

Муниципальное бюджетное общеобразовательное учреждение
«Средняя общеобразовательная школа № 115 г. Челябинска»
(МБОУ «СОШ № 115 г. Челябинска»)

ПРИКАЗ

25.08.2025

№ 317

г. Челябинск

**Об организации работы по
обеспечению информационной
безопасности**

В целях реализации всесторонних мер по повышению информационной безопасности, ограничения доступа обучающихся к видам информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и развитию детей, а также не соответствующей задачам образования

ПРИКАЗЫВАЮ:

1. Утвердить:

- План основных мероприятий по обеспечению информационной безопасности участников образовательных отношений в МБОУ «СОШ № 115 г. Челябинска» на 2025-2026 учебный год (Приложение 1);
- Правила использования сети Интернет в МБОУ «СОШ № 115 г. Челябинска» (Приложение 2);
- Инструкцию для работников школы о порядке действий при осуществлении контроля использования обучающимися сети Интернет (Приложение 3);
- Инструкцию для обучающихся по обеспечению информационной безопасности при использовании сети Интернет (Приложение 4);
- Положение о порядке и условиях присутствия (допуска) детей при проведении зрелищных мероприятий. (Приложение 5).

2. Яровому Николаю Михайловичу, ответственному лицу за обеспечение информационной безопасности, проводить тематические занятия (лекции) с работниками МБОУ «СОШ № 115 г. Челябинска» по вопросам обеспечения информационной безопасности, в том числе предупреждение и пресечение имущественных преступлений, совершаемых злоумышленниками с

использованием информационно-телекоммуникационных технологий с занесением записи в Журнал информационной безопасности (Приложение 6).

3. Контроль за исполнением приказа возложить на заместителя директора по безопасности Ярового Николая Михайловича.

Директор

Н.Б. Пикатова

С приказом от 25.08.2025 № 317 ознакомлены:

Чадин А.А.

Калинина Е.А.

Аmineва А.Д.	Лимонова К.А.
Анчугина А.Ю.	Малеева Л.В.
Архангельская А.Ю.	Маркина Г.В.
Архипова Д.Ю.	Масленцева Н.Д.
Арефьева И.А.	Мельникова Н.А.
Баруля О.А.	Меньшикова А.А.
Васильева О.В.	Мизин С.А.
Верховых Е.А.	Микаленус Я.В.
Власова О.О.	Мирошниченко Е.С.
Гарашук В.И.	Назарова Д.С.
Гоменюк Т.А.	Плотникова И.М.
Грызунова А.М.	Плетнева С.И.
Егорова Е.С.	Поляшова Н.В.
Ефепанова И.А.	Попова А.В.
Ефимова А.А.	Прядко О.В.
Закирова Л.А.	Прилипухова Н.А.
Захарова А.С.	Рогожина М.Ю.
Завьялова А.И.	Разумовская И.А.
Иванова О.В.	Сиражитдинов Д.Д.
Иванова А.А.	Свирский И.С.
Истомина Д.А.	Смирнова А.М.
Кагановская П.Е.	Сухомлинова А.М.
Кандакова Е.А.	Суслова О.А.
Капралова Е.А.	Уфаркина Д.И.
Кармишина М.В.	Холина Е.А.
Кондратьев В.В.	Черепанова Е.Я.
Краснянская Ю.С.	Черюсова С.С.
Кудряшова П.А.	Чуманова Л.Л.
Кукаркина Е.Ю.	Шайхтдинова Е.А.
Курочкина В.В.	Шамаева Т.Г.
Лейнгард О.З.	Шумина Е.К.

Лимонова Ю.П. <i>lef</i>	Яковлева М.В. <i>chief</i>
	Яровой Н.М. <i>Яр</i>

Исполнитель: Яровой Н.М.

Зам. директора по безопасности 8 (351) 741-04-10

Приложение 1
к приказу от 25.08.2025 № 317

**План основных мероприятий по обеспечению
информационной безопасности участников образовательных отношений
на 2025-2026 учебный год**

Задачи:

- развитие информационной компетентности детей и подростков, их родителей (законных представителей), работников, о характере и видах современных информационных угроз, представляющих опасность для здоровья и развития детей, вреде, причиняемом современными средствами массовой коммуникации, и существующих способах его предупреждения и минимизации.

- профилактика у обучающихся интернет-зависимости, игровой зависимости и правонарушений с использованием информационно-телекоммуникационных технологий, формирование навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде через обучение их способам защиты от вредной информации

- формирование у детей и подростков критического отношения к информации, распространяемой в сетях Интернет и мобильной (сотовой) связи посредством СМИ и иных электронных средств массовой коммуникации, и умений эффективно применять меры самозащиты от информации, причиняющей вред здоровью и развитию детей, и нежелательных для них контактов в сети Интернет.

- предупреждение и пресечение имущественных преступлений, совершаемых злоумышленниками с использованием информационно-телекоммуникационных технологий.

№	Мероприятия	Сроки	Ответственный
Для обучающихся			
1	Информирование обучающихся: о видах информации, способной причинить вред их здоровью и развитию детей, и ее негативных последствиях; о способах незаконного распространения информации, способной причинить вред здоровью и развитию детей, в сетях Интернет и мобильной (сотовой) связи (в том числе путем рассылки SMS-сообщений незаконного содержания).	Сентябрь	Классные руководители, учителя информатики
2	Обучение школьников правилам ответственного и безопасного пользования услугами Интернет и мобильной (сотовой) связи, в том числе способам защиты от противоправных и иных общественно опасных посягательств в информационно-телекоммуникационных сетях.	в течение учебного года	Классные руководители, учителя информатики

3	Проведение специальных уроков по медиабезопасности.	1 раз в триместр	Классные руководители, учителя информатики
4	Проведение внеурочных занятий с учащимися по теме «Приемы безопасной работы в интернете».	в течение учебного года	Классные руководители, учителя информатики
5	Проведение классных часов, направленных на предупреждение социального, расового, национального и религиозного неравенства.	По плану воспитательной работы	Зам. директора по воспитательной работе, классные руководители, учителя информатики
6	Участие во Всероссийском образовательном проекте «Урок Цифры»	в течение учебного года (по графику)	Учителя информатики, классные руководители
7	Организация свободного доступа обучающихся к высококачественным и сетевым образовательным ресурсам, в том числе к системе современных учебных материалов по всем предметам	в течение учебного года	Руководитель ОУ
8	Правила безопасного использования сети Интернет для школьников младших классов. Тематический урок «Безопасность в Интернете»	1 раз в триместр	Учителя информатики, классные руководители
9	Размещение правил безопасного использования сети Интернет для обучающихся на сайте школы	в течение учебного года	Уфаркина Д.И.
10	Проведение тематических бесед: «Безопасность в интернете» «Сетевой этикет» «Форумы и чаты в Интернете»	Классные часы	Верховых Е.А. Классные руководители
11	Участие в конкурсах, олимпиадах, связанных с Информационной безопасностью	в течение учебного года	Верховых Е.А., Яровой Н.М., учителя информатики, классные руководители
Для педагогов			
13	Проведение тематических занятий (лекций) по вопросам обеспечения информационной безопасности, в том числе предупреждение и пресечение имущественных преступлений, совершаемых злоумышленниками с использованием информационно-	в течение учебного года	Яровой Н.М

	телекоммуникационных технологий.		
14	Внедрение в практику: формирование у обучающихся компетентности пользования Интернетом, обеспечивающее их безопасность в интернет-пространстве.	в течение учебного года	Учителя информатики
15	Участие в обучающих семинарах для руководителей, учителей по созданию надежной системы защиты детей от противоправного контента в образовательной среде школы и дома.	в течение учебного года	Яровой Н.М учителя школы
16	Ознакомление членов пед. коллектива с нормами 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»	сентябрь	Яровой Н.М
17	Организация свободного доступа учителей к высококачественным и сетевым образовательным ресурсам, в том числе к системе современных учебных материалов по всем предметам	в течении года	Пикатова Н.Б.
Для родителей			
19	Разъяснительная работа с родителями, направленная на защиту детей от негативного влияния СМИ (на родительских собраниях). «О негативном влиянии агрессивного контента СМИ и иных СМК на детскую психику и способах его предупреждения».	в течение учебного года	Яровой Н.М, классные руководители
20	Ознакомление родителей с информацией по защите детей от распространения вредной для них информации.	сентябрь	Классные руководители
21	Размещение на сайте школы рекомендаций и информации для родителей по 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»	сентябрь	Уфаркина Д.И.
22	Индивидуальное консультирование и обучение родителей по вопросам: - профилактика формирования интернет и игровой зависимости у детей; - применению эффективных мер защиты детей от информации, причиняющей вред их здоровью и развитию, и нежелательных для них контактов в сетях; - формирования навыков защиты персональных данных.	в течение учебного года	Классные руководители, социально-психологическая служба
23	Родительское собрание «Безопасность детей в Интернете»	сентябрь	Верховых Е.А., Яровой Н.М
Внедрение систем исключения доступа к информации, несовместимой с задачами гражданского становления детей, а также средств фильтрации и иных аппаратно-программных и технико-технологических устройств			
24	Мониторинг функционирования и	в течении года	Учителя

	использования в школе программного продукта, обеспечивающего контент-фильтрацию Интернет-трафика		информатики
25	Мониторинг качества предоставления провайдером услуги доступа к сети Интернет образовательным учреждением с обеспечением контент-фильтрации Интернет-трафика	в течении года	Учителя информатики

Приложение 2
к приказу от 25.08.2025 № 317

Правила использования сети Интернет в МБОУ «СОШ № 115 г. Челябинска»

1. Общие положения

1.1. Использование сети Интернет в образовательном учреждении направлено на решение задач учебно-воспитательного процесса.

1.2. Настоящие Правила регулируют условия и порядок использования сети Интернет в образовательном учреждении.

1.3. Настоящие Правила имеют статус локального нормативного акта образовательного учреждения.

2. Организация использования сети Интернет в образовательном учреждении

2.1. Правила вводятся в действие приказом директора школы.

2.2. Директор школы отвечает за обеспечение эффективного и безопасного доступа к сети Интернет в школе, а также за выполнение установленных правил.

2.3. Во время уроков и других занятий в рамках учебного плана контроль использования обучающимися сети Интернет осуществляет учитель, ведущий занятие.

При этом учитель:

наблюдает за использованием компьютера и сети Интернет обучающимися;

принимает меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу.

2.4. Во время свободного доступа обучающихся к сети Интернет вне учебных занятий, контроль использования ресурсов Интернета осуществляют педагогические работники, ответственные за используемую точку доступа к сети Интернет.

Работник образовательного учреждения:

наблюдает за использованием компьютера и сети Интернет обучающимися;

принимает меры по пресечению обращений к ресурсам, не имеющих отношения к образовательному процессу;

сообщает классному руководителю о преднамеренных попытках обучающегося осуществить обращение к ресурсам, не имеющим отношения к образовательному процессу.

2.5. При использовании сети Интернет в школе обучающимся предоставляется доступ только к тем ресурсам, содержание которых не противоречит законодательству Российской Федерации, и которые имеют прямое отношение к образовательному процессу.

Выполнение такого требования осуществляется с помощью специальных технических средств и программного обеспечения контентной фильтрации, установленного в школе.

2.6. Пользователи сети Интернет в школе должны учитывать, что технические средства и программное обеспечение не могут обеспечить полную фильтрацию ресурсов сети Интернет вследствие частого обновления ресурсов. В связи с этим

существует вероятность обнаружения обучающимися ресурсов, не имеющих отношения к образовательному процессу и содержание, которых противоречит законодательству Российской Федерации. Участникам использования сети Интернет в школе следует осознавать, что школа не несет ответственности за случайный доступ к подобной информации, размещенной не на Интернет-ресурсах школы.

2.7. Принципы размещения информации на Интернет-ресурсах школы призваны обеспечивать:

соблюдение действующего законодательства Российской Федерации, интересов и прав граждан;

защиту персональных данных обучающихся, учителей и сотрудников;

достоверность и корректность информации.

2.8. Персональные данные обучающихся (включая фамилию и имя, класс/год обучения, возраст, фотографию, данные о месте жительства, телефонах и пр., иные сведения личного характера) могут размещаться на Интернет-ресурсах, создаваемых школой, только с письменного согласия родителей или иных законных представителей обучающихся.

Персональные данные учителей и сотрудников школы размещаются на ее Интернет-ресурсах только с письменного согласия лица, чьи персональные данные размещаются.

2.9. В информационных сообщениях о мероприятиях, размещенных на сайте школы

без уведомления и получения согласия упомянутых лиц или их законных представителей, могут быть указаны лишь фамилия и имя обучающегося либо фамилия, имя и отчество учителя, сотрудника или родителя.

2.10. При получении согласия на размещение персональных данных представитель школы обязан разъяснить возможные риски и последствия их опубликования. Школа не несет ответственности за такие последствия, если предварительно было получено письменное согласие лица (его законного представителя) на опубликование персональных данных.

3. Использование сети Интернет в образовательном учреждении

3.1. Использование сети Интернет в школе осуществляется, как правило, в целях образовательного процесса.

3.2. По разрешению администрации школы учителя, сотрудники и обучающиеся вправе:

размещать собственную информацию в сети Интернет на Интернет-ресурсах школы; иметь учетные записи на Интернет-ресурсах школы.

3.3. Обучающемуся запрещается:

обращаться к ресурсам, содержание и тематика которых не допустимы для несовершеннолетних и/или нарушают законодательство Российской Федерации (эротика, порнография, пропаганда насилия, терроризма, политического или религиозного экстремизма, национальной, расовой и т.п. розни, иные ресурсы схожей направленности);

осуществлять любые сделки через Интернет;

осуществлять загрузки файлов на компьютер школы без специального разрешения;

распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.

**Инструкция
для работников МБОУ «СОШ № 115 г. Челябинска»
«О порядке действий при осуществлении контроля
использования обучающимися сети Интернет»**

1. Настоящая инструкция устанавливает порядок действий работников школы при обнаружении:

- обращения обучающихся к контенту, не имеющему отношения к образовательному процессу;
- отказа при обращении к контенту, имеющему отношение к образовательному процессу, вызванного техническими причинами.

2. Контроль использования обучающимися сети Интернет осуществляют:
во время занятия – проводящий его учитель и (или) педагогический работник школы, специально выделенный для помощи в проведении занятий;
во время использования сети Интернет для свободной работы обучающихся – педагогические работники школы.

3. Учитель:

определяет время и место работы обучающихся в сети Интернет с учетом использования в образовательном процессе соответствующих технических возможностей, а также длительность сеанса работы одного обучающегося;

наблюдает за использованием обучающимися компьютеров и сети Интернет;

способствует осуществлению контроля объемов трафика школы в сети Интернет;

запрещает дальнейшую работу обучающегося в сети Интернет на уроке (занятии) в случае нарушения им порядка использования сети Интернет и предъявляемых к обучающимся требований при работе в сети Интернет;

доводит до классного руководителя информацию о нарушении обучающимся правил работы в сети Интернет;

принимает необходимые меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу.

4. При обнаружении ресурса, который, по мнению учителя, содержит информацию, запрещенную для распространения в соответствии с законодательством Российской Федерации, или иного потенциально опасного для обучающихся контента, он сообщает об этом ответственному за проверку работоспособности системы контентной фильтрации.

5. В случае отказа доступа к ресурсу, разрешенному в школе, учитель также сообщает об этом ответственному за проверку работоспособности системы контентной фильтрации.

**Инструкция
для обучающихся по обеспечению информационной безопасности
при использовании сети Интернет в МБОУ «СОШ № 115 г. Челябинска»**

С каждым годом молодежи в интернете становится больше, а школьники одни из самых активных пользователей Рунета. Между тем, помимо огромного количества

возможностей, интернет несет и проблемы. Эта памятка должна помочь тебе безопасно находиться в сети.

Компьютерные вирусы

Компьютерный вирус – это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. В дополнение к этому, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена зараженная программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет.

Методы защиты от вредоносных программ:

1. Используй современные операционные системы, имеющие серьезный уровень защиты от вредоносных программ;
2. Постоянно устанавливай патчи (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;
3. Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ устанавливаться на твоём персональном компьютере;
4. Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
5. Ограничь физический доступ к компьютеру для посторонних лиц;
6. Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников;
7. Не открывай компьютерные файлы, полученные из ненадежных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

Сети WI-FI

Wi-Fi – это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистрировала бренд "WECA", что обозначало словосочетание "WirelessFidelity", который переводится как "беспроводная точность".

До нашего времени дошла другая аббревиатура, которая является такой же технологией. Это аббревиатура "Wi-Fi". Такое название было дано с намеком на стандарт высшей звуковой техники Hi-Fi, что в переводе означает "высокая точность".

Да, бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в интернет. Но многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными.

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 твоё 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.

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.

Электронные деньги

Электронные деньги – это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги.

Электронные деньги появились совсем недавно и именно из-за этого во многих государствах до сих пор не прописано про них в законах.

В России же они функционируют и о них уже прописано в законе, где их разделяют на несколько видов – анонимные и не анонимные. Разница в том, что анонимные – это те, в которых разрешается проводить операции без идентификации пользователя, а в неанонимных идентификация пользователя является обязательной.

Также следует различать электронные фиатные деньги (равны государственным валютам) и электронные нефтяные деньги (не равны государственным валютам).

Основные советы по безопасной работе с электронными деньгами:

1. Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства;

2. Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;

3. Выбери сложный пароль. Преступникам будет не просто угадать сложный пароль.

Надежные пароли – это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак и т.п. Например, \$tR0ng!;

4. Не вводи свои личные данные на сайтах, которым не доверяешь.

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. Этот 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".

Кибербуллинг или виртуальное издевательство

Кибербуллинг – преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет сервисов.

Основные советы по борьбе с кибербуллингом:

1. Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт;

2. Управляй своей киберрепутацией;

3. Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;

4. Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно;

5. Соблюдай свою виртуальную честь смолоду;

6. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;

7. Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;

8. Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

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, зайти 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 самую 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 скриншотов;

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.

Фишинг или кража личных данных

Обычной кражей денег и документов сегодня уже никого не удивишь, но с развитием интернет-технологий злоумышленники переместились в интернет, и продолжают заниматься "любимым" делом.

Так появилась новая угроза: интернет-мошенничества или фишинг, главная цель, которого состоит в получении конфиденциальных данных пользователей – логинов и паролей.

На английском языке phishing читается как фишинг (от fishing – рыбная ловля, password – пароль).

Основные советы по борьбе с фишингом:

1. Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;
2. Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;
3. Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем;
4. Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты;
5. Установи надежный пароль (PIN) на мобильный телефон;
6. Отключи сохранение пароля в браузере;
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.

Цифровая репутация

Цифровая репутация – это негативная или позитивная информация в сети о тебе.

Компрометирующая информация, размещенная в интернете, может серьезным образом отразиться на твоей реальной жизни. "Цифровая репутация" – это твой имидж, который формируется из информации о тебе в интернете.

Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких - все это накапливается в сети.

Многие подростки легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Ты даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять тебя на работу.

Комментарии, размещение твоих фотографий и другие действия могут не исчезнуть даже после того, как ты их удалишь. Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о тебе окружающие люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой – как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.

Основные советы по защите цифровой репутации:

1. Подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети;
2. В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только "для друзей";
3. Не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать.

Авторское право

Современные школьники – активные пользователи цифрового пространства. Однако далеко не все знают, что пользование многими возможностями цифрового мира требует соблюдения прав на интеллектуальную собственность.

Термин "интеллектуальная собственность" относится к различным творениям человеческого ума, начиная с новых изобретений и знаков, обозначающих

собственность на продукты и услуги, и заканчивая книгами, фотографиями, кинофильмами и музыкальными произведениями.

Авторские права – это права на интеллектуальную собственность на произведения науки, литературы и искусства. Авторские права выступают в качестве гарантии того, что интеллектуальный/творческий труд автора не будет напрасным, даст ему справедливые возможности заработать на результатах своего труда, получить известность и признание.

Никто без разрешения автора не может воспроизводить его произведение, распространять, публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать/исполнять в эфире или размещать в Интернете.

Использование "пиратского" программного обеспечения может привести к многим рискам: от потери данных к твоим аккаунтам до блокировки твоего устройства, где установлена нелегальная программа. Не стоит также забывать, что существуют легальные и бесплатные программы, которые можно найти в сети. О портале Сетевичок.рф - твой главный советчик в сети. Здесь ты можешь узнать о безопасности в сети понятным и доступным языком, а при возникновении критической ситуации обратиться за советом. А также принять участие в конкурсах и стать самым цифровым гражданином!

Приложение 5
к приказу от 25.08.2025 № 317

Положение о порядке и условиях присутствия (допуска) детей при проведении зрелищных мероприятий

1. Общие положения

Настоящее Положение разработано на основании Федерального закона от № 436-ФЗ от 29.12.2010 г. «О защите детей от информации, причиняющей вред их здоровью и развитию» (в ред. от 28.04.2023 г.) и других законодательных актов Российской Федерации для обеспечения административных и организационных мер по защите детей от информации, причиняющей вред их здоровью и развитию.

Положение определяет порядок и условия присутствия детей на публичных показах, при публичном исполнении, демонстрации посредством зрелищного мероприятия информационной продукции, запрещенной для детей.

2. Основные понятия, используемые в настоящем Положении

В настоящем Положении используются следующие основные понятия:

зрелищное мероприятие - демонстрация информационной продукции в месте доступном для детей, и в месте, где присутствует значительное число лиц, не принадлежащих к обычному кругу семьи, в том числе посредством проведения театрально-зрелищных мероприятий, культурно-просветительных и зрелищно-развлекательных мероприятий;

места, доступные для детей - общественные места, доступ ребенка в которые и (или) нахождение ребенка в которых не запрещены, в том числе общественные места, в которых ребенок имеет доступ к продукции средств массовой информации и (или) размещаемой в информационно-телекоммуникационных сетях информационной продукции;

информационная безопасность детей – состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию;

информационная продукция – информация, распространяемая посредством зрелищных мероприятий;

доступ детей к информации - возможность получения и использования детьми свободно распространяемой информации;

информационная продукция для детей - информационная продукция, соответствующая по тематике, содержанию и художественному оформлению физическому, психическому, духовному и нравственному развитию детей;

информация, причиняющая вред здоровью и (или) развитию детей, - информация (в том числе содержащаяся в информационной продукции для детей), распространение которой среди детей запрещено или ограничено в соответствии с Федеральным законом от № 436-ФЗ от 29.12.2010 г. «О защите детей от информации, причиняющей вред их здоровью и развитию» (в ред. от 28.04.2023 г.);

информация порнографического характера - информация, представляемая в виде натуралистических изображения или описания половых органов человека и (или) полового сношения либо сопоставимого с половым сношением действия сексуального характера, в том числе такого действия, совершаемого в отношении животного;

классификация информационной продукции - распределение информационной продукции в зависимости от ее тематики, жанра, содержания и художественного оформления по возрастным категориям детей в порядке, установленном Федеральным законом от № 436-ФЗ от 29.12.2010 г. «О защите детей от информации, причиняющей вред их здоровью и развитию» (в ред. от 28.04.2023 г.);

натуралистические изображение или описание - изображение или описание в любой форме и с использованием любых средств человека, животного, отдельных частей тела человека и (или) животного, действия (бездействия), события, явления, их последствий с фиксированием внимания на деталях, анатомических подробностях и (или) физиологических процессах;

оборот информационной продукции - предоставление и (или) распространение информационной продукции, включая публичный показ, публичное исполнение (в том числе посредством зрелищных мероприятий), распространение посредством эфирного или кабельного вещания, информационно-телекоммуникационных сетей, в том числе сети Интернет, и сетей подвижной радиотелефонной связи;

знак информационной продукции - графическое и (или) текстовое обозначение информационной продукции в соответствии с классификацией информационной продукции, предусмотренной частью 3 статьи 6 Федерального закона от 29 декабря 2010 г № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

3. Виды информации, причиняющей вред здоровью и (или) развитию детей

1. К информации, причиняющей вред здоровью и (или) развитию детей, относится:

1) информация, предусмотренная частью 2 пункта 3 настоящего Положения и запрещенная для распространения среди детей;

2) информация, которая предусмотрена частью 3 пункта 3 настоящего Положения с учетом положений статей 4.1, 4.2, 4.3, 4.4 настоящего Положения и распространение которой среди детей определенных возрастных категорий ограничено.

2. К информации, запрещенной для распространения среди детей, относится информация:

1) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;

2) способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

3) обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению

к людям или животным, за исключением случаев, предусмотренных Федеральным законом от № 436-ФЗ от 29.12.2010 г. «О защите детей от информации, причиняющей вред их здоровью и развитию» (в ред. от 28.04.2023 г.);

3.1) содержащая изображение или описание сексуального насилия;

4) отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи;

5) оправдывающая противоправное поведение;

6) содержащая нецензурную брань;

7) содержащая информацию порнографического характера;

3. К информации, распространение которой среди детей определенных возрастных категорий ограничено, относится информация:

1) представляемая в виде изображения или описания жестокости, физического и (или) психического насилия (за исключением сексуального насилия), преступления или иного антиобщественного действия;

2) вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;

3) представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;

4) содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

4. Классификация информационной продукции

4.1. Информационная продукция для детей, не достигших возраста шести лет

К информационной продукции для детей, не достигших возраста шести лет, может быть отнесена информационная продукция, содержащая информацию, не причиняющую вреда здоровью и (или) развитию детей (в том числе информационная продукция, содержащая оправданные ее жанром и (или) сюжетом эпизодические ненатуралистические изображение или описание физического и (или) психического насилия (за исключением сексуального насилия) при условии торжества добра над злом и выражения сострадания к жертве насилия и (или) осуждения насилия).

4.2. Информационная продукция для детей, достигших возраста шести лет

К допускаемой к обороту информационной продукции для детей, достигших возраста шести лет, может быть отнесена информационная продукция, предусмотренная статьей 4.1 настоящего Положения, а также информационная продукция, содержащая оправданные ее жанром и (или) сюжетом:

1) кратковременные и ненатуралистические изображение или описание заболеваний человека (за исключением тяжелых заболеваний) и (или) их последствий в форме, не унижающей человеческого достоинства;

2) ненатуралистические изображение или описание несчастного случая, аварии, катастрофы либо ненасильственной смерти без демонстрации их последствий, которые могут вызывать у детей страх, ужас или панику;

3) не побуждающие к совершению антиобщественных действий и (или) преступлений эпизодические изображение или описание этих действий и (или) преступлений при условии, что не обосновывается и не оправдывается их допустимость и выражается отрицательное, осуждающее отношение к лицам, их совершающим.

4.3. Информационная продукция для детей, достигших возраста двенадцати лет

К допускаемой к обороту информационной продукции для детей, достигших возраста двенадцати лет, может быть отнесена информационная продукция,

предусмотренная статьей 4.2 настоящего Положения, а также информационная продукция, содержащая оправданные ее жанром и (или) сюжетом:

1) эпизодические изображение или описание жестокости и (или) насилия (за исключением сексуального насилия) без натуралистического показа процесса лишения жизни или нанесения увечий при условии, что выражается сострадание к жертве и (или) отрицательное, осуждающее отношение к жестокости, насилию (за исключением насилия, применяемого в случаях защиты прав граждан и охраняемых законом интересов общества или государства);

2) изображение или описание, не побуждающие к совершению антиобщественных действий (в том числе к потреблению алкогольной и спиртосодержащей продукции, участию в азартных играх, занятию бродяжничеством или попрошайничеством), эпизодическое упоминание (без демонстрации) наркотических средств, психотропных и (или) одурманивающих веществ, табачных изделий при условии, что не обосновывается и не оправдывается допустимость антиобщественных действий, выражается отрицательное, осуждающее отношение к ним и содержится указание на опасность потребления указанных продукции, средств, веществ, изделий;

3) не эксплуатирующие интереса к сексу и не носящие возбуждающего или оскорбительного характера эпизодические ненатуралистические изображение или описание половых отношений между мужчиной и женщиной, за исключением изображения или описания действий сексуального характера.

4.4. Информационная продукция для детей, достигших возраста шестнадцати лет

К допускаемой к обороту информационной продукции для детей, достигших возраста шестнадцати лет, может быть отнесена информационная продукция, предусмотренная пунктом 4.3 настоящего Положения, а также информационная продукция, содержащая оправданные ее жанром и (или) сюжетом:

1) изображение или описание несчастного случая, аварии, катастрофы, заболевания, смерти без натуралистического показа их последствий, которые могут вызывать у детей страх, ужас или панику;

2) изображение или описание жестокости и (или) насилия (за исключением сексуального насилия) без натуралистического показа процесса лишения жизни или нанесения увечий при условии, что выражается сострадание к жертве и (или) отрицательное, осуждающее отношение к жестокости, насилию (за исключением насилия, применяемого в случаях защиты прав граждан и охраняемых законом интересов общества или государства);

3) информация о наркотических средствах или о психотропных и (или) об одурманивающих веществах (без их демонстрации), об опасных последствиях их потребления с демонстрацией таких случаев при условии, что выражается отрицательное или осуждающее отношение к потреблению таких средств или веществ и содержится указание на опасность их потребления;

4) отдельные бранные слова и (или) выражения, не относящиеся к нецензурной брани;

5) не эксплуатирующие интереса к сексу и не носящие оскорбительного характера изображение или описание половых отношений между мужчиной и женщиной, за исключением изображения или описания действий сексуального характера.

5. Знак информационной продукции

1. Обозначение категории информационной продукции знаком информационной продукции и (или) текстовым предупреждением об ограничении распространения информационной продукции среди детей осуществляется с соблюдением требований Федерального закона от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (в ред. от 28.04.2023 г.) ее производителем и (или) распространителем следующим образом:

1) применительно к категории информационной продукции для детей, не достигших возраста шести лет, - в виде цифры "0" и знака "плюс";

2) применительно к категории информационной продукции для детей, достигших возраста шести лет, - в виде цифры "6" и знака "плюс" и (или) текстового предупреждения в виде словосочетания "для детей старше шести лет";

3) применительно к категории информационной продукции для детей, достигших возраста двенадцати лет, - в виде цифры "12" и знака "плюс" и (или) текстового предупреждения в виде словосочетания "для детей старше 12 лет";

4) применительно к категории информационной продукции для детей, достигших возраста шестнадцати лет, - в виде цифры "16" и знака "плюс" и (или) текстового предупреждения в виде словосочетания "для детей старше 16 лет";

5) применительно к категории информационной продукции, запрещенной для детей, - в виде цифры "18" и знака "плюс" и (или) текстового предупреждения в виде словосочетания "запрещено для детей".

2. Производитель, распространитель информационной продукции размещают знак информационной продукции и (или) текстовое предупреждение об ограничении ее распространения среди детей перед началом демонстрации зрелищного мероприятия. Размер знака информационной продукции должен составлять не менее чем пять процентов площади экрана.

3. Размер знака информационной продукции должен составлять не менее чем пять процентов площади афиши или иного объявления о проведении соответствующего зрелищного мероприятия, объявления о показе, а также входного билета, приглашения либо иного документа, предоставляющих право посещения такого мероприятия.

4. Текстовое предупреждение об ограничении распространения информационной продукции среди детей выполняется на русском языке, а в случаях, установленных Федеральным законом от 1 июня 2005 года № 53-ФЗ "О государственном языке Российской Федерации", на государственных языках республик, находящихся в составе Российской Федерации, других языках народов Российской Федерации или иностранных языках.

6. Порядок и условия присутствия (допуска) детей при проведении зрелищных мероприятий (включая демонстрацию фильмов при кино- и видеообслуживании)

1. Дети допускаются на зрелищные мероприятия при условии соответствия их возраста категории информационной продукции зрелищного мероприятия.

2. При посещении детьми публичных проектов, зрелищных мероприятий (включая демонстрацию фильмов при кино- и видеообслуживании) необходимо выполнять следующие условия:

- В присутствии родителей или иных законных представителей детей, достигших возраста шести лет, допускается оборот информационной продукции, предусмотренной пунктом 4.3 настоящего Положения.

- До начала демонстрации посредством зрелищного мероприятия информационной продукции ей присваивается знак информационной продукции. В случае демонстрации нескольких видов информационной продукции для детей разных возрастных категорий указанный знак должен соответствовать продукции для старшей возрастной категории. Указанный знак размещается на афишах и иных объявлениях о проведении зрелищного мероприятия, а также на входных билетах, приглашениях и иных документах, предоставляющих право его посещения.

- В случае если в рекламном объявлении дается информация о цикле мероприятий, предназначенных для детей разных возрастных категорий, знак классификации информационной продукции проставляется напротив названия каждого мероприятия.

3. Демонстрация посредством зрелищного мероприятия информационной продукции, содержащей информацию, предусмотренную пунктом 5 настоящего Порядка, предваряется непосредственно перед началом зрелищного мероприятия

звуковым сообщением о недопустимости или об ограничении присутствия на такой демонстрации детей соответствующих возрастных категорий;

4. Организатор зрелищного мероприятия, посредством которого демонстрируется информационная продукция, содержащая информацию, запрещенную для распространения среди детей в соответствии с частью 2 пункта 3 настоящего Положения, обязан не допускать на такое мероприятие лиц, не достигших восемнадцатилетнего возраста. В целях выполнения указанной обязанности, а также в случае возникновения у лица, непосредственно осуществляющего реализацию входных билетов, приглашений и иных документов, предоставляющих право посещения зрелищного мероприятия, посредством которого демонстрируется информационная продукция, содержащая информацию, запрещенную для распространения среди детей в соответствии с частью 2 пункта 3 настоящего Положения, или лица, контролирующего проход на такое зрелищное мероприятие, сомнения в достижении лицом, желающим приобрести входной билет, получить приглашение или иной документ, предоставляющий право посещения зрелищного мероприятия, либо пройти на такое зрелищное мероприятие (далее - посетитель), совершеннолетия лицо, непосредственно осуществляющее реализацию входных билетов, приглашений и иных документов, предоставляющих право посещения зрелищного мероприятия, или лицо, контролирующее проход на такое зрелищное мероприятие, вправе потребовать у посетителя документ, удостоверяющий личность (в том числе документ, удостоверяющий личность иностранного гражданина или лица без гражданства в Российской Федерации) и позволяющий установить возраст этого посетителя.

5. Демонстрация информационной продукции, содержащей информацию, запрещенную для распространения среди детей в местах, доступных для детей, а также предоставление доступа к информационной продукции, распространяемой посредством информационно-телекоммуникационных сетей, в том числе сети Интернет, в местах, доступных для детей осуществляется с соблюдением требований к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию.

7. Ответственность за правонарушения в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию

Ответственность за правонарушения в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию, влечет за собой ответственность в соответствии с законодательством Российской Федерации.

Приложение 6
к приказу от 25.08.2025 № 317

Журнал информационной безопасности

№ п/п	ФИО	Дата проведения	Тема	Подпись