УТВЕРЖДЕНО:
Директор ОГАУ ДО ОСШ по футболу
(наименование общеобразовательной организации)

_____/А.Ю. Фомин/
подпись расшифровка подписи

Приказ № 37 от 09.01.2024 г.

Инструкция пользователя по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций

1. Назначение и область действия.

Настоящая инструкция определяет возможные аварийные ситуации, связанные с функционированием информационных систем персональных данных (далее-ИСПДн) в ОГАУ ДО ОСШ по футболу (далее – учреждение), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций. Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания в случае реализации рассматриваемых угроз. Задачей данной инструкции является: определение мер защиты от прерывания; определение действий восстановления в случае прерывания. Действие настоящей инструкции распространяется на всех сотрудников учреждения, имеющих доступ к ресурсам ИСПДн.

2. Порядок реагирования на аварийную ситуацию
2.1. Действия при возникновении аварийной ситуации. В настоящем документе под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн. Все нештатные ситуации заносятся в «Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания, выполнения профилактических работ, установки и модификации аппаратных и программных средств». В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники учреждения предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с руководителями структурных подразделений. По необходимости иерархия может быть нарушена с целью получения высококвалифицированной консультации в кратчайшие сроки.

2.2. Уровни реагирования на инцидент При реагировании на инцидент важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации: Уровень 1 – Незначительный инцидент. Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты. Эти инциденты решаются ответственными за реагирование сотрудниками. Уровень 2 – Авария. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты. Эти инциденты выходят за рамки управления ответственными за реагирование сотрудниками. К авариям относятся следующие инциденты: отказ элементов ИСПДн и средств защиты из-за: повреждения водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения), а также подтопления в

период паводка или проливных дождей; сбой системы кондиционирования. Отсутствие администратора ИСПДн и администратора безопасности более чем на сутки из-за: химического выброса в атмосферу; сбоев общественного транспорта; эпидемии; массового отравления персонала; сильного снегопада; торнадо; сильных морозов. Уровень 3 – Катастрофа. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн, классифицируется как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к прерыванию работоспособности ИСПДн и средств защиты на сутки и более. К катастрофам относятся следующие инциденты: пожар в здании; взрыв; просадка грунта с частичным обрушением здания; массовые беспорядки в непосредственной близости.

3.Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении
аварийных ситуаций.

3.1. Технические меры. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как: системы обеспечения отказоустойчивости; системы резервного копирования и хранения данных; системы контроля физического доступа. Системы жизнеобеспечения ИСПДн включают: пожарные сигнализации и системы пожаротушения; системы вентиляции и кондиционирования; системы резервного питания. Все критичные помещения учреждения (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

3.2. Организационные меры.

Ответственные за реагирование сотрудники ознакомляют всех сотрудников учреждения, находящихся в их зоне ответственности, с данной инструкцией в срок, не превышающий 3-х рабочих дней с момента выхода нового сотрудника на работу. Должно быть проведено обучение должностных лиц учреждения, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций. Должностные лица должны получить базовые знания в следующих областях: оказание первой медицинской помощи; пожаротушение; эвакуация людей; защита материальных и информационных ресурсов; методы оперативной связи со службами спасения и лицами, ответственными за реагирование сотрудниками на аварийную ситуацию; выключение оборудования, электричества, водоснабжения, газоснабжения. Администраторы ИСПДн и администраторы безопасности должны быть дополнительно обучены методам частичного и полного восстановления работоспособности элементов ИСПДн. Навыки и знания должностных лиц по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение должностных лиц порядку действий при возникновении аварийной ситуации.