

Информационная безопасность в образовательной организации

1. Основные направления обеспечения информационной безопасности в ОО
2. Типы интернет-рисков
3. Работа педагога с персональными данными
4. Практикум по обеспечению информационной безопасности ОО

Информационная безопасность детей

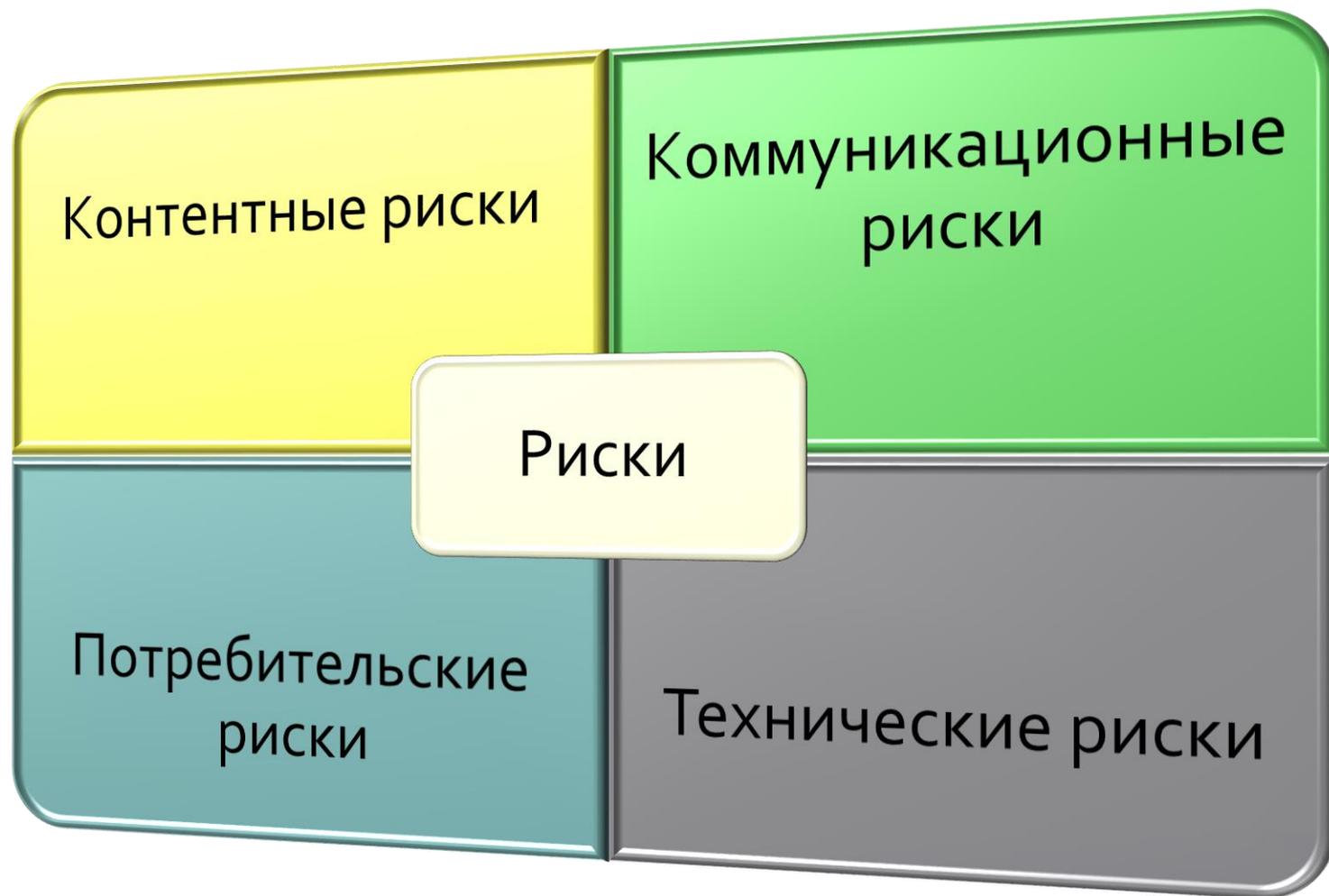
- это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию
- (Федеральный закон от 29.12.2010 No 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»).

Отвечая на вопрос «Что должна делать школа по вопросам использования Интернета детьми?», значительная часть родителей считает, что в школе детей должны

- информировать о безопасном использовании Интернета (42 %)
- обучать навыкам безопасного использования Интернета (38 %)
- обучать эффективно пользоваться современными ИКТ (39 %).

Каждый пятый родитель хотел бы, чтобы и его также информировали в школе об интернет-угрозах и правилах безопасного использования Интернета

Риски и угрозы информационной безопасности в школе



Контентные риски

возникают в процессе использования находящихся в Сети материалов

текстов

картинок

аудио- и видеофайлов

ссылок на различные ресурсы

содержащих информацию

противозаконную

неэтичную

вредоносную

Способы защиты от негативной информации

Федеральный закон №139-ФЗ от 28 июля 2012 года «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» установил процедуру блокировки контента, запрещенного к распространению в Сети на территории РФ.

К такому контенту относятся:

- детская порнография;
- пропаганда наркотиков;
- пропаганда суицидальных действий.



Информационная компетентность

Достоверность
информации

Авторское
право

Как работает
ПОИСК

Коммуникационные риски

возникают в процессе общения и межличностного взаимодействия пользователей в Сети

при общении в

чатах

онлайн-мессенджерах

социальных сетях

сайтах знакомств

форумах

блогах

Примеры

кибербуллинг

незаконные контакты (например, груминг, сексуальные домогательства)

знакомства в Сети и последующие встречи с интернет-знакомыми в реальной жизни

Особенности коммуникации в Интернете

Доступность и
непрерывность

Невидимость, или
бестелесность

Анонимность

Ощущение
вседозволенности

Персонализация

Ограничители
общения

Ускорение темпов
коммуникации

Иллюзия
активности

Трансграничность

Мониторинг детей в социальных сетях «Герда»

<https://gerdabot.ru/>

Потребительские риски

возникают в процессе приобретения товаров и услуг через Интернет.

включают

риск приобретения

финансовый риск

товара низкого качества

контрафактной и фальсифицированной продукции

потери денежных средств без приобретения товара или услуги

хищения финансовой информации с целью мошенничества.

Технические риски





Рис. 14. Ответы российских подростков 12–17 лет на вопрос «Давал ли ты когда-либо пароль от своего аккаунта в социальной сети или электронной почте?» (Исследование цифровой компетентности, Фонд Развития Интернет при поддержке Google, 2013 г.)

Никому не давали
свой пароль

61%

56%

Близкому другу

19%

22%

Родителям

12%

14%

Братьям / сестрам

8%

8%

Незнакомым
людям

1%

1%

3% опрошенных затруднились с ответом

Обеспечение информационной безопасности обучающихся педагогами

1. Объясните учащимся правила поведения в Интернете. Расскажите о мерах, принимаемых к нарушителям, ответственности за нарушение правил поведения в сети.
2. Совместно с учащимися сформулируйте правила поведения в случае нарушения их прав в Интернете.
3. Приучайте несовершеннолетних уважать права других людей в Интернете. Объясните им смысл понятия «авторское право», расскажите об ответственности за нарушение авторских прав.
4. Проявляйте интерес к "виртуальной" жизни своих учеников, и при необходимости сообщайте родителям о проблемах их детей.
5. Научите учеников внимательно относиться к информации, получаемой из Интернета. Формируйте представление о достоверной и недостоверной информации. Наставляйте на посещение проверенных сайтов.
6. Обеспечьте профилактику интернет-зависимости учащихся через вовлечение детей в различные внеклассные мероприятия в реальной жизни (посещение театров, музеев, участие в играх, соревнованиях), чтобы показать, что реальная жизнь намного интереснее виртуальной.
7. Периодически совместно с учащимися анализируйте их занятость и организацию досуга, целесообразность и необходимость использования ими ресурсов сети для учебы и отдыха с целью профилактики интернет-зависимости и обсуждайте с родителями результаты своих наблюдений.
8. В случае возникновения проблем, связанных с Интернет-зависимостью, своевременно доводите информацию до сведения родителей, привлекайте к работе с учащимися и их родителями психолога, социального педагога.
9. Проводите мероприятия, на которых рассказывайте о явлении Интернет-зависимости, ее признаках, способах преодоления.
10. Систематически повышайте свою квалификацию в области информационно-коммуникационных технологий, а также по вопросам здоровьесбережения.
11. Станьте примером для своих учеников. Соблюдайте законодательство в области защиты персональных данных и информационной безопасности. Рационально относитесь к своему здоровью. Разумно используйте в своей жизни возможности интернета и мобильных сетей.

Организация работы с обучающимися

- *Учебная программа*
**«Интернет: возможности, компетенции, безопасность»,
рекомендованная Министерством образования и науки РФ**
 - Факультет психологии МГУ им. М.В. Ломоносова
 - Федеральный институт развития образования
 - Фонд Развития Интернет
- Ссылки:
 - <http://detionline.com> (<http://detionline.com/internet-project/about>)
 - <http://detionline.com/assets/files/research/BookTheorye.pdf> —
теория
 - [http://detionline.com/assets/files/research/Book Praktikum.pdf](http://detionline.com/assets/files/research/Book_Praktikum.pdf) —
практика