Приложение 2 к приказу № 198
от «1» сентября 2025 г.

УТВЕРЖДАЮ
Директор МАУДО «СШОР «Красный Яр»
_____ Л.И. Пашкеева
«1» сентября 2025 г.

ПОЛОЖЕНИЕ
о защите информации и обеспечении информационной безопасности в МАУДО «СШОР «Красный Яр»

1. Общие положения

1.1. Настоящее Положение о защите информации и обеспечении информационной безопасности (далее – Положение) определяет общий порядок получения, обработки, использования и защиты в муниципальном автономном учреждении дополнительного образования «Спортивная школа олимпийского резерва «Красный Яр» (МАУДО «СШОР «Красный Яр») (далее - Учреждение) определенной в соответствии с законодательством Российской Федерации информации ограниченного доступа, а также общие требования к информационным системам Учреждения, содержащим такую информацию.

1.2. Настоящее Положение разработано в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», распоряжением Москомспорта от 13.12.2013 г. № 565 «Об организации защиты информации и обеспечения информационной безопасности», иными федеральными законами и правовыми актами Российской Федерации.

1.3. В настоящем Положении под *информацией ограниченного* доступа понимается образующаяся в процессе деятельности Учреждения или поступившая в Учреждение информация (сведения, сообщения, данные и т.п.), доступ к которой ограничен законодательством Российской Федерации, в том числе:

1) сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

2) сведения, составляющие тайну следствия и судопроизводства;

3) сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом РФ и федеральными законами (врачебная, налоговая, банковская тайна, сведения о должнике, просроченной задолженности и ее взыскании и любые другие персональные данные должника, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений и т.д.);

4) служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами (служебная тайна), в том числе: сведения

экономического характера, сведения по финансовым вопросам, сведения, связанные с обеспечением безопасности МАУДО «СШОР «Красный Яр»;

5) сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна);

6) отдельные сведения при осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд в соответствии со ст. 3.3 Федерального закона от 18.07.2011 № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц»;

7) иные сведения, включенные руководителем Учреждения в перечень информации, подлежащей защите в Учреждении**.**

1.4. К информации ограниченного доступа не могут быть отнесены сведения, обязательные к раскрытию Учреждением в соответствии с законодательством Российской Федерации.

1.5. Настоящее Положение не распространяется на обработку обезличенных персональных данных, а также персональных данных, сделанных общедоступными субъектом персональных данных.

1.6. Учреждение организует обеспечение безопасности хранения и обработки информации, указанной в пункте 1.3 настоящего Положения.

Под *обработкой информации ограниченного доступа* понимается любое действие или совокупность действий, совершаемых с использованием средств автоматизации или без использования таких средств, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение информации.

1.7. Мероприятия по защите информации, указанной в пункте 1.3 настоящего Положения (далее - информация ограниченного доступа), осуществляются Учреждением во взаимосвязи с мерами по обеспечению установленной конфиденциальности проводимых работ.

1.8. Обработка персональных данных в Учреждении осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Перечень обрабатываемых персональных данных, принципы и правила их обработки в МАУДО «СШОР «Красный Яр» устанавливается отдельными локальными актами и утверждаются приказом директора МАУДО «СШОР «Красный Яр».

1.9. Объектами защиты информации в Учреждении являются:

1) средства и системы информатизации и связи (средства вычислительной техники, локальная вычислительная сеть, средства и системы связи и передачи информации, материальные носители информации, средства звукозаписи, переговорные и телевизионные устройства, средства изготовления и тиражирования документов), используемые для обработки и хранения информации ограниченного доступа.

2) технические средства и системы, не обрабатывающие информацию, но размещенные в помещениях, где обрабатывается информация ограниченного доступа;

3) помещения для обработки информации ограниченного доступа.

1.10. Ответственность за выполнение требований настоящего Положения возлагается на должностное лицо, ответственное за защиту информации и

обеспечение информационной безопасности в Учреждении (далее - ответственное должностное лицо), а также лиц, допущенных к обработке и хранению информации ограниченного доступа.

1.11. Непосредственное руководство мероприятиями по организации защиты информации ограниченного доступа в Учреждении осуществляет директор Учреждения.

2. Обеспечение защиты информации в Учреждении

2.1. Защита информации в Учреждении представляет собой комплекс организационных и технических мер и включает в себя обеспечение защиты информации ограниченного доступа от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации.

2.2. Для организации защиты информации ограниченного доступа директор Учреждения принимает следующие меры:

1) утверждает перечень информации, подлежащей защите;

2) назначает лицо, ответственное за защиту информации и обеспечение информационной безопасности в Учреждении;

3) утверждает списки сотрудников Учреждения, которые в соответствии со своими должностными обязанностями допускаются к работе с информацией ограниченного доступа;

4) определяет перечень помещений для обработки информации ограниченного доступа;

5) обеспечивает знакомство под роспись при приеме на работу в Учреждение работников, с перечнем информации, подлежащей защите в Учреждении;

6) осуществляет контроль за обеспечением защиты информации ограниченного доступа;

7) обеспечивает внутриобъектовый режим и охрану помещений, предназначенных для обработки и хранения информации ограниченного доступа.

3. Требования к информационной безопасности в Учреждении

3.1. Находящиеся в ведении Учреждения информационные системы и ресурсы, содержащие информацию ограниченного доступа, подлежат обязательной защите.

3.2. Информация ограниченного доступа должна обрабатываться с использованием защищенных систем и средств информатизации и связи или с использованием технических и программных средств технической защиты информации ограниченного доступа.

3.3. В целях обеспечения защиты информации ограниченного доступа сотрудники Учреждения обязаны:

1) хранить в тайне пароль (пароли), позволяющие получить доступ к информации ограниченного доступа;

2) при служебной переписке использовать исключительно электронную

почту в домене mossport.ru или mos.ru;

3) поддерживать в актуальном состоянии антивирусное программное обеспечение, регулярно проводить его обновление;

4) исключить физический доступ посторонних лиц к закрепленным за ними средствам обработки информации ограниченного доступа;

5) неукоснительно выполнять предписания уполномоченных органов и должностных лиц по эксплуатации средств связи, вычислительной техники, материальных носителей информации, оргтехники и другого оборудования, установленного в помещении;

6) немедленно вызывать сотрудника, ответственного за защиту информации и обеспечение информационной безопасности в Учреждении, а также поставить в известность руководителя Учреждения в случае утери ключевого носителя электронно-цифровой подписи или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

- нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей при их наличии) на аппаратных средствах или иных фактов совершения в его отсутствие попыток несанкционированного доступа к рабочей станции;

- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств рабочей станции;

- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию рабочей станции, выхода из строя или неустойчивого функционирования узлов рабочей станции или периферийных устройств (дисководов, принтеров и т.п.), а также перебоев в системе электроснабжения;

- некорректного функционирования установленных на рабочей станции технических средств защиты;

- не предусмотренных формуляром рабочей станции отводов кабелей и подключенных устройств;

- присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленной за ним рабочей станции в подразделении;

8) при прекращении или расторжении трудового договора, передать Учреждению (сотруднику, ответственному за защиту информации и обеспечение информационной безопасности в Учреждении), имеющиеся в пользовании материальные носители информации, содержащие информацию ограниченного доступа.

3.4. Работникам Учреждения запрещается:

1) использовать компоненты программного и аппаратного обеспечения Учреждения в неслужебных целях;

2) самовольно вносить изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и аппаратные средства;

3) для предотвращения заражения компьютеров вредоносным программным обеспечением, в том числе с полной потерей данных, запрещается открывать вложенные файлы и переходить по ссылкам из писем, полученных из недостоверных источников;

4) осуществлять обработку информации ограниченного доступа в присутствии не допущенных к данной информации лиц;

5) записывать и хранить информацию ограниченного доступа на неучтенных носителях информации;

6) оставлять включенной без присмотра свою рабочую станцию, не активизировав средства защиты от несанкционированного допуска (временную блокировку экрана и клавиатуры);

7) передавать кому-либо свой персональный носитель электронно-цифровой подписи (кроме руководителя Учреждения и руководителя структурного подразделения Учреждения), делать неучтенные копии носителя электронно-цифровой подписи (на любой другой носитель) и вносить какие-либо изменения в носитель электронно-цифровой подписи;

8) использовать свой персональный носитель электронно-цифровой подписи для формирования цифровой подписи любых электронных документов, кроме регламентированных технологическим процессом на его рабочем месте;

9) оставлять без личного присмотра на рабочем месте или где бы то ни было свой персональный носитель электронно-цифровой подписи, машинные носители и распечатки, содержащие информацию ограниченного доступа;

10) умышленно использовать недокументированные уязвимости, свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок необходимо ставить в известность ответственное должностное лицо.

3.5. Допускается использование только учтенных носителей информации ограниченного доступа, которые подвергаются регулярной ревизии и контролю.

3.6. При использовании работниками Учреждения носителей информации ограниченного доступа необходимо:

1) использовать носители информации ограниченного доступа исключительно для выполнения своих служебных обязанностей;

2) обеспечивать физическую безопасность носителей информации ограниченного доступа всеми разумными способами;

3) извещать ответственное должностное лицо и руководителя Учреждения о фактах утраты (кражи) носителей информации ограниченного доступа.

3.7. При использовании носителей информации ограниченного доступа запрещено:

1) использовать носители информации ограниченного доступа в личных целях;

2) передавать носители информации ограниченного доступа другим лицам (за исключением руководителя Учреждения и ответственного должностного лица);

3) хранить носители информации ограниченного доступа вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам, не имеющим допуска к работе с информацией ограниченного доступа;

4) выносить носители информации ограниченного доступа из служебных помещений для работы с ними без согласования руководителя Учреждения.

3.8. Любое взаимодействие (обработка, прием/передача информации) инициированное сотрудником Учреждения между информационной системой

Учреждения, содержащей информацию ограниченного доступа и неучтенными (личными) носителями информации, рассматривается как несанкционированное.

3.9. В случае выявления фактов несанкционированного и/или нецелевого применения носителей информации ограниченного доступа инициализируется служебная проверка, проводимая комиссией, состав которой определяется директором Учреждения.

3.10. По факту несанкционированного и/или нецелевого применения носителей информации ограниченного доступа составляется акт расследования инцидента, который передается директору Учреждения для решения вопроса о принятии мер согласно локальным нормативным актам Учреждения и законодательству Российской Федерации.

3.11. Информация, хранящаяся на носителях информации ограниченного доступа, подлежит обязательной проверке на отсутствие вредоносного программного обеспечения.

3.12. В случае увольнения или перевода работника в другое структурное подразделение Учреждения, предоставленные носители информации ограниченного доступа изымаются.

4. Правила доступа в помещения для обработки информации ограниченного доступа

4.1. Объектами охраны Учреждения являются:

1) помещения, в которых происходит обработка информации ограниченного доступа с использованием средств автоматизации или без использования таких средств;

2) помещения, в которых установлены компьютеры, серверы и коммутационное оборудование, защищенные средствами криптографической защиты информации (далее - СКЗИ), участвующие в обработке информации ограниченного доступа.

4.2. Бесконтрольный доступ посторонних лиц в помещения, указанные в п.4.1. Положения, должен быть исключён.

4.3. Ответственность за соблюдение положений настоящей статьи несут сотрудники, обрабатывающие информацию ограниченного доступа.

4.4. Все помещения, предназначенные для обработки и хранения информации ограниченного доступа должны быть оборудованы охранной сигнализацией либо таких помещения должно быть организовано круглосуточное дежурство.

4.5. Доступ посторонних лиц в помещения, в которых ведётся обработка информации ограниченного доступа, должен осуществляется только ввиду служебной необходимости. При этом, на момент присутствия посторонних лиц в помещении должны быть приняты меры по недопущению ознакомления посторонних лиц с информацией ограниченного доступа.

Нахождение в помещениях посторонних лиц без сопровождающего не допустимо.

4.6. В нерабочее время помещения, указанные в п.4.1. Положения должны закрываться на ключ и передаваться под охрану. При этом все окна и двери в смежные помещения должны быть надёжно закрыты, материальные носители информации ограниченного доступа и ключевые документы убраны в

запираемые шкафы (сейфы), средства вычислительной техники выключены либо заблокированы.

5. Заключительные положения

5.1. В целях обеспечения защиты информации и обеспечения информационной безопасности Учреждение имеет право привлекать к проведению работ по технической защите информации в установленном порядке организации, имеющие лицензии на соответствующие виды деятельности.

5.2. При проведении Учреждением совместных работ с физическими лицами, юридическими лицами, органами государственной власти, органами местного самоуправления, связанных с обработкой информации ограниченного доступа, должна быть обеспечена техническая защита информации ограниченного доступа независимо от места проведения работ.

5.3. Публикация на официальном сайте Учреждения в информационно-телекоммуникационной сети «Интернет» информации, содержащей персональные данные, осуществляется в соответствии с законодательством Российской Федерации.

5.4. Публикация на официальном сайте Учреждения в информационно-телекоммуникационной сети «Интернет» информации, содержащей сведения, составляющие государственную и иную охраняемую законодательством Российской Федерации тайну, сведения конфиденциального характера, а также информации ограниченного доступа не допускается.

5.5. Учреждение имеет право пройти добровольную аттестацию на соответствие требованиям к технической защите информации ограниченного доступа в порядке, установленном законодательством Российской Федерации.

5.6. Настоящее Положение обязательно для исполнения всеми работниками Учреждения.

5.7. Нарушение требований к работе с информацией ограниченного доступа, влечет материальную, дисциплинарную, гражданскую, административную и уголовную ответственность в соответствии с законодательством Российской Федерации.