Приложение № 2
к комплексной программе организации профилактической работы
на 2026-2027 гг.,
утвержденной приказом от 01.04.2026г. № 68,
согласованной на педагогическом совете,
с учетом мнения родителей
(законных представителей) обучающихся,
протокол №4 от 27.03.2026г.

ПОДПРОГРАММА
«Кибербезопасность и кибергигиена»

Чита, 2026

ПАСПОРТ ПОДПРОГРАММЫ

Наименование подпрограммы	Кибербезопасность и кибергигиена
Разработчик подпрограммы	Администрация муниципального бюджетного образовательного учреждения «_____»
Соисполнители подпрограммы	СЮТ № 2, МБУ ДО "Детская музыкальная школа № 4"; МБУК «ЦБС» Библиотека №12; МБУ Спортивная школа №7, СК «Русич», ФК «Forvard», Федерация киокушин Забайкальского края, СК «Апачи» отдел полиции Ингодинский УМВД России по городу Чите; КДН и ЗП Ингодинского административного района г. Читы; Центр занятости населения; отдел опеки и попечительства комитета образования администрации городского округа «Город Чита».
Цель подпрограммы	Формирование у обучающихся устойчивых знаний, умений и навыков безопасного и этичного поведения в цифровой среде, способствующих защите персональных данных, предотвращению угроз киберпреступлений и обеспечению конфиденциальности информации.
Задачи подпрограммы	1.Формирование у обучающихся осведомленности о цифровых рисках (фишинг, спам, вирусы, хакерские атаки и мошеннические схемы); 2. Формирование навыков безопасного пользования сетью Интернет (безопасное использование гаджетов, приложений и сетей, соблюдение правил анонимизации и шифрования данных); 3. Профилактика социально-негативных явлений, в том числе агрессивного и деструктивного поведения несовершеннолетних в информационно-телекоммуникационной сети «Интернет», а также формированию у детей, подростков и молодежи конструктивных и уважительных форм общения в социальных сетях. 4. Обучение правилам компьютерной гигиены (правилам ухода за устройствами, установки антивирусных программ, обновления программного обеспечения и своевременного резервного копирования данных); 5. Повышение роли семьи в обучении детей правильному поведению в сети Интернет, активное сотрудничество педагогов и родителей в обеспечении детской кибербезопасности.
Сроки реализации подпрограммы:	2026– 2027 гг.
Этапы реализации подпрограммы:	2026-2027годы, программа реализуется в один этап

Ожидаемые результаты	1.Улучшены знания 90 % обучающихся о правилах безопасного поведения в интернете, угрозы кибератак, фишинга, вирусных атак и других видов интернет-мошенничества. 2. Стабилизировано/сокращено количество инцидентов, связанных с распространением конфиденциальной информации, попаданием в ловушки злоумышленников и участием в сомнительных действиях в интернете, на 10 % ежегодно. 3. В сетевых аккаунтах обучающихся сокращено количество сообщений, содержащих признаки агрессии, насилия, ненависти и травли и другого вида сетевого преследования, на 10 % ежегодно; 4. Произошли положительные изменения в коммуникативном поведении: переход к конструктивному общению в социальных сетях, основанному на взаимном уважении и толерантности; проявление эмпатии и готовности поддержать других пользователей в сложных ситуациях; 5. Сформированы основные навыки цифровой зрелости, обучающиеся приобрели привычку критически относиться к информации, поступающей из разных каналов, развивая способности распознавать ложные данные и манипуляционные техники. 6. 75 % родителей (законных представителей) активно участвуют в поддержании информационной гигиены, усиливают уровень осознания опасностей, повышают качество мониторинга использования детьми электронных устройств.

Характеристика текущее состояния, основные направления организации работы по кибербезопасности и цифровой гигиене

По данным открытых источников за 2025 год, Россия остаётся одной из приоритетных целей киберпреступников. С июля 2024 года по сентябрь 2025 года на страну пришлось 14–16% всех успешных кибератак в мире. По итогам 2025 года общее количество успешных кибератак выросло на 20–45% по сравнению с предыдущим годом, а в 2026 году может увеличиться ещё на 30–35%.

Проблемы безопасности детей и подростков в сети «Интернет» (далее — Интернет, сеть) последние годы становятся особенно актуальными в связи с бурным развитием IT-технологий и со свободным использованием детьми и подростками современных информационно-коммуникационных технологий.

Общение несовершеннолетних в сети «Интернет» стало нормой сегодняшнего дня: 80% подростков в возрасте от 14 до 17 лет проводят время в Интернете от 3 часов в день, 23% подростков более 7 часов каждый день. Интернет-ресурсы встроены в повседневную жизнь многих детей и подростков в качестве средства развлечения, обучения и общения. Коммуникация в Интернет-пространстве разнообразна: тематические форумы, чаты стриминговых сервисов и онлайн-игр, мессенджеры, но ключевым местом концентрации общения являются социальные сети.

Профилактика негативных социальных явлений, в том числе агрессивного и деструктивного поведения несовершеннолетних, в Интернете является одним из приоритетных направлений деятельности педагогов образовательных организаций.

К особенностям цифрового общения в Интернете можно отнести:

- иллюзию анонимности (возможность создания фейковых аккаунтов, сокрытия данных о себе);

- физическую безопасность (нет риска непосредственно подвергнуться ответной физической агрессии, что создает иллюзию физической безопасности);

- отсутствие временных и пространственных ограничений (общение может происходить круглосуточно, вне зависимости от места нахождения участников, может прерываться на неопределенные сроки и вновь возобновляться по той же теме);

- публичность (к общению в беседах, на форумах, в обсуждениях и комментариях часто есть доступ у неограниченного круга лиц, которые могут стать участниками или свидетелями обсуждения);

- ощущение отсутствия ответственности (несовершеннолетний думает, что за написанные слова в реальной жизни ему ничего, кроме ответных сообщений или удаления его комментария не будет);

- сохранность (в отличие от очного диалога, переписки сохраняются хранилищах сервисов, есть возможность их копирования, пересылки, фотографирования, цитирования, в том числе вырванных из контекста предложений и фраз);

- понятность (воспринимать печатный текст проще чем речь человека, кроме того, есть возможность его перечитать, скопировать и проверить);

- отстраненность (участники переписки не чувствуют эмоции друг друга, не видят настоящие реакции на написанные слова, реагируют на мини картинки и смайлы. Такая ситуация создает условия, в которых несовершеннолетний может не увидеть грань, после которой его сообщение становиться жестоким в отношении другого и может ранить).

Важной особенностью цифрового общения является разделение людей и цифровых пространств на две группы, с которыми коммуницируют педагоги.

Первая, значимая группа – это та, взаимодействие с которой отражается на реальной жизни (чаты классов, групп, секций, родительских комитетов, переписки одноклассников, друзей), с данной группой уместно использовать медиативные и восстановительные технологии и стараться сохранить отношения.

Вторая группа – существует только в цифровой среде и не касается реальной жизни (тематические форумы, чаты стриминговых сервисов и онлайн-игр, комментарии в социальных сетях). С данной группой следует быть более осторожными и в случае деструктивного конфликта, агрессии, угроз уместней всего будет прекратить общение и ограничить возможность агрессора писать сообщения (удалить из друзей, заблокировать, добавить в «черный список»).

Цифровое пространство имеет целый ряд опасностей и рисков для несовершеннолетних:

домогательство, педофилия;

склонение к противоправным действиям;

вовлечение в опасные группы и движения;

доступность психологически небезопасного контента, который может вызвать повышение уровня тревожности или развитие аутодеструктивного, в том числе суицидального поведения;

онлайн-травля (кибербуллинг);

завладение личной информацией или материалами, а также возможность создания правонарушителями фейковых медиаматериалов (фотографий / видео / аккаунтов) с целью шантажа или травли;

кража денежных средств;

кража паролей / аккаунтов в социальных сетях или играх;

доступность материалов, предназначенных для старшей аудитории;

зависимость от сетевых игр, онлайн-казино и иных азартных игр;

зависимость от социальных сетей;

столкновение с фейковой информацией на непроверенных источниках.

Задача педагогов создать для обучающихся безопасные условия пребывания в онлайн пространстве, максимально подготовить их к возможным угрозам и научить несовершеннолетних правильно общаться в сети, обеспечивать цифровую гигиену, распознавать информационные угрозы и правильно действовать в случае возникновения сложной ситуации.

Для профилактики конфликтных ситуаций, травли, проявления несовершеннолетними агрессивного и деструктивного поведения в социальных сетях и реальной жизни важно создавать и развивать службы медиации (примирения), которые станут проводниками и трансляторами принципов медиативного и восстановительного подходов, смогут способствовать разрешению возникающих между участниками образовательных отношений конфликтных ситуаций, и проводить просветительские и развивающие мероприятия.

За 2025-2026 учебный год проведено 2 восстановительные (примирительные) процедуры, в том числе касающихся поведению обучающихся в сети интернет .

За 2025 год проведен мониторинг 440 сетевых аккаунтов обучающихся, выявлено 0 деструктивных аккаунтов.

С целью выявления/мониторинга участия родителей (законных представителей) обучающихся 1-4 классов в формировании интернет-интересов своих детей, в сентябре 2025 г. обеспечено прохождение анонимного онлайн анкетирования родителей обучающихся 1-4 классов «Родительское посредничество детской медиа активности».

Основные итоги опроса:

30,9 % обучающихся используют гаджеты для только для игр, 22,9 % - для развивающих/учебных занятий, 13,7 % - просматривают аккаунты блогеров (без фильтрации контента);

77,8% матерей (и 11,5% отцов) регулируют время, которое ребенок проводит с гаджетом, что является положительным знаком ответственности родителей;

71,2% родителей периодически смотрят информацию, выбранную детьми, что важно для обеспечения диалога между родителями и детьми;

В тоже время:

80,3% детей 1-4 классов используют гаджеты самостоятельно, что вызывает беспокойство о возможности использования ненадлежащего контента;

43,7% детей используют гаджеты до 3 часов в день, что может быть приемлемым, если контент образовательный и развивающий, однако, 10,1% детей используют гаджеты более 3 часов, что является нарушением гигиенических норм;

10,7 % родителей никогда не обсуждают с детьми происходящее на экране во время игры или при использовании приложения и веб-сайта и т.д;

75,7 % родителей совместно не просматривают цифровой контент, не играют в совместные игры.

Представленные данные опроса подтверждают необходимость проведения классными руководителями/советниками директоров по воспитанию информационно-просветительских мероприятий с родителями обучающихся по наличию рисков высокого уровня (80,3%) самостоятельного (бесконтрольного) использования гаджетами обучающихся 1-4 классов.

С целью мониторинга цифровой активности и диагностики цифровых рисков обучающихся 8-11 классов организовано прохождение онлайн анкетирования «Опросник киберагрессии. В результате мониторинга выявлены следующие основные действия опрошенных обучающихся:

70 % опрошенных сталкивались с фейковой информацией в интернете: из них 30,4 % — в общественно значимых темах, 21 % — с политическими фейками, и 18,5 % — с недостоверной информацией, связанной с проведением специальной военной операции (СВО);

84,7 % опрошенных никогда не совершали действий цифрового манипулирования;

82,5 % опрошенных не пытались намеренно блокировать или игнорировать других людей в социальных сетях;

53,2 % опрошенных никогда не оскорбляли или дразнили других детей, используя сеть Интернет.

В тоже время:

46,8 % опрошенных целенаправленно блокировали общение в социальных сетях или мессенджерах, игнорировали и организовывали коллективное исключение из социальных сетей, причиняя глубокие психологические травмы другим детям;

31,2 % опрошенных обучающихся публично оскорбляли кого-то в социальной сети, используя текстовые сообщения, что правоохранительными органами может квалифицироваться как административное правонарушение или преступление;

20,6 % опрошенных звонили по телефону, чтобы оскорбить и/или подразнить кого-либо;

15, 4 % опрошенных постоянно используют ложные данные для коммуникации, тем самым подрывая доверие в онлайн-сообществах.

Наиболее критична ситуация в том, что 3 % опрошенных размещали компрометирующею информацию, фото, видео без согласия другого человека, чтобы причинить ему нравственные страдания и/или посмеяться над ним. Данные действия являются уголовно наказуемыми и требуют срочных мер административного реагирования.

Данные анкетирования подтверждают необходимость разработки и реализации данной подпрограммы и проведения дополнительных мероприятий с обучающимися и их родителями (законными представителями) по профилактике кибердевиаций обучающихся, проявляющихся под воздействием информации негативного характера, распространяемой в сети Интернет.

Сроки и этапы реализации подпрограммы

Реализация подпрограммы с 2026 по 2027год.

Подпрограмма реализуется в один этап.

Перечень основных мероприятий подпрограммы

Примерный перечень основных мероприятий подпрограммы с указанием сроков их реализации приведен в приложении к настоящей программе.

Информация о финансовом обеспечении подпрограммы

Финансирование подпрограммы осуществляется за счет средств текущей деятельности МБОУ «СОШ №42» и соисполнителей подпрограммы.

Приложение

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ МЕРОПРИЯТИЙ
на учебный год

№ п/п	Наименование мероприятий	Дата проведения	Ответственный
1.	Создание стенда «Уголок информационной безопасности»	Январь	Соц. педагог
2.	Информирование родителей по вопросам обеспечения информированной безопасности детей, распространения памяток, листовок	Ежеквартально	Кл. руководители
3.	Беседы с обучающимися на тему «Проблемы компьютерной зависимости»	В течении учебного года	Кл. руководители соц. педагог
4.	Изготовление буклетов на тему «Безопасный интернет», «Интернет и дети»	Декабрь-февраль	
5.	Мониторинг групп и личных страниц обучающихся в социальных сетях	Ежемесячно	Соц. педагог,
6.	Проведение классных часов, викторин «Вредоносные программы в Интернете», «Социальные сети: опасные при обращении с виртуальными друзьями», «Защита персональных данных», «Медиабезопасность детей и подростков» т.д.	Раз в месяц	Кл. руководители
7.	Освещение информации по вопросам кибербезопасности, видов Интернет и телефонного мошенничества	В течении года	Соц. педагог, педагог психолог
8.	Круглый стол по теме «Защита от телефонного и интернет мошенничества»	Январь	Зам. директора по ВР, кл. руководители
9.	Проведение теста на определение интернет-зависимости у детей.	1 раз в год	Педагог-психолог
10.	Конкурс рисунков «Мой друг -интернет»	Март	Учитель ИЗО
11.	Беседа « Правила работы в сети Интернет»	Март	Кл. руководители, соц. педагог
12.	Беседы и презентации «Основы безопасности детей и молодежи в Интернете», «Опасные Интернет -сайты»	Апрель	Зам. директора по ВР
13.	Круглый стол по теме «Полезная информация и безопасные сайты для подростков в сети Интернет»	Май	Зам. директора по ВР
14.	Освещение вопросов по информационной безопасности на педагогическом совете школы	Август	Зам. директора по ВР
15.	Профилактическая беседа с приглашением специалистов служб системы профилактики	По плану	Социальный педагог