

Муниципальное бюджетное общеобразовательное учреждение «Средняя
общеобразовательная школа № 1 с. Новосысоевка»

Рассмотрено
на педагогическом совете
от 06.02.2025, № 4

Утверждено
И.о. директора МБОУ «СОШ №1 с.
Новосысоевка»

_____ Н.Ю. Смелая

ПОЛОЖЕНИЕ

об информационной безопасности

1. Общие положения

1.1. Информационная безопасность является одним из составных элементов комплексной безопасности в Муниципальном бюджетном учреждении «Средняя общеобразовательная школа №1 с. Новосысоевка» (далее — Школа), порядок организации работ по её созданию и функционированию.

1.2. В соответствии с пунктом 6, пп.2 статьи 28 «Компетенция, права, обязанности и ответственность образовательной организации» Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»; Федерального закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»; распоряжения Правительства РФ от 28.04.2023 № 1105-р «О концепции информационной безопасности детей в Российской Федерации»; Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных" и имеет статус локального нормативного акта образовательной организации. Если нормами действующего законодательства РФ предусмотрены иные требования, чем настоящим Положением, применяются нормы законодательства РФ.

1.3. Под информационной безопасностью Школы следует понимать состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности. Система информационной безопасности направлена на предупреждение угроз, их своевременное выявление, обнаружение, локализацию и ликвидацию.

1.4. Использование сети Интернет в образовательной организации подчинено следующим принципам:

- соответствие образовательным целям;
- способствование гармоничному формированию и развитию личности;
- уважение закона, авторских и смежных прав, а также иных прав, чести и достоинства других граждан и пользователей сети Интернет;
- приобретение новых навыков и знаний;
- расширение применяемого спектра учебных и наглядных пособий;
- социализация личности, введение в информационное общество.

1.5. К объектам информационной безопасности в Школе относятся:

- информационные ресурсы, содержащие конфиденциальную информацию, представленную в виде документированных информационных массивов и баз данных;
- информацию, защита которой предусмотрена законодательными актами РФ, в т. ч. персональные данные;
- средства и системы информатизации — средства вычислительной и организационной техники, локальной сети, общесистемное и прикладное программное обеспечение, автоматизированные системы управления рабочими местами, системы связи и передачи данных, технические средства сбора, регистрации, передачи, обработки и отображения информации.

1.6. Система информационной безопасности (далее - СПБ) должна обязательно обеспечивать:

- конфиденциальность (защиту информации от несанкционированного раскрытия или перехвата);
- целостность (точность и полноту информации и компьютерных программ);
- доступность (возможность получения пользователями информации в пределах их компетенции).

1.7. Обеспечение информационной безопасности осуществляется по следующим направлениям:

- правовая защита - это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
- организационная защита - это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба ;
- инженерно-техническая защита - это использование различных технических средств, препятствующих нанесению ущерба.

2. Цели и задачи обеспечения безопасности информации

2.1. Главной целью обеспечения безопасности информации, циркулирующей в Школе, является реализация положений законодательных актов Российской Федерации и нормативных требований по защите информации ограниченного доступа (далее по тексту - конфиденциальной или защищаемой информации) и предотвращение ущерба в результате разглашения, утраты, утечки, искажения и уничтожения информации, ее незаконного использования и нарушения работы информационной среды Школы.

2.2. Основными целями обеспечения безопасности информации являются:

- предотвращение утечки, хищения, искажения, подделки информации, циркулирующей в Школе;
- предотвращение нарушений прав личности обучающихся, работников Школы на сохранение конфиденциальности информации;
- предотвращение несанкционированных действий по блокированию информации.

2.3. Основными задачами обеспечения безопасности информации являются:

- соответствие положениям законодательных актов и нормативным требованиям по защите информации;

- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба интересам Школы, нарушению нормального функционирования и развития Школы;

- создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции в системе информационных отношений;

- эффективное пресечение незаконных посягательств на информационные ресурсы, технические средства и информационные технологии, в том числе с использованием организационно-правовых и технических мер и средств защиты информации;

- развитие системы защиты, совершенствование ее организации, форм, методов и средств предотвращения, парирования и нейтрализации угроз информационной безопасности и ликвидации последствий ее нарушения;

- развитие и совершенствование защищенного юридически значимого электронного документооборота;

- создание механизмов, обеспечивающих контроль системы информационной безопасности и гарантии достоверности выполнения установленных требований информационной безопасности;

- создание механизмов управления системой информационной безопасности.

3. Правовые нормы обеспечения информационной безопасности

3.1. Школа имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных обучающихся, работников Школы, требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз.

3.2. Школа обязана обеспечить сохранность конфиденциальной информации.

3.3. Администрация школы:

- назначает ответственного за обеспечение информационной безопасности;

- издаёт нормативные и распорядительные документы, определяющие порядок выделения сведений конфиденциального характера и механизмы их защиты;

- имеет право включать требования по обеспечению информационной безопасности в коллективный договор;

- имеет право включать требования по защите информации в договоры по всем видам деятельности;

- разрабатывает перечень сведений конфиденциального характера;

- имеет право требовать защиты интересов школы со стороны государственных и судебных инстанций.

3.4. Организационные и функциональные документы по обеспечению информационной безопасности:

- приказ директора Школы о назначении ответственного за обеспечение информационной безопасности;

- должностные обязанности ответственного за обеспечение информационной безопасности;

- перечень защищаемых информационных ресурсов и баз данных;

- инструкция, определяющая порядок предоставления информации сторонним организациям по их запросам, а также по правам доступа к ней сотрудников Школы и др.

3.5. Порядок допуска сотрудников Школы к информации предусматривает:

- принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;

- ознакомление работника с нормами законодательства РФ и Школы об информационной безопасности и ответственности за разглашение информации конфиденциального характера;

- инструктаж работника специалистом по информационной безопасности;

- контроль работника ответственным за информационную безопасность при работе с информацией конфиденциального характера.

4. Использование сети Интернет

4.1. Использование сети Интернет в Школе осуществляется в целях образовательного процесса. В рамках развития личности, ее социализации и получения знаний в области компьютерной грамотности лицо может осуществлять доступ к ресурсам не образовательной направленности.

4.2. Работники Школы вправе:

- размещать информацию в сети Интернет на интернет-ресурсах Школы;

- иметь учетную запись электронной почты на интернет-ресурсах Школы.

4.3. Работникам Школы запрещено размещать в сети Интернет и на образовательных ресурсах информацию:

- противоречащую требованиям законодательства РФ и локальным нормативным актам Школы;

- не относящуюся к образовательному процессу и не связанную с деятельностью Школы;

- нарушающую нравственные и этические нормы, требования профессиональной этики.

4.4. Обучающиеся Школы вправе:

- использовать ресурсы, размещенные в сети Интернет, в том числе интернет-ресурсы Школы, в порядке и на условиях, которые предусмотрены настоящим Положением.

- размещать информацию и сведения на интернет-ресурсах Школы.

4.5. Обучающемуся запрещено:

- находиться на ресурсах, содержание и тематика которых недопустима для несовершеннолетних и/или нарушает законодательство РФ;

- в осуществлять любые сделки через интернет;

- загружать файлы на компьютер Школы без разрешения уполномоченного лица;

- распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.

4.6. Запрет и снятие такого запрета на допуск пользователей к работе в сети Интернет устанавливает уполномоченное лицо, назначенное приказом директора Школы.

4.7. Если в процессе работы пользователем будет обнаружен ресурс, содержимое которого не совместимо с целями образовательного процесса, он обязан незамедлительно сообщить об этом уполномоченному лицу с указанием интернет-адреса (URL) и покинуть данный ресурс.

4.8. Уполномоченное лицо обязано:

- принять сообщение пользователя;
- принять меры по отключению выхода на данный ресурс с интернет-ресурсов Школы;

- если обнаруженный ресурс явно нарушает законодательство РФ - сообщить о нем по специальной «горячей линии» для принятия мер в соответствии с законодательством РФ (в течение суток).

Передаваемая информация должна содержать:

- интернет-адрес (URL) ресурса;
- тематику ресурса, предположения о нарушении ресурсом законодательства РФ либо несовместимости с задачами образовательного процесса;
- дату и время обнаружения;
- информацию об установленных в образовательной организации технических средствах ограничения доступа к информации.

5. Мероприятия по обеспечению информационной безопасности

5.1. Для обеспечения информационной безопасности в Школе требуется проведение следующих первоочередных мероприятий:

- защита интеллектуальной собственности Школы;
- защита компьютеров, локальных сетей и сети подключения к системе Интернета;
- организация защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся Школы;
- учет всех носителей конфиденциальной информации.

6. Организация работы с информационными ресурсами и технологиями

6.1. Система организации делопроизводства:

- учет всей документации Школы, в т. ч. и на электронных носителях, с классификацией по сфере применения, дате, содержанию;
- регистрация и учет всех входящих (исходящих) документов Школы в специальном журнале информации о дате получения (отправления) документа, откуда поступил или куда отправлен, - классификация (письмо, приказ, распоряжение и т. д.);
- регистрация документов, с которых делаются копии, в специальном журнале (дата копирования, количество копий, для кого или с какой целью производится копирование);
- особый режим уничтожения документов.

6.2. В ходе использования, передачи, копирования и исполнения документов также необходимо соблюдать определенные правила:

6.2.1. Все документы, независимо от грифа, передаются исполнителю под роспись в журнале учета документов.

6.2.2. Документы, дела и издания с грифом «Для служебного пользования» («Ограниченного пользования») должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах. При этом должны быть созданы условия, обеспечивающие их физическую сохранность.

6.2.3. Выданные для работы дела и документы с грифом «Для служебного пользования» («Ограниченного пользования») подлежат возврату в канцелярию в тот же день.

6.2.4. Передача документов исполнителю производится только через ответственного за организацию делопроизводства.

6.2.5. Запрещается выносить документы с грифом «Для служебного пользования» за пределы школы.

6.2.6. При смене работников, ответственных за учет и хранение документов, дел и изданий, составляется по произвольной форме акт приема-передачи документов.

6.3. Для организации делопроизводства приказом директора школы назначается ответственное лицо. Делопроизводство ведется на основании инструкции по организации делопроизводства, утвержденной директором школы. Контроль за порядком его ведения возлагается на ответственного за информационную безопасность.

7. О системном администрировании и обязанностях ответственного за информационную безопасность

7.1. Задачи, связанные с мерами системного администрирования, обеспечивающего информационную безопасность, являются частью работы системного администратора в МБОУ «СОШ №25 г. Салаира».

7.2. Для решения задач информационной безопасности системный администратор обязан:

- следить за соблюдением требований по парольной защите, в том числе осуществлять изменение паролей по мере необходимости (утрата пароля, появление новых пользователей в связи с изменением кадрового состава и п.р);

- обеспечивать функционирование программно-аппаратного комплекса защиты по внешним цифровым линиям связи;

- обеспечивать мероприятия по антивирусной защите, как на уровне серверов, так и на уровне пользователей;

- обеспечивать нормальное функционирование системы резервного копирования.

8. Антивирусная защита

7.1. Правила пользования внешними сетевыми ресурсами (Интернет, электронная почта и т.д.). Основным способом проникновения компьютерных вирусов на компьютер пользователя в настоящее время является Интернет и электронная почта. В связи с этим не допускается работа без организации антивирусной защиты. Антивирусная защита организуется посредством лицензионного антивирусного программного обеспечения.

7.2. Обновление базы используемого антивирусного программного обеспечения осуществляется автоматически не реже 1 раза в день.

7.3. За своевременное обновление антивирусного программного обеспечения отвечает системный администратор.

9. Алгоритм реагирования на запрещенный информационный контент (приложение 1)

Действия руководителя организации и педагогических работников по созданию условия для обеспечения Безопасности детей В соответствии с Концепцией образовательные организации обязаны обеспечить Безопасность детей. Ответственность за ее обеспечение несет руководитель образовательной организации (далее – Руководитель). Кроме этого, в обеспечении Безопасности должны принимать участие все работники образовательной организации в пределах своей компетенции.

9.1. Руководитель утверждает приказ об организации Безопасности в образовательной организации с указанием ответственного за ее обеспечение. Ведет общий

контроль исполнения поручений в сфере инфобезопасности. Утверждает локальные акты по вопросам инфобезопасности. Организует взаимодействие с социальными партнерами, госорганами, общественными организациями по вопросам инфобезопасности.

9.2. Заместитель Руководителя:

- организует мониторинг соблюдения работниками законодательства в сфере инфобезопасности и защиты прав детей;

- предлагает проекты локальных актов, планов мероприятий и других документов в сфере обеспечения инфобезопасности в образовательной организации.

9.3. Ответственный за Безопасность:

- контролирует исправность работы системы контент-фильтрации ресурсов сети Интернет;

- организывает мониторинг исполнения мероприятий, направленных на защиту детей от негативной информации – причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, в том числе включенных в план мероприятий по обеспечению Безопасности обучающихся образовательной организации;

- организывает просветительские мероприятия с социальными партнерами и (или) обеспечивает участие работников образовательной организации в таких мероприятиях;

- готовит списки педагогических работников, которым необходимо пройти профессиональное обучение в сфере защиты детей от видов информации, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования;

- предоставляет ежегодный отчет о состоянии реализации мероприятий, направленных на защиту детей от негативной информации в образовательной организации.

9.4. Учитель и воспитатель:

- контролирует, чтобы содержание частей ООП и их реализация обеспечивали комфортную атмосферу для детей, позволяли обучить детей вопросам информационной безопасности;

- подбирает средства обучения и воспитания, которые соответствуют законодательству, в том числе с позиции информационной безопасности.

9.5. Классный руководитель:

- реализует воспитательные мероприятия, в том числе по вопросам Безопасности;
- взаимодействует с родителями, чтобы углубить их знания в сфере инфобезопасности, объясняет, как обучить этому детей.

9.6. Педагог-психолог:

- проводит просветительскую и профилактическую работу по вопросам психологической уязвимости в цифровой среде;

- проводит индивидуальную работу с детьми и родителями, если они пострадали от действий в интернете – мошенничества, буллинга и т. д.

9.7. Администратор сайта образовательной организации:

- мониторит наполнение сайта школы и детского сада, в том числе на соответствие законодательства о защите прав детей;

- контролирует, чтобы наполнение госабликов соответствовало правилам инфобезопасности, в том числе создает просветительский контент по этим вопросам.

9.8. Педагог-библиотекарь:

- контролирует безопасность использования цифровых ресурсов библиотеки;
- мониторит состав библиотечного фонда, чтобы в нем отсутствовала литература экстремистского характера и другая, способная причинить вред психике детей.

Алгоритм реагирования на запрещенный информационный контент

В соответствии с Федеральным законом от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации», разработан механизм внесудебного блокирования запрещенной информации, что позволяет оперативно исключить к ней доступ в любой мобильной или проводной сети.

Роскомнадзор принимает сообщения от граждан, юридических лиц, индивидуальных предпринимателей, органов государственной власти, органов местного самоуправления о наличии на страницах сайтов в сети «Интернет» противоправной информации.

В целях оперативного реагирования на появление в сети «Интернет» запрещенной информации, Роскомнадзор предлагает направлять заявки в единую автоматизированную информационную систему (далее – ЕАИС) «Единый реестр» посредством заполнения формы, размещенной по адресу <https://eais.rkn.gov.ru/feedback/>

Процедура рассмотрения заявок в ЕАИС «Единый реестр» представлено на рисунке 1.



Рисунок 1. Рассмотрение заявок в ЕАИС «Единый реестр»