Муниципальная бюджетная организация
дополнительного образования
Дворец творчества детей и молодёжи «Радуга»

Нютагай засагай нэмэлтэ болбосоролой бюджедэй эмхи «Радуга»
rehen хуугэдэй ба залуушуулай уран һайханай ордон

ПРИНЯТО:
на Педагогическом совете
МБО ДО ДТДиМ «Радуга»
Протокол № 1 от 26.08.2025 г.

Утверждаю:
Директор МБО ДО ДТДиМ «Радуга»
В.В. Анашкина
Приказ № 62 от 26.08.2025 г.

Инструкция
пользователей информационных систем персональных данных МБО ДО ДТДиМ «Радуга»» по обеспечению безопасности обрабатываемых персональных данных»

2025 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция разработана для обеспечения защиты персональных данных (далее – ПДн) в МБО ДО Дворец творчества детей и молодежи «Радуга».

1.2. Пользователями информационных систем персональных данных (далее ИСПДн) являются сотрудники, допущенные к работе в ИСПДн, в соответствии с приказом об утверждении лиц, допущенных к обработке персональных данных.

1.3. Наиболее вероятными каналами утечки информации для информационных систем персональных данных (ИСПДн) являются:

– просмотр информации с экранов дисплеев мониторов и других средств ее отображения;

– воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения), конфиденциальности и доступности информации, работоспособности технических средств и средств защиты информации.

1.4. Данная инструкция действует в МБО ДО ДТДиМ «Радуга».

2. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

2.1. Работники, получившие доступ к персональным данным, обязаны хранить в тайне сведения ограниченного доступа, ставшие им известными во время работы или иным путем, и пресекать действия других лиц, которые могут привести к разглашению такой информации.

2.2. Прекращение доступа к персональным данным не освобождает работника от взятых им обязательств по неразглашению сведений ограниченного доступа.

2.3. Знать и выполнять требования действующих нормативно-правовых актов, а также локальных нормативных актов, регламентирующих порядок обработки и защиты ПДн при их обработке.

2.4. Выполнять указания и требования Администратора ИСПДн и Администратора безопасности информационной системы персональных данных.

2.5. Выполнять на автоматизированном рабочем месте только те процедуры, которые определены для него должностными обязанностями.

2.6. Знать и строго выполнять правила работы со средствами защиты информации (средствами разграничения доступа), используемыми на персональных компьютерах.

2.7. Хранить в тайне своя аутентификационные данные (пароль доступа в информационную систему),

2.8. Хранить в тайне информацию о системе защиты, установленной в ИСПДн.

2.9. Располагать средства вывода информации, содержащей персональные данные так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией.

2.10. Обо всех выявленных нарушениях, связанных с информационной безопасностью, а также для получения консультаций необходимо обратиться к Администратору безопасности информационной системы персональных данных.

2.11. Пользователям запрещается:

– разглашать сведения, содержащие ПДн, третьим лицам, без письменного согласия субъекта ПДн;

– подключать к автоматизированному рабочему месту личные машинные носители информации и мобильные устройства;

– самостоятельно устанавливать или модифицировать программные и технические средства, изменять установленный алгоритм функционирования технических и программных средств, вскрывать и ремонтировать технические средства;

– привлекать посторонних лиц для производства ремонта или настройки автоматизированных рабочих мест без согласования с администратором безопасности ИСПДн или Администратором ИСПДн;

– самовольно вносить какие-либо изменения в конфигурацию программных и технических средств автоматизированных рабочих мест или устанавливать дополнительно любые программные и технические средства;

– производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств;

– использовать компоненты программного и технического обеспечения ИСПДн в неслужебных целях;

– оставлять посторонних лиц без присмотра в помещениях, где ведется обработка ПДн;

– использовать сведения ограниченного доступа при подготовке открытых публикаций, докладов, научных работ и т.д.;

– открывать общий доступ к папкам на своей рабочей станции; – отключать (блокировать) средства защиты информации;

– сообщать (или передавать) посторонним лицам аутентификационные данные и другие атрибуты доступа к ресурсам ИСПДн;

– самостоятельно изменять аутентификационные данные.

3. ПРАВА ПОЛЬЗОВАТЕЛЯ

Пользователь имеет право:

3.1. Участвовать в служебных расследованиях по фактам нарушений установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов ИСПДн, если данное нарушение произошло под его аутентификационными данными.

3.2. Требовать обеспечения рабочего места необходимыми средствами защиты информации.

3.3. Требовать от администратора безопасности смены аутентификационных данных в случае появления сведений или подозрений на то, что эти данные стали известны третьим лицам.

4.ДЕЙСТВИЯ ПОЛЬЗОВАТЕЛЕЙ В СЛУЧАЕ ВОЗНИКНОВЕНИЯ НЕШТАТНЫХ СИТУАЦИЙ

4.1. Под нештатной ситуацией понимается происшествие, связанное со сбоем в функционировании элементов информационной системы и вероятностью нарушения доступности, конфиденциальности, целостности защищаемой информации.

Наиболее вероятные нештатные ситуации:

– сбой программного обеспечения;

– выход из строя или сбой в работоспособности технических средств ИСПДн (рабочих станций, источников бесперебойного питания, аппаратных средств защиты информации и т.д.);

– обнаружение вредоносной программы;

– информирование средствами защиты информации пользователей об вредоносном воздействии на элементы ИСПДн;

– попытка несанкционированного доступа (НСД) к элементам ИСПДн или непосредственно к персональным данным;

– компрометация или утрата аутентификационной информации;

– физическое повреждение или хищение оборудования технических средств ИСПДн;

– невыполнение пользователями установленных правил информационной безопасности, использование ИСПДн с нарушением технических и нормативных требований;

– несанкционированные изменения состава программных и аппаратных средств (конфигурации) ИСПДн пользователями;

– техногенные и природные проявления нештатных ситуаций;

– другие события, которые могут привести к несанкционированному доступу к персональным данным, их утечке, уничтожению или нарушению целостности, а также события, негативно влияющие на функционирование ИСПДн.

4.2. Лицо, обнаружившее нештатную ситуацию обязано немедленно поставить в известность Администратора безопасности ИСПДн или Администратора ИСПДн.

4. ОТВЕТСТВЕННОСТЬ

4.1. Работники МБО ДО ДТДиМ «Радуга», виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

4.2. Каждый работник Учреждения, получивший для работы доступ к персональным данным, несет личную ответственность за сохранность и конфиденциальность информации.