УПРАВЛЕНИЕ ОБЩЕГО ОБРАЗОВАНИЯ
АДМИНИСТРАЦИИ ГОРОДА ЛИВНЫ

ПРИКАЗ

17 августа 2021 года № 163

О реализации Плана мероприятий по выполнению
Концепции по обеспечению информационной безопасности детей,
производства и оборота информационной продукции для детей
в городе Ливны на 2021 – 2027 годы

В соответствии с Федеральными законами от 25 июля 2002 года № 114-ФЗ «О противодействии экстремистской деятельности», от 27 июля 2006 года № 152-ФЗ «О персональных данных», от 29 декабря 2010 года № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации», распоряжением Губернатора Орловской области от 30 июля 2021 года №51-р, распоряжением администрации города Ливны от 17.08.2021 года №540 «Об утверждении Плана мероприятий по выполнению Концепции по обеспечению информационной безопасности детей, производства и оборота информационной продукции для детей в городе Ливны на 2021 – 2027 годы», в целях повышения эффективности мер, направленных на защиту прав и интересов несовершеннолетних в части защиты от информации, причиняющей вред их здоровью и развитию, информирования учащихся о социально опасных явлениях и мерах защиты в сети Интернет, в том числе социальных сетях, формирования у детей навыков самостоятельного и ответственного потребления информационной продукции, ответственности за свои действия в информационном пространстве, повышения уровня медиаграмотности детей, а также противодействия распространению информации, причиняющей вред здоровью и развитию несовершеннолетних, п р и к а з ы в а ю:

1. Считать утратившим силу приказ управления общего образования администрации города Ливны от 12 октября 2018 года № 231 «О реализации Плана мероприятий по выполнению Концепции по обеспечению информационной безопасности детей, производства и оборота

информационной продукции для детей в городе Ливны на 2018 – 2020 годы»».

2. Принять к исполнению План мероприятий по выполнению Концепции по обеспечению информационной безопасности детей, производства и оборота информационной продукции для детей на 2021 – 2027 годы на территории города Ливны (приложение 1).

3. Руководителям образовательных организаций:

3.1. Назначить ответственных лиц за обеспечение информационной безопасности детей и подростков;

3.2. Организовать многоступенчатую систему внутреннего контроля (со стороны учителей, ответственных лиц, администрации образовательной организации) за проведением мероприятий по защите детей от информации, наносящей вред их здоровью и духовному развитию;

3.3. Обеспечить доступ к сети Интернет с использованием лицензионного программного обеспечения;

3.4. Обеспечить установку контент-фильтра на каждый компьютер, подключенный к сети Интернет, к которому имеют доступ дети;

3.5. Организовать постоянный контроль исправного состояния контент-фильтров, препятствующих доступу к Интернет-сайтам, содержащим информацию, причиняющую вред здоровью и развитию детей;

3.6. Проводить проверки эффективности контентной фильтрации не реже 1 раза в месяц;

3.7. Проводить постоянный мониторинг безопасности официальных сайтов образовательных организаций;

3.8. Обеспечить контроль безопасности содержания приобретаемой информационной продукции для детей в соответствии с возрастными категориями;

3.9. Проводить не реже 1 раза в квартал ревизию библиотечных фондов на выявление литературы, причиняющей вред развитию и здоровью детей, в том числе экстремистского характера;

3.10. Обновлять не реже 1 раза в четверть в библиотеках учреждений данные из Федерального списка экстремистских материалов;

3.11. Организовать медиаобразование педагогов как условие обеспечения информационной безопасности (консультации, курсы, обучающие семинары);

3.12. Обеспечить реализацию программ профилактики игровой зависимости среди детей и подростков;

3.13. Организовать проведение среди родителей обучающихся просветительских мероприятий по вопросам медиабезопасности детей и подростков (приложение 4);

3.14. Внимательно относиться к рассмотрению предложений о проведении тренингов и лекций, программ (курсов) для обучающихся по вопросам нравственности, профилактики девиантного поведения (в том

числе, алкоголизма, наркомании, правонарушений и др.), предупреждения идеологии экстремизма и терроризма.

3.15. При поступлении предложений от общественных (некоммерческих, религиозных, и других) организаций или инициативных граждан о проведении тренингов и лекций, программ (курсов) и иных мероприятиях для обучающихся по вопросам духовного развития, нравственности, патриотического воспитания, профилактики девиантного поведения (в том числе алкоголизма, наркомании, правонарушений), предупреждения идеологии экстремизма и терроризма, и иным вопросам необходимо проверять факт отсутствия сведений о соответствующих организациях (гражданах) в:

- Едином федеральном списке организаций, в том числе иностранных и международных организаций, признанных в соответствии с законодательством Российской Федерации террористическими, размещенном на сайте Федеральной службы безопасности Российской Федерации;

- Перечне некоммерческих организаций, в отношении которых судом принято вступившее в законную силу решение о ликвидации или запрете деятельности по основаниям, предусмотренным Федеральным законом от 25 июля 2002 года № 114-ФЗ «О противодействии экстремистской деятельности», размещенном на сайте Министерства юстиции Российской Федерации;

- Перечне организаций и физических лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму, размещенном на сайте Федеральной службы по финансовому мониторингу.

3.16. Уточнять наличие рецензий (отзывов) на предлагаемые лекции (тренинги), курсы (программы) для обучающихся.

3.17. Изучать материалы, планируемые к использованию при проведении лекций (тренингов), курсов (программ), в части:

- соответствия возрастному цензу;

- использования сведений из нормативных правовых актов, специализированной (профессиональной) литературы, официальных источников;

- отсутствия информации, причиняющей вред здоровью и развитию детей, в том числе проверять факт отсутствия данных материалов в Федеральном списке экстремистских материалов, размещенном на сайте Министерства юстиции Российской Федерации.

3.18. При необходимости принимать решение о проведении экспертизы информационной продукции в целях обеспечения информационной безопасности в соответствии со статьей 4 Федерального закона от 29 декабря 2010 года № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», приказа Министерства связи и массовых коммуникаций Российской Федерации от 29.08.2012 № 217 «Об утверждении

порядка проведения экспертизы информационной продукции в целях обеспечения информационной безопасности детей».

3.19. Решение о проведении мероприятий внеурочной деятельности принимать по согласованию с родительскими комитетами (родителями, законными представителями) во исполнение требований статьи 44 Федерального закона от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации».

3.20. Обеспечить присутствие на проводимых лекциях (тренингах), курсах (программах) педагогических и (или) руководящих работников, компетентных в вопросах оценки содержания излагаемой информации с точки зрения возможности ее негативного психоэмоционального влияния на детей, и представителей родительского комитета (родителей, законных представителей) с целью своевременного реагирования, в том числе приостановки (прекращения) лекций (тренингов), курсов (программ).

3.21. Обязать педагогов и руководящий работников принимать деятельное участие в обеспечении исполнения требований части 9 статьи 13 Федерального закона от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации» о запрете использования, в том числе при проведении внеурочных мероприятий сторонними организациями и лицами, методов и средств обучения и воспитания, образовательных технологий, наносящих вред физическому или психическому здоровью обучающихся.

3.22. Оформить в соответствии с Федеральным законом от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», ст. 44 Федерального закона от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации» уведомление родителей (законных представителей) о снятии ответственности с руководителя образовательной организации в случае предоставления ими своим детям личных средств связи с выходом в сеть «Интернет» при посещении образовательной организации и ознакомить с данным уведомлением под роспись.

3.23. Обновить и доработать в соответствии с современной нормативно-правовой базой пакет документов, регламентирующий доступ педагогов, обучающихся и воспитанников к сети Интернет, обеспечивающий ограничение доступа обучающихся и воспитанников к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования.

3.24. Разместить на информационных стендах в фойе учреждений и в кабинетах, оснащенных персональными устройствами для выхода в сеть «Интернет», памятки, содержащие основные советы по обеспечению информационной безопасности обучающихся, воспитанников (приложения №2, 3).

3.25. Обеспечить на официальных сайтах функционирование самостоятельного и специализированного раздела «Информационная

безопасность», в рамках которого предусмотреть размещение следующей информации:

№	Раздел/подраздел	Формат представления материалов	Содержание материалов
1.	Локальные нормативные акты в сфере обеспечения информационной безопасности обучающихся	Копии документов в формате *PDF	Размещаются копии документов, т.е. сканированный вариант документа, соответствующий требованиям к параметрам сканирования. Размещаются документы, регламентирующие организацию и работу с персональными данными, планы мероприятий по обеспечению информационной безопасности обучающихся и другие.
2.	Нормативное регулирование	Копии документов в формате *PDF	Публикуются актуальные сведения о федеральных и региональных законах, письмах органов власти и другие нормативно-правовые документы, регламентирующие обеспечение информационной безопасности несовершеннолетних. Допускается вместо копий размещать гиперссылки на соответствующие документы на сайтах органов государственной власти.
3.	Педагогическим работникам	Текст на странице сайта Копии документов в формате *PDF	Размещаются методические рекомендации и указывается информация о мероприятиях, проектах и программах, направленных на повышение информационной грамотности педагогических работников.
4.	Обучающимся	Текст на странице сайта	Размещается информационная памятка (Приложение №3) и указывается информация о мероприятиях, проектах и программах, направленных на повышение информационной грамотности обучающихся.
5.	Родителям (законным представителям) обучающихся	Текст на странице сайта	Размещается информационная памятка (Приложение №4).
6.	Детские безопасные сайты	Текст на странице сайта	Размещается информация о рекомендуемых к использованию в учебном процессе безопасных сайтах, баннеры безопасных детских сайтов.

3.26. Принимать участие в организации и проведении мероприятий Единого урока по безопасности в сети «Интернет» (приложение 5) и

направлять отчеты об итогах участия в мероприятиях Единого урока по безопасности (приложение 6) на электронный адрес: livuoo@yandex.ru.

4. Отделу развития системы образования управления общего образования администрации города Ливны:

4.1. Осуществлять организацию изучения вопроса осуществления функционирования контентной фильтрации в образовательных организациях, подведомственных управлению общего образования администрации города Ливны, не реже 1 раза в полугодие.

4.2. Проводить ежегодный мониторинг организационно-административных мероприятий, направленных на обеспечение ограничения доступа обучающихся к видам информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, реализуемых образовательными организациями.

4.3. Своевременно направлять отчеты об итогах проведения Единого урока по безопасности в сети «Интернет» в образовательных организациях города Ливны в управление общего образования Департамента образования Орловской области.

5. Отделу дошкольного и общего образования управления общего образования администрации города Ливны:

5.1. Осуществлять организацию изучения вопроса работы комиссий по выявлению, изъятию и уничтожению экстремистских материалов, включённых в Федеральный список экстремистских материалов, в библиотечном фонде не реже 1 раза в полугодие.

5.2. Контролировать процесс медиаобразования педагогов как условия обеспечения информационной безопасности (консультации, курсы, обучающие семинары).

6. Контроль за исполнением настоящего приказа оставляю за собой.

Начальник управления Ю. А. Преображенский

Приложение 1
к приказу управления общего образования
администрации города Ливны
от 17 августа 2021 г. № 163

План мероприятий
по выполнению Концепции по обеспечению информационной безопасности детей, производства и оборота информационной продукции для детей в городе Ливны на 2021 – 2027 годы

№	Содержание пунктов плана	Срок исполнения	Ответственные исполнители	Ожидаемый результат
Глава 1. Организационно-подготовительный этап				
1.	Размещение на сайтах, порталах образовательных организаций сведений о ресурсах для детей и родителей (законных представителей), информации о возможностях по организации родительского контроля за доступом к сети Интернет	2021 – 2027 годы	Образовательные организации	Информирование родителей о механизмах предупреждения доступа несовершеннолетних к информации, причиняющей вред их здоровью и (или) развитию
2.	Подготовка и направление в образовательные организации методических и информационных материалов для педагогических работников, специалистов психолого-педагогических служб, по вопросам формирования культуры безопасного поведения несовершеннолетних в интернет-пространстве, предупреждения рисков вовлечения их в противоправную деятельность в сети Интернет	2021 – 2027 годы	Образовательные организации	Обеспечение образовательных организаций города Ливны, психолого-педагогических и медико-социальных центров, учреждений социальной защиты по вопросам формирования культуры безопасного поведения несовершеннолетних в интернет-пространстве, предупреждения рисков вовлечения их в противоправную деятельность в сети Интернет

Глава 2. Внедрение систем исключения доступа к информации, несовместимой с задачами гражданского становления детей, а также средств фильтрации и иных аппаратно-программных и технико-технологических устройств				
3.	Контроль за осуществлением подведомственными организациями договорных отношений с провайдерами, предоставляющими услуги доступа к сети Интернет, в части обеспечения контент-фильтрации интернет-трафика	2021 – 2027 годы	Образовательные организации	Проведение оценивания обеспечения доступа к сети Интернет с использованием контент-фильтрации трафика в подведомственных организациях (не менее 10% организаций ежегодно)
4.	Выявление фактов распространения материалов порнографического и экстремистского содержания, сведений о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, склонения несовершеннолетних к противоправным действиям, призывов к самоубийствам, пропаганды экстремистских сообществ, а также производства и распространения книжной продукции, продукции средств массовой информации, печатной продукции, аудиовизуальной продукции на любых видах носителей, программ для электронных вычислительных машин и базы данных, а также информации, распространяемой посредством зрелищных мероприятий, информационно-телекоммуникационных сетей, в том числе сети Интернет и сетей подвижной радиоте-	2021 – 2027 годы	Образовательные организации	Пресечение фактов распространения материалов порнографического и экстремистского содержания, сведений о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, склонения несовершеннолетних к противоправным действиям, призывов к самоубийствам, пропаганды экстремистских сообществ

	лефонной связи			
5.	Проведение мониторинга социальных сетей Интернет по выявлению распространения материалов порнографического содержания, информации о жестокости по отношению к детям и с их стороны, экстремистского характера, пропаганды наркотических средств, психотропных веществ или их прекурсоров и других преступлений, совершаемых в сети Интернет или с ее использованием	2021 – 2027 годы	Образовательные организации	Пресечение фактов распространения материалов порнографического и экстремистского содержания, сведений о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, склонения несовершеннолетних к противоправным действиям, призывов к самоубийствам, пропаганды экстремистских сообществ
Глава 3. Профилактика у детей и подростков интернет-зависимости, игровой зависимости и правонарушений с использованием информационно-коммуникационных технологий, формирование у несовершеннолетних навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде через обучение их способам защиты от вредной информации				
6.	Организация обучения детей культуре информационной безопасности в рамках действующих учебных дисциплин в образовательных организациях, тематической внеурочной деятельности и дополнительного образования, программ воспитания и социализации обучающихся	2021 – 2027 годы	Образовательные организации	Повышение правовой культуры и юридической грамотности подростков
7.	Проведение обучающих занятий, консультаций, информационно-просветительских акций для обучающихся, родителей (законных представителей), педагогов по вопросам	2021 – 2027 годы	Образовательные организации	Повышение правовой культуры и юридической грамотности подростков, их родителей (законных представителей), педагогов

	защиты персональных данных детей			
8.	Организация функционирования детского телефона доверия для оказания детям и их родителям (лицам их заменяющим) консультативно-психологической помощи по телефону, информирования о деятельности детского телефона доверия, в том числе через сеть Интернет	2021 – 2027 годы	Образовательные организации	Оказание экстренной психологической (консультативной) помощи 100 процентам несовершеннолетних, обратившихся по телефону доверия, в том числе с проблемой интернет-зависимости и игровой зависимости
9.	Проведение тематических конкурсных мероприятий (конкурсов, игр, викторин) по ознакомлению несовершеннолетних с основами информационной безопасности детей в учреждениях для детей, подростков и молодежи	2021 – 2027 годы	Образовательные организации	Вовлечение в социально значимую деятельность большего количества несовершеннолетних в городе Ливны. Участие в конкурсных мероприятиях не менее одной тысячи несовершеннолетних ежегодно
10.	Проведение в образовательных организациях Единого урока по безопасности в сети Интернет и его мероприятий	2021 – 2027 годы (октябрь – ноябрь)	Образовательные организации	100-процентное участие образовательных организаций
11.	Участие обучающихся, родителей (законных представителей) обучающихся и работников образовательных организаций в ежегодных мероприятиях «Сетевичок»	2021 – 2027 годы	Образовательные организации	100-процентное участие образовательных организаций
12.	Проверка библиотечных фондов на предмет выявления литературы, включенной в федеральный список экстремистских материалов	2021 – 2027 годы	Образовательные организации	Обеспечение доступа детей и подростков к литературным изданиям, не имеющим информации, ограниченной и (или) запрещенной для распространения среди несовершеннолетних

13.	Проведение различных мероприятий (семинаров, совещаний, круглых столов) для педагогических работников образовательных организаций по вопросу обеспечения информационной безопасности для всех участников образовательного процесса	2021 – 2027 годы	Образовательные организации	Повышение правовой культуры и юридической грамотности педагогических работников.
14.	Организация повышения компетенции родителей (законных представителей) и работников образовательных организаций города Ливны в области цифровой грамотности и информационной безопасности на образовательном портале «Учеба.онлайн»	2021 – 2027 годы	Образовательные организации	Повышение цифровой грамотности родителей (законных представителей) детей, в том числе по вопросам обеспечения информационной безопасности
Глава 4. Информационное просвещение граждан о возможности защиты детей от информации, причиняющей вред их здоровью и (или) развитию				
15.	Проведение в образовательных организациях тематических родительских собраний, классных часов о возможном вреде информации в средствах массовой информации и сети Интернет и способах защиты детей от информации, причиняющей вред их здоровью и развитию	2021 – 2027 годы	Образовательные организации	Повышение правовой культуры и юридической грамотности подростков и их родителей (законных представителей).
16.	Круглый стол по итогам реализации Плана мероприятий по выполнению Концепции по обеспечению информационной безопасности детей, производства и оборота информационной продукции для детей в городе Ливны за 2021 – 2027 годы	2027 год	Управление общего образования администрации города Ливны, образовательные организации	Подведение итогов за 2021 – 2027 годы и стратегия дальнейшего развития

Разработана Временной комиссией
Совета Федерации по развитию
информационного общества

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. Обращайся за помощью к взрослым - родители, опекуны и администрация сайтов всегда помогут.
5. Пройди обучение на сайте «Сетевичок» и получи паспорт цифрового гражданина!

Разработана Временной комиссией
Совета Федерации по развитию
информационного общества

Информационная памятка для обучающихся по безопасной работе в сети Интернет

С каждым годом молодежи в Интернете становиться 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 заражённая 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 серьёзный 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 инсталлироваться на твоем 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 ненадёжных 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 «Wireless Fidelity», 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 работе 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 брандмауэр. 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 её 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 информацию: 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 неанонимные. 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 нефиатные 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, StROng!;.
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 «тёма13»;

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:

1. Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги.
2. Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?
3. Необходимо обновлять операционную систему твоего смартфона.
4. Используй антивирусные программы для мобильных телефонов.
5. Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение.
6. После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies.
7. Периодически проверяй какие платные услуги активированы на твоем номере.
8. Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь.
9. 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.

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 окружающее 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 ко многим рискам: от потери данных к твоим аккаунтам до блокировки твоего устройства, где установлена нелегальная программа. Не стоит также забывать, что существует 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!

Разработана Временной комиссией
Совета Федерации по развитию
информационного общества

Памятка для родителей об информационной безопасности детей

Определение термина «информационная безопасность детей» содержится в Федеральном законе № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», регулирующем 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 № 436-ФЭ информацией, причиняющей вред здоровью и (или) развитию детей, является:

- информация, запрещенная для распространения среди детей;
- информация, распространение которой ограничено среди детей определенных возрастных категорий.

К информации, запрещенной для распространения среди детей, относится:

1. Информация, побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в т.ч. 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, пиво и напитки, изготавливаемые на его основе; 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 и животным.
4. Отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи.
5. Оправдывающая противоправное поведение.
6. Содержащая нецензурную брань.
7. Содержащая информацию порнографического характера.

К информации, распространение которой ограничено среди детей определенного возраста, относится:

1. Информация, представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия.

2. Вызывающая у детей страх, ужас или панику, в т.ч. 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.

С учетом этого Вам предлагаются правила работы в сети Интернет для различных возрастных категорий, соблюдение которых позволит обеспечить информационную безопасность ваших детей.

Общие правила для родителей

1. Независимо от возраста ребенка используйте программное обеспечение, помогающее фильтровать и контролировать информацию, но не полагайтесь полностью на него. Ваше внимание к ребенку - главный метод защиты.
2. Если Ваш ребенок имеет аккаунт на одном из социальных сервисов (LiveJoumal, blogs.mail.ru, vkontakte.ru и т.п.), внимательно изучите, какую информацию помещают его участники в своих профилях и блогах, включая фотографии и видео.
3. Проверьте, с какими другими сайтами связан социальный сервис Вашего ребенка. Странички Вашего ребенка могут быть безопасными, но могут и содержать ссылки на нежелательные и опасные сайты (например, порносайт, или сайт, на котором друг упоминает номер сотового телефона Вашего ребенка или Ваш домашний адрес).
4. Поощряйте Ваших детей сообщать обо всем странном или отталкивающем и не слишком остро реагируйте, когда они это делают (из-за опасения потерять доступ к Интернету дети не говорят родителям о проблемах, а также могут начать использовать Интернет вне дома и школы).
5. Будьте в курсе сетевой жизни Вашего ребенка. Интересуйтесь, кто его друзья в Интернет так же, как интересуетесь реальными друзьями.

Возраст от 7 до 8 лет

В Интернете ребенок старается посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому родителям особенно полезны будут те отчеты, которые предоставляются программами по ограничению использования Интернета, т. е. Родительский контроль или то, что вы сможете увидеть во временных файлах. В результате, у ребенка не будет ощущения, что за ним ведется постоянный контроль, однако, родители будут по-прежнему знать, какие сайты посещает их ребенок. Дети в данном возрасте обладают сильным чувством семьи, они

доверчивы и не сомневаются в авторитетах. Они любят играть в сетевые игры и путешествовать по Интернету, используя электронную почту, заходить на сайты и чаты, не рекомендованные родителями.

Советы по безопасности в сети Интернет для детей 7-8 лет

1. Создайте список домашних правил посещения Интернета при участии детей и требуйте его выполнения.
2. Требуйте от Вашего ребенка соблюдения временных норм нахождения за компьютером. Покажите ребенку, что Вы наблюдаете за ним не потому что Вам это хочется, а потому что Вы беспокоитесь о его безопасности и всегда готовы ему помочь.
3. Компьютер с подключением к Интернету должен находиться в общей комнате под присмотром родителей.
4. Используйте специальные детские поисковые машины.
5. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
6. Создайте семейный электронный ящик, чтобы не позволить детям иметь собственные адреса.
7. Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего программного обеспечения.
8. Приучите детей советоваться с Вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.
9. Научите детей не загружать файлы, программы или музыку без вашего согласия.
10. Не разрешайте детям использовать службы мгновенного обмена сообщениями.
11. В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.
12. Не забывайте беседовать с детьми об их друзьях в Интернете, как если бы речь шла о друзьях в реальной жизни.
13. Не делайте «табу» из вопросов половой жизни, так как в Интернете дети могут легко наткнуться на порнографию или сайты «для взрослых».
14. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

Возраст детей от 9 до 12 лет

В данном возрасте дети, как правило, уже наслышаны о том, какая информация существует в Интернете. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко

заблокировать при помощи средств Родительского контроля.

Советы по безопасности для детей от 9 до 12 лет

1. Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.
2. Требуйте от Вашего ребенка соблюдения норм нахождения за компьютером.
3. Наблюдайте за ребенком при работе за компьютером, покажите ему, что Вы беспокоитесь о его безопасности и всегда готовы оказать ему помощь.
4. Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.
5. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
6. Не забывайте принимать непосредственное участие в жизни ребенка, беседовать с детьми об их друзьях в Интернете.
7. Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету.
8. Позволяйте детям заходить только на сайты из «белого» списка, который создайте вместе с ними.
9. Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.
10. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
11. Создайте Вашему ребенку ограниченную учетную запись для работы на компьютере.
12. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах и опасениях.
13. Расскажите детям о порнографии в Интернете.
14. Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.
15. Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

Возраст детей от 13 до 17 лет

В этом возрасте подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и

фильмы. Мальчикам в этом возрасте больше по нраву сметать все ограничения, они жаждут грубого юмора, азартных игр, картинок «для взрослых». Девочки предпочитают общаться в чатах, при этом они гораздо более чувствительны к сексуальным домогательствам в Интернете.

Зачастую в данном возрасте родителям уже весьма сложно контролировать своих детей, так как об Интернете они уже знают значительно больше своих родителей. Тем не менее, не отпускайте детей в «свободное плавание» по Интернету. Старайтесь активно участвовать в общении ребенка в Интернете.

Важно по-прежнему строго соблюдать правила Интернет-безопасности - соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернете. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей.

Советы по безопасности в этом возрасте от 13 до 17 лет

1. Создайте список домашних правил посещения Интернета при участии подростков и требуйте безусловного его выполнения. Обговорите с ребенком список запрещенных сайтов («черный список»), часы работы в Интернете, руководство по общению в Интернете (в том числе в чатах).
2. Компьютер с подключением к сети Интернет должен находиться в общей комнате.
3. Не забывайте беседовать с детьми об их друзьях в Интернете, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы.
4. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
5. Необходимо знать, какими чатами пользуются Ваши дети. Поощряйте использование модерируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.
6. Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из сети Интернет.
7. Приучите детей не выдавать свою личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.
8. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
9. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами

рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

10. Расскажите детям о порнографии в Интернете. Помогите им защититься от спама. Научите подростков не выдавать в Интернете своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.
11. Приучите себя знакомиться с сайтами, которые посещают подростки.
12. Научите детей уважать других в интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде — даже в виртуальном мире.
13. Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.
14. Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.

Постоянно контролируйте использование Интернета Вашим ребенком! Это не нарушение его личного пространства, а мера предосторожности и проявление Вашей родительской ответственности и заботы.

ЕДИНЫЙ УРОК БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ

Единый урок по безопасности в сети «Интернет» для детей возможно провести в следующих формах, которые могут быть использованы как отдельно, так и совместно:

1. Проведение традиционного урока, классного часа и деловой игры.
2. Демонстрация мультфильма и/или видео-урока;
3. Проведение Всероссийской контрольной работы по информационной безопасности на портале www.Единыйурок.дети;
4. Организация участия детей в международном квесте (онлайн-конкурсе) по цифровой грамотности «Сетевичок» на сайте www.Сетевичок.рф;
5. Подготовить и выдвинуть различные творческие работы и Интернет-ресурсы на Национальную премию в области информационного пространства детства «Премия Сетевичок» и Всероссийский конкурс социальной рекламы на тему информационной безопасности детей на сайте www.премиясетевичок.рф, а в октябре организовать участие детей в «народном голосовании» за участников конкурсов;
6. Организовать семинар или занятие с участием приглашенного эксперта;
7. Организовать раздачу листовок и распространение через дневники обучающихся тематических брошюр, которые можно распечатать самостоятельно.

Особое направление Единого урока – просвещение родителей (законных представителей) детей. Общеобразовательным организациям необходимо провести информирование о мерах информационной безопасности детей в рамках уже запланированных родительских собраний, либо при наличии возможности провести специальное родительское собрание, осветив следующие темы:

1. Важность обеспечения цифровой и информационной грамотности детей и подростков;
2. Основные рекомендации по обеспечению персональной безопасности;
3. Методы и функции родительского контроля.

В ходе родительского собрания родителям (законным представителям) детей могут быть выданы листовки и тематические брошюры, а также может быть организована демонстрация видеообращения члена Совета Федерации Л. Н. Боковой и привлечение родителей (законных представителей) детей к участию в исследовании родительской общественности на сайте проекта «Сетевичок» www.родители.сетевичок.рф.

Педагогические работники, сотрудники администраций учреждений, дошкольных образовательных организаций, общеобразовательных организаций могут принять участие в следующих мероприятиях и активностях:

1. Всероссийская конференция по формированию цифрового детского пространства «Сетевичок»;
2. Мониторинг информатизации системы образования;
3. Мониторинг работы педагогов-психологов общеобразовательных организаций с последующей выработкой единых рекомендаций для психологов;
4. Выдвинуть свои Интернет-ресурсы на Национальную премию в области информационного пространства детства «Премия Сетевичок»;
5. Курсы повышения квалификации по следующим направлениям: «Психологическая поддержка детей», «ИКТ-компетентность», «Защита детей от информации, причиняющей вред их здоровью и развитию, в образовательной организации» и другие;
6. Педагогический турнир по информационной безопасности «Сетевичок»;
7. Добавление тематических материалов в Электронную библиотеку образования.

Все вышеуказанные мероприятия носят некоммерческий характер, а по итогам участия детей и педагогических работников в сетевых мероприятиях они смогут бесплатно получить подтверждающие участие в мероприятиях документы.

Для вышеуказанных целей на сайте Экспертного совета по информатизации системы образования и воспитания при Временной комиссии Совета Федерации по развитию информационного общества www.Единыйурок.рф в разделе «Проекты», категория «Единый урок безопасности в сети» размещена подробная и актуальная информация.

_____

Наименование образовательной организации

Информация об итогах Единого урока по безопасности в сети «Интернет» в _____ году

№	Показатель	Результаты
1.	Общее количество детей	
2.	Общее количество родителей (законных представителей)	
3.	Общее количество педагогических работников	
4.	Количество вовлеченных детей в проведение Единого урока	
4.1.	Количество участников Всероссийской контрольной работы по информационной безопасности на портале Единого урока www.Единыйурок.дети	
4.2.	Количество участников международного квеста по цифровой грамотности «Сетевичок» на сайте www.Сетевичок.рф	
4.3.	Количество работ, поданных на Всероссийский конкурс социальной рекламы на тему информационной безопасности детей	
4.4.	Количество Интернет-ресурсов, поданных на Национальную премию в области информационного пространства детства «Премия Сетевичок»	
4.5.	Количество проведенных семинаров или занятий с участием приглашенного эксперта	
4.6.	Количество распространенных среди детей листовок и брошюр	
5.	Количество вовлеченных родителей (законных представителей) детей в проведение Единого урока	
5.1.	Количество проведенных родительских собраний	
5.2.	Количество распространенных среди родителей (законных представителей) детей листовок и брошюр	
6.	Количество вовлеченных педагогических работников в проведение Единого урока	
6.1.	Количество участников Всероссийской конференции по формированию цифрового детского пространства «Сетевичок»	
6.2.	Количество участников-респондентов мониторинга информатизации системы образования	
6.3.	Количество участников-респондентов мониторинга работы педагогов-психологов общеобразовательных организаций	
6.4.	Количество Интернет-ресурсов педагогических работников, поданных на Национальную премию в области информационного пространства детства «Премия Сетевичок»	
6.5.	Количество педагогических работников, прошедших на сайте Экспертного совета курсы повышения квалификации по следующим направлениям: «Психологическая поддержка детей», «ИКТ-компетентность», «Защита детей от информации, причиняющей вред их здоровью и развитию, в образовательной организации» и другие	
6.6.	Количество участников педагогического турнира по информационной безопасности «Сетевичок»	
6.7.	Количество тематических материалов, добавленных в Электронную библиотеку образования на сайте Экспертного совета	
7.	Количество публикаций на официальном сайте ОО о проведении Единого урока по безопасности в сети «Интернет» в _____ году	