

**Министерство труда и социальной политики Приморского края
краевое государственное автономное учреждение социального
обслуживания
«Комплексный центр помощи семье и детям «Содействие» г. Уссурийска»**

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 0091169853B6DAD0BFF10B2C6DA79DF189
Владелец: Жовниренко Игорь Анатольевич
Действителен: с 17.09.2026 до 11.12.2027

УТВЕРЖДАЮ
Директор КГАУСО «Комплексный центр
помощи семье и детям
«Содействие» г. Уссурийска»

_____ И.А. Жовниренко

«_____» _____ 2026 г.

РАБОЧАЯ ПРОГРАММА

«Информационная безопасность детей»



Уссурийск
2026 г.

Пояснительная записка

Наименование программы: рабочая программа «Информационная безопасность детей».

Направленность: социально-педагогическая, профилактическая.

Адресат: воспитанники КГАУСО «Комплексный центр помощи семье и детям «Содействие» г. Уссурийска».

Возраст обучающихся: 7–17 лет (с разбивкой на три возрастные группы).

Срок реализации: 1 учебный год (сентябрь — май), 36 учебных часов.

Нормативно-правовая база:

- Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации».
- Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
- Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы (утв. Указом Президента РФ от 09.05.2017 № 203).
- Концепция информационной безопасности детей Российской Федерации (утв. распоряжением Правительства РФ от 02.06.2021 № 1569-р).

Актуальность. Дети и подростки ежедневно пользуются интернетом, мобильной связью и цифровыми устройствами, однако уровень осознания рисков остаётся низким. Особенно уязвимы дети, находящиеся в трудной жизненной ситуации, воспитанники учреждений социального обслуживания и школьники отдалённых сельских территорий, где доступ к специалистам по цифровой безопасности ограничен. Программа направлена на формирование практических навыков безопасного поведения в цифровой среде и профилактику противоправных посягательств.

Отличительные особенности. Программа построена на принципе «от практики к осознанию»: каждая встреча включает разбор жизненных ситуаций, ролевые игры, работу с карточками-кейсами и создание личных алгоритмов действий. Учитывает сельскую специфику: ограниченный доступ к технике, нестабильный интернет, один компьютер на семью. Все материалы адаптированы для проведения в условиях минимального технического оснащения.

Цель: формирование у детей и подростков компетенций безопасного и ответственного поведения в информационно-телекоммуникационных сетях, навыков защиты от противоправных и иных общественно опасных посягательств.

Задачи:

1. **Обучающие:** познакомить с основными видами онлайн-угроз (мошенничество, фишинг, кибербуллинг, груминг, нежелательный контент); научить распознавать признаки опасных ситуаций; сформировать навыки защиты персональных данных и настройки приватности.
2. **Развивающие:** развить критическое мышление при оценке информации; сформировать привычку обращаться за помощью к взрослым; развить навыки самоконтроля при использовании цифровых устройств.
3. **Воспитательные:** воспитать ответственное отношение к цифровому следу и цифровой репутации; сформировать понимание правовой ответственности за действия в сети; воспитать культуру общения в интернет-среде.
4. **Профилактические:** профилактика кибервиктимности, вовлечения в деструктивные сообщества, интернет-зависимости; формирование алгоритма действий при столкновении с угрозой.

Принципы реализации:

- **Возрастная адекватность** — содержание и формы работы соответствуют возрасту, интересам и жизненному опыту участников.
- **Практикоориентированность** — не менее 60% времени каждой встречи отводится на практическую часть.
- **Безопасность среды** — запрет на обсуждение личных историй участников и демонстрацию реальных переписок; все примеры — обезличенные.
- **Опора на взрослых** — во всех алгоритмах действий закреплён шаг «рассказать надёжному взрослому».
- **Доступность** — материалы адаптированы для проведения при минимальном техническом оснащении (1 компьютер + проектор или даже без них).
- **Добровольность и конфиденциальность** — участие по желанию, личная информация участников не разглашается.

Структура содержания (модульный подход)

Программа состоит из 5 модулей. Каждый модуль проводится в трёх возрастных адаптациях (7–10, 11–13, 14–17 лет).

Модуль	Название	Кол-во часов	Краткое содержание
1	«Цифровой мир: правила входа»	6	Что такое интернет, как он работает, базовые правила безопасности, личные данные, понятие «цифровой след»
2	«Защита аккаунтов и приватности»	6	Пароли, настройки приватности в соцсетях и мессенджерах, геолокация, камеры, микрофоны
3	«Опасные контакты: распознаём угрозу»	8	Мошенничество, фишинг, груминг, деструктивные сообщества, признаки манипуляции, алгоритм действий
4	«Общение в сети: травля и её профилактика»	8	Кибербуллинг, роль свидетеля, ответственность за слова в сети, цифровая этика, эмоции и конфликты онлайн
5	«Ответственность, помощь, самоконтроль»	8	Правовые аспекты (клевета, угрозы, чужие фото), куда обращаться, телефоны доверия, баланс экранного времени, подведение итогов

Календарно - тематический план (36 часов)

Модуль 1. «Цифровой мир: правила входа» (6 часов)

№	Тема занятия	Возраст	Форма	Кол-во часов
1	Что такое интернет и как он работает	7–10	Беседа-игра	1
2	«Светофор ссылок»: какие ссылки безопасны	7–10	Игра-практикум	1
3	Личные данные: что нельзя рассказывать в сети	11–13	Разбор кейсов	1
4	Цифровой след: всё ли можно «удалить»	14–17	Дискуссия	1
5	Базовые правила: «5 шагов безопасности»	7–13	Создание памяток	1
6	Практикум «Найди ошибку» (итог модуля)	все	Квест-станции	1

Модуль 2. «Защита аккаунтов и приватности» (6 часов)

№	Тема занятия	Возраст	Форма	Кол-во часов
7	Надёжный пароль: как его придумать	11–13	Мастер-класс	1
8	Настройка приватности в соцсетях	14–17	Практикум (на проекторе)	1
9	Геолокация, камера, микрофон: кто следит	11–17	Беседа + чек-лист	1
10	«Один компьютер на всех»: безопасность при общем доступе	7–13	Беседа-практикум	1
11	Wi-Fi и мобильная связь: безопасное подключение	14–17	Мини-лекция	1
12	Практикум «Настрой свой профиль» (итог модуля)	все	Работа с чек-листами	1

Модуль 3. «Опасные контакты: распознаём угрозу» (8 часов)

№	Тема занятия	Возраст	Форма	Кол-во часов
13	Онлайн-мошенничество: признаки обмана	11–13	Разбор кейсов	1
14	Фишинг: поддельные сайты и письма	14–17	Практикум	1
15	«Выигрыш», «срочно», «секрет»: ловушки в сообщениях	7–10	Игра-сортировка	1
16	Груминг: кто такой «новый друг» и почему он «особенный»	14–17	Беседа-диалог	1
17	Деструктивные сообщества и группы «смерти»	14–17	Лекция-предупреждение	1
18	Незнакомцы в сети: алгоритм «остановись — спроси»	7–10	Ролевая игра	1
19	«Суд над мошенником» (итог модуля)	11–17	Деловая игра	1
20	Памятка «4 шага, если тебе угрожают в сети»	все	Создание памяток	1

Модуль 4. «Общение в сети: травля и её профилактика» (8 часов)

№	Тема занятия	Возраст	Форма	Кол-во часов
21	Что такое кибербуллинг и как он выглядит	11–13	Беседа + карточки	1
22	Роль свидетеля: почему молчание — это тоже участие	14–17	Дискуссия	1
23	«Шутка или травля?» — где граница	11–14	Разбор кейсов	1
24	Эмоции в сети: как реагировать на обидные слова	7–10	Ролевая игра	1
25	Цифровая этика: как общаться уважительно	11–17	Тренинг	1
26	«Как попросить о помощи и не бояться»	14–17	Тренинг	1
27	Создание комикса/постера «Стоп-	7–13	Творческая	1

	травля»		мастерская	
28	Итоговая викторина «Я в сети» (итог модуля)	все	Интерактивная викторина	1

Модуль 5. «Ответственность, помощь, самоконтроль» (8 часов)

№	Тема занятия	Возраст	Форма	Кол-во часов
29	Что считается правонарушением в сети	14–17	Лекция-диалог	1
30	Клевета, угрозы, чужие фото: ответственность	14–17	Разбор кейсов	1
31	Куда обращаться: телефоны, службы, взрослые	все	Создание «карты помощи»	1
32	Экранное время: сколько — слишком много	11–13	Дискуссия	1
33	Интернет-зависимость: признаки и что делать	14–17	Беседа-диалог	1
34	«Правила моего цифрового поведения»	все	Индивидуальная работа	1
35	Итоговый квест «Цифровой компас»	все	Квест по станциям	1
36	Подведение итогов. Награждение. Рефлексия	все	Праздник-презентация	1

Содержание модулей (детализация)

Модуль 1. «Цифровой мир: правила входа»

Для 7–10 лет:

- Что такое интернет простыми словами: «большая библиотека, где есть всё — и полезное, и опасное».
- Кто такой «автор сайта» и почему не все сайты добрые.
- Правило «Стоп — Подумай — Спроси взрослого».
- Личные данные: что это (имя, адрес, школа, телефон, фото) и почему их нельзя давать незнакомцам.
- Игра «Светофор ссылок»: карточки с ссылками сортируются на красные/жёлтые/зелёные.
- Создание «карточки безопасности» (адрес, телефон родителя, 112).

Для 11–13 лет:

- Как устроен интернет: серверы, поисковики, социальные сети — кратко и понятно.
- Личные данные и персональные данные (по закону № 152-ФЗ — в доступной форме).
- Цифровой след: что остаётся после тебя в сети. Примеры, как старые посты влияют на репутацию.
- Практикум «Что выложить, а что нет»: карточки с типами контента (фото дома, селфи в школьной форме с логотипом, номер телефона в описании профиля).
- 5 базовых правил: не вводить данные по чужой ссылке, не отправлять коды из SMS, не переходить по ссылкам от незнакомцев, не скачивать без разрешения, рассказывать взрослому.

Для 14–17 лет:

- Углублённое понимание цифрового следа: индексация поисковиками, архивы сайтов (Wayback Machine), скриншоты и пересылка.
- Репутационные риски: как цифровой след влияет на поступление, трудоустройство, личную жизнь.
- Проблема «удаления» данных: почему «удалить» не значит «исчезло».
- Дискуссия: «Стоит ли публиковать всё, что думаешь? Где граница свободы слова и ответственности?»
- Создание личного чек-листа «Перед публикацией задай себе 3 вопроса».

Модуль 2. «Защита аккаунтов и приватности»

Для 7–10 лет:

- Понятие «пароль» — как ключ от дома: никому не даём.
- Игра «Хороший/плохой пароль»: детям показывают пароли, они оценивают.
- Чек-лист «Мой телефон безопасен»: блокировка экрана, не раздавать пароль от Wi-Fi, не устанавливать приложения без спроса.
- Беседа «Один компьютер на всех»: если дома один компьютер — как не оставить свои данные открытыми (выйти из аккаунта, очистить историю).

Для 11–13 лет:

- Мастер-класс по паролям: правило «фраза + цифра + спецсимвол», длина не менее 8 символов, разные пароли для разных сервисов.
- Настройка приватности в популярных соцсетях: кто видит профиль, кто может писать, кто видит фото. Пошаговый чек-лист (распечатанный).
- Геолокация: как приложения отслеживают местоположение, как отключить. Камера и микрофон: какие приложения имеют доступ и как проверить.
- Практикум «Настрой свой профиль»: на проекторе пошагово показывают настройки, дети отмечают в чек-листе, что сделали.

Для 14–17 лет:

- Углублённое изучение приватности: метаданные фотографий (EXIF-данные), как по фото определить местоположение.
- Двухфакторная аутентификация: что это, зачем нужна, как настроить.
- Публичный Wi-Fi: риски, VPN (как технология безопасности, не как инструмент обхода блокировок), почему нельзя вводить пароли в публичных сетях.
- Фишинговые страницы входа: как отличить поддельную страницу входа от настоящей (адресная строка, сертификат).

Модуль 3. «Опасные контакты: распознаём угрозу»

Для 7–10 лет:

- «Незнакомцы в интернете — как незнакомцы на улице»: правило «не отвечай, не дружи, не встречайся».
- Игра-сортировка «Ловушки в сообщениях»: карточки с типичными сообщениями мошенников («выиграл», «срочно», «бесплатно»).
- Ролевая игра «Незнакомец пишет в игре»: отработка фраз «Я не буду с тобой общаться», «Я расскажу взрослому».
- Алгоритм «Стоп — Спроси — Расскажи».

Для 11–13 лет:

- Онлайн-мошенничество: типичные схемы («возврат денег», «блокировка аккаунта», «розыгрыш приза»).
- Фишинг: поддельные сайты, копии известных страниц. Практикум: распознать фишинговую страницу по признакам (адрес, дизайн, ошибки в тексте).
- Груминг (в доступной форме): «новый друг», который говорит «ты особенный», «это наш секрет», «не говори родителям». Как распознать манипуляцию.
- Алгоритм 4 шагов: сохранить доказательства → заблокировать → рассказать взрослому → пожаловаться в поддержку.

Для 14–17 лет:

- Углублённый разбор груминга: этапы (контакт, формирование доверия, изоляция, эксплуатация). Признаки на каждом этапе.
- Деструктивные сообщества: группы, пропагандирующие самоповреждение, расстройства пищевого поведения, «игры с смертью». Как их вербуют, как распознать, что друга пытаются втянуть.
- Социальная инженерия: как мошенники используют эмоции (страх, жадность, любопытство, жалость). Разбор схемы «срочная помощь другу, чей аккаунт взломан».
- Деловая игра «Суд над мошенником»: ролевой разбор сценария мошенничества с назначением ролей (потерпевший, мошенник, судья, адвокат, прокурор).

Модуль 4. «Общение в сети: травля и её профилактика»

Для 7–10 лет:

- «Добрые и злые слова»: как обидные слова в интернете ранят так же, как и вживую.
- Ролевая игра «Как реагировать на обидные слова»: фразы «Стоп, мне неприятно», «Перестань», «Я расскажу взрослому».
- Правило: не отвечай обидой на обиду.
- Творческая мастерская: рисунок или комикс «Стоп-травля».

Для 11–13 лет:

- Кибербуллинг: формы (травля в чате, создание групп ненависти, рассылка унижающих фото, бойкот).
- Разбор кейсов «Шутка или травля?»: где проходит граница.
- Роль свидетеля: почему молчать — это участие. Что может сделать свидетель (поддержать, рассказать взрослому, не распространять).
- Цифровая этика: как общаться уважительно, не писать в гневе, не пересылать чужие личные сообщения.

Для 14–17 лет:

- Углублённая дискуссия о кибербуллинге: психологические последствия для жертвы и агрессора.
- Мобинг (коллективная травля): как возникает, как развивается, как остановить.
- Тренинг «Как попросить о помощи и не бояться»: отработка фраз, ролевые сценки с педагогом/воспитателем.
- Ответственность: что считается клеветой (ст. 128.1 УК РФ), нарушением неприкосновенности частной жизни (ст. 137 УК РФ). Разбор кейсов.

Модуль 5. «Ответственность, помощь, самоконтроль»

Для 7–10 лет:

- «Кто может помочь»: карта помощи — дети рисуют/записывают, кому можно рассказать (родитель, воспитатель, учитель, 112, телефон доверия 8-800-2000-122).
- Экранное время: «сколько можно играть» — простое правило «20 минут — перерыв».
- Создание «карточки безопасности» с контактами.

Для 11–13 лет:

- Дискуссия о экранном времени: как понять, что времени в сети слишком много. Признаки: не успеваешь делать уроки, не хочешь гулять, злость без телефона.
- Куда обращаться: телефон доверия 8-800-2000-122, линия помощи «Дети онлайн» 8-800-250-15-15, полиция 112.
- Создание «карты помощи»: индивидуальный список контактов и действий.

Для 14–17 лет:

- Правовые аспекты: клевета (ст. 128.1 УК РФ), нарушение неприкосновенности частной жизни (ст. 137 УК РФ), угроза убийством или причинением тяжкого вреда здоровью (ст. 119 УК РФ), распространение чужих изображений без согласия. Разбор в доступной форме, без излишней детализации.
- Интернет-зависимость: признаки, что делать, как сократить время в сети без стресса. Рекомендации по цифровому детоксу.
- «Правила моего цифрового поведения»: каждый формулирует 3–5 личных правил и подписывает.
- Итоговый квест «Цифровой компас» (для всех возрастов): 5 станций — распознай фишинг, выбери пароль, найди признаки кибербуллинга, проверь источник, назови контакт для помощи.

Методическое обеспечение

Формы работы:

Форма	Доля в программе	Назначение
Беседы и мини-лекции	20%	Введение в тему, подача базовой информации
Разбор кейсов	20%	Распознавание угроз на конкретных примерах
Рольевые игры и тренинги	20%	Отработка навыков и алгоритмов действий
Практикумы с ИКТ	15%	Настройка приватности, работа с паролями
Творческие задания	10%	Создание памяток, постеров, комиксов
Дискуссии	10%	Развитие критического мышления
Квесты и викторины	5%	Закрепление материала, итоговый контроль

Дидактические материалы:

- Набор карточек-кейсов (30+ сценариев, обезличенных, по возрастам).
- Чек-листы приватности для популярных соцсетей.
- Шаблоны паролей и памятки «Как создать надёжный пароль».
- Бланки «Карточка безопасности» (адрес, телефон, 112).
- Бланки «Карта помощи» (контакты, алгоритмы).
- Бланки «Правила моего цифрового поведения».
- Шаблоны для комиксов и постеров.
- Презентации по темам модулей.
- Карточки «Светофор ссылок».

Техническое оснащение (минимальное):

- 1 компьютер или ноутбук с проектором.
- Доступ к интернету (желательно, но не обязательно — все основные задания проводятся с распечатками).
- Печатные материалы (карточки, чек-листы, бланки).
- Ватман, фломастеры, стикеры, ножницы.

Контроль и оценка результатов

Входная диагностика (сентябрь):

- Анкета из 10 вопросов для детей: «Знаешь ли ты, что такое личные данные?», «Что сделаешь, если незнакомец напишет в сети?», «Знаешь ли ты телефон доверия?» и т. д.
- Заполняется в первый день, результаты фиксируются в журнале.

Промежуточный контроль (после каждого модуля):

- Практическое задание: «Распознай угрозу», «Настрой профиль», «Составь алгоритм действий».
- Наблюдение: ведущий фиксирует, кто активно участвует, кто затрудняется, кто отказывается.
- Короткая обратная связь в конце встречи: «Одна вещь, которую я сегодня запомнил».

Итоговый контроль (май):

- Итоговый квест «Цифровой компас» (5 станций с практическими заданиями).
- Повторное анкетирование (те же 10 вопросов).
- Сравнение результатов входной и итоговой диагностики.
- Рефлексия: «Что изменилось в моём поведении в сети?»

Критерии эффективности:

Критерий	Показатель
Знание базовых правил	$\geq 80\%$ участников называют минимум 3 правила из 5
Умение распознавать угрозу	$\geq 75\%$ правильно определяют фишинговое сообщение и признаки груминга
Знание алгоритма действий	$\geq 80\%$ называют последовательность «сохранить — заблокировать — рассказать — пожаловаться»
Знание контактов помощи	$\geq 90\%$ называют телефон доверия 8-800-2000-122 и 112
Навык создания пароля	$\geq 70\%$ создают пароль, соответствующий критериям надёжности

Ожидаемые результаты

По окончании программы дети будут:

- Знать 5 базовых правил цифровой безопасности и применять их.
- Распознавать признаки фишинга, мошенничества, груминга и кибербуллинга.
- Уметь создавать надёжные пароли и настраивать приватность в соцсетях.
- Знать алгоритм действий при столкновении с угрозой (сохранить — заблокировать — рассказать — пожаловаться).
- Знать телефоны и службы, куда можно обратиться за помощью.
- Понимать, что цифровой след остаётся навсегда, и относиться к публикации информации осознанно.
- Знать основы правовой ответственности за действия в сети.

Воспитанники учреждений социального обслуживания дополнительно:

- Будут иметь заполненную «карточку безопасности» с контактами.
- Будут иметь «карту помощи» с алгоритмами и телефонами.

Для отдалённых сельских территорий:

- Все материалы выданы в печатном виде и доступны для использования дома без интернета.
- Педагоги и социальные педагоги получили рекомендации по поддержанию навыков.

Список используемых источников

Книги:

1. Асмолов А.Г., Семенов А.Л., Уваров А.Ю. «Российская школа и новые информационные технологии: взгляд в будущее».
2. Мурсалиева Г. «Дети в сети. Шлем безопасности ребёнку в интернете».
3. Левченко А. «Дети онлайн: опасности в сети».

Нормативные документы:

4. ФЗ № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».
5. ФЗ № 152-ФЗ «О персональных данных».
6. Концепция информационной безопасности детей РФ (распоряжение Правительства РФ № 1569-р от 02.06.2021).

Методические материалы:

7. Материалы портала «Сетевичок» — сетевичок.рф (всероссийский конкурс для детей по кибербезопасности).
8. Рекомендации Минпросвещения РФ по обеспечению информационной безопасности детей.
9. «Полезный и безопасный интернет. Правила безопасного использования интернета для детей младшего школьного возраста: методическое руководство» (под ред. Г.У. Солдатовой).
10. Методические рекомендации по проведению мероприятий в рамках «Недели информационной безопасности».
11. Проект «Вебландия. Лучшие сайты для детей» (Российская государственная детская библиотека, «Билайн»).