

КОМИТЕТ ПО ОБРАЗОВАНИЮ АДМИНИСТРАЦИИ ГОРОДА УЛАН-УДЭ
МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ
«ДЕТСКО-ЮНОШЕСКИЙ ЦЕНТР «БЕЗОПАСНОЕ ДЕТСТВО»
ГОРОДА УЛАН-УДЭ»

Рассмотрена на заседании
методического совета
Протокол № 1
от «27» августа 2026 г.

Принято на Педагогическом
совете Протокол № 1
от «27» августа 2026 г.



Дополнительная общеобразовательная общеразвивающая
программа технической направленности
«Кибербезопасность»

Возраст обучающихся: 15-17 лет

Срок реализации: 1 год

Автор-составитель:
Мадагуев Тимур Маратович
Педагог дополнительного образования

Улан-Удэ, 2026 год

I. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1. Основные характеристики программы:

1.1. Дополнительная общеразвивающая общеразвивающая программа «Кибербезопасность» (далее - Программа) реализуется в соответствии с технической направленностью дополнительного образования.

Программа составлена с учетом:

- Федеральный Закон «Об образовании в РФ» № 273 – ФЗ от 29.12.2012 г.;
- Федеральный закон от 31 июля 2020 г. N 304-ФЗ "О внесении изменений в Федеральный закон "Об образовании в Российской Федерации" по вопросам воспитания обучающихся";
- Концепция развития дополнительного образования детей до 2030 года (распоряжение Правительства РФ от 31.03.2022 г. №678-р);
- Приказ Министерства просвещения России от 27 июля 2022 г №629 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»;
- Методические рекомендации по проектированию дополнительных общеобразовательных общеразвивающих программ Министерства образования и науки России ФГАУ «Федерального института развития образования» 2015 г.;
- Приказ Министерства образования и науки РФ от 23 августа 2017 г. N 816 "Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ";
- Приказ Министерства образования и науки Российской Федерации и Министерства просвещения Российской Федерации от 05.08.2020 № 882/391 «Об организации и осуществлении образовательной деятельности по сетевой форме реализации образовательных программ;
- Закон РБ от 13.12.2013г. №240 – V «Об образовании в Республике Бурятия»;
- Концепция развития дополнительного образования детей в Республике Бурятия от 24.08.2015 № 512-р;
- Санитарно-эпидемиологические требования к устройству, содержанию и организации режима работы образовательных организаций дополнительного образования детей (СанПиН 2.4.4.3648 – 20);
- Постановление Главного государственного санитарного врача РФ от 28 января 2021 г. №2 «Об утверждении санитарных правил и норм СанПиН 1.2.3685-21 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания». (VI. Гигиенические нормативы по устройству, содержанию и режиму работы организаций воспитания и обучения, отдыха и оздоровления детей и молодежи);
- Устав МБУ ДО «ДЮЦ «Безопасное детство» города Улан-Удэ».

1.2. Актуальность программы

Исследование проблемы безопасности детей и подростков в сети Интернет последние годы является особенно актуальным, в связи с бурным развитием ИТтехнологий и со свободным использованием детьми и подростками современных информационно - коммуникационных технологий (Интернет, сотовая (мобильная) связь). Дополнительная общеобразовательная общеразвивающая программа

«Кибербезопасность» разработана в связи с возросшей потребностью обеспечения информационной безопасности детей и подростков при организации урочной и внеурочной деятельности. Программа разработана для следующих уровней общего образования: начального общего образования. Направленность дополнительной общеобразовательной программы - естественнонаучная. Программа разработана с учетом требований законов Российской Федерации: «Об образовании в Российской Федерации», «О защите детей от информации, причиняющей вред их здоровью и развитию» и «Санитарно-эпидемиологических требований к условиям и организации обучения в общеобразовательных учреждениях» и "Санитарно-эпидемиологических требований к устройству, содержанию и организации режима работы образовательных организаций дополнительного образования детей". В требованиях ФГОС к предметным результатам освоения курса информатики для уровней начального, основного общего и среднего общего образования отсутствует предметная область «Кибербезопасность», но в рамках метапредметных результатов и предметных умений дисциплины «Информатика» вопросы информационной безопасности обозначены. Новизна дополнительной общеобразовательной программы «Кибербезопасность» заключена в достижении метапредметных результатов и предметных умений дисциплины «Информатика» по формированию навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в сети интернет, умений соблюдать нормы информационной этики и права.

1.3. Отличительные особенности программы

Программа принципиально новая, за основу взят курс «Основы кибербезопасности» для общеобразовательных организаций авторов Тонких И.М., Комарова М.М., Ледовского В.И., Михайлова А.В., переработана и модифицирована.

Нетрадиционная форма проведения занятий (мультимедиа, проектор, ноутбук).

Вовлечение детей в проведение, игр, сюрпризных моментов.

Очевидно, что естественнонаучная деятельность учит детей быть более ближе к информационным технологиям.

В рамках модернизации российского образования (в частности, дополнительного) изменены концептуальные подходы и методологические установки к образовательному процессу по причине ограниченности, схластости и неэффективности:

- смещены акценты с освоения фундаментальных знаний по предмету на социализацию и профессионализацию личности средствами современных знаний и технологий по направлению деятельности;
- изменены подходы к структуре и содержанию образовательного процесса с учетом интеграции общего и дополнительного образования;
- модифицировано содержание программы в контексте профессионального непрерывного образования (учреждения ДОО – ссузы – вузы);
- изменены подходы к реализации долгосрочной программы (поэтапно с учетом возрастных особенностей).

1.4. Педагогическая целесообразность определена тем, что ориентирует на приобщение каждого ребенка к информационной науке. Позволяет применить полученные знания, умения и навыки кибербезопасности в повседневной деятельности, улучшить образовательный результат, в области информатики. Благодаря естественнонаучному образованию и воспитанию обучающиеся приобретают общую информационную культуру. Кроме того, педагогическая целесообразность образовательной программы основывается на формировании у обучающегося чувства ответственности в исполнении своей индивидуальной, так и групповой работе.

Программа определяется возможностью общего разностороннего развития личности учащегося в процессе предлагаемой ему деятельности. Возможно кратко отразить те основные идеи, на которых базируется программа, не вошедшие в указанные позиции.

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

1.6. Задачи

Образовательные:

1. Способствовать формированию знаний о безопасном поведении при работе с компьютерными программами, информацией в сети Интернет;
2. Формировать умения соблюдать нормы информационной этики;
3. Формировать умения безопасной работы с информацией, анализировать и обобщать полученную информацию.

Развивающие:

1. Развивать компьютерную грамотность информационную культуру личности в использовании информационных и коммуникационных технологий;
2. Развивать умение анализировать и систематизировать имеющуюся информацию;
3. Развивать познавательную и творческую активность в безопасном использовании информационных и коммуникационных технологий;

Воспитательные:

1. Способствовать выработке сознательного и бережного отношения к вопросам собственной информационной безопасности;
2. Способствовать формированию и развитию нравственных, этических, патриотических качеств личности.
3. Стимулировать поведение и деятельность, направленные на соблюдение информационной безопасности.

1.7. Возраст обучающихся, которым адресована программа - 15-17 лет

Образование детей, имеющих особые образовательные потребности, проводится по индивидуальному маршруту в соответствии с индивидуальными особенностями каждого ребенка, медицинскими рекомендациями, рекомендациями специалистов на основе решения ПМПК. Дети с ограниченными возможностями здоровья занимаются по той же программе, но с особым подходом педагога, учитывая все вышеперечисленные рекомендации.

1.8. Формы занятий:

Возможные формы организации деятельности обучающихся на занятии:

- индивидуальная;
- групповая.

Аудиторные и внеаудиторные (в т.ч. самостоятельные) занятия.

Занятия проводятся по группам и индивидуально

Программу возможно использовать при введении карантинных мероприятий (форма обучения: заочная, дистанционная). Видеоуроки, материалы, рекомендации к занятиям согласно календарно-тематическому плану будут расположены на сайте <http://uab-cdo.rh.muzkult.ru/>, в разделе «Дистанционное обучение».

2. Объем программы:

2.1. Объем программы – 72 часа.

2.2. Срок реализации и уровни программы – 1 год.

2.3. Режим занятий

1 раза в неделю по 1 занятию продолжительностью 45 минут (в зависимости от возраста).

3. Планируемые результаты

3.1. Планируемые результаты

Предметные:

1. Сформированы знания о безопасном поведении при работе с компьютерными программами, информацией в сети интернет;
2. Сформированы умения соблюдать нормы информационной этики;
3. Сформированы умения безопасно работать с информацией, анализировать и обобщать полученную информацию.

Метапредметные:

1. Развиваются компьютерная грамотность и информационная культура личности в использовании информационных и коммуникационных технологий;
2. Развиваются умения анализировать и систематизировать имеющуюся информацию;
3. Развиваются познавательная и творческая активность в безопасном использовании информационных и коммуникационных технологий.

Личностные:

1. Выбатывается сознательное и бережное отношение к вопросам собственной информационной безопасности;
2. Формируются и развиваются нравственные, этические, патриотические качества личности;
3. Стимулируется поведение и деятельность, направленные на соблюдение информационной безопасности.

3.2. Способы и формы проверки результатов

Сформулирована методика и способы проверки ожидаемых результатов; система оценочных средств, позволяющих контролировать каждый заявленный результат обучения, воспитания и развития; использование традиционных и современных средств диагностики результативности; использование комплекса средств, подкрепляющих друг друга;

- возможны формы промежуточной и итоговой аттестации, адекватные содержанию и особенностям учащихся; мониторинг эффективности реализации программы.

Контроль осуществляется 2 раза в год – на начало и конец года, и итоговый – на конец обучения по программе.

II. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1.УЧЕБНЫЙ ПЛАН

№	Наименование разделов	Всего часов	Теоретические занятия	Практические занятия	Форма аттестации/ контроля
----------	------------------------------	--------------------	------------------------------	-----------------------------	-----------------------------------

1.	Раздел 1 Информация, компьютер и Интернет.	18	12	6	опрос
2.	Раздел 2 Техника безопасности и экология	16	10	6	зачет
3.	Раздел 3 Мир виртуальный и реальный. Интернет зависимость	10	6	4	зачет
4.	Раздел 4 Методы безопасной работы в Интернете	8	4	4	опрос
5.	Раздел 5 Потребительские опасности в Интернете	8	6	2	зачет
6.	Раздел 6 Основные правила поведения сетевого взаимодействия	4	2	2	опрос
7.	Раздел 7 Государственная политика в области в области защиты информации	4	2	2	опрос
8.	Раздел 8 Промежуточная и итоговая аттестация	4	-	4	зачет
	Итого	72	42	30	

2.2.СОДЕРЖАНИЕ РАЗДЕЛОВ ПРОГРАММЫ

Раздел 1. Информация, компьютер и Интернет.

Тема 1.1. Что такое информация, компьютер и Интернет.

Теория. Компьютер - как он появился, как появился Интернет. Почему компьютер нужно беречь. Где и как искать информацию для урока. Интернет - средство для поиска полезной информации. Как защитить себя от информационной перегрузки. Что такое файл. Как обращаться со своими и чужими файлами, чтобы их не потерять. Какие файлы можно скачивать, а какие нельзя. Полезные и вредные страницы Интернета. Как отличать полезную и правдивую информацию. Ненужные ссылки, ложные ссылки,

реклама. Что такое вредоносные сайты. К чему ведет переход по вредоносным ссылкам. Опасная информация в сети. Возьми с собой электронного помощника. Мобильные устройства. Польза и опасности мобильной связи, Общение в Интернете - переписка, форумы, социальные сети. Совместные игры в Интернете. Обмен данными при совместной работе - скайп, IP-телефония, ICQ. Безопасный обмен данными. На каких устройствах можно сохранить информацию и как с ними правильно обращаться (диски, флэш, карты и пр.). Как работать в группе. Как передать товарищам результаты работы и не повредить их компьютерам. Что такое электронная почта

Практика. Практическая работа №1. Работа с мобильными устройствами (2 ГИС, Госуслуги, Википедия, эл.книги, фотоколлаж, Компас, диктофон, Калькулятор и пр.).
Практическая работа №2. Создание электронной почты

Форма контроля: опрос.

Раздел 2. Техника безопасности и экология

Тема 2.1. Техника безопасности и экология

Теория. Гигиена при работе с компьютером. Правила работы с ПК, электронными книгами и мобильными устройствами. Сколько времени можно проводить за компьютером. Как правильно сидеть за компьютером. Как защитить компьютер от повреждений, Компьютеру тоже нужна забота, Компьютер и среда обитания (растения, животные, другие члены семьи). Везде ли есть Интернет? Может ли компьютер заменить компас. Как мобильные устройства помогают ориентироваться на местности. Воздействие компьютера на зрение и др. органы. Физическое и психическое здоровье. Польза и вред компьютерных игр. Компьютер и недостаток движения. Что делать с компьютером в чрезвычайных ситуациях. Улица и мобильные устройства. Компьютер (мобильные устройства) в грозу.

Практика. Практическая работа №1. Создание буклетов по темам: -«Как может помочь компьютер в сложных чрезвычайных ситуациях» - «Правила поведения на улице с мобильными устройствами» - «Компьютеру тоже нужна забота» (как ухаживать за ПК и мобильными устройствами)

Форма контроля: зачет

Раздел 3. Мир виртуальный и реальный.

Тема 3.1. Интернет зависимость

Теория. Что такое Интернет-сообщество. Как не превратить свою жизнь в виртуальную? Социальные сети. Детские социальные сети. Какую информацию о себе следует выкладывать в сеть? Какая информация принадлежит вам? Не слишком ли много у вас друзей в социальной сети? Если слишком долго находиться в Интернете: что такое интернет-зависимость? Виртуальная личность - что это такое. Сайты знакомств. Незнакомцы в Интернете. Превращение виртуальных знакомых в реальных. Развлечения в Интернете. Игры полезные и вредные. Признаки игровой зависимости

Практика. Практическая работа №1. Создание сообщества класса в детских социальных сетях
Практическая работа №2. Тест «Есть у меня игровая зависимость». Квест «Я умею говорить: «Нет» в сети интернет»

Форма контроля: зачет

Раздел 4. Методы безопасной работы в Интернете

Тема 4.1. Методы безопасной работы в Интернете

Теория. Ищите в Интернете только то, что вам требуется. Как защититься от вредного контента. Что такое контент-фильтры, движение в Интернете (серфинг). Знаки Интернета, рассказывающие об опасной информации. Правильно ли работает

компьютер? Признаки работы вирусов. Вирусы и антивирусы. Обновление баз. Что такое электронные деньги, как с ними правильно обращаться. Почему родители проверяют, что ты делаешь в Интернете?

Практика. Практическая работа №1. Исследовательская работа «Колобанга в поисках вируса» (выявление признаков заражения вирусом).

Форма контроля: опрос.

Раздел 5. Потребительские опасности в Интернете

Тема 5.1. Потребительские опасности в Интернете

Теория. Интернет и экономика - польза и опасность. Кто и как может навредить в Интернете. Электронная торговля - ее опасности. Поиск информации: если у вас требуют личную информацию при скачивании данных. Что такое личная информация. Если вам сообщают о выигрыше в лотерею. Если вам предлагают установить новое приложение. Сколько стоят ошибки в интернете.

Практика. Практическая работа №1. Прохождение интерактивного курса. «Мошеннические действия в Интернете. Киберпреступления». Практическая работа №2. Квест «Покупка в интернет-магазине».

Форма контроля: зачет

Раздел 6. Основные правила поведения сетевого взаимодействия

Тема 6.1. Основные правила поведения сетевого взаимодействия

Теория. Что такое интернет-этикет. Как вести себя в гостях у «сетевых» друзей.

Практика. Практическая работа №1. «Пишу письмо другу»

Форма контроля: опрос.

Раздел 7. Государственная политика в области защиты информации

Тема 7.1. Государственная политика в области защиты информации

Теория. Как государство защищает киберпространство. Войны нашего времени. Что такое кибервойна. Почему государство защищает информацию. Защита государства и защита киберпространства.

Практика. Практическая работа №1 Квест «Война миров»

Форма контроля: опрос.

Раздел 8. Промежуточная и итоговая аттестация.

Форма контроля: зачет

2.3. Календарный учебный график

Группа	Дата начала реализации программы	Дата окончания реализации программы	Кол-во учебных недель	Кол-во учебных часов	Кол-во часов в каникулярное время	Последовательность реализации содержания учебного плана	
						Разделы первого полугодия	Разделы второго полугодия
1	2026	2027	72	72	4	Раздел 1 Информация, компьютер и Интернет. Раздел 2	Раздел 5 Потребительские опасности в Интернете Раздел 6

						Техника безопасности и экология Раздел 3 Мир виртуальный и реальный. Интернет зависимость Раздел 4 Методы безопасной работы в Интернете Раздел 8 Промежуточная и итоговая аттестация	Основные правила поведения сетевого взаимодействия Раздел 7 Государственная политика в области в области защиты информации Раздел 8 Промежуточная и итоговая аттестация
--	--	--	--	--	--	---	---

III. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ И ФОРМЫ АТТЕСТАЦИИ

(формы аттестации, оценочные и методические материалы, иные компоненты)

3.1. Методическое обеспечение программы:

В ходе реализации программы возможно использование различных методов и приёмов организации занятий:

- по источнику получения информации - практический (опыты, упражнения); наглядный (иллюстрация, демонстрация, наблюдения обучающихся); словесный (объяснение, разъяснение, рассказ, беседа, инструктаж, лекция, дискуссия, диспут); работа с книгой (чтение, изучение, реферирование, цитирование, беглый просмотр, конспектирование); идеометод (просмотр, обучение, упражнение, контроль);
- по характеру дидактической цели - приобретение знаний; формирование умений и навыков; применение знаний; формирование творческой деятельности; закрепление и контроль знаний, умений, навыков;
- по характеру познавательной деятельности - поисковые; объяснительно-иллюстративные; репродуктивные; проблемного изложения; эвристические (частично-поисковые); исследовательские;
- по соответствию методов обучения логике общественно-исторического познания - организация наблюдения, накопление эмпирического материала; обобщение теоретической обработки фактических данных; практическая проверка правильности выводов и обобщений, выявление истины, соответствия содержания и формы, явления и сущности;
- по соответствию методов обучения специфике изучаемого материала и форм мышления - научного познания реальной действительности; освоения искусства; практического применения знаний.

Все эти методы и приёмы направлены на стимулирование познавательного интереса обучающихся и формирование творческих учений и навыков. При проектировании

занятий необходимо придерживаться следующих принципов системно-деятельностного подхода: 22 принцип активной включенности школьников в освоение предлагаемой информации; принцип деятельности; принцип доступности; принцип системности; принцип рефлексивности; принцип мотивации; принцип открытости содержания образования. Принцип активной включенности обучающихся в освоение предлагаемой информации предполагает субъектную позицию школьника в образовательном процессе, обращение педагога к личностному опыту учащегося и обогащение его в процессе деятельности на занятии. Важной составляющей в этом случае является создание для школьников условий транслирования информации, полученной в ходе занятий, в принципы собственной жизнедеятельности. Введение деятельностных технологий в обучающий процесс предполагает учет следующих критериев: интерактивность; игровой, театрализованный контекст; совместную деятельность ребенка и взрослого; учет психолого-возрастных особенностей школьников; использование социокультурных технологий. Принцип доступности предполагает адекватность содержания и подачи предлагаемого материала применительно к возрастным и психологическим особенностям школьников, а также имеющемуся у них социальному опыту. Принцип системности позволяет целостно представить учащимся как положительные, так и отрицательные стороны использования сети интернет. Принцип рефлексивности предполагает организацию самостоятельной познавательной деятельности школьников на всех этапах занятий с целью вовлечения их в процесс осмысления полученной информации, соотнесения ее с имеющимся личным социальным опытом и включения приобретенного нового содержания и способов деятельности в собственную практику. Принцип мотивации. Проектировать занятие таким образом, чтобы мотивировать школьников на самостоятельный поиск новой информации относительно использования инфокоммуникационных технологий в познавательных и развивающих целях, стимулировать их творческие и познавательные мотивационные потребности. Использовать средства побуждающего и формирующего воздействия. Эти средства необходимо применять так, чтобы они способствовали развитию различных компонентов и сторон мотивации в их единстве. Поэтому они должны применяться в комплексе, включающем приемы побуждения: и за счет стимулирующего влияния содержания учебного материала, и за счет побуждающей функции методов обучения, и за счет сочетания различных видов деятельности. Все это в совокупности обеспечит 23 динамику развития положительных потребностно-мотивационных состояний учащихся в соответствии со структурой мотивационной основы деятельности. Принцип открытости содержания образования предполагает достаточно гибкое использование педагогом предложенной конструкции, не допуская при этом искажения логики, содержательной точности и достоверности информации.

3.2. Условия реализации программы

Материально-техническое обеспечение реализации дополнительной общеобразовательной программы «Безопасность в сети Интернет» включает следующий перечень необходимого оборудования:

1. Компьютер;
2. Мультимедийный проектор.
3. Доступ к сети Интернет

Кадровое обеспечение:

Требования к образованию ПДО:

- Среднее профессиональное образование;
- Высшее образование (бакалавриат), профиль должен соответствовать направленности ДОП;
- Дополнительное профессиональное образование – профессиональная переподготовка;
- Дополнительное профессиональное педагогическое образования (м.б. освоена после трудоустройства).

3.3.Список литературы

1. Бирюков А.А. Информационная безопасность защита и нападение 2 е издание: Издательство: ДМК-Пресс., 2017, 434 с. 2.
2. Бирюков А.А. Информационная безопасность защита и нападение.: Издательство: ДМК-Пресс., 2012, 474 с. 3.
3. Колесниченко Денис. Анонимность и безопасность в интернете. От чайника к пользователю. Самоучитель Издательство: БХВ-Петербург, 2012, 240с. 45 4.
4. Мазаник Сергей. Безопасность компьютера. Защита от сбоев, вирусов и неисправностей: издательство: ЭКСМО, 2014, 256 с. 5.
5. Мэйволд Э. Безопасность сетей (2-е изд.) Книги» Сетевые Технологии. Название: Безопасностьсетей: Издательство: М.: НОУ "Интуит", 2016,571 с. 6.
6. Платонов В.В. Программноаппаратные средства защитыинформации: учебник для студ. Учрежд.вышш. проф. образования / В. В.Платонов. — М.: Издательский центр «Академия», 2013, 336 с. 7.
7. Проскурин В.Г Защита в операционных системах: Издательство: Горячая линия-Телеком, 2014, 192 с. 8.
8. Савченко Е. Кто, как и зачем следит за вами через интернет: Москва - Третий Рим, 2012, 100 с. 9.
9. Яковлев В.А. Шпионские и антишпионские штучки: Техническая литература Издательство: Наука и Техника, 2015, 320 с. Дополнительная: 1. "Березовый лес" или "лес березовый" /П. Лауфер//Юный эрудит. - 2014. - № 3. - С. 24-26 2.
10. Доценко С.М., Шпак В.Ф. Комплексная информационная безопасность объекта. От теории к практике, Издательство: ООО «Издательство Полигон», 2000, 215 с. 3.
11. Клепа и железный друг//Клепа. - 2014. - № 8. - С. 1-33.Электронная версия журнала: <http://klepa.ru>. 4. Методическое пособие для работников системы общего образования Солдатов Г., Зотова Е., Лебешева М., Шляпников В. «Интернет: возможности, компетенции, безопасность», 2015 - 156с. 5.
12. Сорокина Е.В., Третьяк Т.М. Здоровье и безопасность детей в мире компьютерных технологий и Интернет. [Текст] Учебно-методический комплект. - М.: СОЛОНПРЕСС, 2010. - 176 с.: ил 6.
13. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. Краткий курс. - Феникс, 2

Индивидуальный учебный план группы 1

Дата		Количество часов			Тема	Форма контроля
По плану	По факту	Всего	Теор.	Практ.		
1 неделя		2	2	-	Что такое информация?	беседа
2 неделя		2	-	2	Практическая работа №1. Поиск информации в сети Интернет.	Практическая работа
3 неделя		2	2	-	Что такое компьютер?	беседа
4 неделя		2	-	2	Практическая работа №2. Работа с мобильными устройствами (2 ГИС, Госуслуги, Википедия, эл.книги, фотоколлаж, Компас, диктофон, Калькулятор и пр.).	Практическая работа
5 неделя		2	2	-	Что такое файл?	беседа
6 неделя		2	2	-	Что такое интернет?	опрос
7 неделя		2	2	-	Что такое электронная почта?	беседа
8 неделя		2	-	2	Практическая работа №3. Создание электронной почты	Практическая работа
9 неделя		2	2	-	Безопасный обмен данными.	беседа
10 неделя		2	2	-	Гигиена при работе с компьютером.	беседа
11 неделя		2	2	-	Как защитить компьютер от повреждений?	опрос
12 неделя		2	-	2	Практическая работа №1. Создание буклета по теме: -«Как может помочь компьютер в сложных чрезвычайных ситуациях»	Практическая работа
13 неделя		2	2	2	Везде ли есть Интернет?	Беседа
14 неделя		2	2	-	Практическая работа №2. Создание буклета по теме: - «Правила поведения на улице с мобильными устройствами»	Практическая работа

15 неделя		2	0	2	Промежуточная аттестация.	Зачет
16 неделя		2	2	-	Польза и вред компьютерных игр.	беседа
17 неделя		2	-	2	Практическая работа №3. Создание буклетов по темам: «Компьютеру тоже нужна забота» (как ухаживать за ПК и мобильными устройствами)	Практическая работа
18 неделя		2	2	-	Компьютер (мобильные устройства) в грозу.	Беседа
19 неделя		2	2	-	Что такое Интернет-сообщество?	опрос
20 неделя		2	-	2	Практическая работа №1. Создание сообщества класса в детских социальных сетях	Практическая работа
21 неделя		2	2	-	Социальные сети. Детские социальные сети.	Беседа
22 неделя		2	2	-	Что такое интернет-зависимость?	Опрос
23 неделя		2	-	2	Практическая работа №2. Тест «Есть у меня игровая зависимость».	Практическая работа
24 неделя		2	2	-	Как защититься от вредного контента.	Опрос
25 неделя		2	2	-	Знаки Интернета, рассказывающие об опасной информации.	Беседа
26 неделя		2	-	2	Практическая работа №1. Исследовательская работа «Колобанга в поисках вируса» (выявление признаков заражения вирусом)	Практическая работа
27 неделя		2	2	-	Признаки работы вирусов	Опрос
28 неделя		2	-	2	Практическая работа №2. Создание презентации на тему: «Разновидности вирусов. Черви, трояны, скрипты»	Практическая работа
29 неделя		2	2	-	Интернет и экономика - польза и опасность.	Беседа
30 неделя		2	2	0	Электронная торговля - ее опасности.	Беседе
31 неделя		2	-	2	Практическая работа №1. Квест «Покупка в интернет-магазине»	Практическая работа
32 неделя		0	0	0	Что такое личная информация.	Опрос
33 неделя		2	2	-	Что такое интернет-этикет. Практическая работа №1. «Пишу письмо другу	Практическая работа

34 неделя		2	1	1	Итоговая аттестация	Зачет
35 неделя		2	-	2	Что такое кибервойна. Практическая работа №1 Квест «Война миров»	Практическая работа
36 неделя		2	1	1	Что такое вредоносные сайты?	Беседа
Итого		72				

Контрольно-измерительный материал

Тест №1 «Кибергигиена»

Вопрос №1

Какую информацию нельзя разглашать в Интернете?

- а) свои увлечения
- б) свой псевдоним
- в) домашний адрес

Вопрос №2

Какие данные из нижеперечисленных можно сообщать по электронной почте?

- а) номера банковских карт твоих родителей
- б) секретные слова (ответы) на специальные секретные вопросы, используемые при идентификации вашего аккаунта
- в) свои имя и фамилию

Вопрос №3

Что такое СПАМ:

- а) агрессивное поведение на форумах
- б) массовая рассылка рекламы и прочих объявлений
- в) цепочка непонятных, нелогичных объяснений

Вопрос №4

Что НЕ поможет защитить твою электронную почту от взлома?

- а) создавать разные надежные пароли от своих аккаунтов
- б) не открывать сообщения с незнакомых и подозрительных адресов
- в) сказать свой пароль родителям

Вопрос №5

В сети вы встретились с дразнилками и оскорблениями, вы:

- а) ответите грубостью
- б) заблокируете этого человека и сообщите родителям
- в) никому об этом не говорите

Вопрос №6

Когда можно доверять письму от неизвестного отправителя?

- а) отправитель ссылается на твоих друзей
- б) к тебе обращаются по имени
- в) никогда нельзя доверять письму от неизвестного отправителя

Вопрос №7

Какой из предложенных паролей лучше выбрать для своей электронной почты?

- а) дата рождения
- б) s_7_NR32a
- в) 123456

Вопрос №8

Тебе на электронную почту пришло письмо от незнакомого человека, представившегося знакомым твоей мамы, в котором он просит пройти по ссылке и проголосовать за его проект. Что ты сделаешь?

- а) пройду по ссылке и посмотрю, что за проект
- б) напишу в ответ письмо и спрошу, откуда он знает мою маму

6

- в) удалю письмо. Я ничего не знаю об этом сайте и авторе письма. Скорее всего, это спам

Вопрос №9

Как можно хранить пароль?

- а) написать на листочке и приклеить на монитор
- б) только в памяти (в своей голове)
- в) сохранить в браузере

Вопрос №10

Какое правило безопасного поведения в сети Интернет позволит уберечь себя от вирусов?

- а) не скачивай и не открывай неизвестные тебе или присланные незнакомцами файлы из Интернета
- б) не добавляй незнакомых людей в свои контакты
- в) общаясь в Интернете, будь дружелюбен. Не пиши грубых слов!

Вопрос №11

Как гарантировать 100% защищенность компьютера от заражения вирусами в сети?

- а) установить новое программное обеспечение
- б) таких гарантий нет
- в) посещать только известные сайты

Вопрос №12

Вам пришло письмо: «Чтобы выиграть миллион в нашей лотерее, вам нужно зарегистрироваться на этом сайте (ссылка на сайт). Регистрация закрывается завтра. Не пропустите!». Что вы сделаете?

- а) зайду на сайт и посмотрю, что за лотерея

7

- б) напишу в ответ письмо, где попрошу прислать подробности о лотерее
- в) удалю письмо. Я ничего не знаю об этом сайте и авторе письма. Скорее всего, это спам

Вопрос №13

Что такое Компьютерный вирус?

- а) безобидный червячок
- б) компьютерная программа, нарушающая работу других программ
- в) компьютерный герой-шпион

Вопрос №14

При установке приложения обработки фотографий на смартфон приложении просит доступ к СМС-сообщениям и телефонной книге. Согласиться или нет?

- а) согласиться, поскольку это безопасно
- б) не согласиться, поскольку это небезопасно

Вопрос №15

Что не является персональными данными?

- а) фамилия, имя, отчество
- б) история болезни
- в) дата и место рождения

Тест №2 «Кибергигиена»

Вопрос №1

Ваш друг в социальной сети написал следующее сообщение: "у меня горе помощи, реквизиты на стене". Что Вы будете делать?

- а) отправлю деньги другу
- б) уточню, что случилось и нужна ли помощь не через социальную сеть.
- в) не буду отправлять деньги другу

8

Вопрос №2

Интернет – это...

- а) всемирная компьютерная сеть, соединяющая вместе тысячи сетей.
- б) персональный компьютер
- в) браузер

Вопрос №3

Как называется детский Браузер?

- а) Internet Explorer
- б) Гугуль
- в) Mozilla Firefox

Вопрос №4

Сетевой этикет – это...

- а) правила поведения за столом
- б) правила поведения в обществе
- в) нравственные правила поведения в компьютерных сетях.

Вопрос №5

Что делать, если вы стали жертвой интернет-травли?

- а) Выкинуть компьютер
- б) Ничего не делать, терпеть
- в) Обратиться в администрацию ресурса с просьбой наказать обидчика

Вопрос №6

Что такое Антивирусная программа?

- а) комплекс мероприятий, направленных на обеспечение информационной безопасности

б) любая программа для обнаружения компьютерных вирусов, а также нежелательных программ и восстановления зараженных такими программами файлов

в) мошенники в сети Интернет

Вопрос №7

Нужно ли в интернете всем сообщать свою фамилию, имя, адрес, номер школы?

а) всем виртуальным друзьям нужно рассказать о себе

б) никогда не сообщать личную информацию

в) сообщать только вымышленную информацию

Вопрос №8

Что такое НИК?

а) вымышленное виртуальное имя

б) компьютерная программа

в) компьютерный герой

Вопрос №9

Виртуальный друг предлагает встретиться, ваши действия?

а) встретиться с виртуальным другом в торговом центре

б) сообщить родителям об этом

в) встретиться с виртуальным другом в заброшенном, таинственном месте

Вопрос №10

На вашу электронную почту пришло письмо от неизвестного адресата, вы:

а) сохраните в черновики и откроете позднее

б) откроете немедленно

10

в) некогда не открываете писем от неизвестных адресатов

Вопрос №11

Сколько времени детям, по мнению специалистов, можно проводить за компьютером?

а) пока не выиграешь в любимую игрушку

б) пока не подготовишься к урокам

в) не более часа в день

Вопрос №12

Укажи устройство для подключения компьютера к сети:

а) модем

б) монитор

в) сканер

Вопрос №13

Можно ли отправлять SMS или оставлять свой номер телефона с незнакомого сайта, чтобы получить код доступа к игре или подарку?

а) никогда не следует отправлять SMS или давать свой номер телефона

б) всегда оставлять номер телефона, а SMS слать нельзя

в) всегда отправлять сообщение и давать номер, чтобы получить код доступа

Вопрос №14

Что такое информация?

а) – это компьютерная программа, для чтения книг

б) – это, прежде всего, предоставление каких-либо знаний или фактов о чемлибо

в) – это общение в интернете

11

Вопрос №15

Социальная сеть – это...

а) место, где можно общаться с друзьями и знакомыми, слушать музыку и смотреть фильмы

б) поисковая система

в) интернет-сервис для поиска материалов для реферата

Ответы:

Тест №1

B1	B2	B3	B4	B5	B6	B7	B8	B9	B10
<i>в</i>	<i>в</i>	<i>б</i>	<i>в</i>	<i>б</i>	<i>в</i>	<i>б</i>	<i>в</i>	<i>б</i>	<i>а</i>
B11	B12	B13	B14	B15					
<i>б</i>	<i>в</i>	<i>б</i>	<i>б</i>	<i>а</i>					

Тест №2

B1	B2	B3	B4	B5	B6	B7	B8	B9	B10
<i>б</i>	<i>а</i>	<i>б</i>	<i>в</i>	<i>в</i>	<i>б</i>	<i>б</i>	<i>а</i>	<i>б</i>	<i>в</i>
B11	B12	B13	B14	B15					
<i>в</i>	<i>а</i>	<i>а</i>	<i>б</i>	<i>а</i>					

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат 312785006653143968851816314299382482766709872294

Владелец Антипов Ярослав Юрьевич

Действителен с 06.08.2026 по 06.08.2027