



Роспатриотцентр
росмолодёжь

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

ДЛЯ МОЛОДЕЖИ ПО ФОРМИРОВАНИЮ
НАВЫКОВ ОБРАБОТКИ ИНФОРМАЦИИ

**Федеральное агентство по делам молодежи
Федеральное государственное бюджетное учреждение
«Российский центр гражданского и патриотического
воспитания детей и молодежи»**

Методические материалы

**ДЛЯ МОЛОДЕЖИ ПО ФОРМИРОВАНИЮ НАВЫКОВ
ОБРАБОТКИ ИНФОРМАЦИИ**

Москва, 2025

УДК: 37.06
ББК: 74.200.5

Рекомендовано к изданию Экспертным советом ФГБУ «Роспатриотцентр»

Составители:

Методические материалы для молодежи по формированию навыков обработки информации: [Электрон. ресурс] / сост. О.Ф. Жуков, Е.В. Аверченко. – Москва : ФГБУ «Роспатриотцентр», 2025. – 30 с.

Методические материалы предназначены для молодежи, родителей, педагогов и специалистов, работающих в сфере воспитания и просвещения. В них систематизированы современные подходы к формированию навыков обработки информации и цифровой гигиены. Особое внимание уделено вопросам критического восприятия контента, защите личных данных, профилактике деструктивных явлений в сети, а также развитию культуры онлайн-общения и навыков управления временем в цифровой среде.

Структура материалов включает теоретические пояснения, практические алгоритмы, чек-листы и кейсы, которые делают их удобным инструментом для самостоятельного освоения и практического применения. Методические материалы ориентированы на формирование у молодежи ответственного и безопасного поведения в интернете, развитие критического мышления и цифровой грамотности.

Рецензенты: Ю.В. Рубцов – ведущий научный сотрудник Военного университета им. князя Александра Невского Министерства обороны Российской Федерации, доктор исторических наук, профессор; Н.Г. Михальцо – ведущий научный сотрудник Военного университета им. князя Александра Невского Министерства обороны Российской Федерации, кандидат технических наук.

© Жуков О.Ф., Аверченко Е.В., 2025
© ФГБУ «Роспатриотцентр», 2025

Содержание

Содержание.....	3
1. Актуальность формирования навыков обработки информации	4
2. Зачем нужны навыки обработки информации и цифровая гигиена	5
2.1. Роль информации в жизни молодежи	5
2.2. Риски цифровой среды.....	6
2.3. Правовые гарантии и ответственность	7
3. Умение проверять достоверность информации	8
3.1. Как отличить факт от фейка	8
3.2. Что такое фактчекинг	9
3.3. Как работает фактчекинг. Как распознать фейковые новости.....	10
4. Умение анализировать источник и контекст	12
4.1. Как выявлять манипулятивные сообщения и deepfake.....	12
4.2. Распознавание фишинга и кибермошенничества.....	12
4.3. Ответственное создание контента и распознавание информации, созданной с использованием искусственного интеллекта	13
5. Умение защищать личные данные	14
5.1. Приватность в сети.....	14
5.2. Онлайн–угрозы: груминг, сексторшн, доксинг	15
6. Умение безопасно коммуницировать онлайн	17
6.1. Цифровая этика и культура общения.....	17
6.2. Защита от кибербуллинга, троллинга, сваттинга	19
7. Практические решения для подростков по формированию навыка управления временем и вниманием	20
7.1. Баланс онлайн и офлайн.....	20
7.2. Цифровой детокс: как справиться с выгоранием и зависимостью	21
7.3. Экология информационного поля	23
8. Умение реагировать на угрозы	23
8.1. Алгоритм действий при столкновении с мошенниками и шантажом.....	24
8.2. Куда обращаться за помощью	24
Заключение.....	26
Список литературы	27
Приложение 1	29
Приложение 2	30

1. Актуальность формирования навыков обработки информации

Современного человека окружает беспрецедентный объем информации – соцсети, мессенджеры, новостные ленты и блоги формируют непрерывный поток, который заполняет наше внимание еще до того, как мы успеваем осознать его необходимость. Это удобство мгновенного доступа соседствует с перегрузкой, кажется, что все под рукой, но в итоге пользователь теряет фокус, устает и теряется в хаосе данных.

Особенно чувствительны к этому влиянию молодые люди. Они активнее других вовлекаются в новые темы, реагируют на тренды и именно в цифровой среде формируют собственную картину мира. Однако эта открытость делает их уязвимыми для манипуляций. За любым контентом стоят люди и их цели – и далеко не всегда благие, за внешне нейтральной или даже развлекательной информацией могут скрываться осознанные попытки повлиять на взгляды, поведение и эмоциональное состояние, распространение паники, агрессии или идеи ненависти.

Опасность часто неочевидна. Вредоносный контент редко подается в агрессивной форме, наоборот, он искусно оборачивается в мемы, шутки, яркие визуалы или маскируется под «мнение большинства». При многократном повторении такие сообщения незаметно меняют восприятие реальности, влияя на то, как человек оценивает себя, окружающих и общество в целом. Без развитых навыков критического мышления отличить достоверную информацию от манипуляции становится практически невозможно.

Таким образом, умение ориентироваться в цифровой среде превратилось из технического навыка в жизненно важную компетенцию. Речь уже не просто о поиске достоверной информации в интернете, а о цифровой гигиене – осознанном подходе к потреблению информации, который включает умение оценивать чистоту и достоверность источников, защищать личные данные, распознавать манипуляции и сохранять психическое благополучие.

Настоящие методические материалы разработаны для того, чтобы помочь молодым людям уверенно чувствовать себя в информационном пространстве. Данные материалы не предлагают готовых ответов, но позволяют задать критические правильные вопросы:

- кто стоит за информацией;
- какую цель он преследует;
- как тот или иной контент может повлиять на ваше мировоззрение?

Чтобы понять, как развить эти навыки, сначала необходимо разобраться в двух ключевых аспектах. Какую роль информация играет в жизни молодого поколения и почему она обладает такой силой влияния, и с какими конкретными рисками и вызовами можно столкнуться в цифровой среде.

Анализ этих составляющих позволит перейти к главному – практическим инструментам для формирования осознанного и безопасного взаимодействия с информацией.

2. Зачем нужны навыки обработки информации и цифровая гигиена

2.1. Роль информации в жизни молодежи

Современная молодежь живет в условиях перманентного информационного потока, который охватывает все сферы жизни: от учебы и досуга до формирования личности и мировоззрения. Цифровая среда уже не просто фон, а активный участник процесса взросления, влияющий на выбор жизненных стратегий, модели поведения и даже эмоциональное состояние.

Информационная среда выполняет для молодого поколения сразу несколько ключевых функций.

1) Образование и саморазвитие. Онлайн–курсы, научно–популярные платформы и открытые ресурсы предоставляют беспрецедентный доступ к знаниям. Это позволяет строить индивидуальные образовательные траектории, выходить за рамки школьной программы и постоянно развивать навыки в интересующих областях.

2) Социализация и коммуникация. Для многих молодых людей цифровое пространство – это не просто дополнение к офлайн–жизни, а полноценная социальная сфера. Мессенджеры, соцсети, игровые платформы становятся площадками, где завязываются дружеские и профессиональные контакты, формируются сообщества по интересам и создаются сети поддержки.

3) Самовыражение и идентичность. Интернет предоставляет широкие возможности для творчества и поиска себя. Создавая блоги, видео, музыку или арт–проекты, молодые люди пробуют новые роли, выражают взгляды и формируют собственную идентичность.

4) Расширение кругозора. Цифровые медиа открывают доступ к разнообразию культурных традиций, точек зрения и социальных норм. Это помогает развивать гибкость мышления, учиться толерантности и формировать целостное понимание современного мира.

5) Оперативное участие в актуальной повестке. Новости и события становятся доступными в режиме реального времени. Молодежь быстро реагирует на происходящее, включается в дискуссии, формирует собственную гражданскую позицию и ощущает причастность к происходящему в обществе.

Однако чем активнее информация проникает в жизнь, тем сильнее ее влияние на ценности и жизненные ориентиры. Сегодня цифровые медиа по силе воздействия во многом сопоставимы, а нередко и превосходят традиционные институты социализации – семью и школу. То, что молодые люди читают, смотрят и распространяют, формирует их отношение к себе и другим, влияет на выбор профессии, стиль жизни и поведенческие установки.

Именно поэтому навыки критического мышления и медиаграмотности становятся не дополнительным преимуществом, а необходимым условием сохранения психологического благополучия, самостоятельности суждений и активной гражданской позиции.

2.2 Риски цифровой среды

Развитие цифровых технологий дало молодежи беспрецедентный доступ к информации, возможностям самореализации и общения. Однако одновременно с этим усилились и вызовы, с которыми сталкивается пользователь в виртуальной среде. Особенно восприимчивыми к ним оказываются молодые люди, еще не обладающие устойчивыми навыками критической оценки цифрового контента.

Первым и, пожалуй, наиболее системным риском является дезинформация. Современные механизмы распространения контента позволяют фейковым новостям, слухам и пропаганде стремительно набирать охваты, зачастую опережая проверенные источники. В условиях дефицита медиаграмотности такие искажения реальности легко принимаются за истину, влияя на мировоззрение и поведение, подрывая доверие к официальным институтам и создавая ложную картину мира.

Проблема фейков сегодня в том, что они часто выглядят правдоподобно. Не нужно быть хакером, чтобы запустить ложную новость – достаточно громкого заголовка и пары репостов. Когда информации слишком много, мы часто верим в то, что легче понять или что вызывает сильные эмоции.

Кибербуллинг – еще один острый аспект цифровой среды. Унижение, травля, агрессия, выраженные в комментариях, личных сообщениях или через публикации, нередко приводят к серьезным психологическим последствиям: снижению самооценки, тревожности, депрессии. Цифровая форма такого насилия отличается особой навязчивостью и масштабом, поскольку оно не

ограничивается пространством школы или двора – оно проникает в личное пространство через телефон.

Манипуляции и цифровая вербовка приобретают все более изощренные формы. Под видом сообществ поддержки, тематических групп или идеологических «движений» молодым людям предлагают иллюзию принятия и цели, на деле вовлекая их в деструктивные или даже противоправные практики. Особенно уязвимы в этом отношении те, кто ощущает одиночество или нестабильность в социальной среде.

Интернет–зависимость, проявляющаяся в навязчивом потреблении контента, потере контроля над временем в сети и вытеснении офлайн–активностей, оказывает комплексное воздействие: от ухудшения когнитивных функций и социальной изоляции до нарушений сна и эмоционального выгорания.

Косвенные, но не менее значимые риски связаны с культурой визуального контента. Когда молодые люди все время сверяют себя с «идеальной картинкой» из соцсетей, у них формируется ложное представление о том, что считается нормальным. Это часто вызывает чувство, что «я хуже других», и может приводить к эмоциональным трудностям.

Наконец, цифровая беспечность в вопросах приватности приводит к утечкам персональных данных, которые могут использоваться не только для рекламы, но и для шантажа, давления, или втягивания в мошеннические схемы. Отсутствие привычки к защите личной информации делает пользователя уязвимым на системном уровне.

Особое беспокойство вызывает то, что все вышеперечисленные риски зачастую накладываются друг на друга. Молодые люди, находясь на этапе формирования личности и жизненных установок, оказываются в наиболее чувствительной позиции. Девушки чаще становятся объектами вмешательства в личные границы и манипуляций через эмоциональные каналы, а юноши – через идеологические и радикальные.

Таким образом, цифровая среда, при всей своей полезности, требует внимательного и осознанного участия. Без устойчивых навыков информационной гигиены она может стать не только источником знаний, но и фактором серьезных личностных и социальных рисков.

2.3. Правовые гарантии и ответственность

В Российской Федерации защита детей и молодежи в цифровой среде закреплена в федеральных законах:

- ФЗ № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;

- ФЗ № 152-ФЗ «О персональных данных»;
- ФЗ № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Государство гарантирует защиту от опасного контента и обязанность операторов хранить и обрабатывать персональные данные законно.

Важно знать, ответственность наступает не только для преступников, но и для самих молодых людей. За кибербуллинг, распространение оскорблений, фейков, экстремистских материалов или чужих личных данных может наступать административная и даже уголовная ответственность (ст. 110.1, 128.1, 137, 242, 242.1, 280, 282 УК РФ и др.). Знание правовой базы помогает: защищать себя и свои права; не нарушать закон самому – случайно или по незнанию (например, пересылая экстремистский мем или «шутку»); выстраивать ответственное цифровое поведение. Соблюдение правовых норм – такая же часть цифровой культуры, как умение защищать данные или фильтровать информацию.

3. Умение проверять достоверность информации

3.1. Как отличить факт от фейка

Интернет подарил нам доступ к бесконечному потоку новостей, видео и постов. Но вместе с этим он стал фабрикой мифов и «сенсаций». Заголовки пугают и шокируют, но чаще всего оказываются фейками.

Фейки — это как вирусы. Они заражают сознание и эмоции, играют на страхах и любопытстве. В них легко поверить, даже если у тебя высшее образование или солидный опыт. По данным ЮНИСЕФ, 3 из 4 детей в мире не могут определить достоверность информации в интернете. Чаще всего жертвами дезинформации становятся подростки, которые черпают новости не из СМИ, а из блогов и соцсетей. Алгоритмы подсовывают им то, что совпадает с их интересами, а значит – создают «информационный пузырь», где альтернативных точек зрения просто нет.

Не все вранье выглядит одинаково. О том, какие бывают фейки дает разъяснения ЮНИСЕФ и приводит классификацию 7 типов дезинформации:

- сатира или пародия (шутка, которую приняли за чистую монету);
- связанный контент (когда заголовок не соответствует тексту);
- вводящий в заблуждение контент (факты поданы так, чтобы скрыть ключевую деталь);
- ложный контекст (старые фото/видео выдают за новые);
- имитация источника (фейковый сайт, похожий на настоящее СМИ);

- подделанные цитаты и фото;
- полностью сфабрикованный материал – чистое изобретение, созданное, чтобы нанести вред.

Чем же опасны фейковые новости? Фейковые новости — это не просто шутка или нелепый слух. Они могут напрямую влиять на наши решения и даже на будущее общества.

Во-первых, дезинформация создает путаницу. Когда реальные события смешиваются с выдуманными, становится сложно понять, чему можно доверять. У людей появляется общее ощущение: «нельзя верить ничему». В результате снижается доверие даже к серьезным и ответственным СМИ.

Во-вторых, фейки напрямую затрагивают здоровье. Ложные советы о лечении серьезных заболеваний могут подтолкнуть человека к неправильным решениям и нанести реальный вред.

В-третьих, многие фейковые сообщения специально направлены на то, чтобы расколоть общество. Они подливают масло в огонь конфликтов. Каждая сторона получает свои «факты», которые усиливают поляризацию общества.

И, наконец, у дезинформации есть последствия и для образования. Студенты и школьники, которые опираются на недостоверные материалы в учебных заданиях, рискуют получить заниженные оценки и упустить шанс развить навыки критического мышления.

Таким образом, фейковые новости опасны тем, что они ломают доверие, влияют на здоровье, раскалывают общество и мешают учиться.

3.2. Что такое фактчекинг

Каждый день мы открываем ленту новостей или соцсетей и видим десятки сообщений. Одни вызывают улыбку, другие – тревогу, третьи кажутся невероятно важными. Но как понять, где правда, а где обман? Здесь на помощь приходит фактчекинг – проверка информации на достоверность.

Термин «фактчекинг» пришел из английского языка и дословно означает «проверка фактов». Первоначально это было профессиональной обязанностью журналистов. Перед публикацией они должны были убедиться, что в материале нет ошибок и все утверждения подтверждаются источниками. Сегодня же фактчекинг стал важным навыком для любого человека, потому что информация влияет буквально на все – от здоровья до политических решений.

Фактчекинг позволяет обеспечить:

- а) Защита от манипуляций. Фейки часто используют, чтобы вызвать эмоции (страх, гнев или возмущение). Когда мы проверяем информацию, мы снижаем риск стать игрушкой в руках манипуляторов.

б) Доверие к источникам. Если СМИ или блог регулярно публикуют непроверенные данные, доверие к нему падает. Фактчекинг помогает отличить надежные площадки от сомнительных.

в) безопасность для здоровья. В сети легко встретить советы «лечить рак содой» или «защититься от хакеров с помощью оберега». Проверка фактов позволяет избежать опасных ошибок, которые могут стоить жизни

г) Общественная стабильность. Фейковые новости способны расколоть общество, и разные группы людей начинают опираться на противоположные «факты», и диалог становится невозможным. Фактчекинг помогает снизить уровень конфликтов.

д) Образование и учеба. Студенты и школьники, которые опираются на непроверенные источники, рискуют ошибиться в заданиях и потерять оценки. Навык проверки информации делает обучение качественнее.

3.3. Как работает фактчекинг. Как распознать фейковые новости.

Как же определить фейковые новости в социальных сетях? Как, будучи студентом, избежать фейковых новостей? Как не участвовать в случайном распространении ложной информации в интернете?

Ниже приведены десять советов Центра ресурсов по информационной безопасности лаборатории Касперского, помогающих выявить ложную информацию, распознать поддельные новостные сайты и оценить данные, прежде чем ими делиться:

1) Проверьте источник.

Проверьте веб-адрес страницы, которую вы просматриваете. Иногда в веб-адресах сайтов фейковых новостей содержатся орфографические ошибки или используются редкие доменные расширения, такие как .infonet или .offer. Если вы не знакомы с сайтом, перейдите в раздел «О компании».

2) Оцените автора.

Найдите информацию об авторе, чтобы понять, заслуживает ли он доверия: реальный ли это человек, какая у него репутация, относятся ли его статьи к конкретной области знаний и освещает ли он определенные вопросы? Оцените, в чем может быть мотивация автора.

3) Проверьте другие источники.

Сообщают ли об этом факте другие авторитетные новостные источники или СМИ? Цитируются ли в статье достоверные источники? Профессиональные мировые новостные агентства в соответствии с редакционными правилами обязаны проверять достоверность фактов, кроме того, они имеют для этого обширные ресурсы, поэтому, если они также сообщают об этом факте, это хороший признак.

4) Сохраняйте критическое мышление.

Многие фейковые новости составлены с целью спровоцировать сильные эмоциональные реакции, например, страх или гнев. Сохраняйте критический настрой, спросите себя: с какой целью написана эта статья? Продвигает ли она определенные взгляды или вопросы? Возможно, в статье предпринимается попытка заставить пользователя перейти на другой веб-сайт?

5) Проверьте факты.

Достоверные новости включают множество фактов: данные, статистику, цитаты экспертов и прочие. Если все это отсутствует, задайтесь вопросом – почему. Отчеты с ложной информацией часто содержат неверные даты или измененные сроки, поэтому рекомендуется проверить дату публикации статьи. Это актуальная или устаревшая новость?

6) Оцените комментарии.

Даже реальная статья или видео может не иметь комментариев. Часто ссылки и комментарии к статье могут автоматически создаваться ботами или пользователями, нанятыми для размещения вводящей в заблуждение информации.

7) Оцените собственные убеждения.

У всех нас есть убеждения. Способны ли они повлиять на нашу реакцию на статью? Социальные сети могут создавать эхо-камеры, предлагая статьи, соответствующие вашим поисковым запросам, интересам и мнениям. Чем больше информации из разных источников и с разных точек зрения вы получаете, тем больше вероятность того, что удастся сделать правильные выводы.

8) Проверьте, не является ли статья шуточной.

Сайты сатирических новостей весьма популярны, однако не всегда понятно, является ли новость шуточной или реальной. Перейдите на сам веб-сайт, чтобы понять, типично ли для него публиковать сатирические и смешные истории.

9) Проверьте подлинность изображений.

Изображения в социальных сетях могли быть отредактированы или изменены. Возможные признаки редактирования изображений включают деформацию (прямые линии на заднем фоне выглядят изогнутыми), странные тени, неровные края, нереально идеальный оттенок кожи. Кроме того, изображение может быть реальным, но использоваться в рамках вводящего в заблуждение контекста. Обратный поиск изображений в Яндекс. Картинки, Google позволяет проверить, откуда было взято изображение и было ли оно изменено.

10) Используйте сайты проверки фактов.

Самостоятельно перепроверять все сложно, но есть сервисы, которые уже делают это за нас. Это фактчекинговые платформы, например «Лапша–медиа» <https://lapsha.media/>.

Навык проверки информации нужен не только журналистам, но и каждому из нас в повседневной жизни. Например, если приходит сообщение о «новом смертельном вирусе» или «опасном челлендже в социальных сетях, не стоит пересылать его дальше. Достаточно проверить официальные источники, СМИ и фактчекинговые платформы – и часто окажется, что это миф или искажение.

Главное, что фактчекинг — это привычка не верить на слово. Он помогает сохранять ясность ума в мире, где каждый может стать «автором новостей».

4. Умение анализировать источник и контекст

Если проверка фактов помогает отличить правду от вымысла, то анализ источника и контекста позволяет понять глубже – кто стоит за сообщением, зачем оно создано и какие приемы использованы для воздействия. Этот навык становится особенно важным сегодня, когда технологии развиваются быстрее, чем привычные способы защиты.

4.1. Как выявлять манипулятивные сообщения и deepfake

Технология deepfake позволяет подменять лица и голоса людей в видео- и аудиоматериалах, подобные материалы все чаще используют для шантажа, травли или распространения ложных новостей. На первый взгляд они выглядят очень реалистично, но внимательный взгляд может заметить неестественные движения лица, «плавающий» фон или размытые детали, иногда достаточно прислушаться – голос может звучать чуть «роботизированно» или с неправильной интонацией.

Используй чек–лист «Как распознать deepfake»:

- 1) Обрати внимание на мимику: движения лица и глаз могут быть неестественными.
- 2) Смотри на фон: размытость и «дрожание» часто выдают подделку.
- 3) Заметь детали: лишние пальцы, искаженные уши, странные тени.
- 4) Проверь через обратный поиск картинок или специальные сервисы.

4.2. Распознавание фишинга и кибермошенничества

Фишинг – это способ незаконно получить личные данные, мошенники представляются сотрудниками банка, почтовой службы или соцсети и предлагают срочно пройти по ссылке, «подтвердить аккаунт» или «получить приз». Главный инструмент давления – создание паники: «Ваш счет будет

заблокирован!» или «Вы срочно должны обновить пароль!», в такой ситуации подростки особенно уязвимы, потому что реагируют быстро и не всегда проверяют детали.

Используй чек–лист «Как не попасться на фишинг»:

- 1) Всегда проверяй адрес отправителя: мелкая ошибка в домене — тревожный знак.
- 2) Обращай внимание на язык письма: ошибки и странные формулировки – почти всегда признак подделки.
- 3) Не переходи по ссылкам из подозрительных сообщений.
- 4) Никогда не вводи данные карты или пароль по чужой просьбе.
- 5) При сомнении лучше позвонить напрямую в организацию или спросить у взрослых.

4.3. Ответственное создание контента и распознавание информации, созданной с использованием искусственного интеллекта

Дезинформация – еще один мощный инструмент манипуляции, может выглядеть как новость, мем или «утечка инсайда». Главное ее свойство – влиять на восприятие и формировать нужные взгляды. По классификации ЮНИСЕФ, виды дезинформации разнообразны: от частично искаженных фактов до полностью сфабрикованных историй, сегодня к этому добавился новый вызов – контент, созданный искусственным интеллектом.

Сгенерированные искусственным интеллектом тексты часто звучат красиво, но в них много «воды», мало конкретики, отсутствуют ссылки на реальные источники. В изображениях искусственный интеллект часто ошибается на мелочах – он может рисовать лишние пальцы, искажает надписи, делает странные тени, это можно заметить, если остановиться и внимательно рассмотреть материал.

Используй чек–лист «Как фильтровать сгенерированный искусственным интеллектом контент»:

- 1) Смотри на источник: кто публикует и с какой целью.
- 2) Проверяй дату публикации: старые новости часто выдают за свежие.
- 3) Сравнивай с другими источниками: если информация есть только в одном месте – повод усомниться.
- 4) Обращай внимание на детали: странные формулировки, ошибки или нелепые изображения часто выдают подделку.
- 5) Используй фактчек–сервисы и официальные сайты для проверки.

Таким образом, анализ источника и контекста – это умение видеть за информацией ее скрытые смыслы и цели. Deepfake учит нас замечать технические сбои, фишинг – заставляет проверять достоверность отправителя,

дезинформация и искусственный интеллект – заставляют мыслить критически и не доверять на слово даже самым убедительным материалам. Вместе эти навыки формируют настоящую «цифровую броню», которая помогает подросткам сохранить свободу мышления и уверенность в собственном выборе.

5. Умение защищать личные данные

5.1. Приватность в сети

Сегодня цифровая среда хранит о каждом из нас больше информации, чем мы сами помним. Мы пользуемся смартфонами, компьютерами, планшетами, оплачиваем покупки онлайн, переписываемся в мессенджерах, делаем домашние задания через интернет-сервисы – все это оставляет цифровой след. При этом, чем активнее мы живем онлайн, тем важнее становится вопрос приватности.

Приватность – это право на личное пространство и контроль над тем, кто и какие сведения о нас может видеть. Исследователи отмечают, что приватность включает сразу несколько аспектов: физическую; поведенческую; приватность коммуникаций и персональной информации. Нарушение любого из этих уровней может привести к серьезным последствиям.

Почему это важно?

Информация – это деньги. Рекламные компании анализируют поисковые запросы и покупки, чтобы предлагать товары. Иногда это полезно, но чаще навязчиво. По данным исследования «Технологии защиты детей в интернете», проведенном в 2022 году, каждый четвертый подросток (26 %) сталкивался с кражей личных данных, причем 14 % детей сами публиковали данные банковских карт, а 12 % – паспортные данные. Эти данные часто появляются на черном рынке.

Вмешательство в личную жизнь. Даже невинные действия (поиск лекарства или покупка витаминов) могут стать сигналом для маркетологов или злоумышленников.

Отдельную угрозу представляет шерентинг – публикация родителями фото и данных ребенка в сети без его согласия. Исследование подчеркивает, что это формирует «цифровой портрет» ребенка и делает его уязвимым.

Как защитить свои данные?

Безопасное соединение. На домашнем Wi-Fi ставьте сложный пароль и используйте шифрование WPA2/3 (стандарты шифрования и защиты данных при использовании беспроводного интернета).

Избегайте общественных сетей для покупок и переводов. Будьте осторожны с публичным Wi-Fi, не вводите пароли и данные карт. Если без этого не обойтись – используйте мобильный интернет. К выбору VPN подходите крайне осторожно – некоторые сервисы ненадежны, а в ряде стран их использование ограничено или запрещено.

Соцсети и публикации. Не выкладывайте все данные о себе: фото билетов, точный адрес, номер телефона. Проверьте настройки приватности — ограничьте круг людей, которые видят посты. Удалите из «друзей» случайные контакты и фейки. Помните, что публикации родителей (шерентинг) тоже влияют на цифровую безопасность подростка.

Надежные аккаунты. Используйте разные пароли для разных сервисов, меняйте их каждые полгода. Подключайте двухфакторную аутентификацию (SMS, приложение или биометрию).

Защита устройств. Установите антивирус и обновляйте систему. Не качайте сомнительные приложения. Включайте блокировку экрана и возможность удаленного стирания данных на телефоне.

Используйте чек-лист «Твоя приватность под защитой»:

- 1) У меня стоят сложные пароли и включена двухфакторная защита.
- 2) Я не оплачиваю покупки через общественный Wi-Fi.
- 3) В соцсетях я контролирую, что и кому показываю.
- 4) Я удаляю ненужные приложения и аккаунты.
- 5) Я всегда проверяю ссылки и письма, прежде чем по ним кликнуть.

Таким образом, приватность – это не что-то абстрактное, а конкретная привычка заботиться о себе. Исследования показывают, что дети и подростки часто недооценивают риски утечки данных, но именно внимание к цифровым следам делает жизнь в сети безопасной и спокойной.

5.2. Онлайн-угрозы: груминг, сексторшн, доксинг

Подростковый возраст – один из самых уязвимых периодов. В это время дети ищут себя, испытывают давление сверстников и гормональные изменения, нередко отвергают советы родителей и стремятся к самостоятельности. Именно в этот период многие впервые пробуют строить отношения, и часто делают это в онлайн. При этом подростки редко задумываются о безопасности – используют простые пароли, легко доверяют новым знакомствам, а иногда сами публикуют интимные фото или личные данные.

Груминг – опасная ситуация, когда взрослый человек через интернет завоевывает доверие ребенка, чтобы потом использовать его. Злоумышленники начинают с дружбы, комплиментов или виртуальных подарков, постепенно переводят разговор на личные темы, могут склонять к отправке фото или встрече офлайн

Используй чек–лист «Как защититься от груминга?»:

- 1) Немедленно прекратить общение и заблокировать контакт.
- 2) Сообщить в администрацию платформы.
- 3) Рассказать взрослым.
- 4) При угрозах обращаться в полицию.
- 5) Сохранить скриншоты переписки.

Сексторшн – опасная ситуация шантажа интимными фото или видео. Чаще всего начинается с доверительного общения («познакомимся ближе», «обменяемся фото»), а затем выливается в угрозы: злоумышленник требует новые материалы или деньги, угрожая распространить уже полученные

Реальные случаи показывают, что преступники действуют не только через обман, но и с помощью техники. Например, вирусные программы могут включать веб-камеру без ведома владельца, и злоумышленники получают возможность записать компрометирующие видео, а затем требуют деньги или новые фото. По данным, приведенным Центром ресурсов по информационной безопасности лаборатории Касперского, 20% подростков делятся своими обнаженными фотографиями, почти 40% размещают сообщения непристойного содержания, а 15% из тех, кто отправлял кому-либо фото без одежды, признались, что делились ими с людьми, с которыми общались только в сети интернет.

Используй чек–лист «Если заметил сексторшн?»:

- 1) Сразу прекратить переписку.
- 2) Заблокировать злоумышленника.
- 3) Сообщить в администрацию платформы.
- 4) Рассказать взрослым, не скрывать проблему.
- 5) Обратиться в полицию (шантаж — уголовное преступление).
- 6) Сохранить переписку и скриншоты.

Доксинг – это публикация ваших личных данных (адрес, номер телефона, фото, информация о семье) без согласия, чтобы запугать, унижить или шантажировать

Чаще всего с этим сталкиваются активные пользователи соцсетей или онлайн–игр.

Используй чек–лист «Как защититься от груминга?»:

- 1) Сообщить в администрацию сайта или соцсети.

2) Рассказать взрослым или обратиться в школу/организацию поддержки.

3) При серьезной угрозе сразу обращаться в полицию.

4) Сделать скриншоты материалов, не удалять доказательства.

5) Пересмотреть настройки приватности аккаунтов.

Таким образом, груминг, сексторшн и доксинг – это реальные риски, с которыми подростки сталкиваются все чаще. Несмотря на показное упрямство, подростки очень чувствительны: давление и шантаж могут привести к тяжелым психологическим травмам. Поэтому главное — говорить об этих угрозах открыто, до того как ребенок столкнется с ними лично. Предупрежденный подросток в критический момент вспомнит простой алгоритм действий и сможет защитить себя.

Итоговый алгоритм для любой угрозы это: заблокировать → сообщить в поддержку → рассказать взрослому → сохранить скриншоты → при угрозе жизни или шантаже обратиться в полицию.

6. Умение безопасно коммуницировать онлайн

Онлайн-общение сегодня стало естественной частью жизни подростков: оно открывает мир быстрых коммуникаций, обмена идеями и совместного творчества. Но вместе с удобством приходит и новая ответственность – чтобы цифровые диалоги оставались безопасными и уважительными, важно сочетать два компонента: культуру общения (что делать до конфликта) и алгоритмы защиты (как действовать во время и после инцидента).

Исследования показывают, что наиболее опасны именно личностные атаки и формы психологического насилия. Технологий, которые могли бы полностью исключить такие риски, пока не существует. Поэтому ключевая роль принадлежит грамотному поведению самих пользователей, поддержке взрослых и чётким правилам со стороны платформ.

6.1. Цифровая этика и культура общения

Онлайн-этикет, или нетикет, – это набор правил вежливого, уважительного и безопасного общения в сети. Его соблюдение помогает:

- беречь границы и снижать количество конфликтов;
- делать переписку понятной и конструктивной;
- защищать репутацию и снижать цифровые риски.

Ключевые отличия онлайн-этикета от правил этикета «офлайн»:

- Скорость. Пишем быстрее, чем говорим – именно поэтому важно думать о формулировках.

- След. Всё сказанное онлайн может быть сохранено и показано другим.

- Анонимность. Снижает самоконтроль, поэтому правила особенно важны.

Используй чек–лист «Основы нетикета»:

- 1) Будьте вежливы, избегайте прямых оскорблений и сарказма.
- 2) Пишите ясно и по делу, проверяйте факты и указывайте источники.
- 3) Не публикуйте чужие данные или переписку без разрешения.
- 4) Помните: скриншоты живут дольше постов.
- 5) Шаблоны корректной коммуникации
- 6) Приветствие: «Здравствуйте...», «Добрый день!»
- 7) Спасибо: «Спасибо за помощь!», «Благодарю за информацию!»
- 8) Просьба: «Не могли бы вы подсказать...?»
- 9) Несогласие: «Позвольте не согласиться...», «У меня другая точка зрения...»
- 10) Извинение: «Прошу прощения за ошибку».
- 11) Завершение: «Спасибо за общение!», «Всего доброго!».

Правила поведения в сети:

- при использовании соцсетей уважайте собеседников, отмечайте авторство, не вступайте в «битвы» в комментариях;
- при общении в мессенджерах пишите кратко, предупреждайте собеседника перед звонком, уважайте «тихие часы»;
- при переписке в электронной почте указывайте тему письма, обращайтесь по имени, используйте корректно адресатов при направлении копий и пересылке писем;
- при участии в онлайн-встречах проверяйте звук и видео, не перебивайте, участвуйте активно;
- при участии в играх/форумах соблюдайте правила площадки и не давайте пищу злоумышленникам и агрессивно настроенным пользователям;
- категорически запрещены оскорбления и угрозы, клевета, публикация чужих данных и контента без прав, а также разжигание ненависти – это может привести к блокировкам, жалобам и даже юридическим последствиям.

Используй чек-лист «Пишу – как будто это прочитает любой»:

- 1) Коротко ≠ грубо.
- 2) Критикуем идеи, а не людей.
- 3) Не спамим и не кричим КАПСЛОКОМ.
- 4) Не выкладываем чужое без разрешения.
- 5) Ошибся? — извинись и исправь.

6.2. Защита от кибербуллинга, троллинга, сваттинга

Даже при соблюдении правил общения подростки могут столкнуться с агрессией в сети. Здесь важно знать определения угроз и алгоритмы действий.

Определения и признаки агрессивного поведения в сети:

Кибербуллинг – повторяющиеся агрессивные действия онлайн, цель которых – унижить или запугать жертву.

Троллинг – провокационные сообщения ради конфликта или эмоциональной реакции.

Сваттинг – ложные вызовы экстренных служб по чужому адресу, опасная офлайн-эскалация сетевого конфликта.

Исследования подтверждают, что кибербуллинг и личные атаки крайне опасны для психологического здоровья подростков, с ними невозможно справиться одними лишь технологиями – нужны поведенческие навыки и поддержка взрослых.

Немедленный алгоритм при любой онлайн-агрессии: Стоп–контакт → Блок → Жалоба на платформе → Скриншоты/сохранение доказательств → Сообщить взрослому → При угрозах жизни/здоровью – в полицию.

Используй чек-лист «Как действовать при кибербуллинге?»:

- 1) Не вступать в перепалку: агрессор питается реакцией.
- 2) Заблокировать и пожаловаться с приложением доказательств.
- 3) Обратиться за поддержкой к взрослым или специалисту.
- 4) Настроить приватность, чтобы исключить повторные контакты.
- 5) Отслеживать эмоциональное состояние и при необходимости обращаться за помощью.

Используй чек-лист «Как действовать при троллинге?»:

- 1) Игнорировать: «не кормить тролля».
- 2) При необходимости – короткий фактологичный ответ без эмоций.
- 3) Пользоваться модерацией, жалобами, блокировкой.
- 4) Укрепить приватность, чтобы предотвратить переход в буллинг.

Используй чек-лист «Как действовать при сваттинге?»:

- 1) Немедленно сообщить взрослым или в экстренные службы.
- 2) Сохранить переписку и угрозы.
- 3) Предупредить школу или администрацию площадки.
- 4) Пересмотреть цифровой след: скрыть адрес, убрать геометки, закрыть аккаунты.

В целях минимизации агрессивных проявлений в сети следует предпринять защитные меры и заранее настроить:

- Приватность: закрытые аккаунты, минимум публичных данных.

- Безопасность: уникальные пароли, антивирус, обновления.
- Игровая среда: отключение голосового чата от незнакомцев, фильтры токсичности.
- Сообщество: знание правил площадки, договорённости в семье о быстрых шагах.
- Платформенная поддержка: подростковые режимы, модерация, каналы помощи.

Используй чек-лист «5 шагов защиты» (распечатать и повесить):

- 1) Блок.
- 2) Жалоба.
- 3) Скриншоты.
- 4) Сообщить взрослому.
- 5) Полиция при угрозах.

Эффективная защита подростков от онлайн-рисков возможна только при совместных усилиях государства, школ, родителей, информационных цифровых платформ и самих детей. Главная цель – сформировать поколение осознанных пользователей, которые знают правила цифровой безопасности и умеют действовать при угрозах.

7. Практические решения для подростков по формированию навыка управления временем и вниманием

Цифровая среда открывает огромные возможности для пользователей – от учёбы и работы до общения и развлечений. Именно поэтому важно уметь управлять временем и вниманием: бесконтрольное использование гаджетов быстро приводит к усталости и выгоранию. Решением могут стать практические правила баланса онлайн и офлайн, самопроверка на признаки цифровой перегрузки, пошаговый план цифрового детокса и советы по созданию «экологичного информационного поля».

7.1. Баланс онлайн и офлайн

Начнём с простого вопроса: часто ли ты ловишь себя на том, что бесцельно листаешь ленту? Или испытываешь тревогу, если телефон не под рукой? Если да – это сигнал, что баланс между онлайн и офлайн нарушен.

Сегодня быть «в сети» круглосуточно стало нормой, но все-таки наш мозг не приспособлен к такому ритму: каждое уведомление отнимает кусочек концентрации, внимание «распадается», а усталость растёт. Поэтому важно выстроить собственные правила – когда ты в онлайн, а когда полностью отдаёшь себя реальности.

Алгоритм сохранения баланса:

- Намеренность. Попробуй заходить в приложение только с конкретной целью: «10 минут на переписку и всё».

- Фокус-блоки. Для учёбы и работы отлично подходит техника метод управления временем: 25–40 минут концентрации → 5 минут офлайн–паузы. Есть простые приложения или встроенные таймеры.

- Ритмы дня. Сделай правило: два приёма пищи и прогулка – без телефона.

- Уведомления под контроль. На iOS включи «Режим концентрации», на Android – «Цифровое благополучие», эти функции помогут убрать лишний шум.

- Договоренности. Встречаясь с друзьями, предложи метод «телефоны вниз» как новый стандарт заботы друг о друге. В мессенджерах можно отвечать пакетами: например, в обед и вечером.

Чтобы проверить себя, используй простой чек–лист «Баланс онлайн–офлайн»:

1) Основные правила:

- каждый день у меня есть минимум 2 офлайн–ритуала без телефона;
- проверяю мессенджеры 2–3 раза в день, а не постоянно;
- телефон за час до сна и только вне спальни.

2) Дополнительные правила:

- на развлечения с экраном трачу не более 2 часов в день;
- раз в неделю планирую офлайн–активность (спорт, встреча, хобби).

Баланс – это база. Но что делать, если гаджеты уже стали источником усталости и раздражения? Тогда стоит перейти к следующему шагу.

7.2. Цифровой детокс: как справиться с выгоранием и зависимостью

Мозг реагирует на каждое уведомление как на «мини-награду» – это дает краткий выброс дофамина. Со временем формируется привычка тянуться к телефону автоматически – это и есть цифровая зависимость, в результате которой появляется цифровое выгорание, когда усталость становится фоном, а мотивация падает.

Признаки цифрового выгорания:

- усталость даже после сна;
- нет энергии для приятных дел;
- внимание «скачет», сложно сосредоточиться;
- тревожность или раздражительность без причины;
- головные боли, напряжение в шее и спине;

- проблемы со сном;
- привычка «отдых = телефон».

Если у тебя совпало три или больше пунктов, то пора подумать о цифровом детоксе.

Цифровой детокс – это временное снижение или отказ от гаджетов ради восстановления. Совсем не обязательно «уйти в лес и выкинуть телефон», уровни детокса могут быть разными:

- Мини-режим: один день без соцсетей или коротких видео.
- Цифровой минимум: оставь только 1–2 нужных приложения (например, карты и мессенджер), а остальные заморозь на неделю.
- Полный детокс: неделя или отпуск офлайн.

Чтобы безболезненно осуществить цифровую разгрузку важно помнить, главное – не запрет, а новый формат отдыха. Чтобы детокс не вызвал стресс, нужно подготовиться – настроить телефон (проверить пароли, включить двухфакторную аутентификацию, сделать резервные копии); оповестить близких (предупредить, когда ты будешь на связи); определить «дежурный» гаджет (остальные убрать из доступа); предусмотреть активные замены (спорт, настольные игры, встречи с друзьями, прогулки).

В процессе реализации цифровой разгрузки используй два офлайн-ритуала в день (например, ужин и вечерняя прогулка без телефона); постарайся отказаться от коротких видео – они сильнее всего ломают внимание; удали или заморозь приложения, которые используешь бесцельно; оставляй телефон за пределами спальни за час до сна; проверяй сообщения пакетами (максимум 2–3 раза в день).

После завершения процесса цифровой разгрузки постарайся закрепить положительный результат и постарайся правильно вернуться в онлайн. Для этого проверь уведомления и входы в аккаунты, чтобы исключить проблемы; выбери две-три привычки, которые понравились, и оставь их навсегда; запланируй следующий офлайн-день, чтобы закрепить результат.

Используй чек-лист «Мой цифровой детокс»:

1) Перед стартом:

- Обновил пароли, включил 2FA;
- Сделал бэкапы данных;
- Настроил автоответчик;
- Определил «дежурный» гаджет.

2) Во время:

- Два офлайн-ритуала ежедневно;
- Нет коротких видео и бесконечных лент;
- Телефон вне спальни;

- Проверка сообщений максимум 3 раза в день.

3) *После:*

- Проверил уведомления и логики;
- Оставил 2–3 полезные привычки;
- Запланировал следующий офлайн–день.

7.3. Экология информационного поля

Кроме прочего, важно сохранять экологию информационного поля. Ведь дело не только во времени, проведённом онлайн, важно и то, какой контент мы выбираем. Если лента состоит из негатива, споров и токсичных блогов – энергия уходит в минус. Экология информационного поля помогает сохранить ясность ума и позитивное настроение.

Советы по инфоэкологии:

- Сделай аудит подписок: отпишись от источников, которые вызывают тревогу, зависть или злость.

- Добавь ресурсы, которые вдохновляют: образовательные каналы, научпоп, блоги по интересам.

- Введи правило: «один новый источник = минус два старых».

- Делай ежемесячную чистку, чтобы не захламлять ленту.

Используй чек–лист «Экология инфополя»:

- 1) Раз в месяц провожу чистку подписок;
- 2) В ленте есть минимум один образовательный ресурс;
- 3) Исключены токсичные каналы и чаты;
- 4) Контент для отдыха разнообразный (книги, музыка, живые встречи);

Запомни золотое правило цифрового детокса и баланса онлайн–офлайн – это не запрет технологий, а умение управлять ими. Гаджеты должны помогать тебе учиться, работать и отдыхать, а не забирать внимание и силы. Управляя вниманием, ты возвращаешь себе энергию и делаешь онлайн–среду помощником, а не хозяином.

8. Умение реагировать на угрозы

Иногда даже при всех знаниях цифровой гигиены мы можем столкнуться с опасными ситуациями в сети – от попыток обмана и вымогательства до угроз и кибербуллинга. Важно не только знать риски, но и уметь правильно реагировать: сохранять спокойствие, фиксировать факты и обращаться за помощью.

8.1. Алгоритм действий при столкновении с мошенниками и шантажом

Если тебе пишут незнакомые люди, требуют деньги или угрожают публикацией личных фото/данных, постарайся не поддаваться панике и выполнить следующие защитные действия:

- Не отвечай агрессору, так как любая реакция только подогревает интерес.

- Сохрани доказательства, сделай скриншоты переписки, сообщений, угроз, ссылок.

- Заблокируй контакт, во всех соцсетях есть кнопка «Пожаловаться» и «Заблокировать».

- Проверь свои аккаунты, сразу смени пароли, включи двухфакторную аутентификацию (2FA).

- Сообщи взрослым, обратись к родителям, учителю, тренеру – одному справляться с угрозами не стоит.

- Пожалуйся в сервис, используй встроенные формы жалоб в соцсетях и мессенджерах.

- Обратись за помощью, позвони на телефон доверия или в специализированную организацию.

Используй чек–лист «Что делать при онлайн–угрозах»:

- 1) Сохранил переписку/скриншоты
- 2) Заблокировал злоумышленника
- 3) Пожаловался в соцсеть
- 4) Сменил пароли, включил 2FA
- 5) Рассказал взрослым
- 6) Обратился за помощью

8.2. Куда обращаться за помощью

Иногда ситуация выходит за рамки «сам решу», и тогда важно знать, что ты не один – есть службы и люди, готовые поддержать.

Горячие линии и сервисы призваны противодействовать распространению противоправного контента в сети Интернет, оказывать помощь пользователям сети, органам государственной власти в борьбе с распространением материалов противоправного характера.

Всероссийский детский телефон доверия (бесплатно, круглосуточно) – 8 (800) 200–01–22 (<https://telefon-doveria.ru/?ysclid=mfso11yeue866940107>)

Лига безопасного Интернета в 2011 году создала Горячие линии по приему сообщений о распространении незаконной информации в сети Интернет. На данный момент действует восемь горячих линий

(<https://ligainternet.ru/hotline/>), на этой странице можно оставить свое сообщение о противоправном Интернет–контенте, есть возможность сообщить анонимно или оставить свой адрес электронной почты.

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. При обнаружении на сайтах в сети «Интернет» информации вышеуказанной тематики можно во внесудебном порядке прекратить её распространение путём подачи заявления в уполномоченный Правительством Российской Федерации федеральный орган исполнительной власти, принимающий решение в соответствии с имеющейся компетенцией в порядке, установленном Правительством Российской Федерации.

На официальном сайте Роскомнадзора по адресу <https://eais.rkn.gov.ru/feedback/> любой неравнодушный гражданин может оставить информацию о противоправном контенте путём заполнения специальной электронной формы.

Эксперты уполномоченных ведомств из вышеперечисленного списка оперативно примут решение об ограничении доступа к противоправной информации. В случае признания информации запрещенной к распространению доступ к ней ограничивается операторами связи в установленном законом порядке.

Важно помнить:

- Реагировать на угрозы онлайн – это значит сохранять спокойствие, фиксировать факты и действовать по алгоритму: «защита себя → блокировка → жалоба → обращение за помощью».

- Помощь всегда доступна – у родителей, педагогов и специалистов, по телефону доверия, в чат–боте.

Заключение

Информационная эпоха изменила не только способы коммуникации и получения знаний, но и саму структуру жизни молодежи – цифровая среда стала ключевым пространством социализации, самовыражения и образования, однако вместе с этим она принесла и новые угрозы: дезинформацию, кибербуллинг, цифровые зависимости, риски утечки личных данных и вовлечение в деструктивные практики.

Настоящие методические материалы направлены на то, чтобы вооружить молодежь необходимыми инструментами для безопасной и ответственной жизни в цифровом пространстве, в них представлена информация:

- о значении информации в формировании личности и мировоззрения;
- об основных рисках цифровой среды и механизмах защиты от них;
- об алгоритмах проверки достоверности и анализа источников;
- о практических шагах по сохранению приватности и управлению цифровым временем;
- о правилах онлайн-этикета и модели реагирования на агрессию и мошенничество в сети.

Особое место занимают практические элементы – чек-листы и алгоритмы, которые помогут не только понять проблему, но и подскажут, как действовать в реальных опасных ситуациях. Это делает материалы удобным инструментом как для самих подростков, так и для педагогов, родителей и специалистов по работе с молодежью.

Цифровая гигиена – это не временный тренд, а необходимый навык XXI века, сопоставимый по значимости с грамотностью или правилами личной безопасности. Регулярное применение рекомендаций позволит молодым людям не только защитить себя от угроз, но и научиться использовать интернет как ресурс для развития, творчества и построения здоровых социальных связей. Будущее цифровой среды во многом зависит от того, насколько ответственно сегодняшняя молодежь научится ею пользоваться, а предложенные материалы могут стать опорой для формирования поколения осознанных, критически мыслящих и социально активных граждан.

Список литературы

1. Алгоритм действий для родителей обучающихся по раннему выявлению и реагированию на деструктивное поведение несовершеннолетних, проявляющееся под воздействием информации негативного характера, распространяемой в сети Интернет // АНО «Центр изучения и сетевого мониторинга молодежной среды»; ФГБУ «Центр защиты прав и интересов детей». – Москва, 2020. – 24 с.
2. Армашова, А.В. Предупреждение киберпреступности в отношении несовершеннолетних: проблемы и пути их решения // Право и государство: теория и практика. 2025. № 2. С. 409–411
3. Балановский, В. В. Методические рекомендации и материалы по информационной гигиене в молодежной среде [Электронный ресурс]. – Калининград : Изд-во БФУ им. И. Канта, 2023. – 40 с.
4. Бочавер, А.А., Хломов, К.Д. Кибербуллинг: травля в пространстве современных технологий // Психология. Журнал Высшей школы экономики. – 2014. – Т. 11. – № 3. – С. 177–191
5. Гайворонская, И.Б., Фомина, Т.Ф., Аманжолова, Б.А. Вербовка в экстремистские и террористические организации посредством сети Интернет // Психология и право. – 2020. – Т. 10. – № 4. – С. 152–165
6. Дубень, А.К. Информационная культура молодежи как правовой механизм обеспечения безопасности // Аграрное и земельное право. 2024. № 5(233). С. 119–121
7. Маркеры определения профилей «группы риска» 2.0. Методические рекомендации для специалистов, ответственных за поведенческий анализ рисков деструктивных проявлений в образовательной и молодежной среде [Электронный ресурс] / НИЦ мониторинга и профилактики. – 2023. — URL: <https://clck.ru/3NowLo> (дата обращения: 24.08.2025).
8. Методические рекомендации по внедрению в практику образовательных организаций современных методик в сфере профилактики деструктивного поведения подростков и молодежи (на основе разработок российских ученых). – М.: Федеральный институт оценки качества образования, 2021. – URL: <https://clck.ru/3PKazT> (дата обращения: 25.08.2025).
9. Немчина, В. И., Чурилов, С. А. Инструменты защиты молодежи от негативного воздействия агрессивной цифровой среды // Современные проблемы науки и образования. – 2025. – Т. 14, № 2. – С. 163–172
10. Осипенко, А.Л., Соловьев, В.С. Киберугрозы в отношении несовершеннолетних 22 и особенности противодействия им с применением информационных технологий // Общество и право. — 2019. — № . 3 (69). – С. 23–31
11. Пазухина С. В., Чумаков П. В. Дети в Интернете: исследование отношения родителей к вредной информации // Научно-методический электронный журнал «Концепт». – 2017. – № 9 (сентябрь). – С. 75–84.

12. Розенберг, Н. В. Влияние средств массовой информации на образ жизни молодежи // Наука. Общество. Государство. – 2015. – № 1 (9). – С. 1–8
13. Рыбакова, О. С. Безопасность несовершеннолетних в информационном обществе: анализ киберрисков и угроз // Мониторинг правоприменения. – 2020. – № 2 (35). – С. 65–73
14. Рыжова, Н. И., Государев, И. Б., Громова, О. Н., Магазейщиков, Е. А. Анализ доступности опасного и деструктивного контента в основных источниках информации в Интернете для школьников // Перспективы науки и образования. 2025. № 1. С. 401–422
15. Садовский, М. Э., Иванов, В.Р. Обучение школьников навыкам информационной гигиены в эпоху цифровизации знаний. – // Молодой ученый. — 2025. — № 5 (556). — С. 185–186.
16. Сексуальное вымогательство: гроза подростков и не только [Электронный ресурс] // Kaspersky Daily. – Режим доступа: <https://www.kaspersky.ru/blog/sextortion-stats/12662/?ysclid=mfs98s904h754360545> (дата обращения: 21.09.2025).
17. Солдатова, Г. У., Чигарькова, С. В., Дренева, А. А., Илюхина, С. Н. Мы в ответе за цифровой мир: Профилактика деструктивного поведения подростков и молодежи в Интернете: Учебно–методическое пособие. – М.: Когито–Центр, 2019. – 176 с.
18. Стернин, И.А. Шестернина, А.М. Маркеры фейка в медиатекстах. Рабочие материалы. – Воронеж: ООО «РИТМ»., 2020. – 34 с.
19. Технологии защиты детей: результаты исследования [Электронный ресурс]. – М.: Фонд развития Интернет, 2011. – 104 с. – URL: <https://clck.ru/3PKb7A> (дата обращения: 21.09.2025)

Практический чек–лист цифровой гигиены для молодежи «10 правил безопасности и осознанности в интернете»

1. Проверяй источник информации.

Смотри, кто автор и откуда новость. Не доверяй сомнительным сайтам и аккаунтам.

2. Не верь на слово – проверяй факты.

Используй фактчекинг-сервисы и официальные ресурсы, чтобы отличить правду от фейка.

3. Защищай свои данные.

Никогда не публикуй паспорт, номера карт, домашний адрес и интимные фото.

4. Используй надежные пароли.

Пароль должен быть длинным и уникальным. Для разных сервисов – разные пароли. Подключи двухфакторную аутентификацию.

5. Настрой приватность в соцсетях.

Проверь, кто видит твои посты. Удали случайные контакты и закрой личные данные от посторонних.

6. Не переходи по подозрительным ссылкам.

Не кликай на «выиграй приз», «срочно подтверди аккаунт». Это может быть фишинг или вирус.

7. Будь вежливым и уважительным онлайн.

Соблюдай правила цифрового этикета: не оскорбляй, не публикуй чужие данные без разрешения.

8. Игнорируй троллей и буллеров.

Не отвечай на провокации. Сохрани скриншоты, заблокируй и пожалуйся в сервис.

9. Делай цифровой детокс.

Устраивай офлайн-перерывы: еда, прогулки, сон — без телефона. Это помогает сохранить энергию.

10. Знай, куда обращаться за помощью.

Телефон доверия: 8-800-2000-122.

Лига безопасного интернета: <https://ligainternet.ru/hotline/>

Роскомнадзор: <https://eais.rkn.gov.ru/feedback/>

Мини–кейсы для практики» (короткие реальные ситуации для разбора)

Возраст 10–13 лет

1. «В игре предлагают скачать мод с супероружием».

Ответ: Никогда не скачивай файлы с непроверенных сайтов. Это может быть вирус. Используй только официальные магазины.

2. «В чате появляется обидный комментарий о тебе».

Ответ: Не отвечай обидчику. Сохрани скриншот, расскажи взрослому и заблокируй нарушителя.

3. «В социальной сети советуют «лайфхак», где нужно ввести пароль, чтобы открыть секретный контент».

Ответ: Никогда не вводи свои пароли! Это обман. Пароль хранится только у тебя и родителей.

Возраст 14–17 лет

1. «Приходит письмо на почту: «Вы выиграли смартфон, перейдите по ссылке»».

Ответ: Это фишинг. Никогда не переходи по ссылкам из таких писем. Проверь адрес отправителя и игнорируй подозрительные сообщения.

2. «В социальной сети тебе пишет человек, который представляется ровесником, но просит личные фото»

Ответ: Не отправлять! Это может быть взрослый мошенник (груминг). Прекратить контакт, заблокировать, пожаловаться в соцсеть.

3. «Друг прислал файл через мессенджер: «Смотри срочно!»

Ответ: Сначала уточни у друга, отправлял ли он это. Не открывай подозрительные файлы без проверки.

Возраст 18+ (студенты, молодёжь)

1. «В чате появляется «скидка 90% на авиабилеты» с неизвестной ссылки»

Ответ: Проверить акцию на официальном сайте авиакомпании. Подозрительные сайты — игнорировать.

2. «На форуме пишут: «Переведи 500 Р, и завтра получишь 5000 Р»».

Ответ: Это финансовая пирамида/мошенничество. Игнорировать и блокировать.

3. «В Онлайн-конференции появился неизвестный участник и включил неприемлемый контент».

Ответ: Сообщить администратору, удалить нарушителя, использовать пароль и «зал ожидания» для входа.

4. «Тебе присылают фейковое приглашение от «университета» на конкурс с просьбой заполнить паспортные данные».

Ответ: Проверить конкурс на официальном сайте вуза. Никогда не вводить паспортные данные по ссылкам из писем.