**МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**
**Министерство образования и наука Забайкальского края**
**Городской округ «Город Чита»**
**Муниципальное бюджетное общеобразовательное учреждение**
**«Средняя общеобразовательная школа №55» города Читы**

| РАССМОТРЕНО | СОГЛАСОВАНО | УТВЕРЖДЕНО |
|---|---|---|
| Методическим объединением | Педагогическим советом | Директором |
| Рогалева Е.Н.<br>Протокол №1<br>от 30.08.2023 г. | Багаева Ю.А.<br>Протокол № 2/пс/2023<br>от 31.08.2023 г. | Перунова Г.В.<br>Приказ №16/од/2023<br>от 31.08.2023 |

# РАБОЧАЯ ПРОГРАММА

**учебного курса**

**«Компьютерная и информационная безопасность»**

для обучающихся 10-11 классов
(технологический (информационный) профиль)

**Чита, 2023**

# ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Инфобезопасность является важной частью Цифровой грамотности детей, как социальная цифровая грамотность, наряду с жизненной (пользовательской) цифровой грамотностью и профильной цифровой грамотностью в сфере будущих профессиональных интересов детей для выбора профессии (как внеурочная цифровая деятельность в предметах, в межпредметной практике и в обучении информатике профильном обучении). Цифровая грамотность, включая пользовательскую, профильную и социальную, полученную в школах. Это гарант готовности выпускника школы к цифровому миру, цифровизации профессий в нем и предназначена для обучающихся 10 класса рассчитана на 1 год обучения.

Курс «Информационная безопасность» («Цифровая гигиена») является важной составляющей работы с обучающимися, активно использующими различные сетевые формы общения (социальные сети, игры, пр.) с целью мотивации ответственного отношения к обеспечению своей личной безопасности, безопасности своей семьи и своих друзей.

Отбор тематики содержания курса осуществлен с учетом целей и задач ФГОС среднего общего образования, возрастных особенностей и познавательных возможностей обучающихся 10 класса.

В преподавании курса «Информационная безопасность» («Цифровая гигиена») могут использоваться разнообразные форматы обучения: традиционный урок (коллективная и групповая формы работы), тренинги (в классической форме или по кейс-методу), дистанционное обучение (электронные курсы, видеоролики, почтовые рассылки, микрообучение), смешанный формат.

Основными целями изучения курса «Информационная безопасность» являются:

- ✓ обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз;
- ✓ формирование навыков своевременного распознавания онлайн-рисков (технического, контентного, коммуникационного, потребительского характера и риска интернет-зависимости).

Задачи программы:

- ✓ сформировать общекультурные навыки работы с информацией (умения, связанные с поиском, пониманием, организацией, архивированием цифровой информации и ее критическим осмыслением, а также с созданием информационных объектов с использованием цифровых ресурсов (текстовых, изобразительных, аудио и видео);
- ✓ создать условия для формирования умений, необходимых для различных форм коммуникации (электронная почта, чаты, блоги, форумы, социальные сети и др.) с различными целями и ответственного отношения к взаимодействию в современной информационно-телекоммуникационной среде;
- ✓ сформировать знания, позволяющие эффективно и безопасно использовать технические и программные средства для решения различных задач, в том числе использования компьютерных сетей, облачных сервисов и т.п.;
- ✓ сформировать знания, умения, мотивацию и ответственность, позволяющие решать с помощью цифровых устройств и интернета различные повседневные задачи, связанные с конкретными жизненными ситуациями, предполагающими удовлетворение различных потребностей;
- ✓ сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом.

Цели и задачи учебного предмета соответствуют целям и задачам воспитания в школе. Содержание учебного предмета способствует развитию ключевых компетенций учеников, указанных в рабочей программе воспитания.

Методы обучения и оценки знаний учитывают индивидуальные особенности учащихся и способствуют формированию ценностных ориентаций, предусмотренных в рабочей программе воспитания.

На изучение факультативного курса «Компьютерная и информационная безопасность» в 10 классе отводится 34 часа (1 час в неделю).

# СОДЕРЖАНИЕ ОБУЧЕНИЯ

## 10 КЛАСС

Содержание программы курса внеурочной деятельности «Информационная безопасность» («Цифровая гигиена») соответствует темам основной образовательной программы среднего общего образования по учебным предметам «Информатика» и «Основы безопасности жизнедеятельности». А также расширяет их за счет привлечения жизненного опыта обучающихся в использовании всевозможных технических устройств (персональных компьютеров, планшетов, смартфонов и пр.), позволяет правильно ввести ребенка в цифровое пространство и корректировать его поведение в виртуальном мире.

Основное содержание программы представлено разделами «Безопасность общения», «Безопасность устройств», «Безопасность информации». Каждый раздел курса внеурочной деятельности завершается выполнением творческой работы по одной из тем раздела и проверочного теста.

**Раздел 1. «Безопасность общения»**

*Тема 1. Общение в социальных сетях и мессенджерах.*

Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.

*Тема 2. С кем безопасно общаться в интернете.*

Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.

*Тема 3. Пароли для аккаунтов социальных сетей.*

Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.

*Тема 4. Безопасный вход в аккаунты.*

Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

*Тема 5. Настройки конфиденциальности в социальных сетях.*

Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.

*Тема 6. Публикация информации в социальных сетях.*

Персональные данные. Публикация личной информации.

*Тема 7. Кибербуллинг.*.

Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.

*Тема 8. Публичные аккаунты.*

Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.

*Тема 9. Фишинг.*

Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.

**Раздел 2. «Безопасность устройств»**

*Тема 1. Что такое вредоносный код.*

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

*Тема 2. Распространение вредоносного кода.*

Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.

*Тема 3. Методы защиты от вредоносных программ.*

Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.

*Тема 4. Распространение вредоносного кода для мобильных устройств.*

Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.

**Раздел 3 «Безопасность информации»**

*Тема 1. Социальная инженерия: распознать и избежать.*

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

*Тема 2. Ложная информация в Интернете.*

Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.

*Тема 3. Безопасность при использовании платежных карт в Интернете.*

Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.

*Тема 4. Беспроводная технология связи.*

Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.

*Тема 5. Резервное копирование данных.*

Безопасность личной информации. Создание резервных копий на различных устройствах.

*Тема 6. Основы государственной политики в области формирования культуры информационной безопасности.*

Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.

**Повторение, резерв. 3 часа.**

# ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ УЧЕБНОГО КУРСА «КОМПЬЮТЕРНАЯ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» НА УРОВНЕ СРЕДНЕГО ОБЩЕГО ОБРАЗОВАНИЯ

***Предметные***

*Ученик научится:*

- ✓ анализировать доменные имена компьютеров и адреса документов в интернете;
- ✓ безопасно использовать средства коммуникации,
- ✓ безопасно вести и применять способы самозащиты при попытке мошенничества,
- ✓ безопасно использовать ресурсы интернета.

*Ученик овладеет:*

✓ приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.

*Обучающийсяк получит возможность овладеть:*

- ✓ основами соблюдения норм информационной этики и права;
- ✓ основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности жизнедеятельности;
- ✓ использовать для решения коммуникативных задач в области безопасности жизнедеятельности различные источники информации, включая Интернет-ресурсы и другие базы данных. соблюдать нормы информационной этики и права.

***Метапредметные***

*Регулятивные универсальные учебные действия*.

В результате освоения учебного курса обучающийся сможет:

- ✓ идентифицировать собственные проблемы и определять главную проблему;
- ✓ выдвигать версии решения проблемы, формулировать гипотезы, предвосхищать конечный результат;
- ✓ ставить цель деятельности на основе определенной проблемы и существующих возможностей;
- ✓ выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели;
- ✓ составлять план решения проблемы (выполнения проекта, проведения исследования);
- ✓ описывать свой опыт, оформляя его для передачи другим людям в виде технологии решения практических задач определенного класса;
- ✓ оценивать свою деятельность, аргументируя причины достижения или отсутствия планируемого результата;
- ✓ находить достаточные средства для выполнения учебных действий в изменяющейся ситуации и/или при отсутствии планируемого результата;
- ✓ работая по своему плану, вносить коррективы в текущую деятельность на основе анализа изменений ситуации для получения запланированных характеристик продукта/результата;
- ✓ принимать решение в учебной ситуации и нести за него ответственность.

*Познавательные универсальные учебные действия.*

В результате освоения учебного курса обучающийся сможет:

- ✓ выделять явление из общего ряда других явлений;
- ✓ определять обстоятельства, которые предшествовали возникновению связи между явлениями, из этих обстоятельств выделять определяющие, способные быть причиной данного явления, выявлять причины и следствия явлений;
- ✓ строить рассуждение от общих закономерностей к частным явлениям и от частных явлений к общим закономерностям;
- ✓ излагать полученную информацию, интерпретируя ее в контексте решаемой задачи;
- ✓ самостоятельно указывать на информацию, нуждающуюся в проверке, предлагать и применять способ проверки достоверности информации;
- ✓ критически оценивать содержание и форму текста;
- ✓ определять необходимые ключевые поисковые слова и запросы.

*Коммуникативные универсальные учебные действия.*

В результате освоения учебного курса обучающийся сможет:

- ✓ строить позитивные отношения в процессе учебной и познавательной деятельности;
- ✓ критически относиться к собственному мнению, с достоинством признавать ошибочность своего мнения (если оно таково) и корректировать его;
- ✓ договариваться о правилах и вопросах для обсуждения в соответствии с поставленной перед группой задачей;
- ✓ делать оценочный вывод о достижении цели коммуникации непосредственно после завершения коммуникативного контакта и обосновывать его.
- ✓ целенаправленно искать и использовать информационные ресурсы, необходимые для решения учебных и практических задач с помощью средств ИКТ;
- ✓ выбирать, строить и использовать адекватную информационную модель для передачи своих мыслей средствами естественных и формальных языков в соответствии с условиями коммуникации;
- ✓ использовать компьютерные технологии (включая выбор адекватных задаче инструментальных программно-аппаратных средств и сервисов) для решения информационных и коммуникационных учебных задач, в том числе: вычисление, написание писем, сочинений, докладов, рефератов, создание презентаций и др.;
- ✓ использовать информацию с учетом этических и правовых норм;
- ✓ создавать информационные ресурсы разного типа и для разных аудиторий, соблюдать информационную гигиену и правила информационной безопасности.

***Личностные***

- ✓ осознанное, уважительное и доброжелательное отношение к окружающим людям в реальном и виртуальном мире, их позициям, взглядам, готовность вести диалог с другими людьми, обоснованно осуществлять выбор виртуальных собеседников;
- ✓ готовность и способность к осознанному выбору и построению дальнейшей индивидуальной траектории образования на базе ориентировки в мире профессий и профессиональных предпочтений, с учетом устойчивых познавательных интересов;
- ✓ освоенность социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах;
- ✓ сформированность понимания ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

## ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

### 10 КЛАСС

| № п/п | Наименование разделов и тем программы | Количество часов | | | Электронные образовательные ресурсы |
|---|---|---|---|---|---|
| | | Всего | Контрольные работы | Практические работы | |
| 1 | Безопасность общения | 13 | 1 | 4 | https://www.yaklass.ru/p/informatika |
| 2 | Безопасность устройств | 8 | 1 | 2 | https://www.yaklass.ru/p/informatika |
| 3 | Безопасность информации | 12 | 1 | 3 | https://www.yaklass.ru/p/informatika |
| 4 | Резерв | 3 | | | https://www.yaklass.ru/p/informatika |
| **ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ** | | **34** | **3** | **9** | |

**ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ**
**11 КЛАСС**

| № п/п | Наименование разделов и тем программы | Количество часов | | | Электронные образовательные ресурсы |
|---|---|---|---|---|---|
| | | Всего | Контрольные работы | Практические работы | |
| 1 | Принципы построения системы информационной безопасности | 13 | 1 | 4 | https://www.yaklass.ru/p/informatika |
| 2 | Организационно-техническое обеспечение компьютерной безопасности | 8 | 1 | 2 | https://www.yaklass.ru/p/informatika |
| 3 | Защита информации в Интернете | 12 | 1 | 3 | https://www.yaklass.ru/p/informatika |
| 4 | Резерв | 3 | | | https://www.yaklass.ru/p/informatika |
| **ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ** | | **34** | **3** | **9** | |

## ПОУРОЧНОЕ ПЛАНИРОВАНИЕ

**10 КЛАСС**

| № п/п | Тема урока | Количество часов | | | Дата изучения | Электронные образовательные ресурсы |
|---|---|---|---|---|---|---|
| | | Всего | Контрольные работы | Практические работы | | |
| 1 | Общение в социальных сетях и мессенджерах | 1 | | | 05.09.2023 | https://www.yaklass.ru/p/informatika |
| 2 | С кем безопасно общаться в интернете | 1 | | | 12.09.2023 | https://www.yaklass.ru/p/informatika |
| 3 | Пароли для аккаунтов социальных сетей | 1 | | | 19.09.2023 | https://www.yaklass.ru/p/informatika |
| 4 | Безопасный вход в аккаунты | 1 | | | 26.09.2023 | https://www.yaklass.ru/p/informatika |
| 5 | Настройки конфиденциальности в социальных сетях | 1 | | 1 | 03.10.2023 | https://www.yaklass.ru/p/informatika |
| 6 | Публикация информации в социальных сетях | 1 | | 1 | 10.10.2023 | https://www.yaklass.ru/p/informatika |
| 7 | Кибербуллинг | 1 | | | 17.10.2023 | https://www.yaklass.ru/p/informatika |

| | | | | | | |
|---|---|---|---|---|---|---|
| 8 | Публичные аккаунты | 1 | | | 24.10.2023 | https://www.yaklass.ru/p/informatika |
| 9 | Фишинг | 2 | | | 07.11.2023 | https://www.yaklass.ru/p/informatika |
| 10 | Выполнение творческой работы. | 3 | 1 | 2 | 14.11.2023 | https://www.yaklass.ru/p/informatika |
| 11 | Что такое вредоносный код | 1 | | | 21.11.2023 | https://www.yaklass.ru/p/informatika |
| 12 | Распространение вредоносного кода | 1 | | | 28.11.2023 | https://www.yaklass.ru/p/informatika |
| 13 | Методы защиты от вредоносных программ | 2 | | | 05.12.2023 | https://www.yaklass.ru/p/informatika |
| 14 | Распространение вредоносного кода для мобильных устройств | 1 | | | 12.12.2023 | https://www.yaklass.ru/p/informatika |
| 15 | Выполнение творческой практической работы. | 3 | 1 | 2 | 19.12.2023 | https://www.yaklass.ru/p/informatika |
| 16 | Социальная инженерия: распознать и избежать | 1 | | | 26.12.2023 | https://www.yaklass.ru/p/informatika |
| 17 | Ложная информация в Интернете | 1 | | | 16.01.2024 | https://www.yaklass.ru/p/informatika |
| 18 | Безопасность при использовании платежных карт в Интернете | 1 | | | 23.01.2024 | https://www.yaklass.ru/p/informatika |

| | | | | | | |
|---|---|---|---|---|---|---|
| 19 | Беспроводная технология связи | 1 | | | 30.01.2024 | https://www.yaklass.ru/p/informatika |
| 20 | Резервное копирование данных | 2 | | 1 | 06.02.2024 | https://www.yaklass.ru/p/informatika |
| 21 | Основы государственной политики в области формирования культуры информационной безопасности | 1 | | | 13.02.2024 | https://www.yaklass.ru/p/informatika |
| 22 | Выполнение творческой практической работы. | 3 | 1 | 2 | 20.02.2024 | https://www.yaklass.ru/p/informatika |
| 23 | Повторение, резерв | 3 | | | 27.02.2024 | https://www.yaklass.ru/p/informatika |
| ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ | | 34 | 3 | 9 | | |

## УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

## ОБЯЗАТЕЛЬНЫЕ УЧЕБНЫЕ МАТЕРИАЛЫ ДЛЯ УЧЕНИКА

нет

## МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ УЧИТЕЛЯ


- Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. - М.: ГЛТ, 2016. - 586 с
- Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. - Ст. Оскол: ТНТ, 2010. - 384 с.
- Жук, А.П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2013. - 392 с.
- Сергеева, Ю.С. Защита информации. Конспект лекций / Ю.С. Сергеева. - М.: А-Приор, 2011. - 128 с.
- Хорев, П.Б. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - М.: Форум, 2013. - 352 с.
- Чекалин Защита информации в системах мобильной связи / Чекалин и др. - М.: Горячая линия -Телеком, 2005. - 171 с.


## ЦИФРОВЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ И РЕСУРСЫ СЕТИ ИНТЕРНЕТ

- Единое содержание общего образования [https://edsoo.ru/constructor/]
- Российская электронная школа [https://resh.edu.ru/]

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат 726890861408610707646499642787991539916156533305

Владелец Перунова Галина Владимировна

Действителен С 19.02.2024 по 18.02.2025