Министерство
образования и науки
Республики Калмыкия

Бюджетное учреждение
дополнительного образования
Республики Калмыкия
«Центр развития одаренных
детей»

358014, Республика Калмыкия, г. Элиста, проспект имени Петра Анацкого,1
т.8(84722)67590, e-mail: rcdt-elista@mail.ru, www.rcdt-rk.ru

Приказ № 119

от «15» 09 2026 г. г. Элиста

Об утверждении Положения об информационной безопасности в
БУ ДО РК «ЦРОД»

В целях обеспечения защиты информации, соблюдения требований законодательства РФ в области информационной безопасности, в т.ч. Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», а также для организации надёжного функционирования информационных систем учреждения,

приказываю:

1. Утвердить Положение об информационной безопасности бюджетного учреждения дополнительного образования Республики Калмыкия «Центр развития одарённых детей» (далее — Положение) согласно приложения к настоящему приказу.
2. Назначить ответственным за организацию и контроль выполнения требований Положения системного администратора Борисова И.В, который обязан:

- организовать ознакомление сотрудников с Положением под подпись;
- обеспечить внедрение и поддержание мер информационной безопасности в соответствии с утверждённым Положением;
- проводить периодические проверки соблюдения требований информационной безопасности;
- своевременно информировать руководство о выявленных нарушениях и рисках в области информационной безопасности.

3. Очирову Э.В., инженеру- программисту разместить электронный экземпляр Положения на официальном сайте учреждения в течение 3 рабочих дней с даты подписания настоящего приказа.

4. Руководителям структурных подразделений (Рыбакова А.В., Таняев Д.Д):
   - ознакомить подчинённых сотрудников с Положением об информационной безопасности под подпись в течении 10 дней;
   - обеспечить выполнение сотрудниками требований Положения в рамках их должностных обязанностей.
5. Всем сотрудникам учреждения соблюдать требования Положения об информационной безопасности и нести персональную ответственность за их нарушение в соответствии с действующим законодательством РФ.
6. Контроль за исполнением настоящего приказа оставляю за собой.

Директор И.Б.Пугаева

С приказом ознакомлены:

Должность	Ф. И. О.	Дата	Подпись
системный администратор	Борисов И.Э.	15.09.26	

Приложение
к приказу БУДО РК «ЦРОД»
от «15» 09 2026 г. № 119

Положение
об информационной безопасности в бюджетном учреждении дополнительного образования Республики Калмыкия «Центр развития одаренных детей»

I. Общие положения.

1.1. Положение об информационной безопасности в БУДО РК «ЦРОД» (далее - Учреждение) разработано в соответствии с требованиями Федерального закона от 27.07.2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006г. № 152–ФЗ «О персональных данных», постановления Правительства Российской Федерации от 01.11.2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.2. Цель настоящего Положения - установление надлежащего порядка работы и создание безопасных условий для посетителей и работников учреждения, информационной безопасности, а также иных нарушений общественного порядка.

1.3. Настоящее Положение утверждается приказом директора учреждения и действует на неопределенный срок.

1.4. Изменения и дополнения к настоящему Положению принимаются по мере необходимости.

1.5. Положение определяет политику учреждения по безопасности информационных и коммуникационных ресурсов и технологий и общий порядок обращения с документами, содержащими служебную информацию ограниченного распространения.

1.6. В настоящем Положении используются следующие основные термины и понятия:

- информационный обмен – процесс передачи и получения информации между пользователями и информационной системой, а также между элементами информационной системы;
- авторизованный субъект доступа – работник учреждения, которому предоставлены соответствующие права доступа к элементам информационных систем персональных данных (далее ИСПДн);
- администратор безопасности – лицо или группа лиц, ответственных за реализацию мероприятий по защите информации и осуществляющих постоянную организационную поддержку функционирования применяемых средств защиты информации;
- атака на информационную систему – любое действие, выполняемое нарушителем, которое приводит к реализации угрозы, путем использования уязвимостей системы;
- безопасность информации – защищенность информации от нарушения конфиденциальности, нарушения целостности, утраты или снижения степени доступности, а также незаконного тиражирования;
- целостность информации – возможность внесения изменений только авторизованным субъектам доступа;
- доступность информации – возможность доступа к информации авторизованного субъекта доступа;
- внешний воздействующий фактор – воздействующий на систему фактор, внешний по отношению к объекту информатизации;

- внутренний воздействующий фактор – воздействующий на систему фактор, внутренний по отношению к объекту информатизации;
- вредоносные программы – программы, приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации или нарушению работы;
- угроза безопасности информации – потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному ее тиражированию, которое наносит ущерб собственнику, или пользователю информации;
- защита информации – деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на информацию;
- организационные меры защиты – это меры, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности информации;
- технические средства защиты – электронные устройства и специальные программы, выполняющие самостоятельно или в комплексе с другими средствами функции защиты информации (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации);
- система информационной безопасности – совокупность организационных мероприятий, технических средств защиты, а также специального персонала, предназначенных для обеспечения информационной безопасности;
- нарушитель – лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения) и использующее для этого различные возможности, методы и средства.

1.7. Положение устанавливает:
- объекты защиты информации и субъекты доступа к информации информационных систем и ресурсов;
- основные угрозы информационной безопасности учреждения;
- основные принципы построения системы защиты информации учреждения;
- меры, методы и средства обеспечения информационной безопасности учреждения.

II. Объекты, подлежащие защите.

2.1. В учреждении обрабатывается информация, содержащая сведения ограниченного распространения (служебная информация, персональные данные), и открытые сведения. Защите подлежат все информационные системы учреждения, независимо от их местонахождения, числящиеся на бухгалтерском учете учреждения.

2.2. Основные объекты, подлежащие защите:
- информационные системы персональных данных, а также открытая (общедоступная) информация, необходимая для работы учреждения, независимо от формы и вида ее представления;
- процессы обработки информации в информационных системах учреждения, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации;

- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации.

2.3. Особенности объектов, подлежащих защите:

- территориальная распределённость элементов информационных систем;
- объединение в единую систему большого количества разнообразных технических средств обработки и передачи информации;
- необходимость обеспечения непрерывности функционирования учреждения;
- высокая интенсивность информационных потоков;
- разнообразие категорий пользователей.

III. Цели и задачи системы обеспечения информационной безопасности.

3.1. Субъекты доступа к информации

Субъектами доступа к информации при обеспечении информационной безопасности учреждения являются:

- работники учреждения, участвующие в информационном обмене в соответствии с возложенными на них должностными обязанностями;
- физические лица, сведения о которых накапливаются, хранятся и обрабатываются в информационных системах учреждения (в соответствии со ст.14 Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных»;
- сотрудники внешних организаций, занимающихся разработкой, поставкой, ремонтом и обслуживанием оборудования или информационных систем.

3.2. Перечисленным субъектам доступа к информации необходимо обеспечить:

- своевременность доступа к необходимой им информации (ее доступность);
- достоверность (полноту, точность, актуальность, целостность) информации;
- конфиденциальность (сохранение в тайне) определенной части информации, защиту от навязывания ложной (недостоверной, искаженной) информации;
- возможность осуществления контроля и управления процессами обработки и передачи информации;
- защиту информации от незаконного распространения.

3.3. Цели защиты информации

Основной целью, на достижение которой направлено настоящее Положение, является защита от возможного нанесения субъектом доступа к информации материального, физического, морального или иного ущерба посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи. Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств информации:

- доступности информации для авторизованных субъектов доступа (устойчивого функционирования системы, при котором авторизованные субъекты доступа имеют возможность получения необходимой информации);
- целостности и аутентичности (подтверждение авторства) информации, хранимой и обрабатываемой в системах мэрии, и передаваемой по каналам связи;
- конфиденциальности – сохранения в тайне определенной части информации, хранимой, обрабатываемой и передаваемой по каналам связи.

Необходимый уровень доступности, целостности и конфиденциальности информации обеспечивается методами и средствами, соответствующими множеству значимых угроз.

3.4. Основные задачи системы обеспечения информационной безопасности учреждения для достижения основной цели защиты и обеспечения указанных свойств информации система обеспечения информационной безопасности учреждения должна обеспечивать решение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба субъектам информационных отношений, нарушению нормального функционирования систем учреждения;
- создание механизма оперативного реагирования на угрозы безопасности информации;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;
- защиту от вмешательства в процесс функционирования систем учреждения посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);
- разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам учреждения – обеспечение доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей; обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);
- защиту от несанкционированной модификации используемых в системах учреждения программных средств, а также защиту систем от внедрения несанкционированных программ, включая компьютерные вирусы; защиту информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

3.5. Основные пути решения задач системы обеспечения информационной безопасности учреждения.

Основные цели обеспечения информационной безопасности и решение перечисленных выше задач достигаются:

- учетом всех подлежащих защите информационных систем учреждения;
- учетом действий персонала, осуществляющего обслуживание и модификацию программных и технических средств корпоративной информационной системы;
- полнотой, реальной выполнимостью и непротиворечивостью требований локальных нормативных актов учреждения по вопросам обеспечения информационной безопасности;
- подготовкой должностных лиц (работников), ответственных за организацию и осуществление практических мероприятий по обеспечению информационной безопасности; - наделением каждого работника (пользователя) учреждения минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам учреждения;
- четким знанием и строгим соблюдением всеми пользователями информационных систем учреждения требований локальных нормативных актов учреждения по вопросам обеспечения информационной безопасности;
- персональной ответственностью за свои действия каждого работника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам учреждения;
- непрерывным поддержанием необходимого уровня защищенности элементов информационных систем учреждения;

- применением программно –аппаратных средств защиты информации и непрерывной административной поддержкой их использования; эффективным контролем над соблюдением пользователями информационных ресурсов учреждения требований по обеспечению информационной безопасности

IV. Основные угрозы информационной безопасности учреждения.

4.1. Существует два вида угроз информационной безопасности: Искусственные угрозы – это угрозы, вызванные деятельностью человека; Естественные угрозы – это угрозы, вызванные воздействиями на информационную систему и ее элементы объективных физических процессов техногенного характера или стихийных природных явлений, не зависящих от человека.

4.2. Наиболее значимыми угрозами информационной безопасности учреждения (способами нанесения ущерба субъектам информационных отношений) являются:

- нарушение функциональности компонентов информационных систем учреждения, блокирование информации, нарушение технологических процессов, срыв своевременного решения задач;
- нарушение целостности (искажение, подмена, уничтожение) информационных ресурсов учреждения, а также фальсификация (подделка) документов;
- нарушение конфиденциальности (разглашение, утечка) персональных данных.

4.3. Основные источники угроз безопасности информации учреждения:

- непреднамеренные (ошибочные, случайные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также требований безопасности информации и другие действия пользователей информационных систем учреждения (в том числе работников, отвечающих за обслуживание и администрирование элементов информационных систем), приводящие к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности элементов информационных систем;
- преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т.п.) действия легально допущенных к информационным ресурсам учреждения пользователей (в том числе работников, отвечающих за обслуживание и администрирование элементов информационных систем), которые приводят к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности элементов информационных систем учреждения;
- удаленное несанкционированное вмешательство посторонних лиц из внешних сетей общего назначения (прежде всего через сеть Интернет), через легальные и несанкционированные каналы подключения к таким сетям, используя недостатки протоколов обмена, средств защиты и разграничения удаленного доступа к информационным ресурсам;
- ошибки, допущенные при разработке элементов информационных систем учреждения и их систем защиты, ошибки в программном обеспечении, отказы и сбои технических средств (в том числе средств защиты информации);
- технические сбои элементов информационных систем.

4.4. Пути реализации угроз информационной безопасности учреждения

4.4.1. Пути реализации непреднамеренных искусственных угроз информационной безопасности учреждения Работники учреждения, являющиеся авторизованными

субъектами доступа информационных систем, а также работники, обслуживающие отдельные элементы информационных систем, являются внутренними источниками случайных воздействий. Основные пути реализации непреднамеренных искусственных (субъективных) угроз безопасности информации учреждения (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла):
- неосторожные действия, приводящие к частичному или полному нарушению функциональности элементов информационных систем учреждения;
- неосторожные действия, приводящие к разглашению информации ограниченного распространения или делающие ее общедоступной;
- разглашение, передача или утрата атрибутов разграничения доступа (ключей (логинов), паролей, ключевых носителей и т. п.);
- игнорирование установленных правил при работе с информационными ресурсами;
- проектирование алгоритмов обработки данных, разработка программного обеспечения с возможностями, представляющими опасность для функционирования информационных систем и информационной безопасности учреждения;
- пересылка информации по ошибочному электронному адресу (устройству);
- ввод ошибочных данных;
- неосторожная порча носителей информации;
- неосторожное повреждение каналов связи;
- неправомерное отключение оборудования или изменение режимов работы элементов информационных систем;
- заражение компьютеров вирусами;
- несанкционированный запуск технологических программ, способных вызвать потерю работоспособности элементов информационных систем или осуществляющих необратимые в них изменения (форматирование или реструктуризацию носителей информации, удаление данных);
- некомпетентное использование, настройка или неправомерное отключение средств защиты.
4.4.2. Пути реализации преднамеренных искусственных (субъективных) угроз информационной безопасности: основные возможные пути умышленной дезорганизации доступа к информации (с корыстными целями, по принуждению, из желания отомстить):
- умышленные действия, приводящие к частичному или полному нарушению функциональности элементов информационных систем учреждения;
- действия по дезорганизации функционирования информационных систем учреждения, хищение электронных документов и носителей информации;
- несанкционированное копирование электронных документов и носителей информации;
- умышленное искажение информации, ввод неверных данных;
- отключение или вывод из строя подсистем обеспечения функционирования элементов информационных систем (электропитания, охлаждения и вентиляции, линий и аппаратуры связи);
- перехват данных, передаваемых по каналам связи и их анализ;
- незаконное получение атрибутов разграничения доступа (используя халатность пользователей, путем подделки, подбора пароля);
- несанкционированный доступ к ресурсам информационных систем с рабочих станций авторизованных субъектов доступа;
- хищение или вскрытие шифров криптозащиты информации;

- внедрение аппаратных и программных закладок с целью скрытно осуществлять доступ к информационным ресурсам или дезорганизации функционирования элементов информационных систем учреждения; незаконное использование элементов информационных систем, нарушающее права третьих лиц;
- применение подслушивающих устройств, фото и видео съемка для несанкционированного съема информации.

4.5. Пути реализации основных естественных угроз безопасности информации:
- выход из строя оборудования информационных систем и оборудования обеспечения его функционирования;
- выход из строя или невозможность использования линий связи;
- пожары и стихийные бедствия.

4.6. Модель возможных нарушителей

4.6.1. Типы нарушителей: с учетом категории лиц, мотивации, квалификации, наличия специальных средств:
- некомпетентный (невнимательный) пользователь – работник учреждения (или подразделения внешней организации, занимающейся обслуживанием информационных систем учреждения), предпринимающий попытки выполнения запрещенных действий, доступа к защищаемым ресурсам информационных систем с превышением своих полномочий, ввода некорректных данных, нарушения правил и регламентов работы с информацией, действуя по ошибке, некомпетентности или халатности без умысла и использующий при этом только штатные средства;
- любитель – работник учреждения (или подразделения внешней организации, занимающейся обслуживанием информационных систем учреждения), пытающийся нарушить систему защиты без корыстных целей, умысла или для самоутверждения. При этом используются различные методы получения дополнительных полномочий доступа к ресурсам, недостатки в построении системы защиты и доступные ему штатные средства (несанкционированные действия посредством превышения своих полномочий на использование разрешенных средств), нештатные инструментальные и технологические программные средства, самостоятельно разработанные программы или стандартные дополнительные технические средства;
- внутренний (внешний) злоумышленник – авторизованный субъект доступа (постороннее лицо) действующий целенаправленно (в том числе в сговоре с лицами, не являющимися работниками учреждения). При этом используются методы и средства взлома системы защиты, включая агентурные методы, пассивные средства (технические средства перехвата), методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий, как изнутри, так и извне учреждения.

4.6.2. Внутренние нарушители

Внутренним нарушителем может быть лицо из следующих категорий работников учреждения:
- зарегистрированные пользователи и персонал, обслуживающий технические средства информационных систем учреждения;
- работники, в том числе руководители, не являющиеся зарегистрированными пользователями и не допущенные к информационным ресурсам учреждения, но имеющие доступ в здания и помещения;
- работники, в том числе руководители, задействованные в разработке и сопровождении программного обеспечения.

4.6.3. Внешние нарушители

Внешним нарушителем может быть лицо из следующих категорий:

- работники учреждения, с которыми прекращен (расторгнут) трудовой договор;
- представители внешних организаций, занимающихся разработкой, поставкой, ремонтом и обслуживанием элементов информационных систем;
- члены преступных организаций или лица, действующие по их заданию;
- лица, случайно или умышленно проникшие в локальную вычислительную сеть учреждения из внешних телекоммуникационных сетей (хакеры);
- администраторы автоматизированных систем учреждения, имеющие неограниченный доступ к информационным ресурсам компонентов корпоративной информационной системы. Администраторы автоматизированных систем могут относиться как к внешним, так и к внутренним нарушителям.

4.7. Утечка информации по техническим каналам.

При проведении мероприятий и эксплуатации технических средств устанавливаются следующие каналы утечки или нарушения целостности информации, нарушения работоспособности технических средств:

- побочные электромагнитные излучения информативного сигнала от технических средств учреждения и линий передачи информации;
- наводки информативного сигнала, обрабатываемого техническими средствами локальной вычислительной сети учреждения, на провода и линии, выходящие за пределы контролируемой зоны учреждения, в т.ч. на цепи заземления и электропитания; электрические сигналы или радиоизлучения, обусловленные воздействием на средства передачи информации высокочастотных сигналов, создаваемых с помощью разведывательной аппаратуры, по эфиру и проводам, либо сигналов промышленных радиотехнических устройств (радиовещательные, радиолокационные станции, средства радиосвязи и т.п.), и модуляцией их информативным сигналом;
- акустическое излучение информативного речевого сигнала или сигнала, обусловленного функционированием технических средств обработки информации;
- электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям передачи информации;
- вибрационные сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно–технические коммуникации выделенных помещений;
- воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности ты, вывода элементов информационных систем учреждения из строя, несанкционированного информационного обмена, в том числе электромагнитное, через специально внедренные электронные и программные средства ("закладки"). Перехват информации или воздействие на нее с использованием технических средств может вестись непосредственно из зданий, расположенных в непосредственной близости от учреждения, мест временного пребывания, заинтересованных в перехвате информации или воздействии на нее лиц при посещении ими учреждения, а также с помощью скрытно устанавливаемой автономной автоматической аппаратуры.

V. Основные принципы построения системы защиты информации.

Построение системы защиты информации учреждения и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

5.1. Законность.

Предполагает осуществление защитных мероприятий и разработку системы защиты информации учреждения в соответствии с действующим законодательством в области информации, информатизации и защиты информации, а также других нормативных актов по безопасности информации, утвержденных органами государственной власти. Принятые меры информационной безопасности не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством случаях к ресурсам конкретных информационных систем. Все пользователи информационных систем учреждения должны иметь представление об ответственности за правонарушения в области информации.

5.2. Системность.

Системный подход к построению системы защиты информации в учреждении предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения информационной безопасности учреждения. При создании системы защиты учитываются все слабые и наиболее уязвимые места информационных систем учреждения, а также характер, возможные объекты и направления атак на нее со стороны нарушителей, пути несанкционированного доступа к информации. Система защиты должна строиться с учетом возможности появления принципиально новых путей реализации угроз безопасности.

5.3. Комплексность.

Комплексное использование методов и средств защиты информационных систем предполагает согласованное применение программных и технических средств при построении целостной системы защиты, перекрывающей все значимые каналы реализации угроз. Защита должна строиться эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Основные аспекты внешней защиты определяются Положением об организации внутриобъектового и пропускного режима в учреждении (приказ от 07.04.2026 г. № 54).

5.4. Непрерывность защиты.

Для обеспечения этого принципа необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, перераспределение полномочий). Порядок получения доступа к информационным ресурсам регламентируется в Инструкции пользователя, осуществляющего обработку персональных данных на объектах вычислительной техники.

5.5. Своевременность.

Предполагается упреждающий характер мер обеспечения информационной безопасности, то есть постановка задач по комплексной защите информации и реализация мер обеспечения безопасности информации на ранних стадиях разработки информационных систем. Разработка системы защиты ведется параллельно с разработкой и развитием самой подлежащей защите информационной системы.

5.6. Преемственность и совершенствование.

Предполагает постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава,

анализа функционирования информационных систем учреждения и систем информационной защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

5.7. Персональная ответственность.

Предполагает возложение ответственности за обеспечение информационной безопасности на каждого работника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей работников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

5.8. Минимизация полномочий.

Предполагает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью. Доступ к информации должен предоставляться только в том случае и объеме, если это необходимо работнику для выполнения его должностных обязанностей.

5.9. Гибкость системы информационной безопасности.

Предполагает способность системы информационной безопасности реагировать на изменения внешней среды и условий осуществления учреждением своей деятельности. В число таких изменений входят:

- изменения организационной и штатной структуры учреждения;
- изменение существующих или внедрение принципиально новых информационных систем;
- ввод в эксплуатацию новых технических средств.

5.10. Простота применения средств защиты.

Механизмы и методы системы защиты информации должны быть понятны и просты в использовании. Применение средств и методов защиты не связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных пользователей, а также не требует от пользователя выполнения малопонятных ему операций.

5.11. Обоснованность и техническая реализуемость.

Предполагает, что информационные технологии, технические и программные средства, средства и меры защиты информации реализуются на современном техническом уровне и обоснованы для достижения заданного уровня безопасности информации и экономической целесообразности, а также соответствуют установленным нормам и требованиям по безопасности информации.

5.12. Специализация и профессионализм.

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты осуществляется профессионально подготовленными специалистами защиты информации учреждения.

5.13. Обязательность контроля.

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации. Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого

объекта защиты осуществляется на основе применения средств оперативного контроля и регистрации и охватывает санкционированные и несанкционированные действия пользователей. Выявленные работниками учреждения недостатки системы защиты информации доводятся до сведения непосредственного руководителя. О существенных недостатках сообщается директору учреждения.

VI. Меры, методы и средства обеспечения информационной безопасности.

6.1. Меры обеспечения информационной безопасности.

6.1.1. Законодательные (правовые) меры обеспечения информационной безопасности
К правовым мерам обеспечения информационной безопасности относятся действующие в Российской Федерации законодательные и иные нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Правовые меры обеспечения информационной безопасности носят упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационных систем учреждения.

6.1.2. Технологические меры обеспечения информационной безопасности
К данному виду мер обеспечения информационной безопасности относятся технологические решения и приемы, направленные на уменьшение возможности совершения работниками ошибок и нарушений в рамках предоставленных им прав и полномочий.

6.1.3. Организационные (административные) меры обеспечения информационной безопасности. Организационные (административные) меры обеспечения информационной безопасности – это меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации. Организационными (административными) мерами обеспечения информационной безопасности являются: регламентация доступа в здание учреждения – определяется «Положением об организации внутриобъектового и пропускного режима» (приказ от 07.04.2026 №54); Регламентация допуска работников к использованию информационных ресурсов – определяется «Положением о защите персональных данных работников учреждения» (Приложение №1 приказа от 28.07.2026 №107).

Обучение пользователей – регламентируется «Инструкцией пользователя, осуществляющего обработку персональных данных на объектах вычислительной техники» (Приложение №2 приказа от 28.07.2026 №107); Условия обработки информационных ресурсов конфиденциального характера, ответственность за нарушения установленного порядка пользования информационными ресурсами учреждения определяется «Положением о защите персональных данных работников учреждения» (Приложение №1 приказа от 28.07.2026 №107).

6.1.4. Физические меры обеспечения информационной безопасности.

Физические меры обеспечения информационной безопасности основаны на применении механических, электронных или электронно–механических устройств, специально предназначенных для создания физических препятствий на возможных путях

проникновения и доступа потенциальных нарушителей к элементам информационных систем и защищаемой информации.

6.1.5. Технические меры обеспечения информационной безопасности Технические (аппаратно–программные) меры обеспечения информационной безопасности основаны на использовании электронных устройств и специальных программ и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации).

Ознакомление с Приказом БУ ДО РК «ЦРОД» № 119 от 15.09.2026 г.

№пп	ФИО	Должность	Подпись	Дата	Примечание
1	Адучинова Алефтина Григорьевна	Педагог доп.образования			
2	Ажаева Карина Баатровна	Инспектор по кадрам		15.09.26	
3	Амулакова Гиляна Николаевна	Специалист по связям с общественностью			Отпуск по уходу за ребенком
4	Аржуева Ангелина Олеговна	Педагог доп.образования			
5	Атрощенко Наталья Ивановна	Педагог доп.образования			
6	Бадмаева Светлана Станиславовна	Педагог-психолог			
7	Бадмаева Цагана Владимировна	Уборщик служебных помещений			
8	Бадмхалгаева Татьяна Викторовна	Концертмейстер			
9	Бадышева Лариса Петровна (совм.	Воспитатель (ночной)			
10	Басангова Мария Арвыковна	Оператор котельной			
11	Белькеев Владимир Убушаевич	Оператор котельной			
12	Бембеев Арлтан Григорьевич	Лаборант			
13	Болдырева Гиляна Григорьевна	Педагог доп.образования			
14	Болдырева Наталья Леонидовна	Уборщик служебных помещений			
15	Борисов Игорь Владимирович	Методист		15.09.26	
16	Буваева Герел Федоровна	Педагог доп.образования			
17	Гаряева Екатерина Вячеславовна	Педагог доп.образования			
18	Гердт Галина Ивановна	Методист			
19	Дадаев Бадма Николаевич	Сторож			Отпуск основной
20	Довгополова Джамиля Анатольевна	Заместитель директора по учебно-воспитательной и методической работе			
21	Дорджи-Горяев Сергей Александро	Звукооператор			
22	Дубровина Анастасия Андреевна	Воспитатель (ночной)			
23	Кавтышев Наран Владимирович	Педагог доп.образования			
24	Карвенов Роман Анатольевич	Педагог доп.образования			
25	Кензеева Светлана Николаевна (со	Медицинская сестра			
26	Кикеева Баина Васильевна (осн.)	Педагог доп.образования			
27	Китаева Галина Дорджиевна	Педагог доп.образования			Отпуск по уходу за ребенком
28	Котмашов Чингис Юрьевич	Педагог доп.образования			
29	Котмашова Алтана Юрьевна	Педагог доп.образования			
30	Кузнецов Игорь Михайлович	Водитель автомобиля			Больничный
31	Кульмулдаева Кемя Сапаевна (осн.	Воспитатель (ночной)			
32	Кучеров Иван Николаевич	Педагог доп.образования			
33	Лиджиева Кермен Ивановна	Воспитатель (ночной)			
34	Манджиева Валерия Сергеевна	Педагог доп.образования			
35	Манджиева Марина Алексеевна	Сторож			
36	Манкирова Сенрина Джангровна	Лаборант			
37	Манхаков Арслан Сергеевич	Рабочий по комплексному обслуживанию и ремонту зданий			
38	Махлаев Иван Бадмаевич	Зав.хозяйством			
39	Михайлова Дина Мацаковна	Методист			
40	Мухлаев Дордж Бадмаевич	Педагог доп.образования			
41	Надбитова Людмила Елексаевна	Педагог доп.образования			
42	Намруева Надежда Сергеевна	Педагог доп.образования			Отпуск по уходу за ребенком
43	Натырова Екатерина Михайловна	Методист			
44	Никешин Владимир Владимирович	Преподаватель			
45	Нимгиров Дольган Саналович	Педагог доп.образования			
46	Нимгирова Анжела Германовна (ос	Оператор котельной			
47	Нимгирова Мария Васильевна	Педагог доп.образования			Отпуск неоплачиваемый по разрешению работодателя
48	Ностаев Джангар Владимирович	Электромонтер по обслуживанию и ремонту электрооборудования			
49	Обинов Артем Валерьевич	Педагог доп.образования			
50	Ожелдыкова Екатерина Цереновна	Педагог доп.образования			
51	Омиков Дорджи Батрович	Специалист по госзакупкам			
52	Очиров Эрдни Валерьевич	Инженер-программист			
53	Пихтуров Николай Алексеевич (сов	Рабочий по комплексному обслуживанию и ремонту зданий			СВО
54	Пугаева Ирина Боглаевна	Директор		15.09.26	
55	Пузикова Надежда Очировна	Уборщик служебных помещений			
56	Пюрвеев Арслан Анатольевич	Педагог доп.образования			

57	Рыбакова Анна Владимировна	Заместитель директора - руководитель Регионального центра			Отпуск основной
58	Саллова Анна Ивановна	Методист			
59	Самохина Элеонора Владимировна	Педагог доп.образования			
60	Сереченко Татьяна Анатольевна (о	Педагог доп.образования			Отпуск по уходу за ребенком
61	Таняев Дорджи Дорджиевич	Зам.директора - руководитель Детского технопарк "Кванториум"			
62	Тиминова Оксана Сергеевна	Педагог доп.образования			
63	Тюлеева Гиляна Валериевна	Преподаватель			
64	Убушиева Баира Семеновна	Методист			
65	Утхунов Владимир Васильевич	Преподаватель			
66	Учурова Виктория Анатольевна	Педагог доп.образования			
67	Ушанова Татьяна Алексеевна	Оператор котельной			
68	Халаева Виктория Александровна	Концертмейстер			Отпуск по уходу за ребенком
69	Церенов Наран Константинович	Педагог доп.образования			
70	Церенова Светлана Ивановна	Уборщик служебных помещений			
71	Цовдаева Надежда Эрендженовна	Сторож			
72	Цурюмов Лавган Михайлович	Педагог-организатор			
73	Чалеева Мария Сергеевна	Педагог-организатор			
74	Шавканов Александр Викторович	Педагог доп.образования			
75	Шапошников Владимир Владимиров	Рабочий по комплексному обслуживанию и ремонту зданий			
76	Шараева Вера Бадмаевна	Зав.хозяйством			
77	Эрдни-Горяева Елена Анатольевна	Педагог доп.образования			
78	Эрдниева Эльзята Эрдниевна	Педагог-организатор			
79	Юсуров Бадма Дорджиевич	Педагог доп.образования			
80	Ясалаев Александр Михайлович	Техник систем водоснабжения			