

**Муниципальное автономное общеобразовательное учреждение
«Средняя общеобразовательная школа-сад № 10» города Когалыма
(МАОУ «Школа-сад № 10»)**

Принята на заседании
методического совета
от «31» августа 2024 г.

Утверждаю
Директор МАОУ «Школа – сад» №10
«31» августа 2024 г.

Дополнительная общеобразовательная общеразвивающая программа
техническая направленность
стартовый уровень

«КИБЕРБЕЗОПАСНОСТЬ»

Возраст учащихся: 10-13лет
Срок реализации: 2 месяца

Автор-составитель:
Уразбаев Аманбай Мухамеджанович,
социальный педагог

г. Когалым – 2024г.

1. Комплекс основных характеристик дополнительной общеобразовательной программы «Кибербезопасность»»

1.1. Пояснительная записка

Направленность программы – техническая.

Уровень освоения – стартовый.

Вид деятельности–защита информации.

Место реализации программы – МАОУ «Школа – сад № 10», ул. Северная 1.

Нормативно-правовой основой разработки дополнительной общеобразовательной общеразвивающей программы (далее – Программа) являются следующие документы:

– федеральный закон от 29.12.2012 № 273 «Об образовании в Российской Федерации»;

– СП 2.4.3648-20 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи», утвержденные постановлением главного санитарного врача от 28.09.2020 № 28;

– СанПиН 1.2.3685-21 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания», утвержденные постановлением главного санитарного врача от 28.01.2021 № 2;

– Порядок организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам, утвержденный приказом Минпросвещения от 27.07.2022 № 629;

– Методические рекомендации по проектированию дополнительных общеразвивающих программ, направленные письмом департамента государственной политики в сфере воспитания детей и молодежи Минобрнауки от 18.11.2015 № 09-3242 «О направлении информации».

Актуальность программы

Всеобщая цифровизация помимо безусловных преимуществ привнесла в современную жизнь высокие риски утечки данных, не предназначенных для постороннего использования. С развитием интернет-технологий, увеличением количества высокотехнологичных устройств, которыми мы себя окружаем, риск стать жертвой киберкриминала все больше увеличивается. Вместе с тем растет и важность кибербезопасности и как области информационных технологий, и как комплекса инструментов для обеспечения защиты конфиденциальных данных. Кибербезопасность – состояние или процесс защиты компьютерных систем, направленный на отражение любых типов киберугроз, будь то действия вредоносных программ, разнообразные сетевые атаки вроде брутфорсинга и DDoS-атак или даже обучение персонала методам защиты от приемов социальной инженерии, фишинга и прочих уловок киберпреступников. На сегодняшний день кибербезопасность превратилась в локомотив цифровизации, поскольку ни транспорт, ни энергетику, ни финансовый сектор, ни социальную сферу невозможно трансформировать в «цифру» без обеспечения информационной безопасности. И если раньше речь шла лишь о целостности, конфиденциальности и доступности данных, то сейчас это угроза захвата злоумышленниками управления различными устройствами, системами и даже целыми отраслями, поскольку благодаря всеобщей интернетизации все системы, включая цифровые фабрики, «умные» дома и «умные» города, объединены в единое киберпространство. И весь этот цифровой мир необходимо защищать от информационных и киберугроз, что делает кибербезопасность проблемой XXI века. Цифровое будущее не наступит без кибербезопасности.

Отличительная особенность программы – совершенствование школьного образования и подготовки в сфере информационных технологий, а также популяризация профессий, связанных с информационными технологиями и защитой информации.

Адресат программы - учащиеся в возрасте от 10 до 13 лет без ОВЗ.

Объем программы составляет 18 учебных часов.

Форма обучения – очная. В рамках реализации программы в период временных ограничений, связанных с эпидемиологической или климатической ситуацией, занятия могут быть организованы с применением дистанционных образовательных технологий.

Форма организации образовательной деятельности – групповая. Минимальное количество учащихся в одной группе – 15 учащихся, максимальное – 20 учащихся.

Срок освоения программы – 2 месяца. Программа состоит из 1 модуля

Режим занятий одной группы: 2 раз в неделю по 1 академическому часу. Продолжительность одного академического часа - 45 минут. Недельная нагрузка на одну группу учащихся – 2 часа.

Примерное расписание занятий на одну группу: понедельник, суббота 16.00

1.2. Цель и задачи программы

Цель: освоение обучающимися базовых принципов безопасного поведения в сети интернет и безопасности личного информационного пространства.

Задачи:

- познакомить с отличительными чертами преступлений в сфере кибербезопасности;
- дать представление о тактике, методах и процедурах, используемых киберпреступниками;
- обучать основным способам защиты от киберугроз;
- развивать эффективное использование компьютерных систем;
- развивать мыслительные, творческие, способности обучающихся;
- развивать интеллектуальные и самостоятельно приобретать, и применять на практике полученные знания;
- развивать интерес к кибербезопасности профессиональной деятельности;
- содействовать социальной адаптации обучающихся в современном обществе, проявлению лидерских качеств;
- воспитывать устойчивый интерес к кибербезопасности;
- воспитывать информационную культуру обращения с данными;
- формировать потребность в творческой деятельности, стремление к самовыражению.

1.3. Содержание программы

Учебный план

№ п/п	Наименование разделов	Количество часов			Формы аттестации/ контроля
		Всего	Теория	Практика	
1.	Удивительный мир Интернета	14	8	6	Фронтальный опрос
2.	Безопасность в сети Интернет	4	2	2	Тест
	Итого:	18	5	4	

Содержание учебного плана

Тема 1. Вводное занятие. Кибербезопасность. Ключевые концепции кибербезопасности. Техника безопасности

Теория: Знакомство с основным содержанием курса, с его целями и задачами, порядком и планом работы на учебный год. Инструктаж по технике безопасности.

Форма контроля: фронтальный опрос.

Тема 2. Опасный и удивительный мир Интернета.

Теория: Актуализация знаний детей о различных Интернет - опасностях, предупреждение формирования Интернет - зависимости у детей.

Практика: Выполнение упражнения «Четыре угла». Работа с текстом, направленная на формирование читательской грамотности.

Форма контроля: ответы на вопросы по тексту.

Тема 3. Виды киберугроз.

Теория: знакомство с внешними и внутренними киберугрозами, с основными понятиями и явлениями киберсреды, способными нанести вред не только компьютеру, но и человеку.

Практика: Обучающиеся научатся основным навыкам личной безопасности и необходимости сохранения персональных данных.

Форма контроля: самостоятельная работа.

Тема 4. Мобильное здоровье.

Теория: знакомство с понятием рационального использования средств мобильной связи не причиняя вред физиологическому, эмоциональному и психологическому здоровью.

Форма контроля: опрос.

Тема 5. Игровой сленг.

Теория: знакомство с понятиями сленга и кибербуллинга.

Практика: формирование навыка цифрового этикета.

Форма контроля: опрос.

Тема 6. Цифровое потребление.

Теория: понятие Интернет - мошенничества.

Практика: формирование навыков поведения в опасных ситуациях, связанных с Интернет-мошенничеством.

Форма контроля: опрос.

Тема 7. Интернет – сообщества. Виртуальные друзья.

Теория: Интернет-группы. Их особенности и возможности. Особенности виртуальной дружбы.

Практика: формирование этикета Интернет-общения.

Формаконтроля: опрос.

Тема 8. Безопасность школьников в сети Интернет.

Теория: знакомство с понятием «Интернет-угроза». Приемы безопасности при работе в сети Интернет.

Формаконтроля: опрос.

Тема 9. Правила безопасной работы в сети Интернет.

Теория: повторение изученного материала об информационной безопасности и безопасного поведения Интернет среде.

Практика: создание памятки «Правила безопасной работы в сети».

Формаконтроля: тест.

1.4. Планируемые результаты

Учащиеся будут знать:

1. об Интернет – опасностях и рисках Интернет – зависимости;
2. о личной безопасности и необходимости сохранения персональных данных;
3. о методах борьбы с кибербуллинг;
4. об организации виртуальных площадок для общения;
5. о различных видах Интернет – мошенничества;
6. об особенностях социальных сетей, сообществ;
7. о сущности безопасного использования мобильного телефона.

Учащиеся будут уметь выполнять:

1. основные операции по поиску и обработке информации;

Учащиеся научатся:

1. цифровому этикету;
2. аргументировать своё мнение;
3. различать внешние и внутренние киберугрозы;
4. ориентироваться в информационном пространстве;
5. эффективному поведению в ситуации Интернет - мошенничества.

2. Комплекс организационно-педагогических условий реализации программы «Кибербезопасность»

2.1. Календарный учебный график

Программа реализуется в период с 01.09.2024 по 25.05.2025г.

Примерное расписание занятий на одну группу: понедельник, суббота 16.00

1 группа:

№ п/п	Месяц	Число	Время проведения занятий	Форма занятия	Количество часов	Тема занятия	Место проведения	Форма контроля
1.	СЕНТЯБРЬ		16.00 – 16.45	Лекция	2	Вводное занятие. Кибербезопасность. Ключевые концепции кибербезопасности. Техника безопасности	каб.117	Фронтальный опрос
2.			16.00 – 16.45	Лекция. Занятие - игра	2	Опасный и удивительный мир Интернета	каб.117	Письменный опрос
3.			16.00 – 16.45	Практическая работа	2	Виды киберугроз	каб.117	Текущий контроль. Самостоятельная работа.
4.			16.00 – 16.45	Лекция	2	Мобильное здоровье	каб.117	Фронтальный опрос
5.	ОКТЯБРЬ		16.00 – 16.45	Лекция	2	Игровой сленг	каб.117	Фронтальный опрос
6.			16.00 – 16.45	Лекция	2	Цифровое потребление	каб.117	Фронтальный опрос
7.			16.00 – 16.45	Практическая работа	2	Интернет – сообщества. Виртуальные друзья	каб.117	Текущий контроль. Самостоятельная работа.
8.			16.00 – 16.45	Лекция	2	Безопасность школьников в сети Интернет	каб.117	Фронтальный опрос
9.			16.00 – 16.45	Контрольная работа	2	Правила безопасной работы в сети Интернет	каб.117	Итоговый тест
ИТОГО					18			

2 группа:

№ п/п	Месяц	Число	Время проведения занятий	Форма занятия	Количество часов	Тема занятия	Место проведения	Форма контроля
10.	НОЯБРЬ		16.00 – 16.45	Лекция	2	Вводное занятие. Кибербезопасность. Ключевые концепции кибербезопасности. Техника безопасности	каб.117	Фронтальный опрос
11.			16.00 – 16.45	Лекция. Занятие - игра	2	Опасный и удивительный мир Интернета	каб.117	Письменный опрос
12.			16.00 – 16.45	Практическая работа	2	Виды киберугроз	каб.117	Текущий контроль. Самостоятельная работа.
13.			16.00 – 16.45	Лекция	2	Мобильное здоровье	каб.117	Фронтальный опрос
14.	ДЕКАБРЬ		16.00 – 16.45	Лекция	2	Игровой сленг	каб.117	Фронтальный опрос
15.			16.00 – 16.45	Лекция	2	Цифровое потребление	каб.117	Фронтальный опрос
16.			16.00 – 16.45	Практическая работа	2	Интернет – сообщества. Виртуальные друзья	каб.117	Текущий контроль. Самостоятельная работа.
17.			16.00 – 16.45	Лекция	2	Безопасность школьников в сети Интернет	каб.117	Фронтальный опрос
18.			16.00 – 16.45	Контрольная работа	2	Правила безопасной работы в сети Интернет	каб.117	Итоговый тест
ИТОГО					18			

3 группа

№ п/п	Месяц	Число	Время проведения занятий	Форма занятия	Количество часов	Тема занятия	Место проведения	Форма контроля
-------	-------	-------	--------------------------	---------------	------------------	--------------	------------------	----------------

19.	ЯНВАРЬ		16.00 – 16.45	Лекция	2	Вводное занятие. Кибербезопасность. Ключевые концепции кибербезопасности. Техника безопасности	каб.117	Фронтальный опрос
20.			16.00 – 16.45	Лекция. Занятие - игра	2	Опасный и удивительный мир Интернета	каб.117	Письменный опрос
21.			16.00 – 16.45	Практическая работа	2	Виды киберугроз	каб.117	Текущий контроль. Самостоятельная работа.
22.			16.00 – 16.45	Лекция	2	Мобильное здоровье	каб.117	Фронтальный опрос
23.			16.00 – 16.45	Лекция	2	Игровой сленг	каб.117	Фронтальный опрос
24.	ФЕВРАЛЬ		16.00 – 16.45	Лекция	2	Цифровое потребление	каб.117	Фронтальный опрос
25.			16.00 – 16.45	Практическая работа	2	Интернет – сообщества. Виртуальные друзья	каб.117	Текущий контроль. Самостоятельная работа.
26.			16.00 – 16.45	Лекция	2	Безопасность школьников в сети Интернет	каб.117	Фронтальный опрос
27.			16.00 – 16.45	Контрольная работа	2	Правила безопасной работы в сети Интернет	каб.117	Итоговый тест
			ИТОГО		18			

4 группа

№ п/п	Месяц	Число	Время проведения занятий	Форма занятия	Количество часов	Тема занятия	Место проведения	Форма контроля
28.	АПРЕЛЬ		16.00 – 16.45	Лекция	2	Вводное занятие. Кибербезопасность. Ключевые концепции кибербезопасности.	каб.117	Фронтальный опрос

						ости. Техника безопасности		
29.		16.00 – 16.45	Лекция. Занятие - игра	2		Опасный и удивительный мир Интернета	каб.117	Письменный опрос
30.		16.00 – 16.45	Практическая работа	2		Виды киберугроз	каб.117	Текущий контроль. Самостоятельная работа.
31.		16.00 – 16.45	Лекция	2		Мобильное здоровье	каб.117	Фронтальный опрос
32.		16.00 – 16.45	Лекция	2		Игровой сленг	каб.117	Фронтальный опрос
33.	МАЙ	16.00 – 16.45	Лекция	2		Цифровое потребление	каб.117	Фронтальный опрос
34.		16.00 – 16.45	Практическая работа	2		Интернет – сообщества. Виртуальные друзья	каб.117	Текущий контроль. Самостоятельная работа.
35.		16.00 – 16.45	Лекция	2		Безопасность школьников в сети Интернет	каб.117	Фронтальный опрос
36.		16.00 – 16.45	Контрольная работа	2		Правила безопасной работы в сети Интернет	каб.117	Итоговый тест
ИТОГО				18				

2.2. Условия реализации программы

Материально-технические условия реализации программы

Учебный кабинет площадью из расчета 2 м² на одного учащегося.

Оборудование кабинета: стол для педагога – 1 шт., столы для обучающихся – 15 шт., стул для педагога – 1 шт., стулья для обучающихся – 30 шт., доска меловая – 1 шт.

Средства обучения:

№ п/п	Средства обучения	Количество штук на 1 группу	% использования
1.	Персональный компьютер (ноутбук)	1	100
2.	Проектор	1	100
3.	Экран для проектора	1	100
4.	Аудиоколонки	1	100
5.	Цифровые средства обучения: фильмы, презентации, тренажеры.	20	100

Психолого-педагогические условия реализации программы:

— уважение к человеческому достоинству учащихся, формирование и поддержка их положительной самооценки, уверенности в собственных возможностях и способностях;

- использование в образовательной деятельности форм и методов работы с учащимися, соответствующих их возрастным и индивидуальным особенностям;
- построение образовательной деятельности на основе взаимодействия педагога с учащимися, ориентированного на интересы и возможности каждого ребенка и учитывающего социальную ситуацию его развития;
- поддержка положительного, доброжелательного отношения учащихся друг к другу и взаимодействия учащихся друг с другом в разных видах деятельности;
- поддержка инициативы и самостоятельности учащихся;
- возможность выбора учащимися видов активности;
- защита учащихся от всех форм физического и **психического насилия**.

Кадровые условия: программу реализует педагог дополнительного образования, имеющий высшее педагогическое образование.

Финансовые условия реализации программы:

Прием на обучение по дополнительной общеобразовательной общеразвивающей программе осуществляется за счет реализации Муниципального задания.

2.3. Формы аттестации

Виды контроля:

Вводный контроль	Изучение стартового уровня знаний, умений и навыков по выбранной дисциплине, уровня мотивации к занятию творчеством
Текущий контроль	Изучение уровня освоения тем образовательной программы.
Итоговый контроль	Оценка качества освоения образовательной программы

Формы контроля:

Проверка теоретических знаний	Тестирование, опрос
Проверка практической подготовки	Презентация, зачет

2.4. Оценочные материалы

Оценка результативности выполнения программы осуществляется по трём уровням освоения учащимися образовательной программы: высокий, средний, ниже среднего.

Оценивания теоретических знаний осуществляется по критериям:

1) уровень ниже среднего - большая часть ответов удовлетворяет требованиям «среднего уровня», но в ответе обнаруживаются отдельные пробелы, не препятствующие дальнейшему усвоению программного материала. Учащийся владеет знаниями в объеме менее 50%;

2) средний уровень - соответствие основным требованиям ответа «высокого уровня», но допущены неточности в изложении понятий, объяснений взаимосвязей; объем правильных ответов составляет 50-85%;

3) высокий уровень - наличие точных знаний по теме.

Вид контроля	Время проведения	Цель проведения контроля	Формы и средства выявления результата	Формы фиксации и предъявления результата
--------------	------------------	--------------------------	---------------------------------------	--

Стартовая диагностика	Сентябрь Ноябрь Январь Март	оценка исходного уровня знаний на первом году обучения в начале учебного года.	Опрос	
Текущий контроль	Сентябрь - Май	оценка усвоения учащимися содержания конкретной программы (темы, раздела и т.д.) в период обучения.	Опрос	
Итоговый контроль	Октябрь Декабрь Март Иай	оценка уровня достижений учащихся, заявленных в образовательных программах, по окончанию всего курса образовательной программы.	Тест	Результаты тестирования

2.5. Методические материалы

В процессе реализации программы применяются педагогические технологии:

1. *Здоровьесберегающая технология.* Гигиенические условия в кабинете соответствуют норме (температурный режим, проветривание кабинета, отсутствие монотонных, неприятных звуковых раздражителей). В процессе занятия происходит смена видов учебной деятельности. Проводятся физкультминутки и гимнастика для глаз. В лекции включены вопросы, связанные создоровьем и здоровым образом жизни.

2. *Объяснительно-иллюстративная технология.* Предъявление информации различными способами (объяснение, рассказ, инструктаж, демонстрация, работа с технологическими картами).

3. *Личностно-ориентированного развивающего обучения.* Подразумевает максимальное развитие индивидуальных познавательных способностей ребенка на основе использования имеющегося у него опыта жизнедеятельности.

4. *Групповые технологии.* В процессе занятий обучающиеся выполняют совместные действия по решению задач, коммуницируют.

В период временных ограничений, связанных с эпидемиологической или климатической

ситуацией, в течение которой федеральными и/или региональными и/или местными правовыми актами устанавливается запрет и/или ограничение на реализацию дополнительных общеобразовательных программ в очной форме, реализация программы в этот период осуществляется с применением дистанционных образовательных технологий.

В этот период деятельность организовывается с использованием:

1. Образовательных технологий (мастер-классы, развивающие занятия, консультации, тематические классные часы, конференции и другие активности, проводимые в режиме реального времени при помощи телекоммуникационных систем).

2. Возможностей электронного обучения (формирование подборок образовательных, просветительских и развивающих материалов, онлайн - тренажеров, представленных на сайте Министерства просвещения Российской Федерации по адресу <https://edu.gov.ru/distance> для самостоятельного использования учащимися).

3. Бесплатных интернет - ресурсов, сайтов учреждений культуры, открывших трансляций концертов, мастер-классов, а также организаций, предоставивших доступ к музейным, литературным, архивным фондам.

4. Ресурсов средств массовой информации (образовательные и научно-популярные передачи, фильмы и интервью на радио и телевидении, в том числе эфиры образовательного телеканала «Моя школа»).

5. Образовательных и развивающих материалов на печатной основе (демонстрационные варианты олимпиадных и диагностических заданий, печатные учебные издания).__

№ п/п	Тема программы	Формы занятий	Педагогические технологии	Приёмы и методы организации ОП	Дидактический материал
1.	Вводное занятие. Кибербезопасность. Ключевые концепции кибербезопасности. Техника безопасности	Учебно-практические занятия. Теоретические	Здоровьесберегающая, объяснительно - иллюстративная технология, групповая	Словесные, наглядные	Таблицы, рисунки, демонстрация фильмов, презентаций.
2.	Опасный и удивительный мир Интернета	Учебно-практические занятия. Теоретические	Здоровьесберегающая, объяснительно - иллюстративная технология, групповая	Словесные, наглядные	Таблицы, рисунки, демонстрация фильмов, презентаций.
3.	Виды киберугроз	Учебно-практические занятия. Теоретические	Здоровьесберегающая, объяснительно - иллюстративная технология, групповая	Словесные, наглядные	Таблицы, рисунки, демонстрация фильмов, презентаций.
4.	Мобильное здоровье	Учебно-практические занятия. Теоретические	Здоровьесберегающая, объяснительно - иллюстративная технология, личностно-ориентированная	Словесные, наглядные, практические	Таблицы, рисунки, демонстрация фильмов, презентаций.

			ого развивающего обучения		
5.	Игровой сленг	Учебно- практические занятия. Теоретические	Здоровьесбере гающая, объяснительно - иллюстративн ая технология, групповая	Словесные, наглядные	Таблицы, рисунки, демонстрация фильмов, презентаций.
6.	Цифровое потребление	Учебно- практические занятия. Теоретические	Здоровьесбере гающая, объяснительно - иллюстративн ая технология, групповая	Словесные, наглядные	Таблицы, рисунки, демонстрация фильмов, презентаций.
7.	Интернет – сообщества. Виртуальные друзья	Учебно- практические занятия. Теоретические	Здоровьесбере гающая, объяснительно - иллюстративн ая технология, групповая	Словесные, наглядные	Таблицы, рисунки, демонстрация фильмов, презентаций.
8.	Безопасность школьников в сети Интернет	Теоретические	Здоровьесбере гающая, объяснительно - иллюстративн ая технология	Словесные, наглядные	Таблицы, рисунки, демонстрация фильмов, презентаций.
9.	Правила безопасной работы в сети Интернет	Учебно- практические занятия. Теоретические	Здоровьесбере гающая, объяснительно - иллюстративн ая технология, групповая	Словесные, наглядные	Таблицы, рисунки, демонстрация фильмов, презентаций.

3.Список литературы

Литература для педагога:

1. Тонких И.М. Комаров М.М. Ледовской В.И. Михайлов А.В. ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ Описание курса для средних школ, 2-11 классы. - Москва, 2016 г.
2. Уроки безопасности в школе (КИБЕРуроки). Сборник методических разработок.// МБУ «Центр психолого-педагогической, медицинской и социальной помощи» - г. Пермь, 2022г.
3. Асмолов А.Г., Семенов А.Л., Уваров А.Ю. Российская школа и новые информационные технологии: взгляд в будущее десятилетие. – М., 2010.

4. Солдатова Г.У., Лебешева М.И. Опасное любопытство. Кто и как попадает на сайты, несущие угрозу для здоровья школьников? // Дети в информационном обществе. – 2011.– № 8. – С. 46–55.

Электронные ресурсы для учащихся:

Международный квест по цифровой грамотности. – URL: <https://сетивичок.рф>