## **Памятка 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;

5. Пройди обучение на сайте "Сетевичок" и получи паспорт цифрового гражданина!

## **Советы по безопасности работы в общедоступных сетях Wi-fi**

1. Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;

2. Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;

3. При использовании Wi-Fi отключи функцию "Общий доступ к файлам и принтерам". Данная функция закрыта по умолчанию, однако некоторые пользователи активируют ее для удобства использования в работе или учебе;

4. Не используй публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту;

5. Используй только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно "https://";

6. В мобильном телефоне отключи функцию "Подключение к Wi-Fi автоматически". Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

## **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.

## **Рекомендации по организации работы в информационном пространстве**

1. Перед началом работы необходимо четко сформулировать цель и вопрос поиска информации.
2. Желательно выработать оптимальный алгоритм поиска информации в сети Интернет, что значительно сократит время и силы, затраченные на поиск.
3. Заранее установить временный лимит (2-3 часа) работы в информационном пространстве (просмотр телепередачи, чтение, Интернет).
4. Во время работы необходимо делать перерыв на 5-10 минут для снятия физического напряжения и зрительной нагрузки.
5. Необходимо знать 3-4 упражнения для снятия зрительного напряжения и физической усталости.
6. Работать в хорошо проветренном помещении, при оптимальном освещении и в удобной позе.
7. Не стоит легкомысленно обращаться со спам-письмами и заходить на небезопасные веб-сайты. Для интернет-преступников вы становитесь лёгкой добычей.
8. При регистрации в социальных сетях, не указывайте свои персональные данные, например: адрес или день рождения.
9. Не используйте в логине или пароле персональные данные.
10. Все это позволяет интернет-преступникам получить данные доступа к аккаунтам электронной почты, а также инфицировать домашние ПК для включения их в бот-сеть или для похищения банковских данных родителей.
11. Создайте собственный профиль на компьютере, чтобы обезопасить информацию, хранящуюся на нем.
12. Не забывайте, что факты, о которых вы узнаете в Интернете, нужно очень хорошо проверить, если выбудете использовать их в своей домашней работе. Целесообразно сравнить три источника информации, прежде чем решить, каким источникам можно доверять.
13. О достоверности информации, помещенной на сайте можно судить по самому сайту, узнав об авторах сайта.
14. Размещая информацию о себе, своих близких и знакомых на страницах социальных сетей, спросите предварительно разрешение у тех, о ком будет эта информация.
15. Не следует размещать на страницах веб-сайтов свои фотографии и фотографии своих близких и знакомых, за которые вам потом может быть стыдно.
16. Соблюдайте правила этики при общении в Интернете: грубость провоцирует других на такое же поведение.
17. Используя в своей работе материал, взятый из информационного источника (книга, периодическая печать, Интернет), следует указать этот источник информации или сделать на него ссылку, если материал был вами переработан.

## **Родителям**

## Общие рекомендации

Дети и подростки используют интернет по-разному и для разных целей по мере взросления. Родители детей из каждой возрастной группы беспокоятся о разных вещах и хотят контролировать разные действия. Однако есть набор общих рекомендаций, которые следует помнить родителям детей и подростков любого возраста.

### Храните имена пользователей и пароли в безопасности

Для многих используемых детьми веб-сайтов требуется имя пользователя и пароль. Убедитесь, что дети знают, что эту информацию нельзя передавать никому, даже друзьям. Возможно, никто не хочет причинить ребенку никакого вреда, но даже в розыгрышах из лучших побуждений что-то может пойти не так и доставить неприятности. Храните имена пользователей и пароли в секрете и обязательно меняйте пароли, если подозреваете, что кто-то мог их узнать.

### Периодически меняйте пароли

Наряду с напоминанием детям о том, что никому нельзя сообщать свои пароли, также рекомендуется периодически менять пароли. Утечки данных происходят постоянно, а утечка паролей подвергает риску кражи личных данных и другим проблемам с кибербезопасностью. Настройте расписание смены паролей учетных записей каждые 3-6 месяцев или каждый раз, когда платформа сообщает о взломах или утечках данных. Вы можете использовать менеджер паролей, чтобы отслеживать все свои пароли в интернете и упростить их поиск вашим детям.

### Не разглашайте личную информацию в интернете

Дети и подростки не должны сообщать никому в интернете свое полное настоящее имя, адрес, район проживания, номер телефона и прочие данные. Общее правило: никогда не сообщать информацию, которая могла бы помочь интернет-хищникам найти их. Даже небольших деталей, таких как название школы или спортивной команды, достаточно, чтобы раскрыть личность. Если дети используют сайты, позволяющие общаться с незнакомцами, например, платформы социальных сетей, убедитесь, что они знают, что эта информация является конфиденциальной.

### Будьте внимательны в социальных сетях

Действия детей и подростков в социальных сетях требуют особой осторожности и внимания. Интернет огромен, но компрометирующие фотографии, грубые комментарии и личная информация могут оставить сильный след, и часто навсегда. Напомните детям, что все опубликованное в интернете сразу становится общедоступным, и любой может увидеть это. Даже частные учетные записи иногда подвергаются утечкам или атакам злоумышленников. Если вы не хотите, чтобы какой-либо неприятный момент повторялся и тревожил ваших детей, объясните им, что нужно внимательно относиться своим публикациям.

## Педагогам

Когда речь заходит об информационной безопасности, обычно мы начинаем думать о компьютерах, сетях, интернете и хакерах. Но для образовательной среды проблема стоит шире: в ограждении учащегося от информации, которая может негативно повлиять на его формирование и  развитие, то есть о пропаганде различной направленности.

**Понятие информационной безопасности**

Под информационной безопасностью понимается защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации.

**Основные угрозы информационной безопасности**

Современная информационная система представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Практически каждый компонент может подвергнуться внешнему воздействию или выйти из строя. Компоненты автоматизированной информационной системы можно разбить на следующие группы:

***Аппаратные средства.*** Это компьютеры и их составные части (процессоры, мониторы, терминалы, периферийные устройства – принтеры, контроллеры, кабели, линии связи и т.д.);

**Программное обеспечение.** Это приобретенные программы, исходные, объектные, загрузочные модули; операционные системы и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т.д.;

**Данные,** хранимые временно и постоянно, на дисках, флэшках, печатные, архивы, системные журналы и т.д.;

**Персонал.**Пользователи, системные администраторы, программисты и др.

Опасные воздействия на компьютерную информационную систему можно подразделить на случайные и преднамеренные. Анализ опыта проектирования, изготовления и эксплуатации информационных систем показывает, что информация подвергается различным случайным воздействиям на всех этапах цикла жизни системы. Причинами случайных воздействий при эксплуатации могут быть:

* аварийные ситуации из-за стихийных бедствий и отключений электропитания;
* отказы и сбои аппаратуры;
* ошибки в программном обеспечении;
* ошибки в работе персонала;
* помехи в линиях связи из-за воздействий внешней среды.

Преднамеренные воздействия – это целенаправленные действия нарушителя. В качестве нарушителя могут выступать служащий, посетитель, конкурент, наемник. Действия нарушителя могут быть обусловлены разными мотивами:

* недовольством служащего своей карьерой;
* взяткой;
* любопытством;
* конкурентной борьбой;
* стремлением самоутвердиться любой ценой.

Можно составить гипотетическую модель потенциального нарушителя:

* квалификация нарушителя на уровне разработчика данной системы;
* нарушителем может быть как постороннее лицо, так и законный пользователь системы;
* нарушителю известна информация о принципах работы системы;
* нарушитель выбирает наиболее слабое звено в защите.

Наиболее распространенным и многообразным видом компьютерных нарушений является несанкционированный доступ. Несанкционированный доступ использует любую ошибку в системе защиты и возможен при нерациональном выборе средств защиты, их некорректной установке и настройке.

Проведем классификацию каналов несанкционированного доступа, по которым можно осуществить хищение, изменение или уничтожение информации:

**Через человека:**

* хищение носителей информации;
* чтение информации с экрана или клавиатуры;
* чтение информации из распечатки.

**Через программу:**

* перехват паролей;
* дешифровка зашифрованной информации;
* копирование информации с носителя.

**Через аппаратуру:**

* подключение специально разработанных аппаратных средств, обеспечивающих доступ к информации;
* перехват побочных электромагнитных излучений от аппаратуры, линий связи, сетей электропитания и т.д.

Особо следует остановиться на угрозах, которым могут подвергаться компьютерные сети. Основная особенность любой компьютерной сети состоит в том, что ее компоненты распределены в пространстве. Связь между узлами сети осуществляется физически с помощью сетевых линий и программно с помощью механизма сообщений. При этом управляющие сообщения и данные, пересылаемые между узлами сети, передаются в виде пакетов обмена. Компьютерные сети характерны тем, что против них предпринимают так называемые удаленные атаки. Нарушитель может находиться за тысячи километров от атакуемого объекта, при этом нападению может подвергаться не только конкретный компьютер, но и информация, передающаяся по сетевым каналам связи.

## Методические и справочные материалы

# [Видеоролик о защите детских персональных данных](https://yandex.ru/video/preview/16104957404796875131)

[Материалы к урокам безопасного интернета](http://ligainternet.ru/encyclopedia-of-security/parents-and-teachers/parents-and-teachers-detail.php?ID=3652)

Методические материалы по вопросам информационной безопасности и защиты персональных данных в сети «Интернет» для несовершеннолетних разных возрастных категорий, а также родителей (законных представителей)

<https://27.rkn.gov.ru/directions/pd/p26200/>

## Методические и справочные материалы

**Проекты и конкурсы Фонда развития Интернета**

Фонд Развития Интернет реализует исследовательские, образовательные и информационно-просветительские проекты, направленные на развитие Интернета, изучение его влияния на пользователей, повышение цифровой компетентности и безопасное использование сети Интернет. Его миссия состоит в содействии развитию сети Интернет как открытой платформы для социальных, образовательных, научных и экономических инноваций [Фонд развития Интернета](http://www.fid.su/projects/contests)

**Международный проект «**Международное измерение информационной безопасности**»**

В условиях транснационального характера вызовов и угроз в ИКТ-сфере проект направлен на критический анализ подходов различных государств и негосударственных акторов к обеспечению информационной безопасности и поиск общих точек для сотрудничества в этой сфере.

[Методические рекомендации](http://legalacts.ru/doc/pismo-minobrnauki-rossii-ot-14052018-n-08-1184-o-napravlenii/%22%20%5Ct%20%22_blank) о размещении на информационных стендах, официальных интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении и  использовании сети "Интернет".
Письмо Департамента государственной политики в сфере общего образования Министерства образования и науки РФ от 14.05.2018 N 08-1184.

## **Раздел сайта "Информационная безопасность"****Нормативное регулирование**

Баннер-ссылка «[Сообщить о противоправном контенте](https://www.edu.yar.ru/safety/hot_line.html)», ведущий на страницу с информацией об алгоритме действий в случае выявления в сети «Интернет» материалов с признаками запрещенной информации и адресами сайтов, на которые можно отправить сообщение.

[Информационные материалы](https://www.edu.yar.ru/safety/hot_line.html), разработанные Роскомнадзором России.
Материалы, рекомендованные к размещению на сайте Роскомнадзором России в целях ограничения доступа к сайтам сети «Интернет», содержащим информацию, распространение которой в Российской Федерации запрещено. Текст и документы для публикации на сайте образовательной организации вы найдете по адресу https://www.edu.yar.ru/safety/hot\_line.html

[Федеральный закон от 24.07.1998 № 124-ФЗ](http://docs.cntd.ru/document/901713538) «Об основных гарантиях прав ребенка в Российской Федерации»
[Федеральный закон от 13.03.2006 № 38-ФЗ](http://docs.cntd.ru/document/901971356) «О рекламе»
[Федеральный закон от 27.07.2006 № 149-ФЗ](http://docs.cntd.ru/document/901990051) «Об информации, информационных технологиях и о защите информации»
[Федеральный закон от 27.07.2006 № 152-ФЗ](http://docs.cntd.ru/document/901990046) «О персональных данных»
[Федеральный закон от 28.12.2010 № 390-ФЗ](http://docs.cntd.ru/document/902253576) «О безопасности»
[Федеральный закон от 29.12.2010 № 436-ФЗ](http://docs.cntd.ru/document/902254151) «О защите детей от информации, причиняющей вред их здоровью и развитию»
[Указ Президента РФ от 31.12.2015 № 683](http://docs.cntd.ru/document/420327289) «О Стратегии национальной безопасности Российской Федерации»
[Указ Президента РФ от 05.12.2016 № 646](http://docs.cntd.ru/document/420384668) «Об утверждении Доктрины информационной безопасности Российской Федерации»
[СанПиН 2.4.2.2821-10](http://docs.cntd.ru/document/902256369) «Санитарно-эпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях»
[Приказ Минкомсвязи России от 16.06.2014 № 161](https://digital.gov.ru/ru/documents/4446/)«Об утверждении требований к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию»
[КОНЦЕПЦИЯ информационной безопасности детей](http://static.government.ru/media/files/mPbAMyJ29uSPhL3p20168GA6hv3CtBxD.pdf)Утверждена распоряжением Правительства Российской Федерации от 2 декабря 2015 г. No2471-р
[Постановление Правительства РФ от 1 ноября 2012 г. N 1119](http://government.ru/docs/all/84743/) «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
[Постановление Правительства РФ от 21 марта 2012 г. N 211](http://docs.cntd.ru/document/902336380) «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»

## **Раздел сайта "Информационная безопасность"****Локальные  нормативные акты  в сфере обеспечения информационной безопасности обучающихся**

План мероприятий образовательной организации по обеспечению информационной безопасности детей

**Локальные акты, регламентирующие работу с персональными данными**

Политика в области обработки персональных данных.

Положение об обработке персональных данных
Положение об обработке персональных данных без использования средств автоматизации
Правила доступа к персональным данным
Правила рассмотрения запросов субъектов персональных данных
Другие локальные акты образовательной организации, относящие к данной тематике

**Сайт и использование сети Интернет**

Положение об официальном web-сайте школы
Положение об использовании сети Интернет
Порядок доступа обучающихся к информационно-телекоммуникационным сетям и базам данных, учебным и методическим материалам, музейным фондам, материально-техническим средствам обеспечения образовательной деятельности
Правила пользования локальной сетью и сетью Интернет
Другие локальные акты образовательной организации, относящие к данной тематике

Используйте при подготовке – материалы, подготовленные  Центром телекоммуникаций и информационных систем в образовании:

## **Раздел  "Информационная безопасность"****Обучающимся**

[Информационная памятка](http://legalacts.ru/doc/pismo-minobrnauki-rossii-ot-14052018-n-08-1184-o-napravlenii/#100075)
Информационная памятка для обучающихся для размещения на официальных интернет-ресурсах на официальных Интернет-ресурсах

**Информация о мероприятиях, проектах и программах, направленных на повышение информационной грамотности обучающихся:**

[Сайт "Азбука цифрового мира"](https://www.edu.yar.ru/azbuka/)
Азбука цифрового мира. Увлекательные комиксы, специализированные тренажёры и интересные игры!

[Сайт "Подросток и закон"](https://podrostok.edu.yar.ru/safety/index.html)