей в случаях, прямо предусмотренных законодательством.

4.16. При передаче персональных данных за пределы учреждения, работники не должны сообщать эти данные третьей стороне без письменного

согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью гражданина или в случаях, установленных федеральным законом.

4.17. Все меры конфиденциальности при сборе, обработке и хранении персональных данных распространяются как на бумажные, так и на электронные (с использованием средств автоматизации и без использования средств автоматизации) носители информации.

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

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

5. Охрана конфиденциальной информации

5.1. В целях охраны конфиденциальной информации работник обязан:

- соблюдать установленный режим охраны такой информации;
- не разглашать конфиденциальные сведения, ставшие ему известными из письменных, устных и иных источников и не использовать эту информацию в личных целях;
- обеспечить невозможность утраты (целостность и сохранность, соблюдение порядка хранения) документов, содержащих указанные сведения;
- обеспечить невозможность несанкционированного доступа к документам, содержащим конфиденциальную информацию, находящимся в его ведении;
- при увольнении представить письменный отчет Руководителю, либо уполномоченному лицу о документах, содержащих конфиденциальные сведения, которые указанное лицо использовало при исполнении своих трудовых обязанностей, а также передать уполномоченному лицу при прекращении трудовых отношений имеющиеся в пользовании работника материальные и иные носители конфиденциальной информации.
- работать только с теми конфиденциальными сведениями и документами, к которым он получил доступ в силу своих служебных обязанностей, знать какие конкретно сведения подлежат защите, а также строго соблюдать правила пользования ими.

5.2. Сотрудники, допущенные к служебной, коммерческой тайне, обязаны незамедлительно сообщить Руководителю учреждения о пропаже документов, машинных носителей информации, содержащих конфиденциальные сведения, а также о несанкционированном доступе лиц к такой информации, или о попытке подобного доступа.

5.3. По факту разглашения конфиденциальной информации, потери документов и иного несанкционированного доступа к конфиденциальным сведениям, проводится служебное расследование, по результатам которого виновные лица привлекаются к ответственности.

5.4. При участии в работе сторонних организаций работник может знакомить их представителей со сведениями, составляющими служебную или коммерческую тайну, только с письменного разрешения Руководителя. Руководитель при этом должен определить конкретные вопросы, подлежащие

рассмотрению, и указать, кому и в каком объеме может быть сообщена информация, подлежащая защите.

5.5. По общему правилу доступ посторонних лиц к сведениям, составляющим врачебную тайну, не допускается, за исключением случаев, установленных действующим законодательством, а также настоящим Положением.

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

5.7. Защита персональных данных от неправомерного их использования или утраты должна быть обеспечена в порядке, установленном действующим законодательством.

5.8. Защита включает в себя следующие меры:

- ограничение и регламентация доступа работников к персональным данным с установлением конкретных прав доступа;
- строгое избирательное и обоснованное распределение документов и информации между работниками организации;
- рациональное и эргономичное размещение рабочих мест работников, имеющих доступ к персональным данным, при котором исключалась бы случайная утечка защищаемой информации;
- ознакомление работников с требованиями нормативно – методических документов по защите информации о персональных данных;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- организация порядка уничтожения информации, содержащей персональные данные работников;
- регламентация обращения документов, содержащих персональные данные, на рабочих местах работников;
- принятие в установленном порядке мер по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства;
- привлечение к дисциплинарной ответственности лиц, виновных в нарушении законодательства о персональных данных.

5.9. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать Обязательство о неразглашении персональных данных.

5.10. При использовании и предоставлении для научных целей персональные данные должны быть обезличены.

6. Ответственность за разглашение конфиденциальной информации

6.1. Работник, который в связи с исполнением трудовых обязанностей получил доступ к сведениям, составляющим конфиденциальную информацию, в случае умышленного или неосторожного разглашения этой

информации при отсутствии в действиях такого работника состава преступления, в соответствии со ст. 192 Трудового кодекса (далее ТК РФ) выносится дисциплинарное взыскание.

6.2. Каждый работник учреждения, получающий для работы конфиденциальный документ (иной материальный носитель конфиденциальной информации), содержащий информацию о персональных данных, несет ответственность за сохранность носителя и конфиденциальность информации.

6.3. Работник, осуществляющий сбор сведений, составляющих коммерческую тайну, незаконными способами в целях разглашения либо незаконного использования этих сведений, а также за их разглашение или незаконное использование, совершенные из корыстной или иной личной заинтересованности и причинивший крупный ущерб учреждению, в соответствии со ст.183 Уголовного кодекса РФ несет уголовную ответственность.

6.4. Лица, которым в установленном законом порядке переданы сведения, составляющие врачебную тайну, с учетом причиненного гражданину ущерба несут за разглашение врачебной тайны дисциплинарную, административную или уголовную ответственность в соответствии с законодательством Российской Федерации, законодательством субъектов Российской Федерации.

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

6.6. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказывается штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.

6.7. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.

Приложение 1
к положению о порядке работы с конфиденциальной информацией в муниципальном автономном учреждении города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства»

ОБЯЗАТЕЛЬСТВО, о неразглашении конфиденциальной информации (персональных данных), не содержащих сведений, составляющих государственную тайну

Я _____
(ФИО)

исполняющий(ая) должностные обязанности по занимаемой должности _____
(должность, наименование отдела)

Предупрежден(а), что на период исполнения должностных обязанностей в соответствии с должностной инструкцией, мне будет предоставлен допуск к конфиденциальной информации (персональным данным), не содержащим сведений, составляющих государственную тайну.

Настоящим добровольно принимаю на себя обязательства:

1. Не разглашать третьим лицам конфиденциальные сведения, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.
2. Не передавать и не раскрывать третьим лицам конфиденциальные сведения, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.
3. В случае попытки третьих лиц получить от меня конфиденциальные сведения, сообщать непосредственному руководителю.
4. Не использовать конфиденциальные сведения с целью получения выгоды.
5. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты конфиденциальных сведений.
6. В течение года после прекращения права на допуск к конфиденциальным сведениям не разглашать и не передавать третьим лицам известные мне конфиденциальные сведения.

Я предупрежден(а), что в случае нарушения данного обязательства буду привлечен(а) к дисциплинарной ответственности и/или иной ответственности в соответствии с законодательством Российской Федерации.

_____ (подпись) _____ (расшифровка)

Дата подписания «____» _____ 20___г.

Приложение 4 к приказу от
«30» декабря 2021 г. № 01-02-144

Перечень сведений конфиденциального характера в муниципальном автономном учреждении города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства»

1. Персональные данные граждан

- фамилия, имя, отчество;
- дата и место его рождения;
- гражданство;
- сведения о состоянии в браке и о составе семьи;
- паспортные данные: номер, серия, дата выдачи;
- сведения о регистрации по месту жительства или по месту пребывания;
- адрес места жительства фактический;
- номер страхового свидетельства государственного пенсионного страхования;
- идентификационный номер налогоплательщика;
- сведения о воинском учете;
- сведения о предыдущих местах работы и основаниях увольнения;
- сведения о трудовом и общем стаже;
- сведения об образовании, квалификации или наличии специальных знаний;
- сведения о заработной плате;
- содержание декларации, подаваемой в налоговую инспекцию;
- сведения о социальных льготах;
- подлинники и копии приказов по личному составу;
- основания к приказам по личному составу;
- сведения о содержании трудового договора, изменений трудового договора, договоров о материальной ответственности;
- документы по оценке деловых и профессиональных качеств Работника при приеме на работу;
- документы, отражающие деятельность конкурсных и аттестационных комиссий;
- документы о результатах служебных расследований;

- подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству предприятия, руководителям структурных подразделений и служб;

- копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения;

- документы бухгалтерского учета, содержащие информацию о расчетах с работником;

- сведения о наличии судимости;

- номер телефона;

- фото;

- трудовая книжка;

- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;

- характеристики;

- рекомендательные письма;

- справки, подтверждающие период работы у работодателя и размер заработной платы;

- наградные документы;

- листки нетрудоспособности;

- медицинские справки;

- иные сведения, относящиеся к персональным данным Работника;

- иные документы, содержащие персональные сведения о работнике.

2. Служебная информация ограниченного распространения

2.1. Сведения о перспективных методах управления учреждением.

2.2. Сведения о ведении и содержании переговоров, целях и содержании совещаний органов управления.

2.3. Сведения, содержащиеся в документах по организации воинского учета и мобилизационной работы.

2.4. Журнал и программа инструктажа по пожарной безопасности, антитеррористической защищенности и гражданской обороны учреждения.

2.5. Схемы размещения инфраструктуры жизнеобеспечения (энергоснабжения, водоснабжения, канализации, теплоснабжения, телефонной связи и др.).

2.6. Содержание переписки, телефонных переговоров, почтовых отправлений, телеграфных, электронных и иных сообщений.

2.7. Организация и состояние системы безопасности жизнедеятельности, в том числе системы защиты информации.

2.8. Организация и состояние охраны и пропускного режима.

2.9. Размещение защищаемых помещений (в которых хранится, циркулирует и обрабатывается конфиденциальная и другая ценная информация со средствами ее хранения, обработки и передачи), организация доступа в них.

2.10. Организация, схемы размещения, возможности и состояние системы охраны техническими средствами, в том числе системы видеонаблюдения, номера электронных ключей.

2.11. Организация, возможности и состояние оперативной связи обеспечения и безопасности жизнедеятельности.

2.12. Организация взаимодействия с правоохранительными и другими государственными органами при проведении совместных мероприятий.

2.13. Сведения, составляющие материалы служебных расследований, проверок, дознания, следствия, судопроизводства.

2.14. Проектная, техническая, эксплуатационная документация на автоматизированные системы (АС), вычислительные сети (ВС), средств связи, в которых обрабатывается и циркулирует конфиденциальная информация.

2.15. Схемы размещения технических средств обработки конфиденциальной информации, коммуникационных линий.

2.16. Сведения о специфических и уникальных программных продуктах.

2.17. Ключи шифрования и электронно-цифровые подписи средств криптографической защиты информации, места и порядок их хранения и выдачи.

2.18. Порядок использования, возможности и состояние систем (средств) криптографической и технической защиты информации, документация на них.

2.19. Организация и состояние систем администрирования, управления доступом в АС и ВС.

2.20. Порядок и места размещения информационных ресурсов, содержащих конфиденциальную информацию учреждения.

2.21. Организация и состояние системы парольной защиты (значение, порядок генерации, использования, смены и прекращения действия паролей) в АС, ВС и других средств вычислительной техники.

2.22. Организация резервирования конфиденциальной информации, места хранения резервных копий конфиденциальной, ценной и другой важной информации.

2.23. Программное обеспечение базового оборудования средств связи.

2.24. База данных абонентских номеров телефонной связи.

3. Информация, составляющая коммерческую тайну

3.1. Сведения о коммерческих замыслах и планах (расширении или свертывании услуг/работ в целом и по отдельным направлениям).

3.2. Содержание и условия коммерческих контрактов, договоров, соглашений и платежей.

3.3. Сведения о целях, задачах, тактике и результатах переговоров с деловыми партнерами.

3.4. Сведения, составляющие коммерческую тайну партнеров, переданные на доверительной основе.

3.5. Содержание регистров бухгалтерского учета и внутренней бухгалтерской отчетности.

3.6. Сведения о фактическом состоянии расчетов по обязательствам.

3.7. Сведения об отдельных финансовых операциях учреждения и о доходах по этим операциям.

3.8. Сведения о внешнеэкономических, валютных и кредитных отношениях с конкретными иностранными и российскими предприятиями, фирмами и организациями.

3.9. Сведения о встречах и переговорах с деловыми партнерами учреждения.

4 Сведения, содержащиеся в документах государственных органов, органов местного самоуправления, других организаций и учреждений с грифом «Для служебного пользования», «Коммерческая тайна», «Конфиденциальная информация».

Приложение 5 к приказу от
«30» декабря 2021 г. №01-02-144

Положение
о внутреннем контроле соответствия обработки ПДн в ИСПДн требованиям к защите персональных данных МАУ «НЦВСМ»

1. Общие положения

1.1. Настоящее Положение о внутреннем контроле соответствия обработки персональных данных требованиям к защите персональных данных МАУ «НЦВСМ» (далее – Положение) разработано с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1.2. Настоящее Положение определяет порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных МАУ «НЦВСМ» и действуют постоянно.

1.3. Для обработки ПДн сотрудников, необходимых для обеспечения кадровой и бухгалтерской деятельности МАУ «НЦВСМ» в соответствии с Трудовым кодексом Российской Федерации, используется ИСПДн.

1.4. Пользователем ИСПДн (далее – Пользователь) является сотрудник МАУ «НЦВСМ», участвующий в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, ПО, данным и средствам защиты информации (далее – СЗИ) ИСПДн.

2. Тематика внутреннего контроля

Тематика внутреннего контроля соответствия обработки ПДн в ИСПДн требованиям к защите ПДн:

2.1. Проверки соответствия обработки ПДн установленным требованиям МАУ «НЦВСМ» разделяются на следующие виды:

- регулярные;
- плановые;
- внеплановые.

2.2. Регулярные контрольные мероприятия проводятся Администратором АИС периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее – План, Приложение № 1) и предназначены для осуществления контроля выполнения требований в области защиты информации МАУ «НЦВСМ».

2.3. Плановые контрольные мероприятия проводятся постоянной комиссией периодически в соответствии с утвержденным Планом проведения контрольных мероприятий и направлены на постоянное совершенствование системы защиты персональных данных ИСПДн МАУ «НЦВСМ».

2.4. Внеплановые контрольные мероприятия проводятся на основании решения комиссии по информационной безопасности (**создается на период проведения мероприятий**). Решение о проведении внеплановых контрольных мероприятий и созданию комиссии по информационной безопасности может быть принято в следующих случаях:

2.4.1. по результатам расследования инцидента информационной безопасности;

2.4.2. по результатам внешних контрольных мероприятий, проводимых регулирующими органами;

2.4.3. по решению генерального директора МАУ «НЦВСМ».

3. Планирование контрольных мероприятий

3.1. Для проведения плановых внутренних контрольных мероприятий лицо, ответственное за обеспечение безопасности персональных данных, разрабатывает План внутренних контрольных мероприятий на текущий год.

3.2. План проведения внутренних контрольных мероприятий включает следующие сведения по каждому из мероприятий:

3.2.1 цели проведения контрольных мероприятий;

3.2.2. задачи проведения контрольных мероприятий,

3.2.3. объекты контроля (процессы, подразделения, информационные системы и т.п.);

3.2.4. состав участников, привлекаемых для проведения контрольных мероприятий;

3.2.5. сроки и этапы проведения контрольных мероприятий.

3.3. Общий срок контрольных мероприятий не должен превышать пяти рабочих дней. При необходимости срок проведения контрольных мероприятий может быть продлен, но не более чем на десять рабочих дней, соответствующие изменения отображаются в Отчете, выполняемом по результатам проведенных контрольных мероприятий.

4. Оформление результатов контрольных мероприятий

4.1. По итогам проведения регулярных контрольных мероприятий результаты проверок фиксируется в Журнале учета событий информационной безопасности (электронный журнал, содержащий записи о событиях информационной безопасности, в том числе о действиях пользователей и эксплуатирующего персонала в ИС).

4.2. По итогам проведения плановых и внеплановых контрольных мероприятий лицо, комиссия, разрабатывает отчет, в котором указывается:

4.2.1. описание проведенных мероприятий по каждому из этапов;

4.2.2. перечень и описание выявленных нарушений;

4.2.3. рекомендации по устранению выявленных нарушений;

4.2.4. заключение по итогам проведения внутреннего контрольного мероприятия.

4.3. отчет передается на рассмотрение генеральному директору МАУ «НЦВСМ».

4.4. Общая информация о проведенных контрольных мероприятиях фиксируется в Журнале учета событий информационной безопасности.

4.5. Результаты проведения мероприятий по внеплановому контролю заносятся в протокол проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных МАУ «НЦВСМ» (Приложение № 2).

5. Порядок проведения плановых и внеплановых контрольных мероприятий

5.1. Плановые и внеплановые контрольные мероприятия проводятся при обязательном участии лица, ответственного за обеспечение безопасности ПДн, также по его ходатайству к проведению контрольных мероприятий могут привлекаться администратор/(ы) АИС, и ответственный за обеспечение безопасности персональных данных информационных систем персональных данных МАУ «НЦВСМ».

5.2. Лицо, ответственное за обеспечение безопасности ПДн, не позднее чем за три рабочих дня до начала проведения контрольных мероприятий уведомляет всех руководителей подразделений, в которых планируется проведение контрольных мероприятий, и направляет им для ознакомления План проведения контрольных мероприятий. При проведении внеплановых контрольных мероприятий уведомление не требуется.

5.3. Во время проведения контрольных мероприятий, в зависимости от целей мероприятий, могут выполнятся следующие проверки:

- Соответствие полномочий Пользователя правилам доступа.
- Соблюдение Пользователями требований инструкций по организации антивирусной, криптографической и парольной политики, инструкции по обеспечению безопасности ПДн.
- Соблюдение Администраторами инструкций и регламентов по обеспечению безопасности информации МАУ «НЦВСМ».
- Соблюдение Порядка доступа в помещения, где ведется обработка персональных данных.
- Знание Пользователей положений Инструкции пользователя по обеспечению безопасности обработки ПДн при возникновении внештатных ситуаций.
- Знание Администраторами инструкций и регламентов по обеспечению безопасности информации МАУ «НЦВСМ».
- Порядок и условия применения средств защиты информации.
- Состояние учета машинных носителей персональных данных.
- Наличие (отсутствие) фактов несанкционированного доступа к ПДн и принятие необходимых мер.
- Проведенные мероприятия по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
- Технические мероприятия, связанные со штатным и нештатным функционированием средств защиты.
- Технические мероприятия, связанные со штатным и нештатным функционированием подсистем системы защиты информации.

Приложение № 1
к положению о внутреннем контроле соответствия
обработки ПДн в ИСПДн требованиям к
защите персональных данных МАУ «НЦВСМ»

ПЛАН

внутренних проверок контроля соответствия обработки ПДн в ИСПДн требованиям к защите персональных данных МАУ «НЦВСМ»

Мероприятие	**Периодичность регулярных мероприятий**	**Периодичность плановых мероприятий**	**Исполнитель**
Контроль соблюдения правил доступа к ПДн	Ежемесячно	Ежегодно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных в МАУ «НЦВСМ»
Контроль соблюдения режима защиты	Ежемесячно	Ежегодно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных в МАУ «НЦВСМ»
Контроль выполнения антивирусной и криптографической политики	Ежемесячно	Ежегодно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных в МАУ «НЦВСМ»
Контроль выполнения парольной политики	Ежеквартально	Ежегодно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных в МАУ «НЦВСМ»
Контроль соблюдения режима защиты при подключении к сетям общего пользования и (или) международного обмена	Ежемесячно	Ежегодно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных в МАУ «НЦВСМ»
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн		Один раз в два года	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных в МАУ «НЦВСМ»
Контроль обновления ПО и единообразия применяемого ПО на всех элементах АИС _____СПО	Ежемесячно	Ежегодно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных в МАУ «НЦВСМ»
Контроль обеспечения резервного копирования		Ежегодно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных в МАУ «НЦВСМ»
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз		Один раз в два года	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных в МАУ «НЦВСМ»
Поддержание в актуальном состоянии нормативно-организационных документов		Ежегодно	Ответственный за организацию обработки ПДн в в МАУ «НЦВСМ»
Контроль запрета на использование беспроводных соединений	Ежемесячно	Ежегодно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных в МАУ «НЦВСМ»

Приложение № 2
к положению о внутреннем контроле соответствия
обработки ПДн в ИСПДн требованиям к
защите персональных данных МАУ «НЦВСМ»

ПРОТОКОЛ № ____

проведения внутренних проверок контроля соответствия обработки ПДн в ИСПДн требованиям к защите персональных данных МАУ «НЦВСМ»

Настоящий Протокол составлен в том, что «__» _____20___ г.
Администратором ИСПДн/ _____
(должность, Ф.И.О. сотрудника)

проведена проверка _____
(тема проверки)

Проверка осуществлялась в соответствии с требованиями:

_____
(название документа)

_____

В ходе проверки проверено:

_____
_____
_____
_____
_____
_____
_____

Выявленные нарушения:

_____
_____
_____
_____
_____
_____
_____

Меры по устранению нарушений:

_____
_____
_____
_____
_____
_____
_____
_____
_____

Срок устранения нарушений: _____

Председатель комиссии:
фамилия и инициалы / подпись / должность

Члены комиссии:
фамилия и инициалы / подпись / должность
фамилия и инициалы / подпись / должность
фамилия и инициалы / подпись / должность

Приложение №3
к положению о внутреннем контроле соответствия
обработки ПДн в ИСПДн требованиям к
защите персональных данных МАУ «НЦВСМ»

ЖУРНАЛ
учёта событий информационной безопасности в
МАУ «НЦВСМ»

Начат: _____20__г.
Окончен: _____20__г.

№ п/п	Дата события	Основания возникновения события	Описание события (мероприятия)	Характеристика события	(ФИО, субъекта)	Должность, ФИО и подпись ответственного за ведение журнала	Примечание

Приложение 6 к приказу от
«30» декабря 2021 г. № 01-02-144

Положение об ответственности работников, допущенных к обработке персональных данных и иной конфиденциальной информации в МАУ «НЦВСМ»

1. Общие положения

Конституцией РФ установлено, что каждый гражданин имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту чести и доброго имени.

Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются (ст. 23, 24 Конституции РФ).

В целях защиты частной жизни личности в связи со сбором персональных данных определена юридическая ответственность за нарушение установленных законодательством правил работы с персональными данными.

2. Ответственность работников, допущенных к обработке персональных данных

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами (ст. 90 ТК).

2.1. Дисциплинарная ответственность

На лицо, ненадлежащим образом относящееся к хранению и сбережению указанной информации, сведений, может быть наложено дисциплинарное взыскание.

Дисциплинарное взыскание может быть наложено на лицо, обязанное должным образом хранить и беречь информацию, касающуюся персональных данных работника, но в результате ненадлежащего хранения, допустившего ее порчу или утрату.

Дисциплинарная ответственность предусмотрена трудовым законодательством (ст. 192-195 ТК РФ).

За совершение дисциплинарного проступка, т.е. неисполнение или ненадлежащее исполнение работником по его вине возложенных на него трудовых обязанностей (в том числе, применительно к рассматриваемой ст. 90 ТК РФ, это могут быть обязанности соблюдения установленного порядка со сведениями конфиденциального характера), работодатель вправе применить предусмотренные ст. 192 ТК дисциплинарные взыскания (замечание, выговор, увольнение по соответствующим основаниям) в порядке, установленном статьей 193 ТК РФ.

За разглашение охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с выполнением им своих трудовых обязанностей, может последовать

расторжение трудового договора (см. п.п. «в» п. 6 ст. 81 ТК). Кроме того, на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, может быть возложена обязанность возместить причиненные этим убытки (см. ст. 8, ч. 2 ст. 139 ГК РФ; п. 7 ч. 1 ст. 243 ТК).

2.2. Административная ответственность

В соответствии со ст. 13.11 КоАП РФ, предусматривающей ответственность за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) накладывается административное взыскание. Нарушение данной нормы влечет за собой предупреждение или наложение штрафа в размере: на граждан — от 300 до 500 рублей; должностных лиц — от 500 до 1000 рублей; юридических лиц — от 5 тысяч до 10 тысяч рублей (в ред. Федерального закона от 22.06.2007 N 116-ФЗ).

В соответствии со ст. 13.14 указанного Кодекса разглашение информации с ограниченным доступом лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, влечет за собой наложение административного штрафа на граждан в размере от 500 до 1 тысячи рублей; на должностных лиц — от 4 тысяч до 5 тысяч рублей (в ред. Федерального закона от 22.06.2007 N 116-ФЗ).

2.3. Гражданско-правовая ответственность

Гражданский кодекс предусматривает защиту нематериальных благ граждан, включая неприкосновенность частной жизни, личную и семейную тайну, деловую репутацию и др.

Соответственно устанавливаются формы гражданско-правовой ответственности в виде денежной компенсации за причиненный моральный вред, обязанности опровержения сведений, порочащих честь, достоинство или деловую репутацию гражданина (работника) и т.п. (ст.ст. 150, 151, 152 ГК).

2.4. Уголовная ответственность

Уголовным кодексом РФ предусматривается уголовная ответственность: за злоупотребления и незаконные действия с информационными данными о частной жизни (ст. 137 УК), за неправомерный отказ должностного лица в предоставлении документов и материалов, непосредственно затрагивающих права и свободы гражданина, если эти деяния причинили вред правам и законным интересам граждан (в т.ч. работникам) (ст. 140 УК).

Согласно ст. 272 УК РФ неправомерный доступ к охраняемой законом компьютерной информации, наказывается штрафом, исправительными работами, либо лишением свободы.

Приложение 7 к приказу от
«30» декабря 2021 г. № 01-02-144

Положение
об обработке и обеспечении безопасности персональных данных, обрабатываемых в информационных системах персональных данных муниципального автономного учреждения города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства»

1. Общие положения

1.1. Настоящее положение об обработке и обеспечении безопасности персональных данных, обрабатываемых в информационных системах персональных данных муниципального автономного учреждения города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства» (далее – Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденным Постановлением Правительства Российской Федерации от 01.11.2012 № 1119, и Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным Постановлением Правительства Российской Федерации от 15.09.2008 № 687.

1.2. Настоящим Положением определяется порядок обработки и обеспечения безопасности персональных данных, при их обработке в информационных системах персональных данных с использованием средств автоматизации и без использования средств автоматизации в муниципальные автономные учреждения города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства» (далее – Учреждение).

1.3. В настоящем Положении используются следующие понятия:

1.3.1. Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

1.3.2. Информационная система персональных данных (далее – Информационная система) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

1.3.3. Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

1.3.4. Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

1.3.5. Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

1.3.6. Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

1.3.7. Обработка персональных данных без использования средств автоматизации (далее – Неавтоматизированный способ) – действия с персональными данными, такие как сбор, систематизация, накопление, хранение, использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.
1.3.8. Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.
1.3.9. Оператор – Учреждение, юридическое или физическое лицо, организующие и осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.
1.3.10. Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.
1.3.11. Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.
1.3.12. Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъекта персональных данных.
1.3.13. Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

2. Порядок обработки персональных данных

2.1. Обработка персональных данных в Информационных системах Учреждения должна осуществляться на основе принципов:
— законности целей и способов обработки персональных данных и добросовестности;
— соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;
— соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
— достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
— недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.
2.2. Обработка персональных данных в Информационных системах Учреждения может осуществляться оператором с письменного согласия субъектов персональных данных, за исключением следующих случаев, когда такого согласия не требуется, если:

— обработка персональных данных осуществляется на основании федерального закона, устанавливающего её цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;
— обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;
— обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
— обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно.
2.3. Обработка оператором специальных категорий персональных данных в Информационных системах Учреждении допускается если:
— субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;
— персональные данные являются общедоступными;
— персональные данные относятся к состоянию здоровья субъекта персональных данных и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц, и получение согласия субъекта персональных данных невозможно;
— обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну.
2.4. В случае если оператор на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.
2.5. Оператор, получающий доступ к персональным данным, должен обеспечивать конфиденциальность таких данных, за исключением случаев:
— в случае обезличивания персональных данных;
— в отношении общедоступных персональных данных.
2.6. Обработка персональных данных в Информационных системах Учреждения осуществляется только с согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных федеральными законами, которыми предусматриваются случаи обязательного предоставления субъектом персональных данных своих персональных данных в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.
2.7. Письменное согласие субъекта персональных данных на обработку своих персональных данных в Информационных системах Учреждения должно включать в себя:
— фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
— наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;
— цель обработки персональных данных;

— перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
— перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
— срок, в течение которого действует согласие, а также порядок его отзыва.
2.8. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных, а в случае обработки общедоступных персональных данных в Информационных системах Учреждения обязанность доказывания того, что обрабатываемые персональные данные являются общедоступными, возлагается на оператора.
2.9. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных в Информационных системах Учреждения дает в письменной форме законный представитель субъекта персональных данных.
2.10. В случае смерти субъекта персональных данных согласие на обработку его персональных данных в Информационных системах Учреждения дают в письменной форме наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.
2.11. Субъект персональных данных имеет право на получение сведений об обработке своих персональных данных в Информационных системах Учреждения, а оператор обязан их предоставить в соответствии со статьями 14 и 20 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

3. Меры по обеспечению безопасности персональных данных при их обработке
3.1. Безопасность персональных данных, обрабатываемых в Информационных системах Учреждения, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.
3.2. Для обеспечения безопасности персональных данных при их обработке в Информационных системах Учреждения осуществляется защита:
— информации, обрабатываемой с использованием технических средств;
— информации, содержащейся на бумажной, магнитной, магнитно-оптической и иной основе (носителях).
3.3. Работы по обеспечению безопасности персональных данных при их обработке в Информационных системах Учреждения являются неотъемлемой частью работ по созданию Информационных систем.
3.4. Информационные системы Учреждения классифицируются оператором.
3.5. Обмен персональными данными при их обработке в Информационных системах Учреждения осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических и программных средств.
3.6. Размещение Информационных систем Учреждения, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.
3.7. Безопасность персональных данных при их обработке в Информационных системах Учреждения обеспечивает оператор или лицо, которому на основании договора оператор поручает обработку персональных данных (далее – Уполномоченное лицо). Существенным условием договора является обязанность

Уполномоченного лица обеспечить конфиденциальность персональных данных и безопасность персональных данных при их обработке в информационной системе.
3.8. При обработке персональных данных в Информационных системах Учреждения безопасность обеспечивается:
— проведением мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
— своевременным обнаружением фактов несанкционированного доступа к персональным данным;
— недопущением воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
— возможностью незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
— постоянным контролем за обеспечением уровня защищенности персональных данных.
3.9. Защита персональных данных, обрабатываемая в Информационных системах Учреждения, обеспечивается за счет средств Учреждения в порядке, установленном федеральными законами.
3.10. Доступ работников Учреждения к персональным данным, обрабатываемым в Информационных системах Учреждения, для выполнения своих должностных обязанностей производится к соответствующим персональным данным на основании списка, утвержденного оператором.

4. Особенности обработки персональных данных, осуществляемых без использования средств автоматизации

4.1. Персональные данные при их обработке, осуществляемой Неавтоматизированным способом, должны обособляться от иной информации, фиксацией их на отдельных материальных носителях персональных данных (далее — Материальные носители), в специальных разделах книг (журналов) или на полях форм (бланков).
4.2. При фиксации персональных данных на Материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой Неавтоматизированным способом, для каждой категории персональных данных должен использоваться отдельный Материальный носитель.
4.3. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – Типовая форма), должны соблюдаться следующие условия:
4.3.1. Типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать:
— сведения о цели обработки персональных данных, осуществляемой Неавтоматизированным способом;
— имя (наименование) и адрес оператора;
— фамилию, имя, отчество и адрес субъекта персональных данных;
— источник получения персональных данных;
— сроки обработки персональных данных;
— перечень действий с персональными данными, которые будут совершаться в процессе их обработки;

— общее описание используемых оператором способов обработки персональных данных.

4.3.2. Типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую Неавтоматизированным способом.

4.3.3. Типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных.

4.3.4. Типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

4.4. При несовместимости целей обработки персональных данных, зафиксированных на одном Материальном носителе, если Материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных:

4.4.1. При необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же Материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных.

4.4.2. При необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется Материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

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

4.6. Правила, предусмотренные пунктами 4.4 и 4.5 настоящего Положения, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном Материальном носителе персональных данных и информации, не являющейся персональными данными.

4.7. Уточнение персональных данных при осуществлении их обработки Неавтоматизированным способом производится путем обновления или изменения данных на Материальном носителе, а если это не допускается техническими особенностями материального носителя, — путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

4.8. Обработка персональных данных, осуществляемая Неавтоматизированным способом, должна производиться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (Материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

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

5. Обязанности лиц, имеющих доступ к персональным данным

5.1. Ответственность за обеспечение безопасности персональных данных и надлежащий режим работы Информационных систем Учреждения возлагается на ответственного за защиту информации, в том числе за обеспечение безопасности персональных данных в информационных системах.

5.2. Работники Учреждения, допущенные к обработке персональных данных в Информационных системах, должны руководствоваться требованиями федеральных законов, нормативно-правовых документов Правительства Российской Федерации, Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации, Министерства информационных технологий и связи Российской Федерации, а также настоящим Положением и инструкцией по работе пользователей в информационных системах.

5.3. В должностные инструкции работников Учреждения, уполномоченных на обработку персональных данных в Информационных системах, должны быть внесены обязанности о необходимости выполнения требований по обеспечению безопасности обрабатываемых ими персональных данных.

5.4. Ответственный за защиту информации, в том числе за обеспечение безопасности персональных данных в информационных системах руководствуется в своей деятельности инструкцией ответственного за защиту информации, в том числе за обеспечение безопасности персональных данных в информационных системах Учреждения.

5.5. При обнаружении нарушений порядка предоставления персональных данных, обрабатываемых в Информационных системах, оператор незамедлительно приостанавливает предоставление персональных данных пользователям Информационных систем Учреждения до выявления причин нарушений и устранения этих причин.

5.6. За нарушение норм настоящего Положения, а также федеральных законов, регламентирующих порядок обработки и обеспечения безопасности персональных данных, работники Учреждения, допущенные к работе с персональными данными в Информационных системах, несут гражданско-правовую, административную, уголовную и дисциплинарную ответственность в соответствии с действующим законодательством.

Приложение 8 к приказу от
«30» декабря 2021 г. №01-02-144

Положение о службе (ответственном лице) информационной безопасности муниципального автономного учреждения города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства»

1. Общие положения

Служба информационной безопасности (далее Служба) муниципального автономного учреждения города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства» (далее Оператор) создается в целях выполнения требований действующего законодательства Российской Федерации, иных нормативно-правовых актов, регламентирующих обеспечение защиты информации, в том числе обеспечение безопасности при обработке персональных данных, а также обеспечение защиты и безопасности информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных.

2. Структура

Структура и штатная численность Службы определяются приказом руководителя Оператора. Служба создаётся на функциональной основе, т.е. без выделения штатных единиц, и включает заместителя руководителя учреждения, в ведении которого находится отдел автоматизированных систем управления, системного администратора, специалиста юридического отдела. Руководство Службой по приказу руководителя возлагается на заместителя руководителя, в ведении которого находится отдел автоматизированных систем управления.

3. Задачи

Основные задачи Службы заключаются в следующем.

1. Разработка и реализация комплекса организационных и технических мер, направленных на выполнение установленных требований к обеспечению безопасности и защите информации, в том числе персональных данных.
2. Обеспечение постоянного контроля в подразделениях Оператора за выполнением установленных требований к обеспечению безопасности и защите информации, в том числе персональных данных.
3. Разработка и внесение предложений руководству Оператора по совершенствованию и развитию корпоративной системы обеспечения безопасности и защиты информации, в том числе персональных данных.

4. Функции

Для выполнения поставленных задач Служба осуществляет следующие функции.

1. Готовит и представляет на рассмотрение руководству Оператора проекты локальных нормативных актов по вопросам обеспечения защиты информации, в том числе персональных данных.
2. Организует и проводит во взаимодействии с заинтересованными подразделениями классификацию информационных систем на этапе создания информационных систем или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем) с целью установления методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных в соответствии с установленными требованиями.
3. Разрабатывает и реализует комплекс организационных и мер по обеспечению защиты информации от:

— неправомерного доступа;
— уничтожения;
— модифицирования;
— блокирования;
— копирования;
— предоставления;
— распространения;

— а также от иных неправомерных действий в отношении такой информации.

4. Для защиты информации, в том числе персональных данных от неправомерного доступа Служба обеспечивает:

— контроль за строгим соблюдением принятых Оператором локальных нормативных актов по работе и защите персональных данных;

— предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

— своевременное обнаружение фактов несанкционированного доступа к информации;

— предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

— возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней.

5. Служба при создании и эксплуатации корпоративных информационных систем:

— самостоятельно разрабатывает и внедряет методы и способы защиты информации, соответствующие установленным требованиям;

— согласовывает исполнителю планируемые для использования в целях защиты информации методы и способы при условии их соответствия установленным требованиям.

6. Служба:

— разрабатывает и реализует меры организационного и технического характера по недопущению воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

— организует и(или) проводит экспертизу технических средств, используемых при обработке информации на предмет соответствия возможностей защиты информации указанных средств установленным требованиям.

7. Служба разрабатывает и реализует меры по информированию и обучению персонала Оператора, в том числе вновь принимаемых на работу лиц, по вопросам защиты информации и персональных данных.

8. Служба контролирует выполнение установленных требований по:

— осуществлению обмена персональными данными при их обработке в информационных системах по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств:

— размещению информационных систем, специального оборудования и охране помещений, в которых ведется работа с персональными данными, организации режима обеспечения безопасности в этих помещениях в части обеспечения сохранности носителей персональных данных и средств защиты информации, а также исключения возможности неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц;

— соблюдению парольной защиты;

— соблюдению установленного регламента работы с электронной почтой;

— соблюдению установленного регламента использования ресурсов сети Интернет.

9. В соответствии с установленными нормативно-правовыми актами, требованиями Служба обеспечивает:

— определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

— разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

— проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

— установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

— обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

— учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

— учет лиц, допущенных к работе с персональными данными в информационной системе;
— контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
— разбор и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
— описание системы защиты информации, в том числе персональных данных;
— ежегодное планирование работы по совершенствованию системы защиты информации, в том числе персональных данных;
— постоянный контроль за обеспечением уровня защищенности информации.

5. Взаимодействие

Для решения поставленных задач и осуществления предусмотренных настоящим Положением функций Служба взаимодействует:
— с руководителем Оператора и его заместителями;
— с любыми иными подразделениями Оператора;
— с государственными, муниципальными органами, учреждениями и организациями, с надзорными органами, а также с иными органами, предприятиями и организациями.
В ходе взаимодействия руководитель и сотрудники Службы:
— в установленном порядке, получают необходимую для осуществления деятельности Службы информацию, разъяснения, уточнения, нормативные и иные документы;
— готовит и в установленном порядке вносит руководству Оператора предложения по проведению организационных и технических мероприятий, изданию локальных нормативных актов, принятию иных мер по установленным направлениям деятельности в сфере защиты информации, в том числе персональных данных;
— готовит и в установленном порядке предоставляет информацию по находящимся в их компетенции вопросам в сфере защиты информации, в том числе персональных данных, по запросам подразделений Оператора, государственных, муниципальных органов, учреждений и организаций, надзорных органов, а также иных органов, предприятий и организаций.

6. Ответственность

Руководитель Службы несет ответственность перед руководством Оператора согласно действующему законодательству, нормативно-правовым и локальным нормативным правовым актам за обеспечение:
— выполнения поставленных перед Службой задач и функций;
— работы с документами и их сохранности, своевременного и качественного исполнения поручений и обращений;
— выполнения требований правил внутреннего трудового распорядка;
Все сотрудники Службы несут ответственность перед руководителем Службы и руководством Оператора за своевременное и качественное выполнение:
— требований выполнения действующего законодательства Российской Федерации, иных нормативно-правовых документов, регламентирующих обеспечение защиты информации, в том числе обеспечение безопасности при обработке персональных данных;
— обязанностей, предусмотренных Трудовым кодексом РФ, правилами внутреннего трудового распорядка, настоящим Положением, трудовыми договорами и должностными инструкциями.

Приложение 9 к приказу от
«30» декабря 2021 г. №01-02-144

ПОЛОЖЕНИЕ
о разграничении прав доступа к обрабатываемым персональным данным в информационных системах персональных данных муниципального автономного учреждения города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства»

Настоящее положение определяет права доступа к обрабатываемым персональным данным в информационных системах персональных данных (далее – ИСПДн) муниципального автономного учреждения города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства» (далее – МАУ «НЦВСМ»), а также уровень доступа к обрабатываемым персональным данным.

Разграничение прав осуществляется на основании Модели угроз безопасности персональных данных, обрабатываемых в ИСПДн МАУ «НЦВСМ», а также исходя из характера и режима обработки персональных данных в ИСПДн МАУ «НЦВСМ».

Работники МАУ «НЦВСМ», которые в рамках своих должностных обязанностей обрабатывают персональные данные субъектов ПДн, должны быть внесены в Перечень лиц, имеющих доступ к персональным данным в ИСПДн.

Уровень прав доступа представлен в Таблице 1.

Таблица 1

№ п/п	Группа	Уровень доступа к ПДн, техническим средствам, прикладному ПО и СЗИ	Разрешенные действия
1	Администратор безопасности информационных систем	Доступ к ПДн, техническим средствам и прикладному ПО. Без доступа к СЗИ	– Модернизация, настройка и мониторинг работоспособности комплекса технических средств (серверов, рабочих мест); – установка, модернизация, настройка и мониторинг работоспособности системного и базового программного обеспечения; – установка, настройка и мониторинг прикладного программного обеспечения; – соблюдение правил, оговоренных в инструкции администратора.
2	Ответственный за защиту информации, в том числе за обеспечение безопасности персональных данных в информационных системах	Доступ к ПДн и СЗИ. Без доступа к техническим средствам и прикладному ПО	– управление правами доступа пользователей к функциям системы; – проверка состояния используемых СЗИ от НСД, проверка правильности их настройки; – обеспечение функционирования и поддержание работоспособности СЗИ; – проведение инструктажа эксплуатационного персонала и пользователей СВТ по правилам работы с используемыми СЗИ; – мониторинг информационной безопасности; – контроль и предотвращение несанкционированного изменения целостности ресурсов; – контроль аппаратной конфигурации защищаемых компьютеров и предотвращение попытки ее несанкционированного изменения.
3	Ответственный за эксплуатацию СКЗИ	Доступ на правах администратора к сертифицированным СКЗИ. Без доступа к ПДн, техническим средствам и СЗИ	– поэкземплярный учет используемых оператором криптосредств, эксплуатационной и технической документации к ним; – контроль за соблюдением условий использования криптосредств, установленных эксплуатационной и технической документацией на СКЗИ и настоящей инструкцией; – учет Пользователей криптосредств; – надежное хранение эксплуатационной и технической документации к криптосредствам, ключевых документов, носителей дистрибутивов криптосредств, бумажных и машинных носителей ПДн; – расследования и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению требуемого уровня безопасности информации; – разработка и принятие мер по предотвращению возможных негативных последствий нарушений.
4	Пользователь	Доступ на правах пользователя к ПДн, прикладному ПО и СЗИ. Без доступа к техническим средствам	– Сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, предоставление записей, содержащих ПДн.

Приложение 10 к приказу от
«30» декабря 2021 г. №01-02-144

Порядок
доступа сотрудников в помещения, в которых ведется обработка персональных данных, хранилища для бумажных и машинных носителей ПДн в ИСПДн

1. Для хранения документов на бумажных носителях в МАУ «НЦВСМ» предназначены следующие помещения:

по адресу: г. Новосибирск, Красный проспект, 167а:

- кабинет № 2 (отдел кадров): металлические огнеупорные шкафы, шкафы;

- кабинет № 9 (отдел по олимпийским видам спорта, отдел по неолимпийским видам спорта): шкафы;

- кабинет № 17 (финансовый отдел): металлический сейф шкаф, шкафы;

- кабинет № 19 (финансовый отдел): металлический сейф шкаф, шкаф;

- кабинет № 21(финансовый отдел): металлический сейф шкаф, шкаф.

2. Для размещения автоматизированных рабочих мест (далее - АРМ) информационных систем персональных данных (далее - ИСПДН) предназначены помещения:

по адресу: г. Новосибирск, Красный проспект, 167а:

- начальник отдела кадров, менеджер по персоналу, специалист по кадровому делопроизводству каб. 2;

- главный бухгалтер, начальник финансового отдела, ведущий бухгалтер, бухгалтер, бухгалтер, бухгалтер каб. 17, 18, 19, 21;

- начальник административно-хозяйственного отдела каб. 5;

- секретарь руководителя каб. 3.

по адресу: г. Новосибирск, Зорге, 82/3:

- бухгалтер каб. 5.

4. Для размещения серверной предназначено помещение:

- каб. 26.

5. Порядок доступа сотрудников МАУ «НЦВСМ» в помещения, в которых ведется обработка персональных данных:

- каждый кабинет запирается на ключ и опечатывается;

- работники учреждения, имеющие доступ в помещения, самостоятельно заходят в кабинеты, лично запирают и опечатывают кабинеты;

- работники учреждения, не имеющие доступа в помещения, где обрабатываются персональные данные, имеют право временно прибывать в указанных помещениях только в присутствии работников, имеющих право доступа в эти помещения.

Приложение 11 к приказу от
«30» декабря 2021 г. №01-02-144

Требования к оборудованию помещений и размещению технических средств, используемых для обработки персональных данных в муниципальном автономном учреждении города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства»

Настоящие Требования определяют порядок оборудования выделенных помещений и условия размещения в них технических средств (персональных компьютеров, серверов и т.п.), используемых для обработки персональных данных в МАУ «НЦВСМ».

Расположение выделенных помещений и размещаемых в них технических средств должно исключать возможность бесконтрольного проникновения в эти зоны посторонних лиц и гарантировать сохранность находящихся в них конфиденциальных документов, содержащих персональные данные.

Размещение оборудования и технических средств, предназначенных для обработки персональных данных, должно соответствовать требованиям техники безопасности, санитарным нормам, а также требованиям пожарной безопасности.

Внутренняя планировка и расположение рабочих мест в выделенных помещениях должны обеспечивать исполнителям сохранность доверенных им конфиденциальных документов и сведений, содержащих персональные данные.

Входные двери выделенных помещений должны быть оборудованы замками, гарантирующими санкционированный доступ в них в нерабочее время.

В выделенные помещения допускаются руководство учреждения, ответственный за информационную безопасность, иные уполномоченные лица и исполнители, имеющие прямое отношение к приему, обработке и передаче персональных данных.

Допуск в выделенные помещения вспомогательного и обслуживающего персонала (уборщицы, электромонтеры и т.д.) производится только при служебной необходимости и в сопровождении ответственного за помещение, при этом необходимо принять меры, исключающие визуальный просмотр конфиденциальных документов, содержащих персональные данные.

По окончании рабочего дня выделенные помещения необходимо закрывать и опечатывать, затем их сдают под охрану с указанием времени приема/сдачи в журнале приема/сдачи помещений.

Сдачу ключей выделенных помещений, а также получение ключей и вскрытие выделенных помещений имеют право производить только работники, внесенные в утвержденный руководством учреждения список.

Учреждение находиться под круглосуточной охраной и видеонаблюдением, администратор по окончании рабочего дня, закрывает ключи от выделенных помещений в специальных шкафах и сдает опечатанные ключи на пост охраны.

Перед вскрытием выделенных помещений должна быть проверена целостность оттисков печатей и исправность замков. При обнаружении нарушения целостности

оттисков печатей, повреждения замков или других признаков, указывающих на возможное проникновение в эти помещения посторонних лиц, помещение не вскрывается, а о случившемся немедленно информируется руководство учреждения.

В случае утраты ключа от входной двери выделенного помещения немедленно ставится в известность руководство учреждения.

В выделенных помещениях, где установлены средства защиты информации от утечки по техническим каналам, запрещается приносить и использовать радиотелефоны/сотовые телефоны и другую радиоаппаратуру.

На случай пожара, аварии или стихийного бедствия должны быть разработаны специальные инструкции, утвержденные руководством учреждения, в которых предусматривается вызов администрации, должностных лиц, вскрытие выделенных помещений, очередность и порядок спасения конфиденциальных документов, содержащих персональные данные, и дальнейшего их хранения.

Приложение 12 к приказу от
«30» декабря 2021 г. №01-02-144

Правила
рассмотрения запросов субъектов персональных данных или их представителей

1. Общие положения

Настоящие Правила разработаны в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее - Федеральный закон), Трудовым кодексом Российской Федерации и определяют порядок обработки поступающих в МАУ «НЦВСМ» обращений субъектов персональных данных или их законных представителей.

2. Права субъектов персональных данных

2.1. В соответствии с действующим законодательством субъект персональных данных или его законный представитель имеет право на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных;
- правовые основания и цели обработки персональных данных;
- цели и применяемые способы обработки персональных данных;
- наименование и место нахождения учреждения, сведения о лицах, которые имеют доступ к персональным данным или которыми могут быть раскрыты персональные данные на основании договора, на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных федеральным законом;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению руководителя, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные федеральными законами или другими нормативными правовыми актами РФ.

2.2. Право субъекта персональных данных на доступ к его персональным данным ограничивается в соответствии с федеральным законом, в том числе в случаях, предусмотренных частью 8 статьи 14 Федерального закона:

- обработка персональных данных, включая персональные данные, полученные в результате оперативно-разыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;
- обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

- обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

- доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

- обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

2.3. Субъект персональных данных вправе требовать от учреждения уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав. Если субъект персональных данных считает, что учреждение осуществляет обработку его персональных данных с нарушением требований Федерального закона или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие учреждения в уполномоченном органе по защите прав субъектов персональных данных или в судебном порядке.

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

3. Порядок работы с запросами, уведомлениями и иными обращениями субъектов персональных данных или их представителей

3.1. При поступлении запроса, уведомления или иного обращения субъекта персональных данных или его представителя, уполномоченными должностными лицами учреждения осуществляется его регистрация в журнале учета обращений субъектов персональных данных.

3.2. Уполномоченные должностные лица учреждения обязаны сообщить в порядке, предусмотренном статьей 14 Федерального закона, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение 30 (тридцати) дней с даты получения запроса субъекта персональных данных или его представителя.

3.3. Уполномоченные должностные лица учреждения обязаны сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение 30 (тридцати) дней с даты получения такого запроса.

3.4. Во всем ином, что не урегулировано настоящими Правилами, при работе с запросами, уведомлениями и иными обращениями по вопросам обработки персональных данных уполномоченные должностные лица учреждения руководствуются действующим законодательством Российской Федерации.

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

ФОРМА ЗАПРОСА ИНФОРМАЦИИ,
КАСАЮЩЕЙСЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ СУБЪЕКТА

Заявление

Прошу предоставить мне для ознакомления обрабатываемую Вами информацию, составляющую мои персональные данные, указать цели, способы и сроки ее обработки, предоставить сведения о лицах, которые имеют к ней доступ (которым может быть предоставлен такой доступ), сведения о том, какие юридические последствия для меня может повлечь ее обработка.

В случае отсутствия такой информации прошу Вас уведомить меня об этом.

(подпись) (ФИО) (дата)

Приложение 2 к правилам
рассмотрения запросов субъектов персональных
данных или их представителей

УВЕДОМЛЕНИЕ
об устранении допущенных нарушений

Настоящим уведомлением сообщаем Вам, что допущенные при обработке персональных данных нарушения, а именно _____

_____,

(указать допущенные нарушения)

устранены.

_____

(должность) *(подпись)* *(расшифровка подписи)*

«___»_____20__г.

Приложение 3 к правилам
рассмотрения запросов субъектов персональных
данных или их представителей

УВЕДОМЛЕНИЕ
об уничтожении ПДн

№ _____ « ___ » _____ 20__г.

На № _____ от _____

_____

(Ф.И.О. субъекта персональных данных)

Уважаемый(ая) _____,

МАУ «НЦВСМ» уведомляет Вас о том, что в связи с достижением «___» _____ 20__ года цели обработки Ваших персональных данных, а именно:

_____

_____

_____

_____,

(указать цель обработки персональных данных)

«___» _____ 20__ года, в соответствии с требованиями статьи 21 Федерального закона № 152-ФЗ от 27.07.2006 г. «О персональных данных», Ваши персональные данные уничтожены.

_____

(должность) *(подпись)* *(расшифровка подписи)*

Приложение 4 к правилам
рассмотрения запросов субъектов персональных
данных или их представителей

Форма журнала
учета обращений и запросов граждан по вопросам обработки персональных данных

Журнал начат "___ " _____ 201__ г.

(Ф.И.О. должностного лица) (должность)

Журнал завершен "___ " _____ 20_ г.

(Ф.И.О. должностного лица) (должность)

На _____ листах

№ п/п	Сведения о запрашивающем лице	Краткое содержание обращения	Цель запроса	Отметка о предоставлении информации или отказе в ее предоставлении	Дата передачи/отказа в предоставлении информации	Подпись ответственного лица	Примечание
1	2	3	4	5	6	7	8

Приложение 13 к приказу от
«30» декабря 2021 г. № 01-02-144

ТИПОВАЯ ФОРМА РАЗЪЯСНЕНИЯ

субъекту персональных данных юридических последствий отказа предоставить свои персональные данные

В соответствии с частью 2 статьи 18 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

мне

_____
(ФИО)

Зарегистрированный(ая) по адресу: _____

_____

документ, удостоверяющий личность _____

_____

Разъяснены юридические последствия отказа предоставить свои персональные данные, предоставление которых является обязательным в соответствии с законодательством.
Я предупрежден(а), что в случае отказа предоставить свои персональные данные уполномоченным лицам МАУ «НЦВСМ» право на труд, право на пенсионное обеспечение и медицинское страхование работников, право на допуск к работе по результатам периодических медицинских осмотров, право на страхование жизни и здоровья, перечисление заработной платы через банк, право на возмещение расходов на оплату найма жилого помещения, направление в служебные командировки, поездки для участия в соревнованиях и тренировочных мероприятиях, право на представление к наградам и поощрениям за результаты трудовой деятельности, не может быть реализовано в полном объеме.

_____ _____ «__» _____ г.
(подпись) (расшифровка подписи)

Приложение 14 к приказу от
«30» декабря 2021 г. № 01-02-144

Перечень
персональных данных, обрабатываемых в муниципальном автономном учреждении города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства»

1. Перечень обрабатываемых персональных данных субъектов персональных данных, являющихся работниками МАУ «НЦВСМ»:

1.1. Обрабатываемые в ИС «Зарплата и кадры»:

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

–дата рождения (число, месяц, год рождения);

–место рождения;

–пол;

–паспортные данные: серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи, адрес по месту регистрации;

–гражданство;

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

–идентификационный номер налогоплательщика;

–адрес места жительства (адрес регистрации, фактического проживания);

–номер контактного телефона или сведения о других способах связи;

–реквизиты страхового свидетельства государственного пенсионного страхования;

–сведения о начисленной и выплаченной заработной плате;

–номер расчётного счёта;

–сведения о воинском учете;

–сведения о семейном положении;

–данные свидетельства о рождении ребёнка;

–сведения о составе семьи и наличии иждивенцев;

–степень родства, фамилии, имена, отчества, даты рождения близких родственников (отца, матери, братьев, сестер и детей), а также мужа (жены); места рождения, места работы, и домашние адреса бывших жен (мужей);

–сведения об установленных размерах должностного оклада (оклада по профессиям рабочих), выплатах компенсационного и стимулирующего и премиях.

1.2. Обрабатываемые в ИС «Бухгалтерия государственного учреждения»:

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

–дата рождения (число, месяц, год рождения);

–пол;

–паспортные данные: серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи, адрес по месту регистрации;

–идентификационный номер налогоплательщика;

–страна регистрации;

–СНИЛС

–структурное подразделение (место работы);

–профессия.

1.3. Обрабатываемые в ИС «Открытие», ИС «Web- ИСПОЛЕНИЕ»:

–фамилия, имя, отчество;

–дата рождения (число, месяц, год рождения);

–место рождения;

–пол;

–паспортные данные: серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи, адрес по месту регистрации;

–гражданство;

–идентификационный номер налогоплательщика;

–адрес места жительства (адрес регистрации, фактического проживания);

–реквизиты страхового свидетельства государственного пенсионного страхования;

–сведения о начисленной и выплаченной заработной плате;

–номер расчётного счёта;

–сведения об установленных размерах должностного оклада (оклада по профессиям рабочих), выплатах компенсационного и стимулирующего и премиях, заработная плата.

–**Обрабатываемые в ИС «СБИС»:**

–фамилия, имя, отчество;

–дата рождения (число, месяц, год рождения);

–место рождения;

–пол;

–паспортные данные: серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи, адрес по месту регистрации;

–гражданство;

–идентификационный номер налогоплательщика;

–адрес места жительства (адрес регистрации, фактического проживания);

–реквизиты страхового свидетельства государственного пенсионного страхования;

–сведения о начисленной и выплаченной заработной плате;

–номер расчётного счёта;

–сведения об установленных размерах должностного оклада (оклада по профессиям рабочих), выплатах компенсационного и стимулирующего и премиях, заработная плата;

– сведения согласно справки 6 НДФЛ.

1.4. Обрабатываемые в ИС «Сотрудники предприятия»:

–фамилия, имя, отчество;

–дата рождения (число, месяц, год рождения);

–пол;

–рабочий стаж;

–должность.

1.5. Обрабатываемые в ИС «Документооборот»:

–фамилия, имя, отчество;

–дата рождения (число, месяц, год рождения);

–пол;

–паспортные данные: серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи, адрес по месту регистрации;

–адрес места жительства (адрес регистрации, фактического проживания).

2. Перечень обрабатываемых персональных данных субъектов персональных данных, не являющихся сотрудниками МАУ «НЦВСМ»:

2.1. Обрабатываемые в ИС «Зарплата и кадры»:

–фамилия, имя, отчество стипендиата или получателя единовременного денежного вознаграждения (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);

–паспортные данные;

–прописка;

–свидетельство о рождении;

–адрес фактического места проживания;

–дата рождения;

–место рождения;

–пол;

–СНИЛС;

–ИНН.

Приложение 15 к приказу от
«30» декабря 2021 г. №01-02-144

Перечень
должностей муниципального автономного учреждения города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства», допущенных к обработке персональных данных, обрабатываемых в ИСПДн

№ п/п	Структурное подразделение	ФИО	Должность
ИС «Зарплата и кадры»			
1.		Филоненко Любовь Вячеславовна	главный бухгалтер
2.	Финансовый отдел	Красовская Лидия Ивановна	Ведущий бухгалтер
3.	Отдел кадров	Шаповалова Евгения Михайловна	Начальник отдела кадров
4.	Отдел кадров	Ломакин Дмитрий Евгеньевич	Менеджер по персоналу
5.	Отдел кадров	Фигуренко Екатерина Сергеевна	Специалист по кадровому делопроизводству
ИС «Бухгалтерия государственного учреждения»			
6.		Филоненко Любовь Вячеславовна	главный бухгалтер
7.	Финансовый отдел	Котенко Оксана Васильевна	Начальник финансового отдела
8.	Финансовый отдел	Немчанинова Татьяна Викторовна	Бухгалтер 1 категории
9.	Финансовый отдел	Логачева Оксана Александровна	Бухгалтер 1 категории
10.	Финансовый отдел	Тарасова Анжела Юрьевна	Ведущий экономист по бухгалтерскому учету и анализу хозяйственной деятельности
11.	Финансовый отдел	Самохина Анастасия Александровна	Бухгалтер 1 категории
ИС «Открытие»			
ИС «Web- ИСПОЛЕНИЕ»			
12.		Филоненко Любовь Вячеславовна	Начальник финансового отдела - главный бухгалтер
13.	Бухгалтерия	Логачева Оксана Александровна	Бухгалтер 1 категории
14.	Бухгалтерия	Немчанинова Татьяна Викторовна	Бухгалтер 1 категории
ИС «СБИС»			
15.		Филоненко Любовь Вячеславовна	Начальник финансового отдела - главный бухгалтер
16.	Финансовый отдел	Красовская Лидия Ивановна	Ведущий бухгалтер
17.	Финансовый отдел	Котенко Оксана Васильевна	Начальник финансового отдела

№ п/п	Структурное подразделение	ФИО	Должность
18.	Финансовый отдел	Немчанинова Татьяна Викторовна	Бухгалтер 1 категории
19.	Финансовый отдел	Логачева Оксана Александровна	Бухгалтер 1 категории
20.	Отдел кадров	Шаповалова Евгения Михайловна	Начальник отдела кадров
21.	Юридический отдел	Зубахина Ольга Владимировна	Начальник юридического отдела
ИС «Сотрудники предприятия»			
22.	Отдел кадров	Шаповалова Евгения Михайловна	Начальник отдела кадров
23.	Отдел кадров	Ломакин Дмитрий Евгеньевич	Менеджер по персоналу
24.	Отдел кадров	Фигуренко Екатерина Сергеевна	Специалист по кадровому делопроизводству
ИС «Документооборот»			
25.	Административно-хозяйственный отдел	Илюшина Вера Романовна	Секретарь руководителя

Приложение 16 к приказу от
«30» декабря 2021 г. № 01-02-144

Порядок уничтожения и обезличивания персональных данных после достижения цели их обработки

1. Настоящий порядок уничтожения и обезличивания персональных данных после достижения цели их обработки (далее - Порядок) разработан для муниципального автономного учреждения города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства» (далее- Учреждение) на основании политики оператора в отношении обработки персональных данных в МАУ «НЦВСМ».

2. Настоящий Порядок вступает в действие с момента его утверждения, изменения и дополнения в Порядок вносятся на основании изменений в локальных нормативных актах Учреждения, регламентирующих данную сферу деятельности Учреждения.

3. Основные понятия, используемые в Порядке:

- персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);

- обработка персональных данных - любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования; обработка персональных данных включает в себя в том числе: сбор; запись; систематизацию; накопление; хранение; уточнение (обновление, изменение); извлечение; использование; передачу (распространение, предоставление, доступ); обезличивание; блокирование; удаление; уничтожение;

- предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

- блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

- уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

- обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

4. В случае предоставления субъектом персональных данных, его законным представителем фактов о неполных, устаревших, недостоверных или незаконно полученных персональных данных Учреждение актуализирует, исправляет, блокирует, удаляет или уничтожает их и уведомляет о своих действиях субъекта персональных данных.

5. Учреждение обязано предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. 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, оператор обязан внести в них необходимые изменения. 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, оператор обязан уничтожить такие персональные данные. Учреждение 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.

6. В случае подтверждения факта неточности персональных данных Учреждение на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязано уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и снять блокирование персональных данных.

7. Учреждение обязано прекратить обработку персональных данных или обеспечить прекращение обработки персональных данных лицом, ответственным за обработку персональных данных:

- в случае выявления неправомерной обработки персональных данных, осуществляемой Учреждением или лицом, ответственным за обработку персональных данных, в срок, не превышающий трех рабочих дней с даты этого выявления;

- в случае отзыва субъектом персональных данных согласия на обработку его персональных данных Учреждением;

- в случае достижения цели обработки персональных данных и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных. В случае отсутствия возможности уничтожения персональных данных в течение указанного срока Учреждение осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

8. Уничтожение документов (носителей), содержащих персональные данные, производится путем сожжения, дробления (измельчения), химического разложения. Для уничтожения бумажных документов может быть использован шредер. Персональные данные на электронных носителях уничтожаются путем стирания или форматирования носителя.

Приложение 1 к порядку уничтожения и
обезличивания персональных данных
после достижения цели их обработки

АКТ № _____
об уничтожении (о прекращении обработки)
персональных данных
(образец)

г. Новосибирск «___» _____ 20___ г.

Комиссия в составе председателя - _____,
членов комиссии - _____,
созданная на основании приказа от «__» _____г. № _____,
руководствуясь Федеральным законом от 27.07.2006 N 152-ФЗ «О персональных данных», составила акт о том, что произведено уничтожение персональных данных или иной конфиденциальной информации, находящейся в МАУ «НЦВСМ», в следующем объеме:

N п/п	Содержание персональных данных	Тип носителя	Объем	Причина уничтожения
1				
2				

Перечисленные носители персональных данных уничтожены путем сжигания полностью (для бумажных носителей), путем стирания или форматирования (для электронных носителей).

Председатель комиссии: _____ _____

Члены комиссии: _____ _____

_____ _____

Приложение 17 к приказу от
«30» декабря 2021 г. № 01-02-144

Инструкция
о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и средств защиты информации в информационных системах муниципального автономного учреждения города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства»

1. Общие положения

1.1. Настоящая Инструкция о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения и средств защиты информации в информационных системах персональных данных МАУ «НЦВСМ» (далее – Инструкция) определяет порядок действий по резервированию и восстановлению работоспособности технических средств (далее – ТС) и программного обеспечения (далее – ПО), средств защиты информации (далее – СЗИ), связанных с функционированием информационной системы персональных данных (далее – ИСПДн) МАУ «НЦВСМ», меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

1.2. Целью Инструкции является превентивная защита элементов ИСПДн от потери защищаемой информации.

1.3. Задачами данной Инструкции является:

- определение мер защиты от потери информации;
- определение действий восстановления в случае потери информации.

1.4. Действие настоящей Инструкции распространяется на всех пользователей МАУ «НЦВСМ», имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

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

1.5. Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается администратор безопасности ИСПДн.

1.6. Ответственным сотрудником за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, назначается администратор безопасности ИСПДн или ответственный за защиту информации, в том числе за обеспечение безопасности персональных данных.

2. Порядок реагирования на инцидент

2.1. В настоящем документе под инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а так же потерей защищаемой информации.

2.2. Происшествие, вызывающее инцидент, может произойти:

- в результате непреднамеренных действий пользователей;
- в результате преднамеренных действий пользователей и третьих лиц;
- в результате нарушения правил эксплуатации технических средств ИСПДн;
- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

2.3. Все действия в процессе реагирования на инцидент должны документироваться ответственным за реагирование сотрудником.

2.4. В кратчайшие сроки, не превышающие одного рабочего дня, администратор безопасности информации, предпринимает меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По

необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

3.1. Технические меры:

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

– системы жизнеобеспечения;
– системы резервного копирования и хранения данных;
– системы контроля физического доступа.

3.1.2. Системы жизнеобеспечения ИСПДн включают:

– пожарные сигнализации;
– системы резервного питания.

3.1.3. Все критичные помещения МАУ «НЦВСМ» (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации.

3.1.4. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

– локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
– источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения.

3.1.5. Система резервного копирования ИС, подразумевает под собой создание копий защищаемой информации. Создание резервных копий осуществляется при помощи стандартных средств Операционной системы или других программных средств на машинный носитель информации, который должен быть учтен в «Журнале учета носителей персональных данных».

3.2. Организационные меры:

3.2.1. Резервное копирование данных должно осуществлять на периодической основе:

– для обрабатываемых персональных данных – не реже раза в неделю;
– для технологической информации – не реже раза в месяц;

3.2.2. Данные о проведение процедуры резервного копирования и восстановления, отражаются в электронном журнале учета.

3.2.3. Съемные носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

3.2.4. Съемные носители должны храниться в несгораемом шкафу (сейфе).

3.2.5. Съемные носители должны храниться не менее года, для возможности восстановления данных.

4. Порядок восстановления работоспособности информационных систем

Восстановление работоспособности ИСПДн осуществляется в случаях сбоев, отказов и аварий технических средств и систем ИСПДн, а также ее программного обеспечения.

Данные работы, в общем случае, осуществляются в следующей последовательности:

– проверка исправности и работоспособности средств обеспечения функционирования ИСПДн;

– восстановление работоспособности (ремонт или замена) средств обеспечения функционирования ИСПДн, при необходимости;

– проверка правильности функционирования общего программного обеспечения ИСПДн;

– восстановление нормального функционирования общего программного обеспечения ИСПДн с использованием дистрибутивов и обновлений к ним или резервных копий настроек, при необходимости;

– проверка правильности функционирования средств защиты информации;

– восстановление нормального функционирования средств защиты информации с использованием дистрибутивов и обновлений к ним, при необходимости;

– проверка правильности функционирования специального программного обеспечения ИСПДн;

– восстановление нормального функционирования специального программного обеспечения ИС с использованием дистрибутивов и обновлений к ним, при необходимости;

– восстановление баз персональных данных с использованием резервной копии в течении одного рабочего дня.

Данные работы осуществляются в соответствии с эксплуатационной документацией на технические и программные средства до полного восстановления работоспособности.

Восстановление персональных данных, созданных после их последнего резервирования, осуществляется пользователями, осуществившими их внесение в базы персональных данных.

Работы по техническому обслуживанию технических и программных средств ИСПДн осуществляется в соответствии с данной инструкцией.

В случае необходимости привлечения для восстановления работоспособности ИСПДн представителей сторонних организаций, должна быть обеспечена невозможность их ознакомления с персональными данными, а также несанкционированного копирования на машинные носители информации. Ответственность за выполнение данного требования возлагается на администратора безопасности информации.

Приложение к Инструкции о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах МАУ «НЦВСМ»

Форма
журнала резервирования и восстановления работоспособности технических средств и программного обеспечения, и средств защиты информации

№	Дата	Вид операции	Устройство	Каталог накопителя	Наименование резервной копии	Место хранения резервной копии	ФИО, проводившего резервирование / восстановление	Подпись, проводившего резервирование / восстановление

Приложение к Инструкции о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах МАУ «НЦВСМ»

Форма журнала учёта машинных носителей персональных данных

Журнал начат «09» марта 2022 г. Журнал завершен «____» _____ 20___ г.

_____ / ФИО, должность / _____ / ФИО, должность /

На _____ листах

№ п/п	Регистрационный номер/дата	Тип/ёмкость машинного носителя персональных данных/серийный номер	Номер экземпляра/ количество экземпляров	Место установки (использования)/дата установки	Ответственное должностное лицо (ФИО)	Расписка в получении (ФИО, подпись, дата)	Расписка в обратном приеме (ФИО, подпись, дата)	Место хранения машинного носителя персональных данных	Сведения об уничтожении машинных носителей персональных данных, стирании информации (подпись, дата)

Приложение 18 к приказу от
«30» декабря 2021 г. №01-02-144

ИНСТРУКЦИЯ

по обращению с сертифицированными ФСБ России средствами криптографической защиты информации

1.Общие положения

1.1. Данная инструкция регламентирует порядок обращения со средствами криптографической защиты информации (далее СКЗИ), сертифицированными ФСБ, в процессе получения, доставки, хранения, тестирования, передачи и установки (инсталляции).

1.2. СКЗИ, включая аппаратные средства, инсталляционные дискеты, ключевую документацию, описания и инструкции к СКЗИ, составляют служебную тайну МАУ «НЦВСМ».

1.3. Приказом руководителя назначается лицо, ответственное за обеспечение безопасности при обращении с СКЗИ.

1.4. Все сотрудники, допущенные к работе с СКЗИ, должны строго выполнять требования настоящей инструкции в части, их касающейся. Указанные сотрудники должны ознакомиться с данной инструкцией под роспись.

2.Обязанности пользователей СКЗИ

Пользователи СКЗИ обязаны:

2.1. Не разглашать конфиденциальную информацию, к которой они допущены, рубежи ее защиты, в том числе сведения о криптоключах;

2.2. Соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;

2.3. Сообщать ответственному пользователю криптосредств о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

2.4. Сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным настоящей Инструкцией, при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

2.5. Вести технический (аппаратный) журнал;

2.6. Немедленно уведомлять ответственного пользователя криптосредств о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

3.Обязанности ответственного пользователя криптосредств

Ответственный пользователь криптосредств обязан:

3.1. Контролировать соблюдение пользователями СКЗИ конфиденциальности при обращении со сведениями, которые им доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых СКЗИ и ключевых документах к ним;

3.2. Обеспечивать надежное хранение эксплуатационной и технической документации к криптосредствам, ключевых документов, носителей информации ограниченного распространения;

3.3. Своевременным выявлением попыток посторонних лиц получать сведения о защищаемой информации, об используемых криптосредствах или ключевых документах к ним;

3.4. Принимать меры по предупреждению разглашения защищаемой информации, а также возможной их утечки при выявлении фактов утраты или недостачи криптосредств, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

3.5. Контролировать соблюдение условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ;

3.6. Расследовать и составлять заключения по фактам нарушения условий использования СКЗИ, которые могут привести к снижению уровня защиты конфиденциальной информации; разрабатывать и принимать меры по предотвращению возможных опасных последствий подобных нарушений;

3.7. Вести журналы поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

3.8. Вести на каждого пользователя СКЗИ лицевой счет.

4.Требования по размещению, специальному оборудованию и охране помещений, в которых производятся работы со СКЗИ

4.1. Размещение, специальное оборудование, охрана и режим в помещениях, в которых производится работа с СКЗИ (далее помещения), должны обеспечивать безопасность СКЗИ и исключать возможность неконтролируемого доступа к СКЗИ.

4.2. Доступ лиц в эти помещения должен быть ограничен и обеспечиваться в соответствии со служебной необходимостью и локальными актами МАУ «НЦВСМ».

4.3. По окончании рабочего дня ответственный сотрудник обязан закрыть помещение, сдать помещение с отметкой в журнале. При вскрытии помещений должны проверяться целостность печатей, и замков. В случае нарушения целостности печатей или замков ответственный сотрудник обязан немедленно сообщить об этом лицу, ответственному пользователю криптосредств.

4.4. Для хранения СКЗИ, инсталляционных дискет, тестовых ключей, нормативной и эксплуатационной документации помещения обеспечиваются металлическими шкафами (хранилищами, сейфами), оборудованными внутренними замками с двумя экземплярами ключей. Сейфы должны быть оборудованы приспособлением для их опечатывания, либо специальным защитным замком для замочной скважины. Дубликаты ключей от хранилищ и входных дверей должны храниться в сейфе ответственного лица, назначаемого руководителем.

5. Порядок обращения со СКЗИ

5.1. СКЗИ, инсталляционные дискеты, тестовые ключи, нормативную и эксплуатационную документацию получает уполномоченный сотрудник МАУ «НЦВСМ» непосредственно у производителя СКЗИ. Безопасность в процессе доставки обеспечивается организационными мерами.

5.2. При транспортировке СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть обеспечены условия, исключающие возможность физических повреждений и внешнего воздействия на записанную информацию, а также копирование.

5.3. Все поступающие СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету.

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

5.5. В соответствии с договором с производителем СКЗИ разрешается сделать одну копию программных СКЗИ (исключая ключевую информацию) для архива, а также сделать одну дополнительную копию каждый раз, когда рабочая копия приходит в негодность и должна быть заменена. При этом ответственный сотрудник должен удостовериться, что каждая произведенная им копия отображает на дисплее авторские права производителя СКЗИ и другие указания в отношении собственности, которые записаны на оригинале.

5.6. Пользователи СКЗИ хранят инсталлирующие криптосредства носители, эксплуатационную и техническую документацию к криптосредствам, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

5.7. Пользователи СКЗИ предусматривают также раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих ключевых документов. При вскрытии сейфа должна быть проверена целостность печатей и замков. В случае нарушения целостности печатей или замков ответственный сотрудник обязан немедленно сообщить об этом лицу, ответственному за обеспечение безопасности при обращении со СКЗИ.

5.8. Хранение инсталляционных дискет СКЗИ и тестовых ключей допускается в одном хранилище с другими документами при условиях, исключающих непреднамеренное их уничтожение или иное, не предусмотренное правилами использования СКЗИ применение.

5.9. В случае отсутствия у сотрудника индивидуального хранилища инсталляционные дискеты СКЗИ и тестовые ключи по окончании рабочего дня должны сдаваться лицу, ответственному за их хранение.

5.10. В случае утери носителя СКЗИ или вероятном копировании сотрудник обязан немедленно сообщить об этом лицу, ответственному за обеспечение безопасности при обращении со СКЗИ.

5.11. Ответственными сотрудниками периодически должен проводиться контроль сохранности СКЗИ, а также всего используемого совместно со СКЗИ программного обеспечения для предотвращения внесения программно-аппаратных закладок и программ вирусов.

5.12. Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно-программные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать. При наличии технической возможности на время отсутствия пользователей СКЗИ указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища.

5.13. Ответственный сотрудник Администрации муниципального района заносит в Журнал учета СКЗИ дату приема-передачи СКЗИ, фамилию, имя, отчество сотрудника, которому передаются СКЗИ, серийный номера СКЗИ. Все операции по передачи СКЗИ производятся под роспись.

5.14. В каждый экземпляр передаваемого СКЗИ должна быть включена ссылка на авторские права производителя, его товарный знак и другие обозначения в форме,

согласованной с производителем. Вся документация на СКЗИ и на продукты, включающие СКЗИ, а также отображаемая на экране при запуске информация о нем должна включать вышеуказанные обозначения.

5.15. Установка (инсталляция) СКЗИ осуществляется в соответствии с требованиями документации на СКЗИ.

6.Восстановление связи в случае компрометации действующих ключей к СКЗИ

6.1. К событиям, связанным с компрометацией ключей, относятся, включая, но не ограничиваясь:

- потеря ключевых носителей;
- потеря ключевых носителей с их последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- нарушение правил хранения и уничтожения (после окончания срока действия) закрытого ключа;
- возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
- нарушение печати на сейфе с ключевыми носителями;
- случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника).

6.2. В случае возникновения обстоятельств, указанных в пункте 6.1 настоящей Инструкции, пользователь обязан немедленно прекратить обмен электронными документами с использованием скомпрометированных закрытых криптографических ключей и сообщить о факте компрометации ответственному пользователю криптосредств.

6.3. О факте компрометации ключевой информации Пользователями совместно с Ответственным пользователем производится информирование всех заинтересованных участников информационного обмена.

6.4. Использование СКЗИ может быть возобновлено только после ввода в действие другого криптографического ключа взамен скомпрометированного.

6.5. Скомпрометированные ключи подлежат уничтожению в соответствии с порядком, установленным в пункте 7 настоящей Инструкции.

7. Уничтожение криптографических ключей

7.1. Уничтожение криптоключей производится путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (уничтожения) криптоключей без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

7.2. Криптоключи стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (дискет, компакт-дисков (CD-ROM), eToken и т.п.). Непосредственные действия по стиранию криптоключей, а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ.

7.3. Ключевые носители уничтожают путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключевой информации. Непосредственные действия по

уничтожению конкретного типа ключевого носителя регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ.

7.4. Бумажные и прочие сгораемые ключевые носители, а также эксплуатационная и техническая документация к СКЗИ уничтожаются путем сжигания или с помощью любых бумагорезательных машин.

7.5. Намеченные к уничтожению (утилизации) СКЗИ подлежат изъятию из аппаратных средств, с которыми они функционировали.

7.6. Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения оформляется в соответствующих журналах поэкземплярного учета. В эти же сроки с отметкой в техническом (аппаратном) журнале подлежат уничтожению разовые ключевые носители и ранее введенная и хранящаяся в СКЗИ или иных дополнительных устройствах ключевая информация.

7.7. Разовые ключевые носители, а также электронные записи ключевой информации, соответствующей выведенным из действия криптоключам, непосредственно в СКЗИ или иных дополнительных устройствах уничтожаются пользователями этих СКЗИ самостоятельно под расписку в техническом (аппаратном) журнале.

7.8. Ключевые документы уничтожаются либо пользователями СКЗИ, либо ответственным пользователем СКЗИ под расписку в соответствующих журналах поэкземплярного учета, а уничтожение большого объема ключевых документов может быть оформлено актом, форма акта представлена в приложении к настоящей Инструкции. Ответственный пользователь СКЗИ обеспечивает хранение данных актов.

7.9. Пользователям СКЗИ разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи. После уничтожения пользователи СКЗИ должны уведомить об этом ответственного пользователя СКЗИ для списания уничтоженных документов с их лицевых счетов. Не реже одного раза в год пользователи СКЗИ должны направлять ответственному пользователю СКЗИ письменные отчеты об уничтоженных ключевых документах.

7.10. Ответственный пользователь СКЗИ делает соответствующие отметки об уничтожении в журнале поэкземплярного учета СКЗИ.

8. Ответственность за нарушение требований Инструкции

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

Приложение 1
к инструкции по обращению с сертифицированными ФСБ
России средствами криптографической защиты информации

АКТ №_____

об уничтожении криптографических ключей и ключевых документов

Комиссия в составе:
Председателя:_____,
членов комиссии: _____
_____
_____
произвела уничтожение криптографических ключей и ключевых документов:

№ п/п	Учетный номер ключевого носителя (документа)	Номер (идентификатор) криптографического ключа, наименование документа	Владелец ключа (документа)	Кол-во ключевых носителей (документов)	Номера экземпляров	Всего уничтожается ключей (документов)	Примечание

Всего уничтожено (_____) криптографических ключей на (_____) ключевых носителях. Записи Акта сверены с записями в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

Уничтожение криптографических ключей выполнено путем их стирания в соответствии с требованиями эксплуатационной и технической документации на соответствующие СКЗИ.

Ключевые носители списаны с учета в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

Председатель комиссии: _____ /_____/
Члены комиссии: _____ /_____/
_____ /_____/
_____ /_____/
_____ /_____/

Приложение 19 к приказу от
«30» декабря 2021 г. №01-02-144

ИНСТРУКЦИЯ

о порядке учета и выдачи средств криптографической защиты информации, электронной подписи, эксплуатационно-технической документации и ключевых документов

1. Учет средств криптографической защиты информации (СКЗИ), сертификатов электронной подписи (ЭП), эксплуатационно-технической документации на СКЗИ и ЭП, ключевых документов и ЭП организуется в соответствии с требованиями нормативной документации ФСБ России, Правилами использования СКЗИ, утвержденными разработчиком СКЗИ.

2. Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету. Единицей поэкземплярного учета ключевых документов считается ключевой носитель многократного использования, ключевой блокнот. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

3. Поэкземплярный учет СКЗИ, поступающих от разработчиков, изготовителей и поставщиков СКЗИ необходимо вести в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

4. Все полученные экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем Журнале поэкземплярного учета пользователям СКЗИ, несущим персональную ответственность за их сохранность.

5. Ответственные пользователи криптосредств заводят и ведут на каждого пользователя СКЗИ лицевой счет, в котором регистрируют числящиеся за ним СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы. Типовая форма лицевого счета пользователя СКЗИ представлена в приложении к настоящей Инструкции.

6. Если эксплуатационной и технической документацией к СКЗИ предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (на весь срок их действия) непосредственно в СКЗИ, то такой разовый ключевой носитель или электронная запись соответствующего криптоключа должны регистрироваться в техническом (аппаратном) журнале, ведущемся непосредственно пользователем СКЗИ.

7. Учет СКЗИ, средств ЭП, эксплуатационной и технической документации, ключевых документов и информации должен быть организован на бумажных носителях.

8. Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ, ответственными пользователями криптосредств под расписку в соответствующих журналах поэкземплярного учета.

9. Учет СКЗИ, средств ЭП, эксплуатационной и технической документации, ключевых документов и информации должен быть организован на бумажных носителях.

10. Ответственным пользователем криптосредств в МАУ «НЦВСМ» является ответственный за защиту информации, в том числе за обеспечение безопасности персональных данных в информационных системах.

11. Ведение непосредственных операций по учету СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы, в соответствии с функциональными обязанностями и инструкциями, возлагается на администратора безопасности информации.

Приложение 1
к инструкции о порядке учета и выдачи
средств криптографической защиты
информации, электронной подписи,
эксплуатационно-технической
документации и ключевых документов

ЛИЦЕВОЙ СЧЕТ ПОЛЬЗОВАТЕЛЯ КРИПТОСРЕДСТВ

Сотрудник_____

(Ф.И.О, должность)

_____

(наименование структурного подразделения)

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов или серийные номера их носителей	Регистрационные номера экземпляров (криптографические номера) ключевых документов	Дата и расписка о получении СКЗИ	Дата и расписка возвращения СКЗИ	Примечание
1	2	3	4	5	6	7

_____

Приложение 20 к приказу от
«30» декабря 2021 г. №01-02-144

ИНСТРУКЦИЯ

о порядке допуска сотрудников МАУ «НЦВСМ» к самостоятельной работе со средствами криптографической защиты информации

1. Настоящая Инструкция разработана в соответствии с законодательством Российской Федерации, нормативными правовыми актами в области защиты информации, а также эксплуатационной документацией на используемые СКЗИ и определяет порядок допуска сотрудников МАУ «НЦВСМ» к самостоятельной работе со средствами криптографической защиты информации (СКЗИ).

2. К самостоятельной работе с СКЗИ допускаются лица:

- назначенные на должности, выполнение обязанностей по которым связано с хранением и использованием СКЗИ;

- прошедшие инструктаж по программе подготовки к самостоятельной работе с СКЗИ, утвержденной руководителем.

3. Программа подготовки сотрудников МАУ «НЦВСМ» к самостоятельной работе с СКЗИ (приложение к настоящей Инструкции) утверждается руководителем и включает в себя:

ознакомление с нормами действующего законодательства Российской Федерации, регулирующими отношения, возникающие при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации, защите информации, прав субъектов, участвующих в информационных процессах и информатизации, правила применения и использовании электронной цифровой подписи в электронных документах, а также информацию об ответственности за нарушение указанных норм;

ознакомление с нормативными актами органов государственного управления Российской Федерации, определяющими порядок разработки, производства, реализации, использования СКЗИ, регламентирующими вопросы взаимодействия участников и информационного обмена с использованием СКЗИ;

изучение должностных инструкций, положений, других локальных нормативных актов МАУ «НЦВСМ» по вопросам деятельности, связанной с разработкой, производством, хранением, реализацией и использованием СКЗИ;

изучение эксплуатационно-технической документации на СКЗИ;

приобретение практических навыков выполнения работ, предусмотренных обязанностями по занимаемой должности.

4. Ответственность за полноту и качество подготовки сотрудников МАУ «НЦВСМ» к сдаче инструктажа на допуск к самостоятельной работе с СКЗИ возлагается на ответственного пользователя криптосредств.

Приложение 1
к инструкции о порядке допуска работников МАУ «НЦВСМ» к самостоятельной работе со средствами криптографической защиты информации

ПРОГРАММА

подготовки к самостоятельной работе со СКЗИ

№ п/п	Изучаемые вопросы (темы)	Кол-во часов	Форма (метод) подготовки	Ответственный за подготовку сотрудников
1	2	3	4	5
1.	Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информатизации и защите информации»	4	самоподготовка	
2.	Федеральный закон от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи»	2	самоподготовка	
3.	Федеральный закон от 4 мая 2011 года № 99-ФЗ «О лицензировании отдельных видов деятельности»	2	самоподготовка	
4.	Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 года № 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности"	2	самоподго-товка	
5.	Эксплуатационно-техническая документация на используемые СКЗИ	10	самоподготовка	
6.	Внутренние нормативные документы МАУ «НЦВСМ»: Должностные инструкции; Инструкция по обращению с сертифицированными ФСБ России средствами криптографической защиты информации; Требования к оборудованию помещений и размещению технических средств, используемых для обработки персональных данных в МАУ НЦВСМ	6	самоподготовка	
7.	Постановление Правительства РФ от 16.09.2020 N 1479 "Об утверждении Правил противопожарного режима в Российской Федерации"	4	самоподготовка	

Приложение 2
к инструкции о порядке допуска работников МАУ «НЦВСМ»
к самостоятельной работе со средствами криптографической защиты информации

ЖУРНАЛ

поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов

Начат: «__»_____ 20__г.

Окончен: «__»_____20__г.

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
				От кого получены	Дата и номер сопроводительного письма	ФИО пользователя СКЗИ	Дата и расписка в получении	Ф.И.О сотрудников органа криптографической защиты, пользователя СКЗИ, производших подключение (установку)	Дата подключения (установки) и подписи лиц, производших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудников органа криптографической защиты пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Приложение 3
к инструкции о порядке допуска работников МАУ «НЦВСМ»
к самостоятельной работе со средствами криптографической защиты информации

ЖУРНАЛ регистрации пользователей СКЗИ

Начат: «__»_____ 20__г.

Окончен: «__»_____20__г.

№ п/п	Должность пользователя	Ф.И.О пользователя	Дата прохождения инструктажа	Подпись пользователя	Номер и дата постановления о допуске	Номер и дата постановления о прекращении допуска
1	2	3	4	5	6	7

_____

Приложение 21 к приказу от
«30» декабря 2021 г. №01-02-144

Политика «чистого стола» и «чистого экрана» в муниципальном автономном учреждении города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства»

Политика «чистого стола» и «чистого экрана» в МАУ «НЦВСМ» (далее-Оператор) внедряется с целью минимизации риска неавторизованного доступа или повреждения документов на бумажных носителях, носителей данных и средств обработки информации.

Оператору следует применять политику «чистого стола» в отношении документов на бумажных носителях и сменных носителей данных, а также политику «чистого экрана» в отношении средств обработки информации с тем, чтобы уменьшить риски неавторизованного доступа, потери и повреждения информации как во время рабочего дня, так и при внеурочной работе.

При применении политики следует учитывать соответствующие риски, а также корпоративную культуру учреждения. Носители информации, оставленные на столах, также могут быть повреждены или разрушены при бедствии, например, при пожаре, наводнении или взрыве.

Требуется применять следующие мероприятия по управлению информационной безопасностью:

– чтобы исключить компрометацию информации, целесообразно бумажные и электронные носители информации, когда они не используются, хранить в надлежащих запирающихся шкафах и/или в других защищенных предметах мебели, а также в архивах Оператора, особенно в нерабочее время;

– носители с важной или конфиденциальной служебной информацией либо информацией ограниченного пользования, когда они непосредственно не используются в работе, следует убирать и запирать (например, в несгораемом сейфе или металлическом шкафу), особенно когда помещение пустует;

– персональные компьютеры и принтеры должны быть выключены по окончании работы;

– следует применять замки, пароли или другие мероприятия в отношении устройств, находящихся без присмотра;

– в нерабочее время фотокопировальные устройства следует запирать на ключ (или защищать от неавторизованного использования другим способом);

– напечатанные документы с важной или конфиденциальной информацией необходимо изымать из принтеров немедленно;

- по окончании рабочего дня, следует отключать все устройства, убирать бумажные и электронные носители, запирать окна и двери и сдавать опечатанный ключ на вахту с отметкой в журнале.

Приложение 22 к приказу от
«30» декабря 2021 г. №01-02-144

Регламент
использования электронной почты в муниципальном автономном учреждении города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства»

1. Общие положения

1.1. Настоящий Регламент разработан в целях установления единого порядка использования корпоративной электронной почты (далее - ЭП) в муниципальном автономном учреждении города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства» (далее – Учреждение), обязательной для использования в работе всеми работниками.

1.2. Настоящий регламент призван обеспечить бесперебойную работу и эффективное использование ЭП в интересах деятельности учреждения.

1.3. Настоящий регламент не определяет порядок работы с документами, направляемыми и получаемыми по ЭП.

1.4. Каждый работник учреждения, имеющий личный почтовый ящик корпоративной ЭП, обязан использовать его в рамках выполнения своих обязанностей.

1.5. Вся информация и сообщения, которые были созданы, отправлены, приняты или сохранены посредством корпоративной ЭП учреждения, принадлежат учреждению, за исключением случаев, предусмотренных законодательством Российской Федерации.

1.6. В пределах функционирования корпоративной ЭП обеспечивается конфиденциальность почтовых сообщений и информации о пользователях ЭП, кроме информации из адресной книги и за исключением случаев, предусмотренных законодательством Российской Федерации.

2. Характеристика корпоративной электронной почты образовательного учреждения

2.1. Корпоративная ЭП учреждения состоит из следующих компонентов:

- Адресная книга, содержащая информацию о пользователях. Информация Адресной книги доступна всем зарегистрированным пользователям.
- Личные папки - локальные дисковые хранилища почтовых сообщений пользователя, необходимые для хранения большого объема сообщений и их архивирования.

Личные папки могут быть созданы как локально, на рабочем месте пользователя, так и на любом доступном внешнем хранилище.

Личные папки используются в следующих целях:

- поддержание размера почтового ящика пользователя, располагающегося на сервере, в пределах обозначенных ему лимитов;
- организация структурированного хранилища путем создания вложенных папок;
- проведение операции архивирования почтовых сообщений, старше заданного срока отправки или получения;
- организация резервного хранилища на выделенном внешнем носителе или сервере.

- Почтовый ящик, содержащий почтовые сообщения пользователей корпоративной ЭП.

Содержимое почтовых ящиков пользователей может храниться следующими способами:

- в почтовом ящике на сервере;
- в личной папке локально на персональном компьютере пользователя;
- в архивных папках, локально на персональном компьютере пользователя;
- в общих папках, специально организованных для работы группы пользователей.

- Листы рассылок.

Список адресов доступен каждому пользователю и включает всех пользователей.

- Адресная книга Пользователя –группа, созданная конкретным пользователем для структуризации своих рассылок. Такие группы недоступны для других пользователей.
- Антивирус - автоматическая система сканирования почтовых сообщений на наличие вредоносного вирусного кода (вирусов). При обнаружении нежелательного содержания в сообщении системой антивируса вставляется сообщение с описанием причины изъятия зараженного содержания сообщения.
- Антиспам - автоматическая система сканирования почтовых сообщений на наличие нежелательной рекламной рассылки (спам).

В ЭП настроена подсистема обнаружения нежелательной почты. Сообщения, которые определены подсистемой антиспам как нежелательные, хранятся в карантине в течение 5 дней с момента поступления, после чего безвозвратно удаляются.

3. Создание личного почтового ящика в корпоративной электронной почте учреждения

3.1. Создание личного почтового ящика и его настройка для работы в корпоративной ЭП осуществляется на основании заявки.

3.2. Для каждого пользователя создается только один личный почтовый ящик.

3.3. Для работы одним пользователем с несколькими почтовыми ящиками выполняется соответствующая настройка.

3.4. Пользователь лично обеспечивает сохранность Личных папок на рабочем месте.

4. Обеспечение контроля почтовых ящиков

4.1. Контроль почтовых ящиков в корпоративной ЭП должен в автоматическом режиме обеспечивать выполнение следующих действий:

- направление сообщения при приближении к установленному лимиту размера личного почтового ящика;
- автоматическое блокирование возможности отправки почтовых сообщений при превышении установленных лимитов размеров личных почтовых ящиков;
- оперативное получение статистики использования и нагрузки на почтовые сервера;
- ограничение до 100 получателей в одном сообщении для всех пользователей;
- ежедневное автоматическое удаление сообщений, хранящихся более 5 дней, из папки Удаленные;
- отправление уведомлений о превышении лимита размера личного почтового ящика. Превышение лимита размера личного почтового ящика автоматически блокируется возможность отправлять сообщения, при этом входящие сообщения продолжают приходить на личный почтовый ящик.

В случае превышения лимита размера личного почтового ящика система автоматически направляет информационное сообщение о необходимости чистки личного почтового ящика. После уменьшения пользователем размера личного почтового ящика до установленного лимита (перемещением электронной почты в личную папку, общую папку или удалением), предусмотрено автоматическое восстановление заблокированных возможностей.

4.2. Каждый пользователь несет персональную ответственность за соблюдение установленного размера личного почтового ящика, а также своевременное архивирование или удаление информации.

5. Удаление личных почтовых ящиков

5.1. Удаление личных почтовых ящиков уволенных работников производится на основании данных об увольнении работника из учреждения.

5.2. Процедура удаления предполагает блокировку личного почтового ящика на 1 месяц и безвозвратное удаление по окончании данного срока.

5.3. Организация передачи информации, относящейся к работе, из личных почтовых ящиков увольняемых работников осуществляется на основании письменного согласия работника.

6. Ограничения использования корпоративной электронной почты

6.1. При пользовании корпоративной ЭП пользователи обязаны соблюдать следующие правила:

- соблюдать общепринятые нормы и правила обмена почтовыми сообщениями;
- строго следовать ограничениям в рассылке сведений, содержащих персональные данные и иную конфиденциальную информацию, по которым установлен особый режим доступа и использования в соответствии с законодательством Российской Федерации, локальными нормативными актами;
- перед отправлением сообщения проверять правописание, грамматику и перечитывать сообщение;
- не рассылать сообщения противозаконного или неэтичного содержания, а также содержащие угрозы в адрес других пользователей;
- запрещается осуществлять рассылку сообщений рекламного или поздравительного характера;
- неукоснительно соблюдать положения настоящего регламента.

6.2. Информация должна рассылаться только тем адресатам, которым она действительно необходима для выполнения служебных функций.

6.3. При систематических (более 3-х раз) нарушениях пользователем настоящего регламента, а также по обоснованной жалобе других работников образовательного учреждения на действия отправителя сообщений личный почтовый ящик такого пользователя может быть заблокирован по решению руководителя на основании представления уполномоченного лица.

6.4. В случае необходимости уполномоченное лицо направляет обоснованную служебную записку руководителю учреждения для принятия решения о наложении дисциплинарного взыскания на пользователя, допустившего нарушение.

6.5. Все пользователи в обязательном порядке знакомятся с настоящим регламентом по работе с корпоративной электронной почтой учреждения, обеспечивая в работе выполнение требований указанных документов.

Приложение к Регламенту
использования электронной почты в муниципальном
автономном учреждении города Новосибирска
«Новосибирский Центр Высшего Спортивного Мастерства»

Памятка
по работе с корпоративной электронной почтой

Регламент использования электронной почты является важным элементом корпоративной политики информационной безопасности МАУ «НЦВСМ». Корпоративная электронная почта может быть использована только в служебных целях. Использование электронной почты в других целях категорически запрещено. Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию непосредственного либо вышестоящего руководителя.

При работе с корпоративной системой электронной почты сотрудникам учреждения запрещается:

- распространять информацию ограниченного доступа, предназначенную для служебного использования, в том числе сведения, составляющие персональные данные и иную конфиденциальную информацию;
- распространять материалы, защищаемые авторскими правами;
- использовать адрес корпоративной почты для оформления подписок;
- публиковать свой адрес либо адреса других сотрудников на общедоступных Интернет-ресурсах (форумы, конференции и т.п.) за исключением случаев служебной необходимости;
- осуществлять массовую рассылку почтовых сообщений рекламного характера;
- рассылать через электронную почту материалы, содержащие вирусы и другие вредоносные продукты и программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ для осуществления несанкционированного доступа;
- распространять угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, запрещённую российским законодательством;
- предоставлять иным лицам пароль доступа к своему почтовому ящику.

С настоящей памяткой ознакомлен

_____	_____	_____
должность работника	дата	подпись расшифровка подписи

Приложение 23 к приказу от
«30» декабря 2021 г. №01-02-144

Регламент использования ресурсов сети Интернет работниками муниципального автономного учреждения города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства»

1. Общее руководство

1. Настоящий Регламент разработан в соответствии с общими Правилами использования сети интернет в муниципальные автономные учреждения города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства» в целях повышения эффективности работы работников учреждения, использующих электронные информационные ресурсы глобальной сети Интернет, и повышения уровня информационной безопасности локальной информационно-вычислительной сети учреждения.

2. Руководство учреждения устанавливает постоянный контроль и полностью специфицирует виды информации, к которой разрешен доступ тому или иному работнику. В случае нарушения работником учреждения данного Регламента работник отстраняется от использования ресурсов сети Интернет.

2. Назначение доступа к сети Интернет

1. Доступ к ресурсам сети Интернет предоставляется работникам учреждения для выполнения ими прямых должностных обязанностей. Глобальная информационная сеть Интернет используется для:

- доступа к мировой системе гипертекстовых страниц (www);
- доступа к файловым ресурсам Интернета (FTP);
- доступа к специализированным (правовым и др.) базам данных;
- контактов с официальными лицами других структур, с сотрудниками структурных подразделений учреждения и т.д.;
- обмена электронной почтой с официальными лицами по не конфиденциальным вопросам производственного характера;
- повышения квалификации работников, необходимой для выполнения работником своих должностных обязанностей;
- поиска и сбора информации по управленческим, финансовым, юридическим вопросам, если эти вопросы напрямую связаны с выполнением работником его должностных обязанностей;
- в целях проведения мероприятий;
- другие цели.

3. Доступ к Интернет-ресурсам

1. Учреждение обеспечивает доступ пользователей локальной сети к ресурсам сети Интернет по специальным каналам связи в соответствии с настоящим Регламентом.

2. Без согласования с руководителем учреждения самостоятельная организация дополнительных точек доступа в Интернет (удаленный доступ, канал по локальной сети и пр.) запрещена.

4. Регистрация пользователя

1. Каждому подключенному к сети компьютеру назначается ответственный за этот компьютер пользователь, информация о котором заносится в базу данных пользователей соответствующего домена локальной сети учреждения. Регистрация выполняется ответственным за работу в сети Интернет. Пользователь обязан хранить свои идентификационные данные (пароли и т.п.) в тайне, запрещена передача идентификационных данных третьим лицам. За все деструктивные действия, произведенные в сети, отвечает сотрудник – пользователь учетной записи (идентификационных данных), использовавшейся при их проведении. При подозрении на то, что идентификационные данные стали известны третьим лицам, пользователь должен немедленно обратиться к ответственному за работу в сети Интернет с целью их изменения.

5. Ограничения при работе в сети Интернет

1. Пользователям глобальной сети Интернет не рекомендуется:

- посещение и использование игровых, развлекательных и прочих сайтов, не имеющих отношения к деятельности учреждения и деятельности пользователя;
- использование электронной почты, досок объявлений, конференций на компьютерах учреждения в личных целях в любое время;
- публикация корпоративного электронного адреса на досках объявлений, в конференциях и гостевых книгах, не связанных с деятельностью учреждения;
- использование некорпоративных e-mail адресов для рассылки служебной информации;
- передача учетных данных пользователя;
- играть в рабочее время в компьютерные игры автономно или в сети;
- единовременное скачивание больших объемов информации;
- посещение ресурсов трансляции потокового видео и аудио (веб-камеры, трансляция ТВ - и музыкальных программ в Интернете), создающих большую загрузку сети и мешающих нормальной работе остальных пользователей;
- подключение к электронной сети под другой учетной записью.

2. Пользователям корпоративной линии подключения учреждения к ресурсам глобальной сети Интернет запрещается:

- создание личных веб-страниц и хостинг (размещение web- или ftp-сервера) на сервере учреждения;
- посещение и использование эротико-порнографических ресурсов сети Интернет, ресурсов националистических организаций, ресурсов, пропагандирующих насилие и терроризм;

• нарушение закона об авторском праве посредством копирования и использования в служебных или личных целях материалов, защищенных законом об авторском праве;

• осуществление деструктивных действий по отношению к нормальной работе электронной системы учреждения и сети Интернет (рассылка вирусов, ip-атаки и т.п.);

• загрузка материалов порнографического содержания, компьютерных игр, анекдотов, других развлекательных материалов;

• передача персональных данных, конфиденциальной информации, сведений, составляющих служебную и коммерческую тайну, третьей стороне;

• проведение незаконных операций в глобальной сети Интернет;

• совершение иных действий, противоречащих законодательству, а также настоящему Регламенту.

6. Обращения в другие организации от имени учреждения

1. Работа в сети Интернет, общение с другими организациями могут быть связаны с необходимостью изложения своих взглядов по отдельным вопросам. Если работник учреждения высказывает в сообщении собственное мнение, то указанный сотрудник обязан предупредить об этом в конце сообщения фразой: «Прошу считать, что в сообщении указано мое личное мнение, которое необязательно отражает взгляды и политику учреждения».

2. Официальные обращения по электронной почте к должностным лицам других учреждений осуществляются по указанию руководителя.

7. Контроль использования ресурсов в сети Интернет

1. Администрация учреждения оставляет за собой право в целях обеспечения безопасности электронной системы производить выборочные и полные проверки всей электронной системы и отдельных файлов без предварительного уведомления работников.

2. Ответственный за работу в сети Интернет ведет учет использования ресурсов сети Интернет, обеспечивает контроль за соблюдением настоящего Регламента, обеспечивает безопасное использование ресурсов сети Интернет в соответствии с «Инструкцией ответственного за доступ к сети Интернет».

Приложение 24 к приказу от
«30» декабря 2021 г. №01-02-144

Инструкция ответственного за доступ к сети Интернет в муниципальном автономном учреждении города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства»

1. Общие положения

1. Ответственный за работу в сети Интернет и ограничение доступа к информационным Интернет-ресурсам назначается руководителем учреждения.

2. Ответственный за работу в сети Интернет и ограничение доступа к информационным Интернет-ресурсам подчиняется непосредственно руководителю учреждения.

3. Ответственный за работу в сети Интернет и ограничение доступа к информационным Интернет-ресурсам руководствуется в своей деятельности Конституцией и законами Российской Федерации, государственными нормативными актами; Правилами и нормами охраны труда, техники безопасности и противопожарной защиты; Уставом и локальными правовыми актами учреждения, а также настоящей инструкцией.

2. Основные задачи и обязанности

1. Ответственный за работу в сети Интернет и ограничение доступа к информационным Интернет-ресурсам в учреждении обеспечивает доступ работников к Интернету:

- Следит за состоянием компьютерной техники и Интернет-канала «точки доступа к Интернету;
- Ведет учет пользователей «точки доступа к Интернету». В случае необходимости лимитирует время работы пользователя в Интернете;
- Оказывает помощь пользователям «точки доступа к Интернету» во время сеансов работы в Сети;
- Участвует в организации повышения квалификации работников по использованию Интернета в профессиональной деятельности;
- Осуществляет регулярное обновление антивирусного программного обеспечения;
- Проводит информирование пользователей по вопросам проверки внешних электронных носителей информации (CD-ROM, флеш-накопителей) на отсутствие вирусов.

3. Права

Ответственный за работу в сети Интернет в учреждении имеет право:

- Участвовать в административных совещаниях при обсуждении вопросов, связанных с использованием Интернета в учреждении;
- Отдавать распоряжения пользователям «точки доступа к Интернету» в рамках своей компетенции;
- Ставить вопрос перед руководителем учреждения о нарушении пользователями «точки доступа к Интернету» правил техники безопасности, регламента работы в Интернете.

4. Ответственность

Ответственный за работу в сети Интернет в учреждении несет полную ответственность за:

- Надлежащее и своевременное выполнение обязанностей, возложенных на него настоящим регламентом и инструкцией.

Приложение 25 к приказу от
«30» декабря 2021 г. №01-02-144

Генеральному директору МАУ «НЦВСМ»
С.В. Даниленко
*От*_____
_____
*Паспорт*_____
Выдан _____
_____
*Дата выдачи*_____*к.п.*_____
*СНИЛС*_____
ИНН _____
адрес по прописке _____
_____
Тел. _____

Заявление

В соответствии с приказом мэрии города Новосибирска о назначении стипендии одаренным детям в области физической культуры и спорта прошу перечислять ежемесячную стипендию на расчетный счет, открытый в филиале Центральный ПАО Банка «ФК Открытие».

_____ _____

(дата) *(подпись)*

Согласие законного представителя субъекта (несовершеннолетнего) на обработку персональных данных

Я _____,
(ФИО родителя или законного представителя)

зарегистрирован по адресу: _____,
документ, удостоверяющий личность: _____
_____,
_____
(ФИО несовершеннолетнего)

в соответствии с ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных», в целях получения стипендии мэрии города Новосибирска одаренным детям в области физической культуры и спорта/ единовременного вознаграждения спортсменам и тренерам города Новосибирска, добившимся высоких спортивных результатов, являясь законным представителем несовершеннолетнего даю свое согласие МАУ «НЦВСМ», расположенному по адресу: г. Новосибирск, Красный проспект, 167а, на обработку персональных данных моего сына/дочери/подопечного, содержащихся в основном документе, удостоверяющем личность, СНИЛС, свидетельстве о постановке на учет физического лица в налоговом органе (ИНН), включая сбор, запись, систематизацию, накопление, хранение, уточнение(обновление, изменение), использование, обезличивание, блокирование, удаление, уничтожение.

Настоящее согласие действует со дня его подписания до дня сдачи годовой бухгалтерской отчетности МАУ «НЦВСМ» или до дня предоставления соответствующего отзыва в письменной форме.

_____ _____

(дата) *(подпись законного представителя субъекта (несовершеннолетнего) персональных данных)*

Согласие на обработку персональных данных

Я _____,

зарегистрирован по адресу: _____,

документ, удостоверяющий личность: _____

_____,

в соответствии с ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных», в целях получения единовременного вознаграждения спортсменам и тренерам города Новосибирска, добившимся высоких спортивных результатов, даю согласие МАУ «НЦВСМ», расположенному по адресу: г. Новосибирск, Красный проспект, 167а, на обработку моих персональных данных, содержащихся в основном документе, удостоверяющем личность, СНИЛС, свидетельстве о постановке на учет физического лица в налоговом органе (ИНН), включая сбор, запись, систематизацию, накопление, хранение, уточнение(обновление, изменение), использование, обезличивание, блокирование, удаление, уничтожение.

Настоящее согласие действует со дня его подписания до дня сдачи годовой бухгалтерской отчетности МАУ «НЦВСМ» или до дня предоставления соответствующего отзыва в письменной форме.

_____ _____

(дата) *(подпись субъекта персональных данных)*

Приложение 26 к приказу от
«30» декабря 2021 г. № 01-02-144

Журнал обучения сотрудников в области защиты персональных данных

Журнал начат «___» _____ 20__ г.
Должность _____
ФИО _____

Журнал завершен «___» _____ 20__ г.
Должность _____
ФИО _____

№ п/п	Тема обучения	Дата	Должность, ФИО обучаемого	Подпись
1	2	3	4	5

Приложение 27 к приказу от
«30» декабря 2021 г. №01-02-144

Журнал проверок осведомленности сотрудников в области защиты персональных данных

Журнал начат «___» _____ 20__ г.
Должность _____
ФИО _____

Журнал завершен «___» _____ 20__ г.
Должность _____
ФИО _____

№ п/п	Предмет проверки	Дата	Должность, ФИО проверяемого	Результат проверки	Подпись
1	2	3	4	5	6

Приложение 28 к приказу от «30» декабря 2021г. № 01-02-144

План мероприятий по защите персональных данных на 2022

№ п/п	Наименование мероприятия	Исполнитель	Периодичность исполнения	Примечание
Документальное регламентирование работы с персональными данными:				
1	Возложение ответственности за обеспечение конфиденциальности персональных данных на работников МАУ «НЦВСМ», допущенных к обработке персональных данных		В течение года	Приказ директора
2	Разработка плана мероприятий по защите персональных данных.	юридический отдел	до 30.12.2022	Утверждается директором
3	Разработка организационно-распорядительных документов по защите персональных данных	ответственный за организацию обработки персональных данных в МАУ «НЦВСМ»	до 30.12.2022	Утверждается директором
4	Внесение изменений в действующие локальные акты	юридический отдел	по мере необходимости	Утверждается директором
Обеспечение защиты персональных данных:				
1	Получение и переоформление письменного согласия субъектов ПД (физических лиц) на обработку ПД.	Отдел кадров	постоянно	Сбор согласий субъектов на обработку ПД.
2	Повышение квалификации сотрудников в области защиты персональных данных	ответственный за организацию обработки персональных данных в МАУ «НЦВСМ»	постоянно	Проведение обучающих семинаров, совещаний.
3	Ограничение доступа к административным компьютерам, сейфам, шкафам. Контроль помещений, где установлены аппаратные средства ИСПДн с целью исключения лиц, не допущенных к обработке ПДн	ответственный за защиту информации, в том числе за обеспечение безопасности персональных данных в информационных системах	постоянно	Установление паролей учетных записей

Приложение 29 к приказу от
«30» декабря 2021 г. №01-02-144

Положение об обеспечении безопасности автоматизированной информационной системы муниципального автономного учреждения города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства»

1.Общие положения

Настоящее Положение определяет требования по обеспечению безопасности автоматизированной информационной системы (далее - АИС) муниципального автономного учреждения города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства» (далее – Оператор).

АИС представляет собой IT-систему, предназначенную для автоматизации процессов формирования, обработки и анализа информации по основным направлениям деятельности Оператора.

Основными функциональными возможностями АИС Оператора являются:

-формирование, хранение и обновление сведений о структуре Оператора;

-формирование, хранение и обновление сведений о работниках Оператора;

-формирование, хранение и обновление сведений о несовершеннолетних работниках и их законных представителях;

- формирование, хранение и обновление сведений о получателях стипендии мэрии города Новосибирска одаренным детям в области физической культуры и спорта (в том числе и данные об их законных представителях)/ единовременного вознаграждения спортсменам и тренерам города Новосибирска, добившимся высоких спортивных результатов.

В качестве информации, подлежащей защите в АИС Оператора, рассматриваются:

-персональные данные работников;

-персональные данные несовершеннолетних работниках, в том числе и данные об их законных представителях;

-персональные данные получателей стипендии мэрии города Новосибирска одаренным детям в области физической культуры и спорта (в том числе и данные об их законных представителях)/ единовременного вознаграждения спортсменам и тренерам города Новосибирска, добившимся высоких спортивных результатов (далее – иных субъектов ПДн).

При обеспечении безопасности персональных данных в информационной системе Оператор руководствуется следующим: выбор средств защиты информации для системы защиты персональных данных; определение типа угроз безопасности персональных данных, актуальных для информационной системы; установление и обеспечение уровня защищённости персональных в информационной системе производится Оператором в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утверждённых постановлением Правительства РФ от 1 ноября 2012 г. N 1119.

Основными группами угроз, на противостояние которым направлены цели и требования безопасности, являются:

-угрозы, связанные с осуществлением несанкционированного доступа (ознакомления) с информацией, содержащей сведения о персональных данных работников и иных субъектов ПДн, при ее обработке и хранении;

-угрозы, связанные с несанкционированным копированием (хищением) информации, содержащей сведения о персональных данных работников и иных субъектов ПДн;

-угрозы, связанные с осуществлением доступа к информации, содержащей сведения о персональных данных работников и иных субъектов ПДн, без разрешения на то ее владельца (субъекта персональных данных);

-угрозы, связанные с нарушением порядка доступа к информации, содержащей сведения о персональных данных работников и иных субъектов ПДн, передаваемой заинтересованным лицам;

-угрозы, связанные с перехватом информации, содержащей сведения о персональных данных работников и иных субъектов ПДн, из каналов передачи данных с использованием специализированных программно-технических средств;

-угрозы, связанные с потерей (утратой) информации, содержащей сведения о персональных данных работников и иных субъектов ПДн, вследствие сбоев (отказов) программного и аппаратного обеспечения;

-угрозы, связанные с внедрением компьютерных вирусов и другого вредоносного программного обеспечения;

-угрозы, связанные с осуществлением несанкционированных информационных воздействий (направленных на «отказ в обслуживании» для сервисов, модификацию конфигурационных данных программно-аппаратных средств, подбор аутентификационной информации и т.п.).

Функциональные требования безопасности охватывают:

-требования к осуществлению аудита безопасности;

-требования к обеспечению подлинности субъектов обмена информацией;

-требования к криптографической поддержке;

-требования к защите информации, содержащей сведения о персональных данных работников и воспитанников;

-требования к идентификации и аутентификации пользователей АИС;

-требования к управлению безопасностью;

-требования к защите системы безопасности.

2. Основные функциональные возможности АИС, связанные с обеспечением безопасности (защитой информации)

2.1. Защита данных пользователя

АИС должна осуществлять функции и политику избирательного (дискреционного) управления доступом. Избирательное управление доступом должно предоставлять возможность ограничивать и контролировать доступ к системе и к информации, содержащей сведения о персональных данных.

Каждый Пользователь, пытающийся получить доступ к АИС, сначала должен проходить процедуру идентификации и аутентификации, а затем, при попытках получения доступа к активам, – авторизацию, т.е. проверку разрешений Пользователя по отношению к какому-либо защищаемому активу.

В АИС доступ к информации должен быть разрешен только уполномоченным на это Пользователям. Модель защиты АИС должна включать компоненты, которые реализуют контроль субъектов доступа, действий, предпринимаемых конкретной сущностью по отношению к объекту доступа.

Каждый объект доступа, представленный в АИС, должен быть однозначно ассоциирован с набором атрибутов безопасности, определяющих безопасность защищаемого объекта. Данный набор атрибутов должен формироваться при создании объекта и впоследствии может меняться.

Изменение их значений должно быть обеспечено только Пользователям, имеющим статус владельца объекта, а также субъектам, которым предоставлены соответствующие полномочия.

Права доступа субъектов к объекту должны определяться посредством списка управления доступом. Список управления доступом должен включать перечень пользователей, которым разрешен доступ к объекту, а также набор допустимых над объектом действий.

2.2. Аудит событий безопасности

АИС должна обеспечивать набор средств аудита, предназначенных для мониторинга и обнаружения нежелательных условий, которые могут возникнуть, а также событий, которые могут произойти в системе. Мониторинг относящихся к безопасности событий должен позволять обнаруживать нарушителей безопасности, а также выявлять попытки несанкционированного доступа к АИС или доступа к защищаемой информации. В частности, определяя политику аудита, уполномоченный администратор АИС должен иметь возможность осуществлять аудит только необходимых типов событий безопасности, таких как неудачные попытки подключения пользователей к АИС. Запись результатов аудита событий безопасности должна осуществляться в журналы регистрации событий аудита, доступ к которому должен быть разрешен только уполномоченному администратору АИС. Просмотр журналов регистрации событий аудита должен выполняется с использованием средств АИС (специализированных инструментальных средств). Данные средства должны предоставлять возможность мониторинга и регистрации только тех событий аудита, которые удовлетворяют заданным критериям, что позволит ограничить объем данных, собираемых о событиях безопасности.

2.3. Идентификация и аутентификация

АИС должна требовать, чтобы все субъекты доступа уникально идентифицировались и аутентифицировались при доступе к АИС с помощью ввода идентификатора и пароля. Идентификация и аутентификация должны осуществляться до выполнения субъектом доступа каких-либо действий. АИС должна поддерживать аутентификацию Пользователей вместе с их авторизацией. Предусматривается, что авторизация Пользователей представляет начальный уровень для разрешения доступа к локальным и сетевым ресурсам.

АИС должна обеспечивать хранение паролей в преобразованном формате. АИС должна предоставлять средства усиления безопасности паролей через использование механизмов, позволяющих определить минимальную длину, время действия (минимальное и максимальное), задать требование уникальности (неповторимости) и время смены пароля.

АИС должна предоставлять механизм блокирования учетной записи пользователя после определенного количества попыток ввода неправильного имени и/или пароля пользователя до ее разблокирования администратором АИС или по истечении времени действия, заданного для счетчика блокировки.

2.4. Защита системы безопасности

АИС должна предоставлять ряд возможностей для обеспечения защиты системы безопасности. Изоляция процессов и поддержания домена безопасности должны обеспечивать безопасное выполнение функций системы безопасности АИС. Возможность осуществления периодического тестирования среды функционирования АИС (аппаратной части) и собственно самих функций системы безопасности АИС должно обеспечивать поддержание уверенности администратора АИС в целостности и корректности функционирования функций системы безопасности.

3. Основные функциональные возможности повышения надежности

АИС должна обеспечивать надежную защиту данных от непредвиденных сбоев или отказов системы, обеспечивая следующие возможности по повышению надежности.

3.1. Резервное копирование данных

В АИС должны входить стандартные средства предотвращения потери данных и их восстановления в случае возможных сбоев. Имеющиеся средства резервного копирования должны предоставлять Пользователям возможность выбора различных стратегий резервного копирования, обеспечивающих необходимый уровень защиты данных в случае возникновения сбоев в работе системы, при этом Пользователям должна предоставляться возможность выполнения резервного копирования данных на несъемные и съемные устройства хранения.

3.2. Восстановление системы

Функциональные возможности восстановления системы должны позволять возвращать АИС в состояние, предшествующее сбою. При этом в АИС не должно происходить потери (либо потери должны быть минимальны) и искажения данных.

3.3. Средства администрирования, управления и поддержки

В состав АИС должны быть интегрированы графические средства администрирования и/или утилиты командной строки, обеспечивающие эффективное полномасштабное и гибкое управление (в том числе мониторинг).

4. Среда безопасности АИС

4.1. Модели угроз, характерные для АИС

4.1.1. Осуществление несанкционированного ознакомления с персональными данными работников и воспитанников.

Источники угрозы – внешний злоумышленник.

Способ (метод) реализации угрозы – перехват информации из каналов передачи данных с использованием специализированных программно-технических средств.

Используемые уязвимости – возможные недостатки механизмов защиты информации при ее передаче по каналам передачи данных, связанные с возможностью несанкционированного ознакомления с передаваемой информацией третьих лиц.

Вид информации, потенциально подверженной угрозе – персональные данные работников и иных субъектов ПДн.

Нарушаемое свойство безопасности – конфиденциальность.

Возможные последствия реализации угрозы – нанесения морального и/или материального ущерба лицу, фигурирующему в перехваченной информации. Нанесение косвенного материального ущерба Оператору.

4.1.2. Осуществление несанкционированного ознакомления с персональными данными работников и иных субъектов ПДн и их модификация (в том числе подмена).

Источники угрозы – внешний злоумышленник.

Способ (метод) реализации угрозы – перехват информации из каналов передачи данных с использованием специализированных программно-технических средств; модификация (в том числе подмена) перехваченной информации и навязывание ложной информации.

Используемые уязвимости – недостатки механизмов защиты информации при ее передаче по каналам передачи данных, связанные с возможностью несанкционированного ознакомления и модификации (в том числе подмены) передаваемой информации.

Вид информации, потенциально подверженной угрозе – персональные данные работников и иных субъектов ПДн.

Нарушаемые свойства безопасности – конфиденциальность, целостность.

Возможные последствия реализации угрозы – нанесения морального и/или материального ущерба лицу, фигурирующему в перехваченной информации из-за несанкционированного раскрытия конфиденциальной информации или распространения раскрытых данных. Нанесение косвенного материального ущерба Оператору.

4.1.3. Нарушение доступности, утрата или искажение предоставляемых персональных данных работников и иных субъектов ПДн вследствие сбоев (отказов) программного и аппаратного обеспечения.

Источники угрозы – программное и аппаратное обеспечение.

Способ (метод) реализации угрозы – сбои (отказы) программного и аппаратного обеспечения.

Используемые уязвимости – недостатки механизмов обеспечения доступности требуемой информации, связанные с возможностью блокирования предоставления информации на недопустимое время.

Вид информации, потенциально подверженной угрозе – персональные данные работников и иных субъектов ПДн.

Нарушаемое свойство безопасности – доступность, достоверность.

Возможные последствия реализации угрозы – нарушение со стороны Оператора взятых на себя обязательств по обработке персональных данных работников и иных субъектов ПДн и может привести к прямому или косвенному материальному ущербу Оператору.

4.1.4. Нарушение согласованности данных в персональных данных работников и иных субъектов ПДн вследствие сбоев (отказов) программного и аппаратного обеспечения, а также ошибок сотрудников Оператора.

Источники угрозы – программное и аппаратное обеспечение, сотрудники Оператора.

Способ (метод) реализации угрозы – сбои (отказы) программного обеспечения и ошибки сотрудников Оператора.

Используемые уязвимости – недостатки механизмов обеспечения согласованности данных в БД АИС, связанные с возможностью нарушения согласованности.

Вид информации, потенциально подверженной угрозе – персональные данные работников и иных субъектов ПДн.

Нарушаемые свойства безопасности активов – достоверность, целостность.

Возможные последствия реализации угрозы – рассогласование в персональных данных работников и иных субъектов ПДн, хранимых в БД АИС, что, в свою очередь, приведет к возможному нанесения морального и/или материального ущерба Оператору.

4.1.5. Осуществление доступа (ознакомления) с персональными данными несовершеннолетнего работника, хранимыми и обрабатываемыми в АИС, без согласия субъекта персональных данных (законного представителя) или окончания срока действия такого согласия.

Источники угрозы – уполномоченные на доступ к персональным данным внутренние и внешние пользователи.

Способ (метод) реализации угрозы – осуществление доступа к персональным данным несовершеннолетних работников с использованием штатных средств, предоставляемых программно-аппаратным обеспечением АИС.

Используемые уязвимости – недостатки механизмов защиты персональных данных несовершеннолетнего работника, связанные с возможностью доступа к ним без письменного согласия субъекта персональных данных или после окончания срока его действия.

Вид информации, потенциально подверженной угрозе – персональные данные несовершеннолетних работников.

Нарушаемые свойства безопасности – конфиденциальность.

Возможные последствия реализации угрозы – несанкционированное ознакомление с персональными данными ведет к нанесению морального и/или материального ущерба несовершеннолетнего работника из-за несанкционированного раскрытия конфиденциальной информации.

4.1.6. Внедрение в информационную систему Оператора вирусов и другого вредоносного программного обеспечения при взаимодействии с внешними системами, а также пользователями с носителей информации, используемых на автоматизированных рабочих местах.

Источники угрозы – внутренние пользователи и персонал Оператора, внешние системы.

Способ (метод) реализации угрозы – внедрение вирусов и другого вредоносного программного обеспечения при взаимодействии с внешними системами (файловый обмен, электронная почта и т.п.), а также при использовании съемных носителей информации на автоматизированных рабочих местах.

Используемые уязвимости – недостатки механизмов защиты информационной системы Оператора от внедрения вирусов и другого вредоносного программного обеспечения, связанные с возможностью внедрения вирусов и другого вредоносного программного обеспечения.

Вид информации, потенциально подверженной угрозе – программное обеспечение информационной системы Оператора.

Нарушаемое свойство безопасности активов – целостность.

Возможные последствия реализации угрозы – нарушение режимов функционирования информационной системы Оператора, потеря (утрата) и искажение информации, снижение уровня защищенности информационной системы Оператора. Ведет к возможному материальному ущербу Оператора.

4.1.7. Осуществление несанкционированных информационных воздействий (модификация конфигурационных данных программно-аппаратных средств, подбор аутентификационной информации и т.п.) на информационную систему Оператора, осуществляемых из внешних систем.

Источники угрозы – внешние злоумышленники, внешние системы.

Способ (метод) реализации угрозы – несанкционированные информационные воздействия с использованием специализированного программно-аппаратного обеспечения.

Используемые уязвимости – недостатки механизмов защиты информационной системы Оператора от несанкционированных внешних воздействий.

Вид информации, потенциально подверженной угрозе – программно-аппаратное обеспечение информационной системы Оператора.

Нарушаемые свойства безопасности активов – конфиденциальность, целостность.

Возможные последствия реализации угрозы – нарушение режимов функционирования информационной системы Оператора, снижение уровня защищенности информационной системы Оператора. Ведет к возможному материальному ущербу.

4.2. Политика и цели безопасности для АИС

АИС должна обеспечить следование приведенным ниже правилам безопасности:

1. Должна быть обеспечена регистрация и учет получения (включая указание срока действия) согласия законного представителя несовершеннолетнего работника на обработку предоставленных им Оператору персональных данных.

2. Должна быть обеспечена возможность надежного хранения персональных данных работников и иных субъектов ПДн (в течение действия срока трудового договора и/или разрешения (согласия) на обработку персональных данных соответственно).

3. Должна быть обеспечена возможность безопасного восстановления АИС после сбоев и отказов программного обеспечения и оборудования.

4. Должна быть обеспечена защита информации, составляющей персональные данные работников и иных субъектов ПДн, при ее обработке, хранении и передаче специализированными средствами защиты.

5. Должно быть обеспечено наличие надлежащих, защищенных от несанкционированного использования, механизмов регистрации и предупреждения администратора АИС о любых событиях, относящихся к безопасности АИС.

6. Должно быть обеспечено наличие надлежащих и корректно функционирующих средств администрирования безопасности информационной системы Оператора, доступных только уполномоченным администраторам.

7. Должны быть предоставлены механизмы аутентификации, обеспечивающие адекватную защиту от прямого или умышленного нарушения безопасности нарушителями с низким потенциалом нападения.

8. Должны быть обеспечены механизмы генерации, надлежащего и защищенного распределения, уничтожения ключевой информации, а также механизмы шифрования, и формирования электронной цифровой подписи. Данные механизмы должны функционировать в соответствии с сертифицированными алгоритмами.

4.3. Политика и цели безопасности для среды функционирования АИС

Среда функционирования АИС должна обеспечить следование приведенным ниже правилам безопасности:

1. Должна быть обеспечена инженерно-техническая укреплённость объектов размещения системы обработки, хранения и передачи информации, содержащей сведения о персональных данных.

2. Объекты размещения системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, должны находиться под круглосуточной охраной.

3. Должна быть исключена возможность несанкционированного физического доступа к программно-аппаратным элементам системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, со стороны посторонних лиц.

4. На объектах системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, должно быть обеспечено наличие и надлежащее использование средств антивирусной защиты, сертифицированных по требованиям безопасности. Должно быть обеспечено регулярное обновление антивирусных баз.

5. Объекты системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, должно быть подключены к внешним вычислительным сетям общего пользования с использованием надлежащих средств межсетевого экранирования, сертифицированных по требованиям безопасности.

6. На объектах системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, должно быть обеспечено отсутствие нештатных программных средств, не имеющих отношение к процессу функционирования Оператора.

7. Должны быть обеспечены установка, конфигурирование и управление программноаппаратными средствами АИС в соответствии с руководствами и согласно оцененным конфигурациям.

8. Персонал, ответственный за администрирование АИС, должен быть благонадежным и компетентным, и руководствоваться в своей деятельности соответствующей документацией.

9. Уполномоченные на работу с АИС операторы должны быть благонадежными, руководствоваться в своей работе эксплуатационной документацией на АИС, а их совместные действия должны быть направлены исключительно на выполнение своих функциональных обязанностей.