ГБОУ ДПО НИРО

Проблемы обеспечения безопасности детей в сети Интернет и пути их решения

Канянина Т.И., к.п.н.

2018

Информационная безопасность

Информационная безопасность детей – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию (Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29 декабря 2010 № 436-ФЗ.)

Информационная безопасность личности – это: а) состояние защищенности, при котором отсутствует угроза причинения вреда информации, которой владеет личность; б) состояние и условие жизнедеятельности личности, при которых отсутствует угроза нанесения вреда личности информацией.

Правовые основы

Федеральный закон «Об основных гарантиях прав ребенка в Российской Федерации» от 3 июля 1998 г. № 124-ФЗ, статья 14 (устанавливает обязанность органов государственной власти Российской Федерации принимать меры по защите ребенка от информации, пропаганды и агитации, наносящих вред его здоровью, нравственному и духовному развитию)

Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. N 149-ФЗ (регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации; при применении информационных технологий, а также при обеспечении защиты информации).

Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29 декабря 2010 № 436-ФЗ (регулирует отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию)

Концепция информационной безопасности детей (утверждена распоряжением Правительства РФ от 2 декабря 2015 г.№ 2471-р).

Информационная безопасность

Федеральный закон от 27.06.2006 г. № 152-ФЗ «О персональных данных» (в соответствии с законом в России существенно возрастают требования ко всем частным и государственным компаниям и организациям, а также физическим лицам, которые хранят, собирают, передают или обрабатывают персональные данные (в том числе фамилию, имя, отчество). … должны выполнить ряд требований по защите персональных данных физических лиц, обрабатываемых в информационных системах организации)

Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» (совершенствовать механизмы ограничения доступа к информации, распространение которой в Российской Федерации запрещено федеральным законом, и ее удаления)

Информационно-образовательная среда


Безопасность ИОС ОУ
Безопасность ресурсов ИОС и её инфраструктуры
Безопасность личной информации субъекта образования, его личной ИОС
Безопасность самого субъекта образования, при его взаимодействии с ИОС

Безопасность ресурсов ИОС и ее инфраструктуры

Угрозы	Риски	Пути решения
Вредоносные программы (компьютерные вирусы)	Утечка или потеря информации, нештатное поведение ПО, резкий рост Интернет-трафика, замедление или полный отказ работы сети	Антивирусные программы DrWEB Антивирус Касперского, AVG, Panda и др., межсетевые экраны, прокси-серверы, системы обнаружения вторжений
Сетевые атаки (покушение на систему безопасности)	Доступ злоумышленников в сеть ОУ, риск утечки персональных данных и другой информации	

Безопасность ресурсов ИОС и её инфраструктуры

Информационные угрозы	Риски	Пути решения
Доступ учащихся к сайтам, которые могут представлять опасность для учащихся или к Интернет-контенту, который может оказать на них негативное воздействие	Кибермошенничество Противоправные действия против личности Неприличный или угрожающий контент Вторжение в частную жизнь	Специализированные средства, разработанные непосредственно для контроля – контент-фильтры. Ведение чёрных и белых списков Интернет-сайтов. Ограничение доступа к социальным сетям.

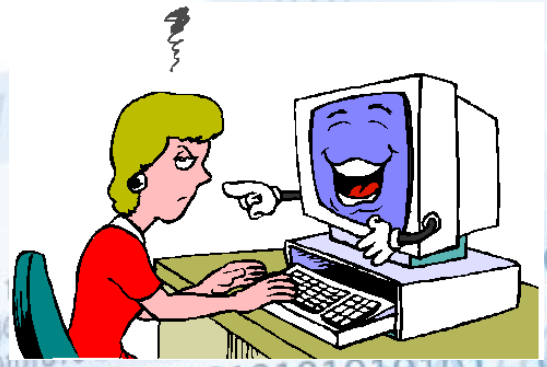
Письмо МО и Н РФ от 28 апреля 2014 г. N ДЛ-115/03

- **- Методическими рекомендациями по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования (**методические рекомендации разработаны с целью обеспечения реализации субъектами Российской Федерации, органами местного самоуправления, осуществляющими функции управления в сфере образования, и образовательными организациями системы организационно-административных мероприятий, направленных на ограничение доступа обучающихся к видам информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования);
- **- Рекомендациями по организации системы ограничения в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования** (в документе дается краткий обзор текущей ситуации в рамках поставленной задачи, проводится анализ существующей системы контентной фильтрации с соответствующими рекомендациями, и приводится вариант модернизации системы контентной фильтрации с учетом этих рекомендаций, для предлагаемой реализации даны схемы и временной регламент взаимодействия основных участников);
- **- Перечнем видов информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования.**

Виды информации в сети Интернете, причиняющие вред здоровью и развитию детей

Контентные риски

Интернет-зависимость

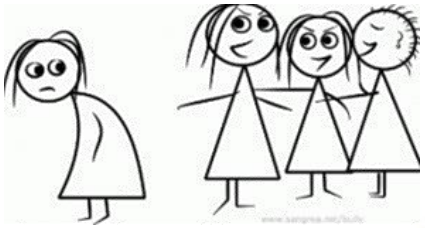


Коммуникационные риски

Технические риски

Потребительские риски

КОММУНИКАЦИОННЫЕ РИСКИ



связаны с межличностными отношениями интернет-пользователей и включают в себя ***незаконные контакты, киберпреследования, киберунижения*** *и др. Для подобных целей используются чаты, онлайн-мессенджеры, социальные сети, сайты знакомств, форумы, блоги и т.д.*

Кибербуллинг – агрессивное, умышленное действие, совершаемое группой лиц или одним лицом с использованием электронных форм контакта, повторяющееся неоднократно и продолжительное во времени в отношении жертвы, которой трудно защитить себя.

Троллинг - вид виртуальной коммуникации с нарушением этики сетевого взаимодействия, выражающийся в виде проявления различных форм провокативного агрессивного, издевательского и оскорбительного поведения.

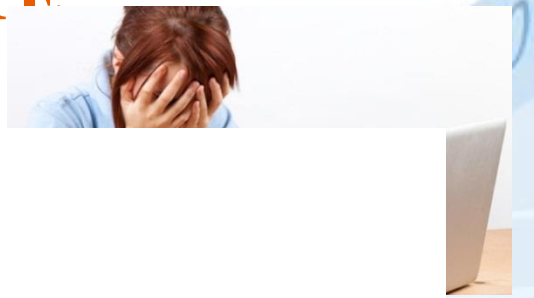
ЧТО ДЕЛАТЬ?

- Объясните детям, что при общении в интернете нужно быть дружелюбным – читать грубости так же неприятно, как и слышать.
- Если у вас есть информация, что кто-то из друзей или знакомых вашего ребенка подвергается буллингу, сообщите об этом классному руководителю – необходимо принять меры по защите ребенка.
- Научите детей правильно реагировать на обидные слова или действия других пользователей. Лучший способ испортить хулигану его выходку – полный «игнор».
- Поддерживайте доверительные отношения с вашим ребенком, чтобы вовремя заметить, если в его адрес начнет поступать агрессия или угрозы. Убедитесь, что оскорбления из сети не перешли в реальную жизнь.
- Помогите ребенку найти выход из ситуации – заблокировать обидчика, написать жалобу модератору, потребовать удаление странички.

КОНТЕНТНЫЕ РИСКИ

материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие насилие, агрессию, эротику и порнографию, нецензурную лексику, информацию, разжигающую, расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр, наркотических веществ и т.д.

КЛАССИФИКАЦИЯ НЕГАТИВНОГО КОНТЕНТА В ИНТЕРНЕТЕ



Противозаконный контент:

- Детская порнография
- Пропаганда наркотиков
- Расовая и религиозная ненависть, экстремизм
- Пропаганда суицида

Вредоносный, но не запрещенный контент:

- Сексуальный контент
- Материалы, содержащие насилие, агрессию, убийства, жестокость
- Пропаганда нездорового образа жизни
- Оскорбительный, унижающий контент
- Нецензурная лексика
- сайты, пропагандирующие чрезмерное похудение

ЧТО ДЕЛАТЬ?

- Используйте технические средства ограничения доступа:

родительский контроль, контентная фильтрация, настройки безопасного поиска

- Расскажите ребенку о негативной информации в сети.

Покажите, как действовать при столкновении с запрещенными сайтами, куда обратиться.

- Следите за активностью ребенка

в сети, проверяйте сайты, которые он посещает.

- Поддерживайте доверительные

отношения с ребенком. Приучите его рассказывать о том, что происходило за день в Интернете, обсуждайте это.

ТЕХНИЧЕСКИЕ РИСКИ

кибердеятельность по отношению к пользователю, которая включает в себя: вирусную атаку, спамминг, взлом страниц, онлайн-мошенничество и т.д.

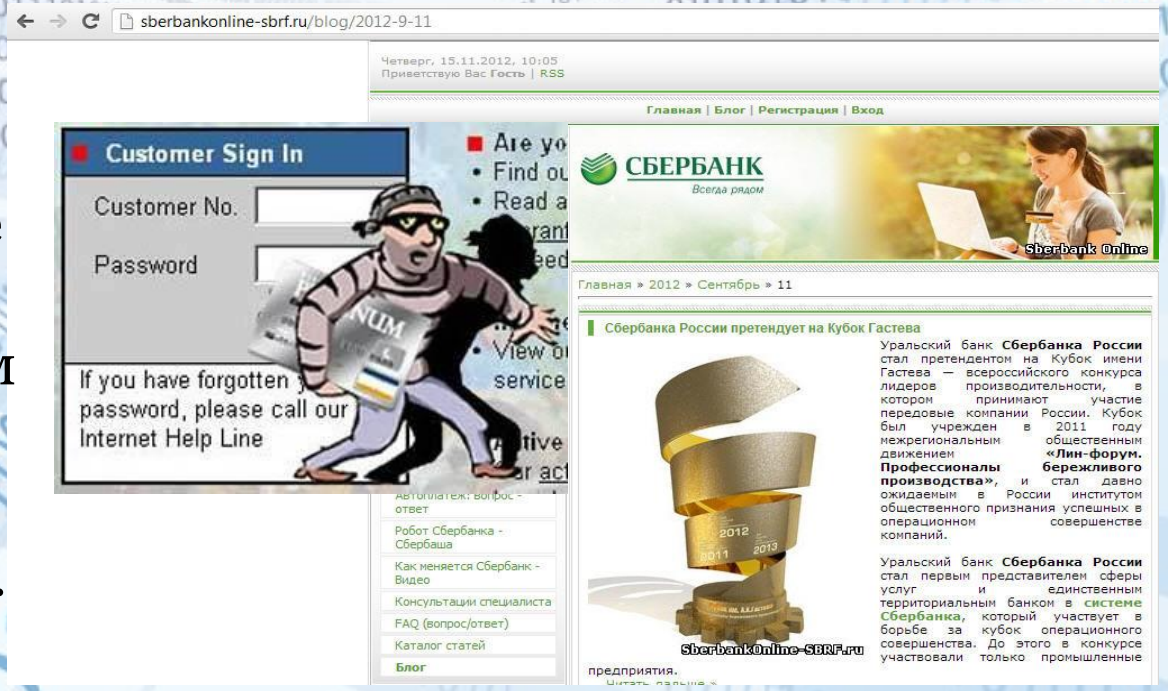
С ЧЕМ СТАЛКИВАЮТСЯ ПОЛЬЗОВАТЕЛИ?

Около 30 % всех обращений на Линию помощи «Дети онлайн» касаются технических рисков

ФИШИНГ: ЛОВИСЬ РЫБКА БОЛЬШАЯ И МАЛЕНЬКАЯ…

(англ. *phishing*, от *fishing* — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям.

Фишинговые сайты выглядят как настоящие. Они воруют информацию, которую пользователь вводит при покупке: банковские реквизиты, пароли, коды и отправляют их мошенникам.



Так выглядит фишинговый сайт Сбербанка

БЕЗОПАСНОСТЬ =

Личная бдительность + Технические средства

- Не скачивайте файлы, присланные незнакомыми
- Отключите автозапуск переносных устройств
- Регулярно делайте резервные копии своих данных
- Используйте разные и сложные пароли

- Установите антивирус, регулярно обновляйте его
- Периодически проверяйте электронные устройства антивирусом
- Используйте учетную запись гостя при повседневной работе за компьютером

ПОТРЕБИТЕЛЬСКИЕ РИСКИ

Включают в себя: риск приобретения товара низкого качества, различные подделки, контрафактная и фальсифицированная продукция, угроза хищения персональной информации с целью кибермошенничества и т.д.

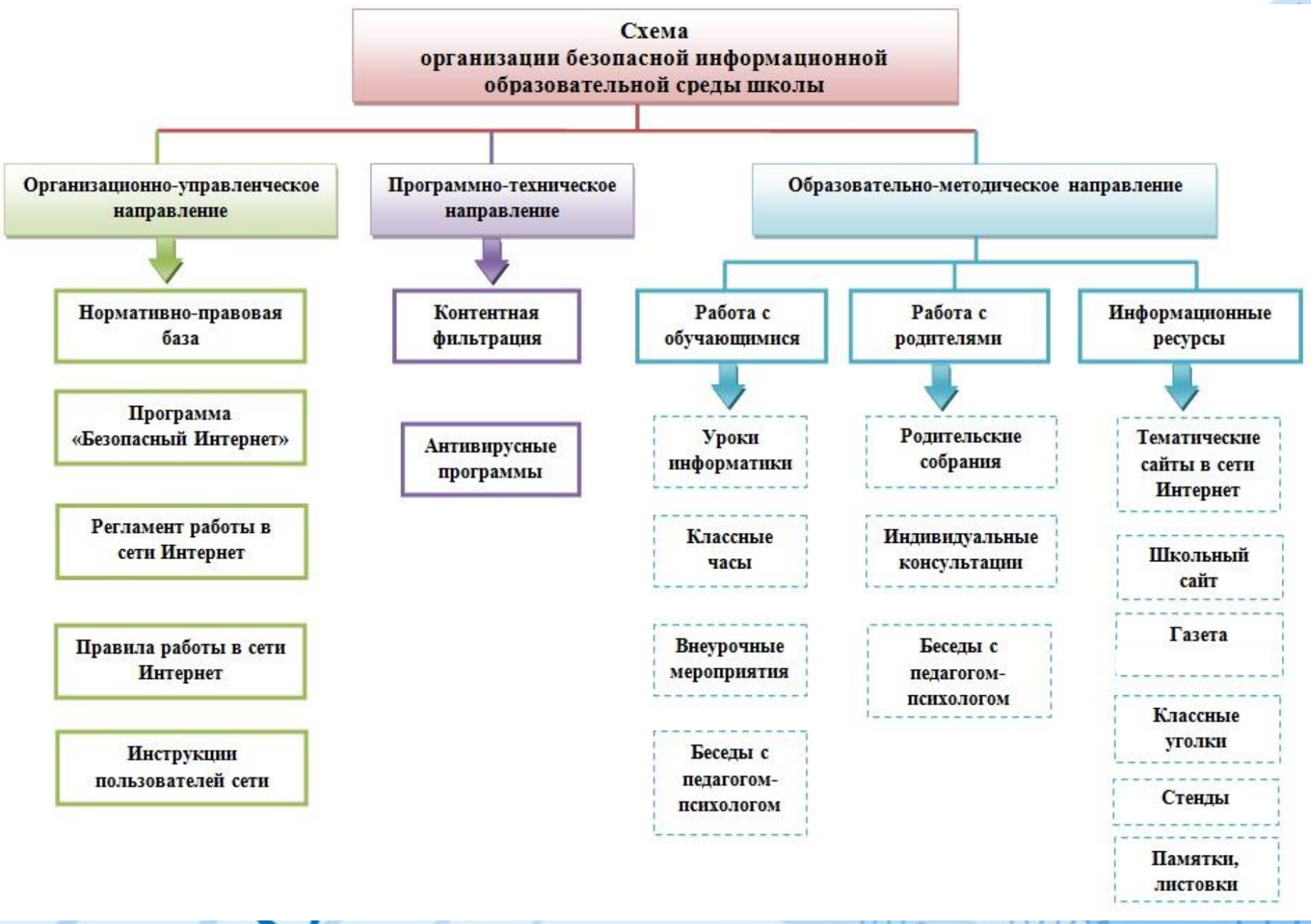


Схема
организации безопасной информационной образовательной среды школы
Организационно-управленческое направление
Программно-техническое направление
Образовательно-методическое направление
Нормативно-правовая база
Программа «Безопасный Интернет»
Регламент работы в сети Интернет
Правила работы в сети Интернет
Инструкции пользователей сети
Контентная фильтрация
Антивирусные программы
Работа с обучающимися
Работа с родителями
Информационные ресурсы
Уроки информатики
Классные часы
Внеурочные мероприятия
Беседы с педагогом-психологом
Родительские собрания
Индивидуальные консультации
Беседы с педагогом-психологом
Тематические сайты в сети Интернет
Школьный сайт
Газета
Классные уголки
Стенды
Памятки, листовки

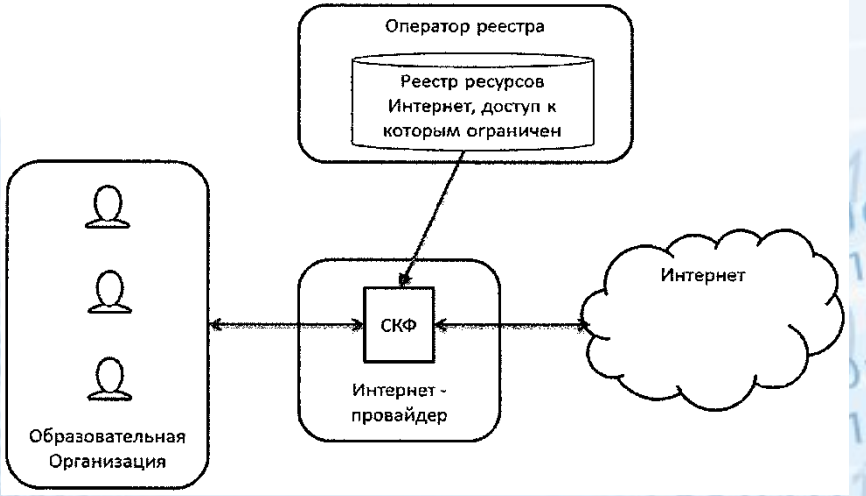
Организация системы безопасности

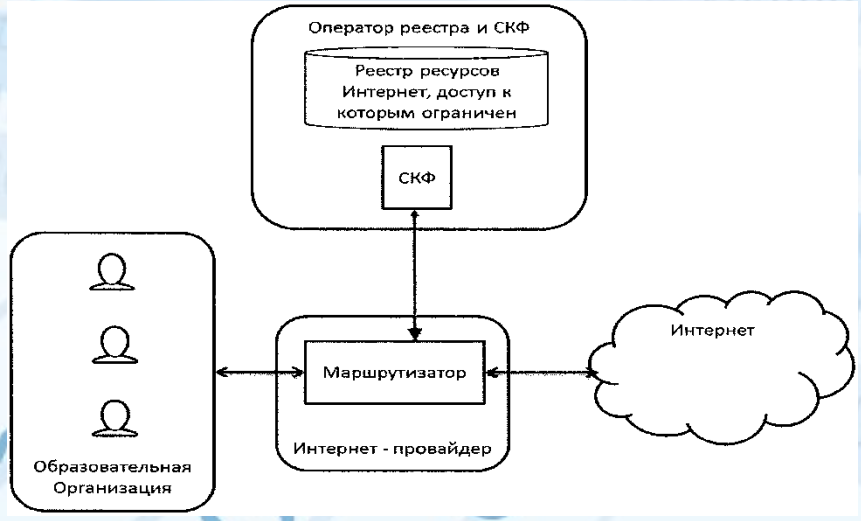
- Организационно-управленческое направление

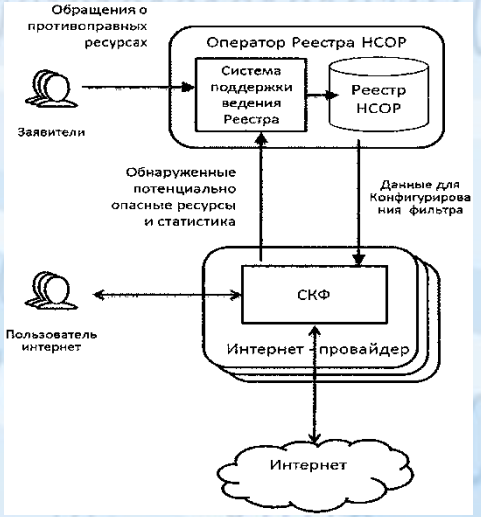
- обеспечение защиты детей от информации, причиняющей вред их здоровью и (или) развитию **посредством использования СКФ**, а также путем осуществления педагогами **визуального контроля работы** детей в сети "Интернет";
- оказание организационной и методической поддержки работникам образовательной организации, в том числе путем их направления **на повышение квалификации** ;
- содействие проведению **автоматизированного мониторинга** использования в образовательных организациях СКФ и мониторинга организационно-административных мероприятий;
- проведение **образовательных и консультационных мероприятий** с родителями обучающихся;
- внесение отдельного положения в договор об оказании образовательных услуг, предусматривающего запрет использования личных средств связи с выходом в сеть "Интернет" или согласие родителей о снятии ответственности с руководителя образовательной организации в случае предоставления своему ребенку данного устройства при посещении образовательного учреждения.

Организация системы безопасности

- Программно-техническое направление







Системы контентной фильтрации

- **Интернет Контроль Сервер (ИКС)**

http://xserver.a-real.ru/description/iks_description.php

- **SkyDNS Школа**

https://www.skydns.ru/school

- **NetPolice Pro**

http://www.netpolice.ru/

- **ContentWasher**

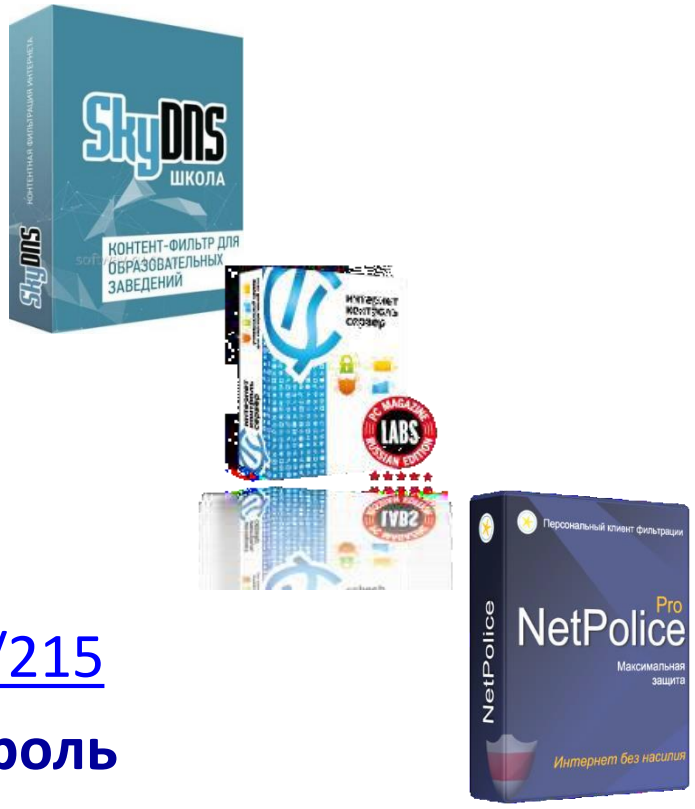
http://www.contentwasher.ru/

- **UserGate Web Filter**

http://www.entensys.com/ru/node/215

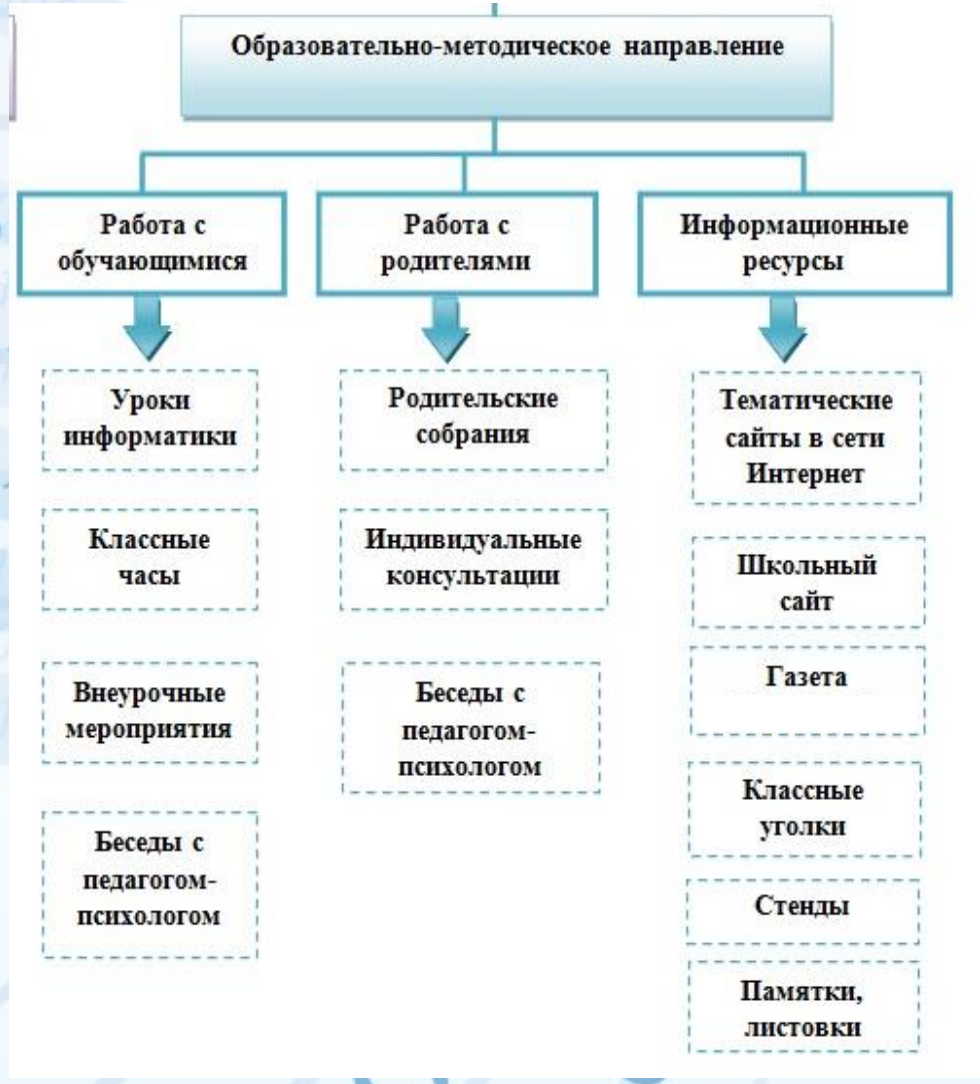
- **KinderGate Родительский Контроль**

http://www.kindergate.ru/ru/product/kindergate-for-school



Организация системы безопасности

- Образовательно-методическое направление



Советы по безопасности в социальных сетях

- **Ограничить** список друзей. Не должно быть случайных и незнакомых людей;
- **Не указывать** телефоны, адреса, дату рождения и другую личную информацию;
- **Управлять** своей **репутацией**. Публиковать и загружать только те вещи, которые не испортят репутацию;
- Если общаешься с незнакомцем, то **не используйте личную информацию**;
- Будьте **осторожны** с загрузкой фото;
- При регистрации используйте **сложные пароли**;
- Используйте **разные пароли** для почты, соцсети и других сайтов.

Советы по кибербуллингу

Кибербуллинг – преследование сообщениями, содержащими оскорбления, агрессию, хулиганство.

- **Не отвечать** оскорблениями на оскорбления, посоветоваться, успокоиться;
- Выяснить, кто стоит за **анонимным аккаунтом**;
- **Не вести** хулиганский образ виртуальной жизни;
- **Игнорировать** единичный негатив;
- **Блокировать** отправку сообщений с определенных номеров (для соцсетей);
- Если ты свидетель кибербуллинга, то выступить **против преследователя**, оценить его действия негативно.

Советы родителям

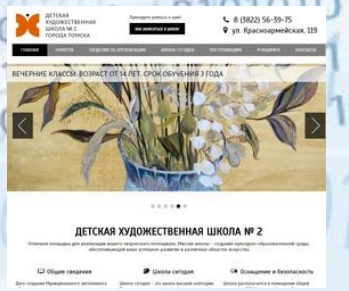
- Независимо от возраста ребенка **используйте программное обеспечение**, помогающее фильтровать и контролировать информацию. **Ваше внимание** к ребенку – главный метод защиты;
- Если ребенок имеет аккаунт в соцсети, внимательно **изучите**, какую **информацию** помещают его участники;
- Проверьте, с какими другими сайтами связан сервис вашего ребенка, **не содержит ли он ссылок** на опасные сайты;
- Поощряйте ваших детей **сообщать обо всем странном** или отталкивающим и не слишком остро реагируйте, когда они это делают);
- Будьте **в курсе** сетевой жизни вашего ребенка.

Организация системы безопасности

- Образовательно-методическое направление

Методические рекомендации о размещении на информационных стендах, официальных интернет – сайтах и других информационных ресурсах ОО и органов, осуществляющих управление в сфере образования, информации о безопасном поведении и использовании сети «Интернет».

Письмо МО и Н РФ от 14.05.2018 №08-1184



Повышение цифровой грамотности

педагог

- Программа повышения квалификации ГБОУ ДПО НИРО педагогических работников образовательных организаций «Современные подходы к обеспечению безопасной работы в сети Интернет». 72 час., совместно с кафедрой психологии, ОБЖ и физической культуры.
- Самообразование
- Единыйурок.ру

ученик

- «Сетевичок»
- Изучение видео-, игровых-, тестовых- материалов на Интернет-источниках по теме защиты информации

Более подробную информацию по вопросам безопасности в сети можно получить на сайтах:

http://www.detionline.ru/

http://www.microsoft.com/rus/protect/default.mspx

Справочник по детской безопасности в Интернет от Google http://www.google.ru/familysafety/

«Компьютерная безопасность. Безопасность жизни» http://blog.chljahsoft.net/3167

«Безопасный Интернет для детей: законодательство, советы, мнения, международный опыт» http://i-deti.org/

Буклет «Безопасный интернет детям» Министерства внутренних дел РФ

http://www.mvd.ru/userfiles/liflets k deti 06.pdf

Материалы III ежегодного Форума Безопасного Интернета http://safor.ru/prezentacii11 .php

Сайт «Дети России Онлайн»

http://detionline.com/