

СОГЛАСОВАНО

Председатель профсоюзного комитета
МБУ ДО «ЦВР» НМР РТ
Т.А. Насибуллина
26.08.2024 г.

РАССМОТРЕНО И ПРИНЯТО
на общем собрании трудового коллектива
Протокол № 1 от 26.08.2024 г.

УТВЕРЖДАЮ

Директор МБУ ДО «ЦВР» НМР РТ



Введено в действие приказом
по МБУ ДО «ЦВР» НМР РТ
№ 58 от 04.09.2024 г.

ПОЛОЖЕНИЕ

об ответственном лице за информационную безопасность МБУ ДО «Центр внешкольной работы» для одарённых детей НМР РТ

1. Общие положения

1.1. Ответственное лицо за информационную безопасность МБУ ДО «Центр внешкольной работы» для одарённых детей НМР РТ (далее – Оператор Центра) назначается 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.

1.2. Оператор Центра назначается приказом директора Центра.

2. Задачи

2.1. Основные задачи Оператора Центра заключаются в следующем:

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

3. Функции

Для выполнения поставленных задач Оператор Центра осуществляет следующие функции:

3.1. Готовит и представляет на рассмотрение руководству проекты локальных нормативных актов по вопросам обеспечения защиты информации, в том числе персональных данных.

3.2. 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.

3.3. 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.

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

- контроль за строгим соблюдением принятого Порядка доступа к конфиденциальной информации, в том числе к персональным данным;
- 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.

3.5. Ответственное лицо при создании и эксплуатации корпоративных информационных систем:

- самостоятельно разрабатывает и внедряет методы и способы защиты информации, соответствующие установленным требованиям;
- согласовывает с исполнителем планируемые для использования в целях защиты информации методы и способы при условии их соответствия установленным требованиям;
- 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;
- 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.

3.6. Ответственное лицо 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 требований к программному обеспечению и его использованию.

3.7. В соответствии с установленными нормативно-правовыми актами требованиями 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;

- подготовку и предоставление отчетов заведующему, а также по требованию

надзорных и иных уполномоченных органов об организационных и технических мероприятиях по защите информации, в том числе персональных данных;

- постоянный контроль за обеспечением уровня защищенности информации.

4. Взаимодействие

4.1. Для решения поставленных задач и осуществления предусмотренных настоящим Положением функций Ответственное лицо взаимодействует:

- с руководителем Центра и его заместителями;
- с любыми иными подразделениями;
- с государственными, муниципальными органами, учреждениями и организациями, с надзорными органами, а также с иными органами, предприятиями и организациями.

5. Ответственность

5.1. Ответственное лицо за информационную безопасность несет ответственность перед руководством Центра согласно действующему законодательству, нормативно-правовым и локальным нормативным правовым актам за обеспечение:

- выполнения поставленных перед подразделением задач и функций,
- работы с документами и их сохранности, своевременного и качественного исполнения поручений и обращений,
- выполнения требований правил внутреннего трудового распорядка,
- соблюдения в подразделении правил противопожарной безопасности.
- 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, коллективным договором, настоящим Положением, трудовыми договорами и должностными инструкциями.

6. Порядок принятия и срок действия Положения


6.1. Данное Положение рассматривается и принимается на общем собрании трудового коллектива и согласуется с председателем профсоюзного комитета Центра на неопределённый срок.

6.2. Положение может быть дополнено в соответствии с вновь изданными нормативными и законодательными актами муниципальных и региональных органов управления, а также по инициативе руководителя учреждения или работников только решением общего собрания трудового коллектива.

6.3. После принятия новой редакции Положения предыдущая редакция утрачивает силу.

6.4. Настоящее Положение вступает в силу с момента его утверждения приказом директора Центра и размещается на официальном сайте Центра.

Лист согласования к документу № 57 от 09.09.2024
Инициатор согласования: Санникова З.А. Директор
Согласование инициировано: 09.09.2024 09:03

Лист согласования		Тип согласования: последовательное		
№	ФИО	Срок согласования	Результат согласования	Замечания
1	Санникова З.А.		 Подписано 09.09.2024 - 09:03	-