

УТВЕРЖДАЮ:



Заведующий МДОБУ д/с «Буратино»

С. Михайловка ММО ПК

Г.В. Колоскова

Приказ от 12.01.2026 г. № 1-Д/1

КОМПЛЕКС МЕР БЕЗОПАСНОСТИ

Раздел 1: Физическая безопасность.

Физическая безопасность включает в себя защиту от внешних угроз.

Технические средства безопасности:

- Образовательные учреждения должны быть оснащены системами видеонаблюдения. Камеры должны охватывать ключевые зоны: входы и выходы, коридоры, общественные пространства, внешняя территория образовательного учреждения, что позволяет осуществлять круглосуточный мониторинг территории.
- Образовательные организации должны быть оборудованы доступными системами оповещения: СОУЭ, тревожные кнопки.
- Организация вывода и протоколирования всей информации о текущей ситуации по высокоскоростным линиям связи на заранее подготовленный внешний дежурный диспетчерский пульт.
- Ограничение доступа в образовательные учреждения: обеспечение технической укреплённости здания, монтаж электронных замковых систем на входные двери, установка специальных турникетов, организация пропускного режима.
- Должен проводиться регулярный мониторинг состояния инженерных систем.

- Образовательные учреждения должны иметь ограждение по периметру всего здания.

Кадровые требования безопасности:

- Охрана должна осуществляться квалифицированными специалистами, прошедшими спецподготовку. У охранного предприятия должна быть соответствующая лицензия.

- Сотрудники охранного предприятия должны регулярно проходить обучение по вопросам безопасности, в том числе действиям в экстренных ситуациях.

- Охранник должен иметь возможность, находясь на одном месте, контролировать все входы и выходы в здание, состояние потенциально опасных инженерных систем, одновременно иметь возможность наблюдать за поддержанием порядка внутри здания и на прилегающей территории, его рабочее место должно иметь доступ к информации от комплексной системы безопасности. Для визуального контроля пост охраны должен быть оборудован монитором, на который транслируется изображение с видеокамер.

В образовательных организациях должен быть установлен строгий контроль за соблюдением правил безопасности, включая инструктажи для сотрудников и учащихся. Проведение регулярных тренировок по эвакуации, что позволяет учащимся и педагогам привыкнуть к действиям в экстренных ситуациях.

Раздел 2: Информационная безопасность.

Информационная безопасность образовательных учреждений – это система мер, направленных на защиту информации и ИТ-инфраструктуры организации от случайного или намеренного вмешательства с целью хищения или повреждения данных.

К информации, которую важно защищать в образовательных учреждениях, относятся:

- личные данные учащихся, преподавательского состава, персонала, оцифрованные архивы;
- информация, обеспечивающая образовательный процесс – базы данных, библиотеки, обучающие программы и т.д.

Отличительная особенность обеспечения информационной безопасности в образовании – в том, что защитные меры должны быть направлены не только на сохранность сведений, но и на защиту учащихся от любых видов пропаганды, манипуляций и информации, запрещенной законом.

Комплекс мер по информационной безопасности:

- правовая защита обучающихся, заключающаяся в создании нормативно-правовой базы регулирования общественных отношений в области обеспечения информационной безопасности;
 - технологическая защита, направленная на создание технических способов блокировки нежелательного контента, ограничения доступа к отрицательной информации, технические возможности осуществления родительского контроля за временем пребывания ребенка в сети и качественный анализ сайтов и интернет-сообществ, посещаемых детьми;
 - психолого-педагогические методы, направленные на работу с ребенком по формированию его медиа и компьютерной грамотности, стратегий поведения при встрече с нежелательным контентом и опасными знакомыми в сети Интернет, формирование критического мышления по отношению к информации, получаемой в сети и др.
- деятельности» позволяет построить пошаговый алгоритм дей-
- Изучение руководителями образовательной организации и педагогами научных и нормативно-правовых основ обеспечения информационной безопасности обучающихся.
 - Разработка необходимых локальных актов по вопросам информационной безопасности в образовательной организации.

Проведение самоаудита и последующее повышение компетентности

участников образовательных отношений в решении задач обеспечения информационной безопасности детей и подростков.

- Оценка безопасности информационной среды образовательной организации.
- Проведение с родителями (законными представителями) воспитанников просветительской работы, нацеленной на повышение культуры информационной безопасности.

При построении системы защиты информации с использованием технических средств необходимо следовать определенным принципам:

- использование только лицензированного программного обеспечения (далее – ПО);
- использование только совместимого ПО, все части системы должны быть совместимыми друг с другом;
- управляемость, легкость администрирования системы, минимальное использование сторонней технической поддержки;
- протоколирование и документирование любых действий пользователей, осуществляемых с файлами, содержащими конфиденциальную информацию, а также случаев несанкционированного доступа;
- затраты на организацию защиты информации должны быть соразмерны величине ущерба, который может быть нанесен собственнику информации.

Раздел 3: Работа с внешними коммуникациями.

Работа с внешними коммуникациями в сфере безопасности образовательных учреждений включает комплекс мер по взаимодействию с различными структурами, информированию заинтересованных сторон и координации действий в случае угроз или чрезвычайных ситуаций. Это направление охватывает как организационные, так и технические, правовые и профилактические аспекты.

Образовательные учреждения должны активно сотрудничать с правоохранительными органами (МВД, ФСБ, МЧС и др.) для обеспечения безопасности. Это может включать:

- проведение совместных мероприятий (например, «недели безопасности», практических занятий);
- регулярные проверки на предмет соблюдения антикоррупционного режима или обнаружения наркотических веществ;
- участие сотрудников правоохранительных органов в профилактических лекциях, уроках, внеклассных мероприятиях для детей;
- координацию действий при реагировании на угрозы, факты дестабилизации работы учреждения, а также при проведении массовых мероприятий.

Информирование заинтересованных сторон

- Для сотрудников и учащихся проводятся инструктажи, классные часы и родительские собрания по вопросам безопасности. Например, обсуждаются правила поведения при чрезвычайных ситуациях, антитеррористические меры, действия при обнаружении подозрительных лиц или предметов. Используются наглядные пособия, памятки, проводятся тренировки и симуляции кризисных ситуаций.
- Для родителей организуются встречи и семинары, где обсуждаются проблемы безопасности, делится опытом и разрабатываются совместные стратегии. Информирование родителей может осуществляться через электронные письма, сообщения в мессенджерах, наглядную агитацию.
- Для общественности возможно сотрудничество с местными организациями, службами экстренной помощи для создания общей стратегии безопасного окружения для детей