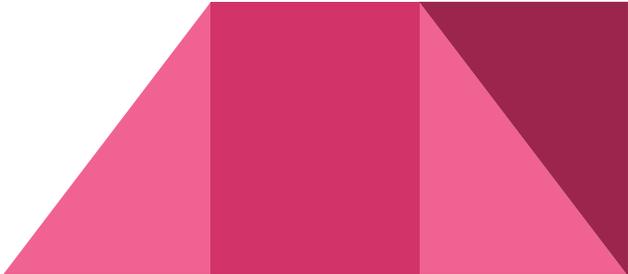


Обеспечение информационной безопасности обучающихся при работе в сети Интернет

Туманов Иван Анатольевич
методист ГБУ ДПО “СПбЦОКОиИТ”
tumanov.i78@gmail.com

- **ФЗ № 149 “Федеральный закон об информации...”**
 - единый реестр запрещенных сайтов и сетевых адресов
eais.rkn.gov.ru
 - **ответственность - на “операторах связи”**
(КоАП РФ, Статья 13.34)

- **ФЗ № 436 “О защите детей от информации, причиняющей вред их здоровью и развитию”**
 - 8 категорий запрещенной информации
 - 4 категории ограниченной информации для возрастных групп
 - 3 возрастные группы
 - необходимость использования “административных и организационных мер, технических и программно-аппаратных средств защиты”
 - **ответственность - на “организующих доступ” (школах)**
(КоАП РФ, Статья 6.17)

- **Технические** (вирусы, хакеры...)
 - Кража информации
 - Шифрование файлов
 - Нагрузка устройства (майнеры)
 - Бот-устройство (использование устройства для атаки на другие узлы в сети)
 - Подмена сайтов (фишинг)
 - Просмотр трафика (незащищенное соединение)
 - Подписка на платные услуги / рассылка платных СМС-сообщений
 - Спам
 - **Социальные** (социальные сети, мессенджеры...)
 - Кибербуллинг (травля)
 - Киберэкстремизм (подстрекание)
 - Интернет-зависимость
 - Домогательства
- 

- **Контроль**
 - Контроль подключения устройств к сетям
 - Контроль сетевого трафика
 - Контроль использования устройств (ПО)
 - Контроль активности в социальных сетях
- **Защита**
 - Использование антивирусов
- Формирование **цифровой грамотности** и **сетевых этикета**

Особенности современного Интернета

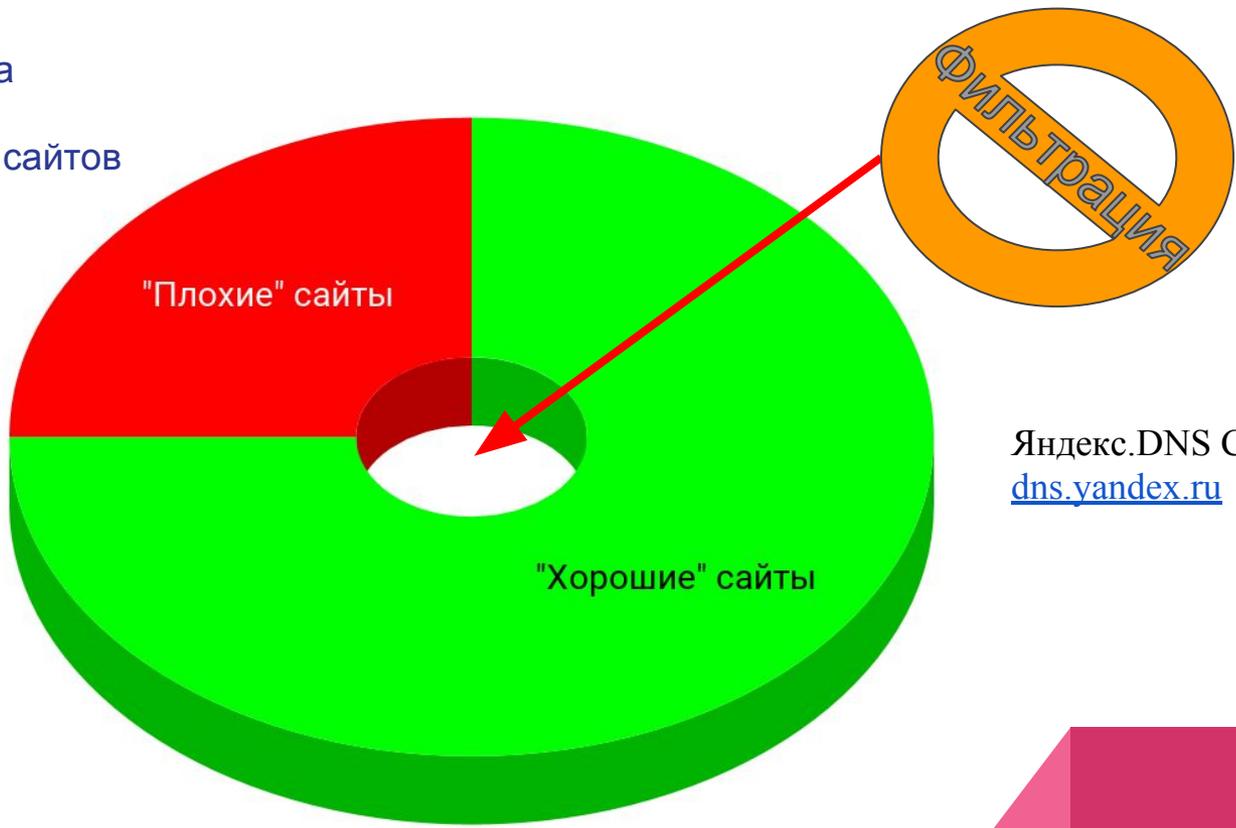
I. Количество сайтов и фильтрация по спискам

Количество активных веб-сайтов в январе 2018 достигло **1,8 млрд.**

Черные списки доступа
не блокируют
большинство "плохих" сайтов

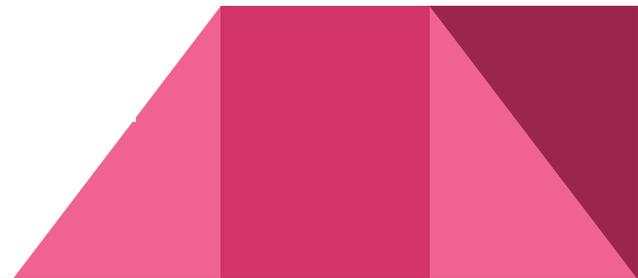


**ЧЕРНЫЙ
СПИСОК**



Яндекс.DNS Семейный
dns.yandex.ru

Белые списки доступа
не позволяют увидеть большинство
"хороших" сайтов



Особенности современного Интернета

II. Фильтрация по содержимому сайтов и страниц

HTTP (общедоступен):



vk.com/club123456789, vk.com/officialpages, vk.com/feed

HTTPS (зашифрован):



`jhgD$kl&*SSDasd235425sedfsfgdfbdf5425sedf$kl&*Ssfgd`

Шифрование (как тонировка стекол в автобусе) позволяет обезопасить данные, но и не позволяет их контролировать.



Невозможно ограничить Вконтакте только разрешенными группами!

Попытку расшивки сайты воспринимают как попытку взлома!

Информационная
безопасность

В сети школы

Вне школьной сети

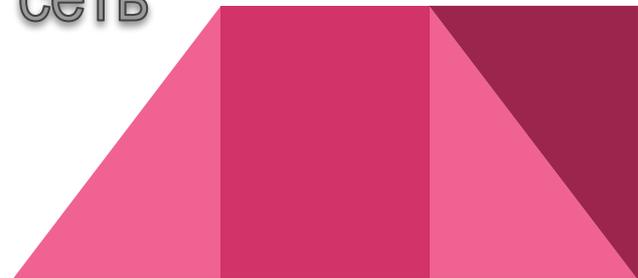
Школьные ПК

Публичная
Wi-fi сеть

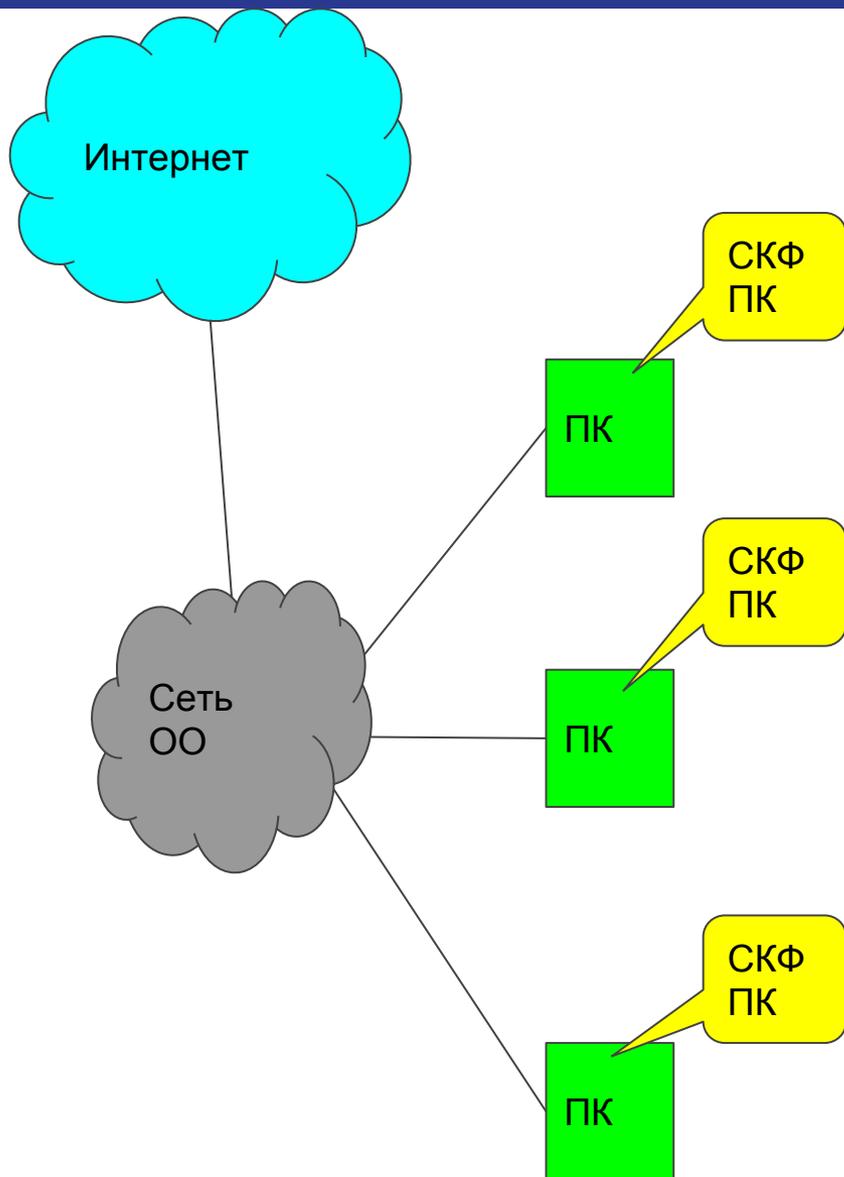
Личные
устройства

Домашний
Интернет

Мобильная
сеть



Системы контентной фильтрации в ЛВС уровня ПК



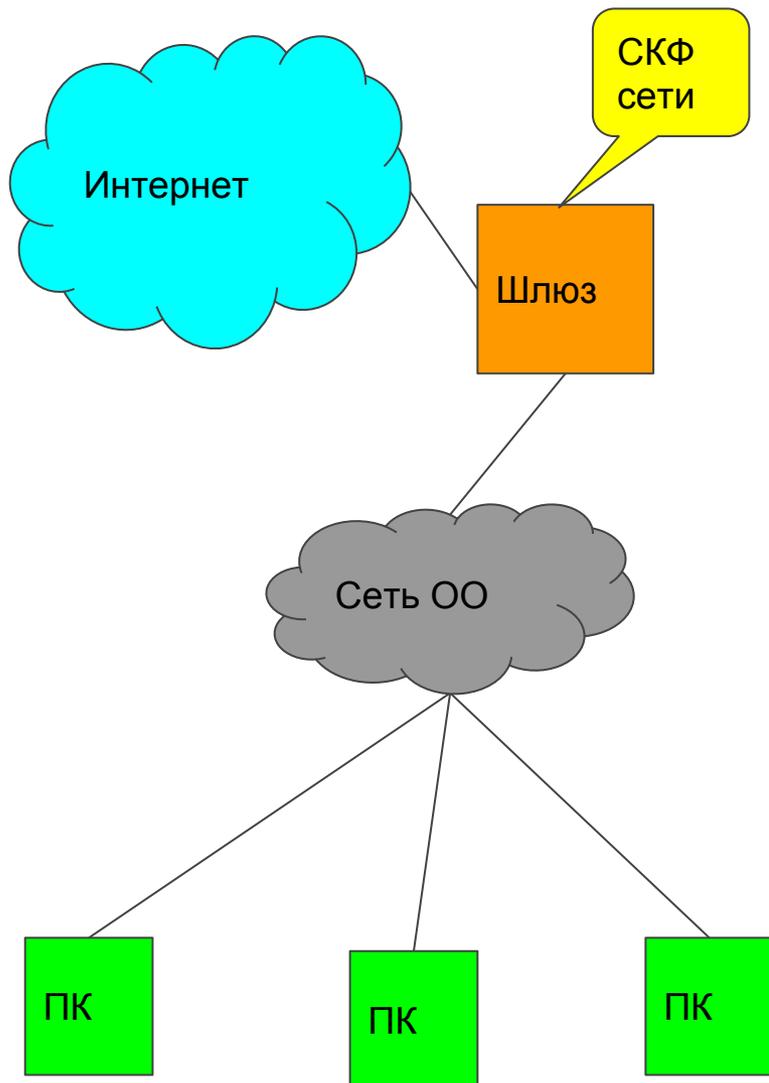
Персональный клиент фильтрации «NetPolice PRO» для образовательных учреждений.

www.netpolice.ru/collection/school

Kinder Gate

www.kindergate-parental-control.com/ru

Системы контентной фильтрации в ЛВС уровня сети



SkyDNS для учебных заведений

www.skydns.ru/

Контент-фильтр

ИКС для школ

xserver.a-real.ru/editions/resheniya/obrazovanie.php

Traffic Inspector School Edition

www.smart-soft.ru/solutions/schools/

UserGate Web Filter

www.entensys.com/ru/products/usergate-web-filter/overview

Ideco

ideco.ru/products/academic-edition

Программы категории “Родительский контроль”

Все разработчики предлагают бесплатные версии, но функционал платных значительно выше.

1. **Kaspersky Safe Kids**
2. **Norton Family parental control (Symantec)**
3. **Bitdefender Parental Control**
4. **Kids Zone Parental Controls**



Данные программы позволяют

- *блокировать покупки, приложения и сайты,*
- *ограничивать время использования устройства (при этом возможность связи с родными останется),*
- *информировать о том, на какие веб-страницы ребенок ходил, что искал, что делал в соцсетях,*
- *отслеживать местоположение устройства и настраивать безопасные зоны (выход из периметра уведомит родителей)*

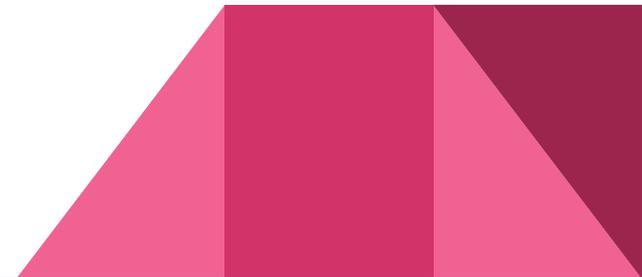
Услуга «Детский Интернет» от МегаФона

Дети не смогут перейти на сайты, которые:

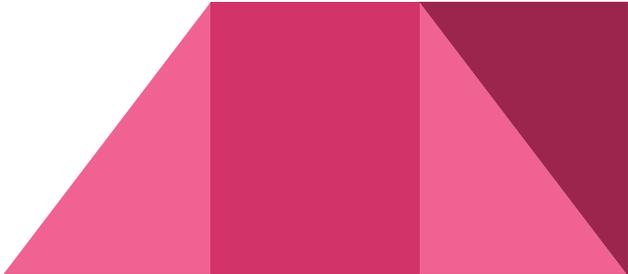
- содержат контент, предназначенный для взрослой аудитории;
- реализуют товары, оборот которых запрещён;
- предлагают азартные игры;
- относятся к опасным категориям для обхода фильтраций.

Формирование цифровой грамотности и сетевого этикета

- Проведение **Единых уроков безопасности** в сети Интернет.
- Проведение **декады безопасности** в сети Интернет.
- Проведение тематических **классных часов**.
- Организация просветительской **работы с родителями**.
- Разработка и реализация **программ внеурочной деятельности**.



Примерная тематика классных часов

- Угрозы личной безопасности в сети Интернет
 - указание мест проживания, учёбы, публикация информации о поездках в отпуск и т.п.
 - Мой профиль в сети Интернет
 - распространение исчерпывающей информации о себе в общедоступной части профиля в интернет-сообществах (телефоны, имена родных, год рождения и т.п.)
 - Цифровой след или “Я в сети”
 - всё, что было опубликовано, останется в Интернете навсегда. Не навредят ли такие материалы в твоей будущей жизни?
 - Приватность и личные границы. Безопасность в социальной сети
 - учимся управлять настройками приватности публикуемой информации
 - Безопасное общение в сети Интернет. Сетевой этикет
 - осваиваем правила общения в сети, распознаём опасные сообщения
- 

Примерная тематика родительских собраний

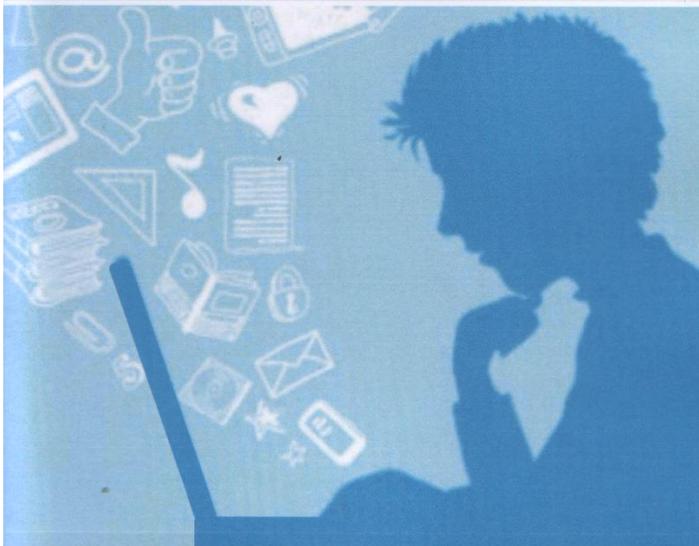
- Безопасность ребенка в сети Интернет. Основные угрозы и как с ними бороться.
- Интернет-зависимость. Как определить и как бороться?
- Мобильное устройство и безопасность в сети Интернет.
- Кибербуллинг. Как помочь ребенку?
- Кибертерроризм и киберэкстремизм. Как защитить себя и ребенка?
- Использование функции “Родительский контроль” при обеспечению информационной безопасности ребенка в сети Интернет.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ по обеспечению информационной безопасности обучающихся при работе в сети Интернет



Санкт-Петербургский центр
оценки качества образования
и информационных технологий

**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по обеспечению информационной
безопасности обучающихся
при работе в сети Интернет**



Разработаны ГБУ ДПО “Санкт-Петербургский центр оценки качества образования и информационных технологий”



Туманов Иван Анатольевич, методист отдела УМР ГБУ ДПО “СПбЦОКОиИТ”

Электронная почта: tumanov.i78@gmail.com

Телефон: (812) 576-34-31, (812) 576-34-37

Официальный сайт отдела УМР: <http://umr.rcokoit.ru>