**Информационная безопасность**

**Для родителей**

1. **ПАМЯТКА ДЛЯ РОДИТЕЛЕЙ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ**

Определение термина "информационная безопасность детей" содержится в Федеральном законе N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию", регулирующим отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию. Согласно данному закону "информационная безопасность детей" – это состояние защищенности, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

В силу Федерального закона N 436-ФЗ информацией, причиняющей вред здоровью и (или) развитию детей, является:

1. информация, запрещенная для распространения среди детей;

2. информация, распространение которой ограничено среди детей определенных возрастных категорий.

1. **«Группы смерти»: как распознать и предотвратить угрозу**

В настоящее время сохраняется опасность вовлечения обучающихся в деструктивные группы, пропагандирующие суицидальное поведение и нападения на образовательные организации. В связи с этим актуален материал от НИЦ Мониторинга и профилактики, представляющий важную информацию о «группах смерти».

В карточках, разработанных специалистами НИЦМП для сотрудников образовательных учреждений и родительского сообщества, можно найти ответы на следующие вопросы:

▫какая история и реальность у «групп смерти»;

▫в чем опасность моральной паники в отношении данного феномена;

▫почему подростки попадают в деструктивные сообщества;

▫как распознать вовлеченность в деструктивные группы;

▫куда можно обратиться за помощью.

*Сами карточки для скачивания здесь:* <https://disk.yandex.ru/d/8kf19hfMbB8O6Q>

1. **Памятки для родителей** *для скачивания***:** <https://disk.yandex.ru/d/PSpL4e2psKns7g>
2. **Как мошенники обманывают подростков: 5 этапов представили в карточках**

⌛ Как мошенники обманывают подростков: 5 этапов представили в карточках

1 Выбор цели

Дети и подростки — в зоне риска. Мошенники ищут их в соцсетях, играх, чатах.

2 Завоевание доверия

Представляются «курьером», «техподдержкой» или «учителем». Создают срочную ситуацию: «аккаунт заблокирован», «ошибка в доставке».

3 Давление и изоляция

Подключают «следователя», угрожают арестом родителей. Переводят общение в Telegram. Запрещают говорить с семьёй.

4 Принуждение к действиям

Говорят: «Переведи деньги на безопасный счёт», «декларируй средства», «пройди проверку».

5 Исчезновение

Получили деньги — заблокировали, исчезли. Ребёнок один на один с паникой и последствиями.

🔎 Главное:

Ни один официальный орган не требует денег или кодов по телефону.

Говорите с детьми. Объясняйте: если страшно — звони родителям.

*Сами карточки для скачивания здесь:* <https://disk.yandex.ru/d/J7-LApSTf0vlSg>

1. Родительский контроль: <https://hi-tech.mail.ru/review/107483-roditelskiy-kontrol-na-telefone/#anchor171049740081479625>

**Для обучающихся**

1. **ПАМЯТКА ДЛЯ ОБУЧАЮЩИХСЯ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ**

**НЕЛЬЗЯ**

1. Всем подряд сообщать свою частную информацию (настоящие имя, фамилию, телефон, адрес, номер школы, а также фотографии свои, своей семьи и друзей);

2. Открывать вложенные файлы электронной почты, когда не знаешь отправителя;

3. Грубить, придираться, оказывать давление - вести себя невежливо и агрессивно;

4. Не распоряжайся деньгами твоей семьи без разрешения старших - всегда спрашивай родителей;

5. Не встречайся с Интернет-знакомыми в реальной жизни - посоветуйся со взрослым, которому доверяешь.

**ОСТОРОЖНО**

1. Не все пишут правду. Читаешь о себе неправду в Интернете - сообщи об этом своим родителям или опекунам;

2. Приглашают переписываться, играть, обмениваться - проверь, нет ли подвоха;

3. Незаконное копирование файлов в Интернете - воровство;

4. Всегда рассказывай взрослым о проблемах в сети - они всегда помогут;

5. Используй настройки безопасности и приватности, чтобы не потерять свои аккаунты в соцсетях и других порталах.

**МОЖНО**

1. Уважай других пользователей;

2. Пользуешься Интернет-источником - делай ссылку на него;

3. Открывай только те ссылки, в которых уверен;

4. Общаться за помощью взрослым - родители, опекуны и администрация сайтов всегда помогут.

1. **ИНФОРМАЦИОННАЯ ПАМЯТКА ДЛЯ ОБУЧАЮЩИХСЯ**

**Социальные сети**

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebook уже зарегистрирован миллиард человек,что является одной седьмой всех жителей планеты. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях,может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.

**Основные советы по безопасности в социальных сетях:**

1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;

2. Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;

3. Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь?

Подумай, прежде чем что-то опубликовать, написать и загрузить;

4. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;

5. Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;

6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;

7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

**Электронная почта**

Электронная почта - это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Обычно электронный почтовый ящик выглядит следующим образом: имя\_пользователя@имя\_домена. Также кроме передачи простого текста, имеется возможность передавать файлы.

**Основные советы по безопасной работе с электронной почтой:**

1. Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге;

2. Не указывай в личной почте личную информацию. Например, лучше выбрать "музыкальный\_фанат@" или "рок2013" вместо "тема13";

3. Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;

4. Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;

5. Если есть возможность написать самому свой личный вопрос, используй эту возможность;

6. Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах;

7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы;

8. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на "Выйти".

**Мобильный телефон**

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами.

Однако, средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений.

Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность.

Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

**Основные советы для безопасности мобильного телефона:**

Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;

Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?

Необходимо обновлять операционную систему твоего смартфона;

Используй антивирусные программы для мобильных телефонов;

Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;

После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies;

Периодически проверяй, какие платные услуги активированы на твоем номере;

Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;

Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

**Online игры**

Современные онлайн-игры - это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки исследуют данный им мир, общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт. За удовольствие они платят: покупают диск, оплачивают абонемент или приобретают какие-то опции.

Все эти средства идут на поддержание и развитие игры, а также на саму безопасность: совершенствуются системы авторизации, выпускаются новые патчи (цифровые заплатки для программ), закрываются уязвимости серверов.

В подобных играх стоит опасаться не столько своих соперников, сколько кражи твоего пароля, на котором основана система авторизации большинства игр.

**Основные советы по безопасности твоего игрового аккаунта:**

1. Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков;

2. Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов;

3. Не указывай личную информацию в профайле игры;

4. Уважай других участников по игре;

5. Не устанавливай неофициальные патчи и моды;

6. Используй сложные и разные пароли;

7. Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

Подраздел Мошенничество

**В целях своевременного информирования населения о новых видах и способах совершения преступлений в сфере информационно-коммуникационных технологий** специализированным подразделением управления по борьбе с киберпреступлениями, функционирующим в системе Министерства внутренних дел России созданы официальные аккаунты «Вестник Киберполиции России» в социальных сетях «Одноклассники» (<https://ok.ru/group/70000008643680>), «Вконтакте» (<https://vk.com/cyberpolice_rus>), кроссплатформенном мессенджере «Телеграм» (t.me/cyberpolice\_rus) и агрегаторе новостей «Дзен» (<https://dzen.ru/id/66f3a635b44c3033e86bf6ce> ), в которых публикуется информация о новых видах дистанционных мошенничеств и рекомендации по соблюдению цифровой гигиены.

**Как понять, что вам пишут со взломанного аккаунта?**

Взлом и подмена аккаунтов — один из самых популярных способов мошенничества. Злоумышленники получают доступ к страницам в мессенджерах или соцсетях и начинают рассылать сообщения от имени настоящего человека.

Обычно цель проста: заставить знакомых жертвы перевести деньги, переслать коды из SMS, установить «удобное приложение» или перейти по фишинговой ссылке. Всё выглядит убедительно, потому что пишет вроде бы ваш друг или коллега, и именно поэтому этот приём так опасен.

Признаки взломанного аккаунта

Странные просьбы. «Срочно переведи деньги», «выручай, у меня неприятности», «проголосуй в конкурсе»

Непривычный стиль общения. Пишет слишком официально или, наоборот, сухо. Использует слова/эмодзи, которых раньше не применял.

Подозрительные ссылки или файлы. «Смотри фото», «Тебе подарок», «Скачай документ» — без объяснений, часто с укороченными или странными ссылками.

Изоляция. «Не звони, я не могу говорить».

Повышенная активность. Начинает писать в нетипичное время (ночью, рано утром). Давит срочностью и не отвечает на ваши отвлекающие вопросы.

Быстрые проверки

Смените канал связи. Напишите/позвоните по привычному номеру или в другом мессенджере. У мошенников чаще всего нет доступа ко всем каналам сразу.

Намеренная «ошибка». Ответьте с заведомо неверной деталью («ты же знаешь, что я поставил машину на ремонт» — ту, которой не существует). Свой человек поправит, злоумышленник — нет.

Пауза. Сделайте «тишину» на 10–15 минут. Мошенники часто сыпят сообщениями, давят срочностью и быстро переключаются на следующую цель.

«Капча памяти». Попросите уточнить 2–3 детали, которые знает только ваш человек: где вы виделись в последний раз, как зовут вашего питомца, какой подарок вы дарили и т.п.



**Как противостоять злоумышленникам: вовлечение в противоправную деятельность через мессенджеры и социальные сети**

*Памятки для размещения:* <https://disk.yandex.ru/d/TmMp0PAcHxEIbw>

**Дропперство**

Памятки: <https://disk.yandex.ru/d/3zv0PLzJ7FAk_g>

**Чем грозит дропперство?!**

Сравнительно недавно в Интернете появилась ещё одна угроза – дропперство. Под видом легкого заработка для подростков скрывается помощь мошенникам и даже террористам.

Уголовная ответственность наступает с 16-летнего возраста, но родители несут ответственность за банковские операции детей с 14 лет.

Мы подготовили карточки, в которых рассказываем, что делают дропперы, можно ли случайно стать соучастником преступления и как обезопасить себя и своих близких.

Обязательно поделитесь карточками с родными, друзьями и знакомыми!

Карточки: <https://disk.yandex.ru/d/Dr0uZGHpXeiEdg>

**Для ДОУ**

1. **ПАМЯТКА ДЛЯ РОДИТЕЛЕЙ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ**

Определение термина "информационная безопасность детей" содержится в Федеральном законе N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию", регулирующим отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию. Согласно данному закону "информационная безопасность детей" – это состояние защищенности, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

В силу Федерального закона N 436-ФЗ информацией, причиняющей вред здоровью и (или) развитию детей, является:

1. информация, запрещенная для распространения среди детей;

2. информация, распространение которой ограничено среди детей определенных возрастных категорий.

2) **Информационная безопасность для дошкольников**

Проблема обеспечения информационной безопасности является как социальной, так и педагогической, она связана с всеобщим и повсеместным использованием гаджетов. Совместная деятельность детского сада и семьи поможет оградить подрастающее поколение от отрицательного влияния информационной среды.

Информационная безопасность детей дошкольного возраста – это состояние их защищенности от информации, способной причинить вред здоровью, а также их духовному, психическому или физическому развитию.

 Какую информацию можно отнести к негативной?

* побуждающую детей к совершению действий, угрожающих их жизни и здоровью, в том числе причинение вреда себе, самоубийство;
* способную пробудить у детей интерес и желание попробовать алкогольную продукцию, табачные изделия, заниматься бродяжничеством;
* содержащую информацию порнографического характера;
* отрицающую семейные ценности;
* оправдывающую жесткость и насилие в отношении людей или животных;
* содержащую нецензурную лексику.

Современный ребенок все больше времени проводит за компьютером или телевизором. В определенной степени это связано с высокой познавательной мотивацией, с любознательностью и стремлением узнать что-то новое.

Правила при использовании телевизора ребенком дошкольного возраста.

1. После просмотра любого видео анализируйте с ребенком значимость увиденного, поведение и поступки героев. Спрашивайте, как поступил бы ваш ребенок в аналогичной ситуации.
2. Оказывайте детям помощь при выборе телепередач и контролируйте время нахождения дошкольника у телевизора. Общее время просмотра телевизора детьми дошкольного возраста не должно превышать 6-7 часов в неделю. Ребенок не должен находиться у экрана более получаса подряд.
3. Покажите ребенку разницу между отечественной и зарубежной телепродукцией. Составьте видеотеку с российскими мультфильмами, детскими фильмами, передачами.
4. Беседуйте с ребенком о том, что существуют запретные передачи, расскажите ему о возрастной маркировке на экране.
5. Важно! Ребенок должен сидеть точно напротив экрана телевизора на расстоянии не меньше двух метров от него.

Компьютерные технологии могут стать эффективным средством развития ребенка дошкольного возраста. Но его необдуманное использование может причинить непоправимый вред здоровью. Компьютерные игры провоцируют перевозбуждение участков головного мозга ребенка, отвечающих за удовольствие. Ребенок становится зависимым и чувствует постоянную необходимость в получении такого удовлетворения. Виртуальная реальность, с которой ребенок сталкивается в ходе игры, меняет его восприятие. Все больше дошкольников пытаются перенести в жизнь то, что увидели на экране или мониторе компьютера.

Существуют требования, которые предъявляются к играм для детей дошкольного возраста:

* в играх должна быть информация о правилах;
* символы и звуковые сигналы должны подсказывать ребенку правильность и последовательность его действий;
* при использовании букв, размер их должен быть больше традиционного компьютерного шрифта;
* изображения должны быть крупными, без отвлекающих мелких деталей;
* в обучающей игре должны использоваться только правильные ответы, доступные дошкольнику;
* не рекомендовано применение оценок в бальной системе.

Правила при использовании компьютера и сети Интернет.

1. Контролируйте, какие сайты посещают дети. Ребенок не должен использовать Интернет свободно.
2. Проговорите о правилах пользования Интернетом. Четко определите временные границы, а также сайты, которые он может посещать.
3. Не разрешайте детям распространять в интернете личную информацию (номер мобильного телефона, адрес, а также размещать фотографии.
4. Рассказывайте ребенку об опасностях, с которыми он может столкнуться в сети Интернет. Ребенок должен знать, что нельзя открывать подозрительные ссылка или файлы, несмотря на их привлекательный вид.
5. Объясните ребенку, что нельзя открывать файлы, полученные от незнакомых людей, так как они могут содержать негативную информацию либо вирусы.
6. Установите на компьютер *(планшет)* антивирусную программу, средства фильтрации входящего контента. При необходимости подключите *«родительский контроль»*.
7. Просматривайте историю посещений интернет-ресурсов на смартфоне, планшете, компьютере, чтобы знать какие сайты посещал ребенок.

Созданные правила должны соответствовать возрастным особенностям и развитию каждого ребенка. Кроме того, педиатры не рекомендуют детям до 7-ми лет пользоваться компьютером/Интернетом. Злоупотребление любым цифровым устройством опасно для физического здоровья ребенка дошкольного возраста, так как может спровоцировать ухудшение зрения, аллергические реакции, гиподинамию, сердечно-сосудистые заболевания.

Знание элементарных правил, отбора и использования информации родителями и детьми позволит сохранить здоровье дошкольников и обеспечить им всестороннее развитие.



1. **Как родителям справиться с гаджет-зависимостью ребенка**

**Как определить зависимость от гаджетов**

Для начала вам нужно осознать, что привязанность ребенка к гаджетам – смартфонам или планшетам – связана с устоявшимися отношениями в семье. Помните: чтобы ваш ребенок избавился от зависимости, ему нужна не сила воли, а благополучное эмоциональное состояние дома. Поэтому следует ввести и соблюдать понятные и четкие правила, которые ограничивают использование гаджетов, всем членам семьи.

Вы можете самостоятельно провести диагностику с помощью готового [**чек-листа**](https://mdou97.edu.yar.ru/bezopasnost/chek_list_priznaki_gadzhet_zavisimosti_u_rebenka.pdf), который поможет определить зависимость от смартфона или планшета. Отмечайте галочкой в кружках наличие того или иного показателя у своего ребенка. Если набрали половину и более галочек, можно говорить о зависимости.

**Как анализировать эмоциональные проблемы ребенка**

Гаджеты становятся опасными, когда виртуальные игры в них вытесняют живую игру, а виртуальный мир становится для ребенка главным источником эмоций. Основные причины зависимости для ребенка — это негативные эмоции, которые он переживает дома. Например: «страшно», «скучно», «непредсказуемо», «обидно», чувства одиночества, ненужности, брошенности.

В этом случае вам необходимо обратить внимание на то, как ребенку живется в эмоциональном смысле: счастлив ли он, часто ли радуется, смеется. Также всем членам вашей семьи необходимо проанализировать, в каком тоне они обычно взаимодействуют с ребенком.

В качестве эксперимента используйте только одобрительный тон в течение нескольких дней и посмотрите, что изменится в поведении ребенка. При этом важно задавать вопросы и слушать ответы малыша, не угрожать и не ругать его. Чаще хвалите ребенка, поощряйте, выражайте интерес к нему.

**Как обсудить проблему в семье**

Если у вас мало времени и много задач, необходимо вводить для ребенка новые правила и новые занятия. Это поможет избежать ситуации, когда ваше удобство становится причиной зависимости ребенка.

Вполне нормально, если какое-то время малыш будет с гаджетом, когда вы заняты своими делами, — если это не повторяется каждый раз, когда вы чем-то заняты. Также можете определить временной интервал, на который ребенку разрешается использовать гаджет. Главное — действуйте последовательно.
Находите другие занятия, помимо гаджетов, не обездвиживайте ребенка с помощью них. Чаще всего гаджет — это ответ на скуку, поэтому вы должны научить детей читать книги, листать журналы, рисовать. Помимо того, нужно водить ребенка на разные площадки, вместе гулять на природе, если есть возможность — возить в музеи и на выставки.

Постоянно создавайте и стимулируйте для ребенка реальные впечатления. Можете предложить ему конструктор, забытые игрушки, материалы для творчества, интересные предметы: для дошкольников это коробка, сумка, скотч, ножницы, веревочка, вата, сыпучие продукты, таз с водой и мелкие предметы для купания в тазу. Поинтересуйтесь у ребенка, как он начинает свою любимую игру, например, «работу» кукольного салона красоты или лечение зверей.

Существует целый вариант досугов в рамках семьи: показать, как собрать природные материалы, разрешить набрать целый пакет, принести их домой и возиться с ними. Также можете дать ребенку на прогулку мячик и позволить поиграть с ним, попросить знакомых с доброй собакой иногда позволять ребенку играть с ней.

Не менее важно просить ребенка оказывать помощь в делах, вовлекать в уход за бытом: разогревать пищу, укладывать волосы, убираться на полке. Например, вы можете попросить ребенка рисовать и лепить для вас, показывать вам сценки, во время которых вы будете благодарным и восхищенным зрителем для ребенка.

**Как сформулировать правила использования гаджетов**

Важнее всего для родителей — разобраться в себе и своих требованиях для ребенка: можно или нельзя играть с гаджетами, это плохо или хорошо, правило действует для всех или только для ребенка. Если взрослый сначала разрешает гаджет, а затем запрещает — поощряет и наказывает гаджетом, у ребенка появится зависимость.

Продумайте с другими членами семьи, как обсудить правила пользования гаджетами. Например, что должно быть сделано до гаджета, каковы реальные задачи и нагрузка, когда играть нельзя, например, за едой, вместо занятий, сколько можно играть.

Затем озвучьте эти правила ребенку и начинайте следовать им. Если ребенок возражает — признайте его чувства, дайте возразить, не ругайте, посочувствуйте, но правило не меняйте. Важно помнить: чтобы ваш ребенок избавился от зависимости, ему нужна не сила воли, а благополучное эмоциональное состояние дома.

В решении этой проблемы важно самим не пользоваться гаджетом без необходимости, откладывать его подальше, уменьшить число аккаунтов в социальных сетях и чатах, больше двигаться и разговаривать. Воспользуйтесь **памяткой**, которая поможет вам ввести правила использования гаджетов в семье.

*Памятка и чек-лист для скачивания здесь:* <https://disk.yandex.ru/d/CMKVqPSUFhNkFQ>