**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ**

**ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ**

**«СПОРТИВНАЯ ШКОЛА ОЛИМПИЙСКОГО РЕЗЕРВА «БОГАТЫРЬ»**

**АРСЕНЬЕВСКОГО ГОРОДСКОГО ОКРУГА**

# ПРИКАЗ

**12 сентября 2025г.** **г. Арсеньев** **№ 117-а**

**О внесении изменений в локальный нормативный акт**

На основании представления об устранении нарушений требований федерального законодательства от 27.08.2025г, № Прдр-20050009-584-25/-20050009

П Р И К А З Ы В А Ю:

1. Внести изменения с 12.09.2025г. в локально-нормативный акт «Положение об обработке персональных данных работников» (в редакции от 09.01.2023г.) согласно приложению № 1 к настоящему приказу.
2. Внести изменения с 12.09.2025г. в локально-нормативный акт «Политика в области обработки и защиты персональных данных» (в редакции от 30.12.2022г.) согласно приложению № 2 к настоящему приказу.
3. Заместителю директора по спортивной работе Мухрановой А.С. в течении 2 (двух) рабочих дней обеспечить ознакомление лиц, указанных в листе ознакомления, с настоящим приказом;
4. Контроль за исполнением настоящего приказа оставляю за собой.

Директор МБУ ДО СШОР «Богатырь» АГО А.К. Шевчук

Приложение № 1

# ИЗМЕНЕНИЯ

## В Положение об обработке персональных данных работников МБУ ДО СШОР «Богатырь» АГО (редакция от 09.01.2023г.)

Внести изменение в пункт 7.1. раздела 7., дополнить текстом следующего содержания:

В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

идентификация и аутентификация субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

ограничение программной среды;

защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);

регистрация событий безопасности;

антивирусная защита;

обнаружение (предотвращение) вторжений;

контроль (анализ) защищенности персональных данных;

обеспечение целостности информационной системы и персональных данных;

обеспечение доступности персональных данных;

защита среды виртуализации;

защита технических средств;

защита информационной системы, ее средств, систем связи и передачи данных;

выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;

управление конфигурацией информационной системы и системы защиты персональных данных.

7.1.1. Меры по идентификации и аутентификации субъектов доступа и объектов доступа обеспечивают присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

7.1.2. Меры по управлению доступом субъектов доступа к объектам доступа обеспечивают управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивают контроль за соблюдением этих правил.

7.1.3. Меры по ограничению программной среды обеспечивают установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключают возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

7.1.4. Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) исключают возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также

несанкционированное использование съемных машинных носителей персональных данных.

7.1.5. Меры по регистрации событий безопасности обеспечивают сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

7.1.6. Меры по антивирусной защите обеспечивают обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

7.1.7. Меры по обнаружению (предотвращению) вторжений обеспечивают обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.

7.1.8. Меры по контролю (анализу) защищенности персональных данных обеспечивают контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

7.1.9. Меры по обеспечению целостности информационной системы и персональных данных обеспечивают обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.

7.1.10. Меры по обеспечению доступности персональных данных обеспечивают авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.

7.1.11. Меры по защите среды виртуализации обеспечивают несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

7.1.12. Меры по защите технических средств исключают несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

7.1.13. Меры по защите информационной системы, ее средств, систем связи и передачи данных обеспечивают защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

7.1.14. Меры по выявлению инцидентов и реагированию на них обеспечивают обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

7.1.15. Меры по управлению конфигурацией информационной системы и системы защиты персональных данных обеспечивают управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

Приложение № 2

# ИЗМЕНЕНИЯ

## В Политике в области обработки и защиты персональных данных МБУ ДО СШОР «Богатырь» АГО (редакция от 30.12.2022г.)

Внести изменение в пункт 7.2. раздела 7., дополнить текстом следующего содержания:

В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

идентификация и аутентификация субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

ограничение программной среды;

защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);

регистрация событий безопасности;

антивирусная защита;

обнаружение (предотвращение) вторжений;

контроль (анализ) защищенности персональных данных;

обеспечение целостности информационной системы и персональных данных;

обеспечение доступности персональных данных;

защита среды виртуализации;

защита технических средств;

защита информационной системы, ее средств, систем связи и передачи данных;

выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;

управление конфигурацией информационной системы и системы защиты персональных данных.

7.1.1. Меры по идентификации и аутентификации субъектов доступа и объектов доступа обеспечивают присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

7.1.2. Меры по управлению доступом субъектов доступа к объектам доступа обеспечивают управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивают контроль за соблюдением этих правил.

7.1.3. Меры по ограничению программной среды обеспечивают установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключают возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

7.1.4. Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) исключают возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также

несанкционированное использование съемных машинных носителей персональных данных.

7.1.5. Меры по регистрации событий безопасности обеспечивают сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

7.1.6. Меры по антивирусной защите обеспечивают обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

7.1.7. Меры по обнаружению (предотвращению) вторжений обеспечивают обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.

7.1.8. Меры по контролю (анализу) защищенности персональных данных обеспечивают контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

7.1.9. Меры по обеспечению целостности информационной системы и персональных данных обеспечивают обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.

7.1.10. Меры по обеспечению доступности персональных данных обеспечивают авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.

7.1.11. Меры по защите среды виртуализации обеспечивают несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

7.1.12. Меры по защите технических средств исключают несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

7.1.13. Меры по защите информационной системы, ее средств, систем связи и передачи данных обеспечивают защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

7.1.14. Меры по выявлению инцидентов и реагированию на них обеспечивают обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

7.1.15. Меры по управлению конфигурацией информационной системы и системы защиты персональных данных обеспечивают управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.