ГАОУ ДПО ВО
ВЛАДИМИРСКИЙ ИНСТИТУТ
РАЗВИТИЯ ОБРАЗОВАНИЯ ИМЕНИ
Л.И. НОВИКОВОЙ

КАФЕДРА
ЦИФРОВОГО ОБРАЗОВАНИЯ И
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тема занятия:

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДЕТЕЙ И СОВРЕМЕННЫЕ ИНТЕРНЕТ-РИСКИ

Лекция серии:
Образовательная деятельность в контексте информационной безопасности детей

к.т.н., зав. кафедрой ЦОИБ ГАОУ ДПО ВО ВИРО
МИШИН Денис Вячеславович

В настоящее время в сфере образования вопросы **информационной безопасности** (в том числе касающиеся защиты ПДн участников образовательного процесса и защиты детей от информации, причиняющей вред их здоровью и развитию) и **Интернет безопасности** признаются Российским государством приоритетными.

ЕДИНЫЙ УРОК БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ

Приказ Минкомсвязи России от 27.02.2018 N 88 "**Об утверждении плана мероприятий по реализации Концепции информационной безопасности детей на 2018 - 2020 годы**»

«**Концепция информационной безопасности детей**», утвержденная распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р.

Современные проблемы и задачи, связанные с теорией и методологией обеспечения **ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ** государства, общества и **человека** находятся на пересечении различных предметных областей:

- технической,
- социологической,
- политологической,
- юридической,
- экономической,
- психологической.

Термин «**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**» имеет различный смысл и трактовку в зависимости от контекста.

Такой концептуальные аспекты, как **объект защиты**, **актуальные угрозы** в различных трактовках понятиях **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**, тоже могут быть различными

*Развитие информационного общества на современном этапе ставит вопрос не только о форматах, вариациях и способах его функционирования и прогресса, но и о **механизмах защиты**, необходимых для успешной эволюции данного общества.*

Что понимают под термином **«Информационная безопасность»** ?

???

Информационная безопасность =
Безопасность информации =
Интернет безопасность =
Безопасность в Интернет =
Кибербезопасность (*Cybersecurity*)
= …

???

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – защищенность личности, общества, государства

Объект защиты – личность, общество, государство

В Доктрине информационной безопасности РФ от 2016 года понятие «***информационная безопасность Российской Федерации***» было раскрыто таким образом:

Указ Президента РФ от 05.12.2016 г. № 646

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РФ - состояние защищенности **личности**, **общества** и **государства** от внутренних и внешних **ИНФОРМАЦИОННЫХ УГРОЗ**, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие РФ, оборона и безопасность государства.

ЗАЩИЩЕННОСТЬ *- обеспеченность средствами поддержания необходимого уровня и/или качества защиты жизненно важных средств, субъектов от снижения пользы и/или увеличения вреда.*

ЗАЩИЩЕННОСТЬ ИС *- способность системы противостоять несанкционированному доступу к конфиденциальной информации, ее искажению или разрушению.*

ЗАЩИЩЕННОСТЬ *— относительно устойчивая возможность удовлетворения своих основных потребностей и обеспеченности собственных прав в любой, даже неблагоприятной ситуации, при возникновении обстоятельств, которые могут блокировать или затруднять их реализацию.*

Понятие **«ИНФОРМАЦИОННАЯ УГРОЗА»** в Доктрине ИБ не дано!

Дезинформация — заведомо ложная или искаженная информация предоставляемая оппоненту для получения требуемого результата.

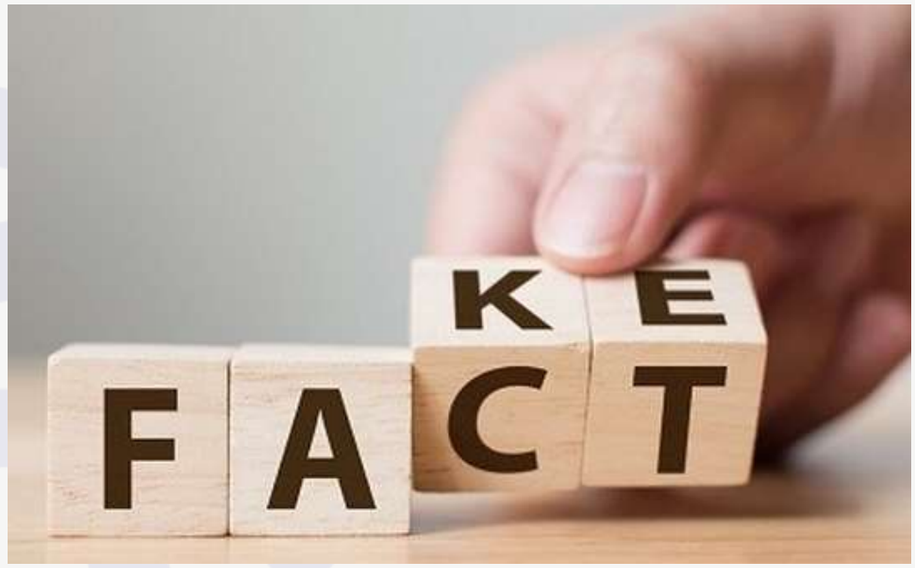
Также дезинформацией (дезинформированием) называется сам процесс манипулирования информацией, как то:

- введение кого-либо в заблуждение путём предоставления неполной информации или полной, но уже не актуальной информации,
- искажения контекста,
- искажения части информации.

Поступок субъекта, против которого направлена дезинформация, может заключаться в принятии нужного манипулятору решения или в отказе от принятия невыгодного для манипулятора решения. Но в любом случае конечная цель — это действие, которое будет предпринято оппонентом.

Виды дезинформации

ВВЕДЕНИЕ В ЗАБЛУЖДЕНИЕ конкретного лица или группы лиц (социальной группы, нации и т.д.) — это прямой обман, предоставление заведомо ложной информации;



МАНИПУЛИРОВАНИЕ (поступками одного человека или группы лиц) — это способ воздействия, направленный непосредственно на изменение направления активности людей.

Выделяют следующие уровни манипулирования:

- усиление существующих в сознании людей (выгодных манипулятору) ценностей, идей, установок,…;
- частичное изменение взглядов на то или иное событие или обстоятельство, факт;
- кардинальное изменение жизненных установок;
- устройство ложных объектов и передислокации войск (в военном деле).

СОЗДАНИЕ ОБЩЕСТВЕННОГО МНЕНИЯ — это формирование в обществе определённого отношения к выбранной проблеме/событию.

Зачем защищать?

Что/кого защищать?

От чего/кого защищать?

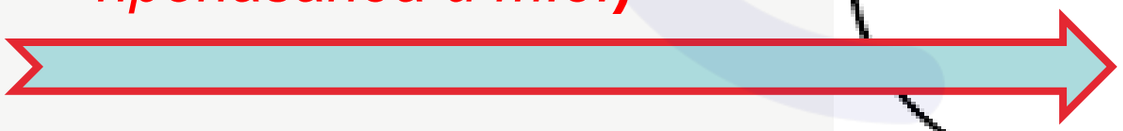
Как защищать?

Зачем защищать?

Что/кого защищать?

От чего/кого защищать?

Внутренние и внешние **информационные угрозы** (*запрещенная, вредоносная информация, дезинформация, пропаганда и т.д.*)



Объект защиты – **личность (ученик, педагог)**

<u>Как защищать?</u>

Правовые (законодательные) **меры**

Организационные меры (регламенты, инструкции)

Технические меры (СЗИ, СКЗИ)

Морально-этические / психологические (кодексы, ценности, психолог)

Цензура / экспертиза (на уровне государства, региона, ОО)

Пропаганда полезной и достоверной информации

Повышение информационной культуры / цифровой грамотности

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – защищенность детей

Объект защиты – личность (ребёнок)

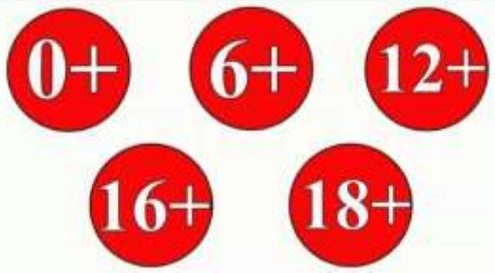
В 2010 году был принят **№ 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию**", где применяется следующий термин:

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДЕТЕЙ - **состояние защищённости детей**, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию

№ 436-ФЗ регулирует отношения, связанные с защитой детей от травмирующего их психику информационного воздействия, жестокости и насилия **в общедоступных СМИ**.

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 по № 436-ФЗ;

№ 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» регулирует отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию, в том числе от такой информации, содержащейся в информационной продукции.



№ 436-ФЗ предусматривает отнесение **информационной продукции** к одной из пяти возрастных категорий или запрещает её распространение среди детей.

ИНФОРМАЦИОННАЯ ПРОДУКЦИЯ — предназначенные для оборота на территории РФ продукция СМИ, печатная продукция, аудиовизуальная продукция на любых видах носителей, программы для ЭВМ и БД, а также информация, распространяемая посредством зрелищных мероприятий, посредством информационно-телекоммуникационных сетей, в том числе сети «Интернет», и сетей подвижной радиотелефонной связи;

ИНФОРМАЦИОННАЯ ПРОДУКЦИЯ ДЛЯ ДЕТЕЙ — информационная продукция, соответствующая по тематике, содержанию и художественному оформлению физическому, психическому, духовному и нравственному развитию детей;

КЛАССИФИКАЦИЯ ИНФОРМАЦИОННОЙ ПРОДУКЦИИ — распределение информационной продукции в зависимости от её тематики, жанра, содержания и художественного оформления по возрастным категориям детей в порядке, установленном № 436-ФЗ;

Зачем защищать?

Что/кого защищать?

От чего/кого защищать?

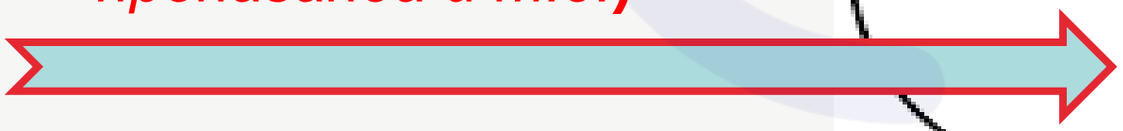
Как защищать?

Зачем защищать?

Что/кого защищать?

От чего/кого защищать?

Внутренние и внешние **информационные угрозы** (*запрещенная, вредоносная информация, дезинформация, пропаганда и т.д.*)



Объект защиты – **личность (ученик, педагог)**

<u>Как защищать?</u>

Правовые (законодательные) **меры**

Организационные меры (регламенты, инструкции)

Технические меры (СЗИ, СКЗИ)

Морально-этические / психологические (кодексы, ценности, психолог)

Цензура / экспертиза (на уровне государства, региона, ОО)

Пропаганда полезной и достоверной информации

Повышение информационной культуры / цифровой грамотности

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – защищенность информации и ИТ-инфраструктуры

Объект защиты- информационные ресурсы и поддерживающая инфраструктура (ИС)

Часто употребляемым в профессиональной среде ИБ и ЗИ (в профильных журналах, пособиях, рекомендациях и т.д.) можно назвать определение, заимствованное из англоязычной литературы:

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ - состояние защищенности **информационных ресурсов** и **поддерживающей инфраструктуры** от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб **субъектам информационных отношений**, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ - состояние защищенности **информации [данных]**, при котором обеспечены ее [их] конфиденциальность, доступность и целостность

ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»

Свойства информации

Как правило, при разговоре об обеспечении ИБ, говорят об обеспечении таких свойств информации, как **конфиденциальность, целостность и доступность**. В зарубежных источниках их называют так же *AIC*-триадой (***Availability, Integrity, Confidentiality***).

Вопросы **безопасности информации и защиты информации**, в основном сводятся к обеспечению данных свойств информации

Иногда к данным трем основным свойствам добавляют дополнительно **подотчётность** (*accountability*)**, достоверность** (*reliability*), **аутентичность или подлинность** (*authenticity*), **аппелируемость** (*non-repudiation*) **и неотрекаемость** (*non-repudiation*).

Информационная безопасность (*information security*): Все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки [ГОСТ Р ИСО/МЭК 13335-1 — 2006 Методы и средства обеспечения безопасности Часть 1 Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий]

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя

Конфиденциальность представляет собой **особый правовой режим информации**, характеризующийся:

- установленным (в силу закона или договора) ограниченным доступом к информации,
- запретом на передачу информации без согласия ее обладателя,
- запретом на распространение информации, вытекающим из предыдущих элементов режима.

С соблюдением **режима конфиденциальности** 149-ФЗ связывает ряд последствий, в частности, ограничения на возмещение убытков, вызванных разглашением конфиденциальной информации, если **потерпевшее лицо не принимало необходимых мер** по соблюдению конфиденциальности информации.

Зачем защищать?

Что/кого защищать?

От чего/кого защищать?

Как защищать?

Зачем защищать?

Что/кого защищать?

От чего/кого защищать?

Угрозы ИБ (*конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности*)

Защита от случайных или преднамеренных воздействий естественного или искусственного характера

Объект защиты – **информация / данные** (информационные ресурсы) и **поддерживающая инфраструктура** (ИС)

<u>Как защищать?</u>

Правовые (законодательные) **меры**

Организационные меры (регламенты, инструкции)

Технические меры (СЗИ, СКЗИ)

Морально-этические / психологические (кодексы, ценности, психолог)

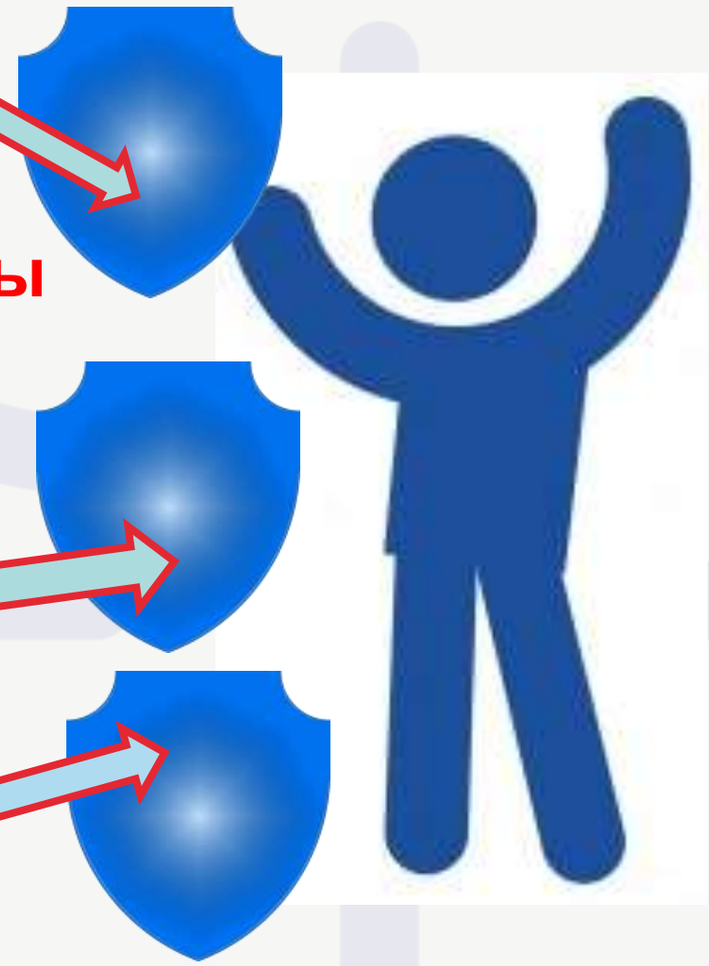
Цензура / экспертиза (на уровне государства, региона, ОО)

Пропаганда полезной и достоверной информации

Повышение информационной культуры / цифровой грамотности

Информация (*не обязательно в цифровой форме*), причиняющая вред здоровью и (или) развитию детей

Внутренние и внешние **информационные угрозы** (дезинформация, пропаганда, мошенничество)



Случайные или преднамеренные воздействия различного характера на защищаемую (ценную) информацию и ИТ-инфраструктуру (Угрозы ИБ)

Защищенность **от информации, способной причинить вред** здоровью и (или) физическому, психическому, духовному, нравственному развитию;

Реализация конституционных прав и свобод на поиск и получение **достоверной, полной, точной, актуальной информации** в любых формах и из любых источников при условии соблюдения требований закона РФ

Защищенность/Безопасность Значимой для ребенка информации – ПДн, различные виды тайн, другие имеющие ценность (дорогостоящие или сложно восстанавливаемые) информационные ресурсы;

Безопасность ребенка (школьника) в современной глобальной информационной среде

Из чего складывается?

Интересы ребенка в сфере ИБ, как субъекта информационных отношений в глобальной информационной среде

1. Реализация конституционных прав и свобод на поиск и получение **достоверной, полной, точной, актуальной** информации в любых формах и из любых источников при условии соблюдения требований закона РФ (149-ФЗ);

2. Защищенность / Безопасность (*конфиденциальность, целостность, доступность*) **значимой для ребенка информации** – ПДн, различных видов тайн, других имеющих ценность (дорогостоящих или сложно восстанавливаемых) информационных и технических ресурсов (149-ФЗ, 152-ФЗ);

3. Защищенность **от информации, способной причинить вред** здоровью и (или) физическому, психическому, духовному, нравственному развитию (436-ФЗ);

4. Защищенность от угроз на физическом, финансовом, эмоционально-психическом, духовно-образовательном, политическом и профессиональном уровнях, возникающих при применении современных цифровых инфо-коммуникационных технологий, включая Интернет (Интернет-безопасность / *cybersecurity &* безопасность в Интернет / *cybersafety*).

Риск ориентированный подход к безопасности детей и подростков в киберпространстве

(*On-line* риски / риски в Интернет)

ФОНД РАЗВИТИЯ ИНТЕРНЕТ

В основе раздела лежит классификация интернет-рисков, разработанная Фондом Развития Интернет при научной поддержке факультета психологии МГУ имени М.В. Ломоносова и Федерального института развития образования РФ

Американские исследователи [Palfrey, Boyd, Sacco] выделяют три группы угроз безопасности детей и подростков в Интернете:

- **небезопасные контакты** (угроза неприемлемого контакта; угрозы связанные с идеологическими, религиозными, экстремистскими призывами);
- **киберагрессия** (троллинг, кибербуллинг: унижения, оскорбления, агрессивные нападки, преследования в Интернет; нарушение приватности; секстинг);
- **материалы «вредного/опасного» содержания** (противоправный контент - относят широкий спектр материалов, демонстрирующих сцены насилия (в видео, графике (других видах изображений), музыке, текстах), экстремистские призывы и поведение, порнографию (в том числе детскую).

Для каждого возрастного периода у детей и подростков характерны свои особенности поведения и соответственно более или менее актуальные угрозы и риски.

Британские ученые С. Ливингстон и Л. Хэддон в рамках исследования **«Дети Европы Онлайн»,** классифицирует риски по 4 группам**:**

- **Риски, связанные с содержанием медиаресурсов** (содержание порнографического или сексуального характера, содержание насильственного или агрессивного характера; неприемлемое содержание; содержание со сценами насилия и крови; содержание, рекламирующее наркотики; содержание информации о причинении себе вреда (анорексия, булимия) или суицид; порнография с насилием, содержание, призывающее к расизму; содержание, содержание, унижающее чувство собственного достоинства).

- **Риски, связанные с контактами** (угроза неприемлемого контакта, возможность неприемлемого сексуального контакта; лица, которые выдают себя за других людей; личные встречи после онлайн-знакомства; другие лица, которые получили доступ к вашим личным данным; содержание с идеологическими, религиозными, экстремистскими призывами).

- **Риски, связанные с поведением** (различные формы агрессивного поведения; буллинг; нежелательное / неприемлемое поведение; несанкционированные попытки доступа к личным данным человека, нарушение приватности; нанесения высказываниями ущерба репутации человека, обмен изображениями или фотографиями , обмен личными данными; сексуальная агрессия или рассылка неприемлемых сообщений интимного содержания (секстинг).

- Другие особые риски (вирусы, спам, всплывающие рекламные окна, недостаточный уровень интернет-безопасности в целом; риски, связанные с поиском надежной информации, риски, связанные с аппаратным или программным компьютерным обеспечением; проведение большого количества времени в Интернете; азартные онлайн-игры; несоблюдение правил онлайн-безопасности; риски, связанные с ущербом для здоровья пользователя; нелегальное скачивание информации).

Украинские исследователе кафедры социальной педагогики ЛНУ им. Т.Шевченко классифицируем Интернет-риски по сферам благополучия для человека:

- **Риски физическому благополучию, связанные с использованием Интернета** (астенопатия, боль в спине, шее, эпилепсия, запястный синдром, тендениты, стенокардия, сыпь на коже лица, хроническая головная боль, головокружение (возникают от длительного пользованием компьютером), снижение концентрации внимания, нарушение сна; встреча с незнакомцами из сети; педофилия; пропаганда психоактивных веществ, призывы к массовому употреблению наркотиков; пренебрежение питанием; причинения себе или другим вреда, суицид и т.д.);

- **Риски психическому благополучию, связанные с использованием Интернета** (распространение личных данных в Интернете, нарушения конфиденциальности и онлайн-неприкосновенности частной жизни; эксплуатация доверия; киберагресия, кибербуллинг, запугивания, разжигание ненависти и нетерпимости, язык вражды, троллинг, содержание порнографического или сексуального характера, секстинг, интернет-сообщения интимного содержания; жестокие и азартные игры; унижения чувства достоинства, нарушение прав человека; низкое качество информации и информационная перегрузка и т.п.);

- **Риски социальному благополучию, связанные с использованием Интернета** (повышенная возбудимость и депрессивные состояния; препятствие для выполнения домашних дел, уменьшение времени общения в реальном мире, зависимость и т.д.);

- **Риски материальному благополучию, связанные с использованием Интернета** (реклама, спам, вирусы; незаконные загрузки; азартные онлайн игры; кибератаки, кибертерроризм, приобретение товара низкого качества, потеря средств, повреждение программного обеспечения компьютера; пиратство; интернет-преступность, интернет-мошенничество, различные формы интернет-маркетинга).

На основе анализа эмпирических данных, все опасности интернет-среды объединены в пять крупных групп рисков:

ФОНД РАЗВИТИЯ ИНТЕРНЕТ

Контентные риски

Возникают в процессе использования материалов, содержащих противозаконную, неэтичную и вредоносную информацию - насилие, агрессию, эротику и порнографию, нецензурную лексику, пропаганду суицида, наркотических веществ и т.д.

Коммуникационные риски

Связаны с межличностными отношениями Интернет- пользователей и включают в себя незаконные контакты (например с целью встречи), киберпреследования, кибернижения, груминг и др.

Потребительские риски

Злоупотребление правами потребителя: риск приобретения товара низкого качества, подделок, контрафактной и фальсифицированной продукции, хищение денежных средств злоумышленником через онлайн-банкинг и т.д.

Технические риски

Возможность повреждения ПО, информации, нарушение ее конфиденциальности или взлома аккаунта, хищения паролей и персональной информации злоумышленниками посредством вредоносного ПО и др. угроз.

Интернет-зависимость

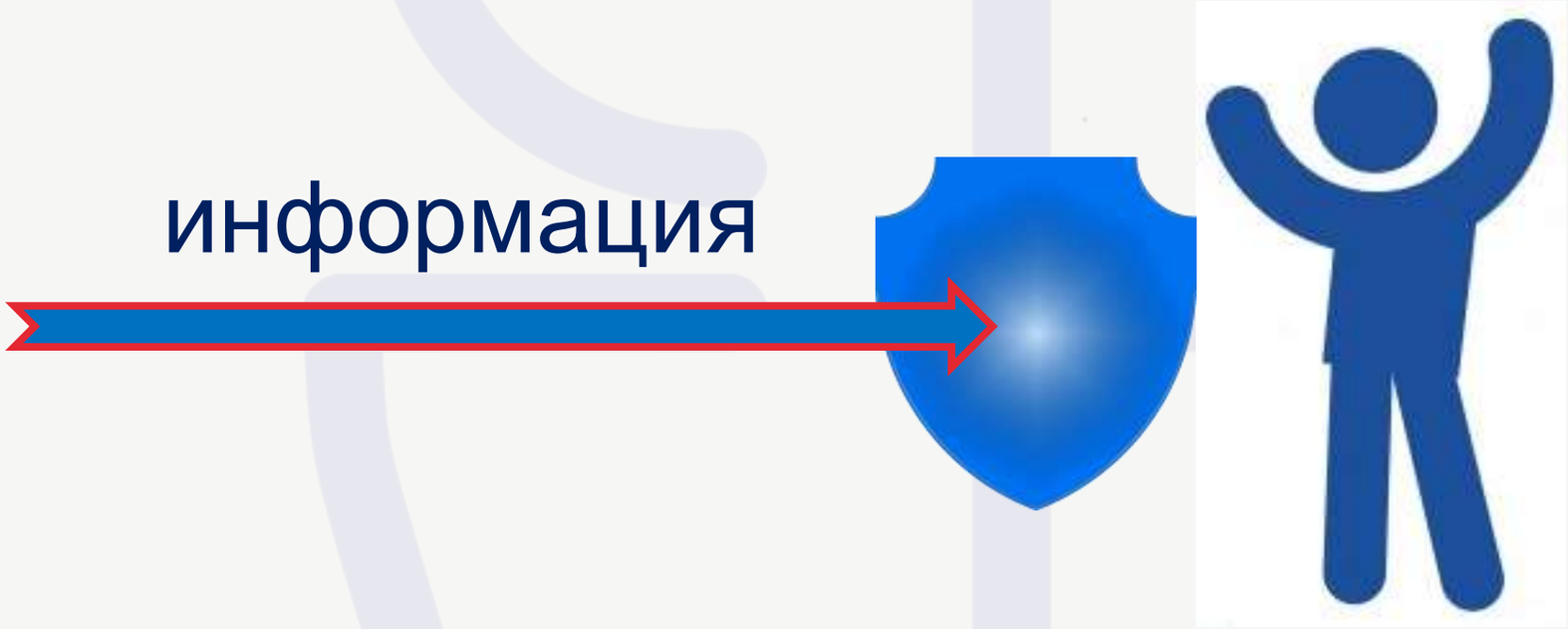
Непреодолимая тяга к чрезмерному использованию Интернета. В подростковой среде проявляется в форме увлечения видео-играми, навязчивой потребности к общению в чатах, круглосуточном просмотре фильмов и сериалов в Сети.

Обращения по типам рисков на Линию помощи «Дети Онлайн»

Проблемы, возникшие в процессе онлайн общения – это основная причина обращений на Линию помощи «Дети Онлайн».

Контентные Интернет-риски

информация



Объект защиты – личность (ребёнок)

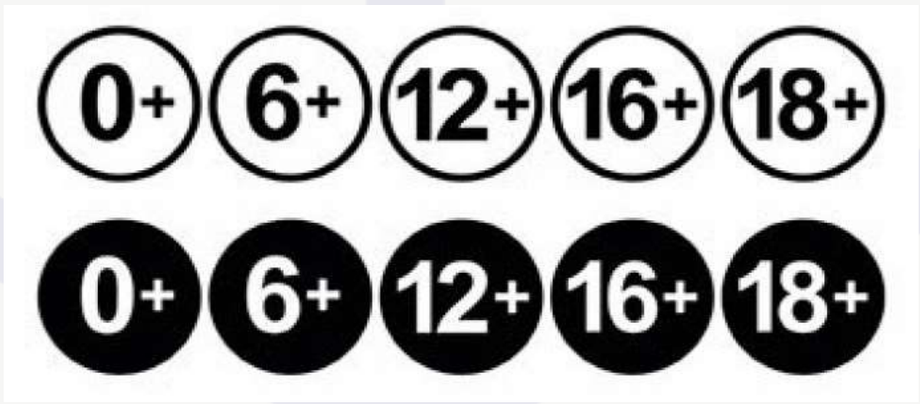
Контентные риски

Возникают в процессе использования материалов, содержащих противозаконную, неэтичную и вредоносную информацию - насилие, агрессию, эротику и порнографию, нецензурную лексику, пропаганду суицида, наркотических веществ и т.д.

ИНФОРМАЦИЯ НЕЖЕЛАТЕЛЬНОГО ХАРАКТЕРА – информация, которая содержит **противозаконную, неэтичную** и **вредоносную информацию**. Некоторые виды информации **ограничены** для распространения среди детей и отдельных возрастных групп

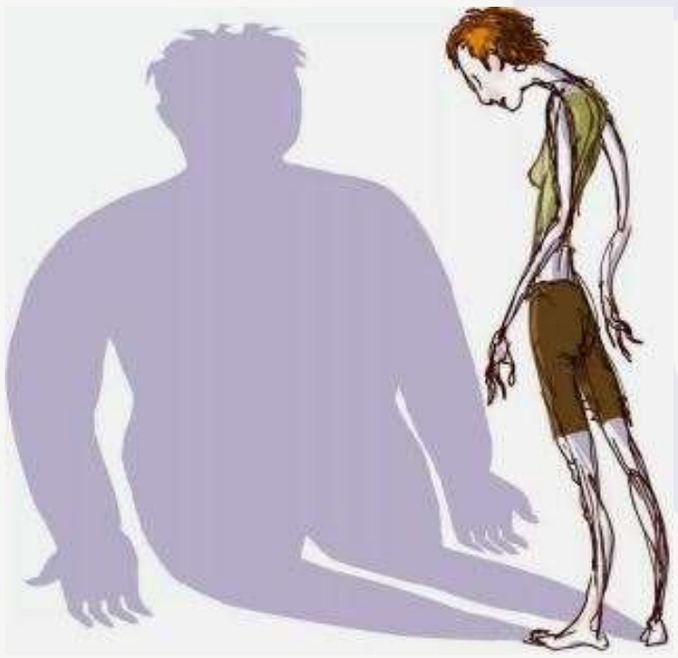
К **ВРЕДОНОСНОЙ ДЛЯ ДЕТЕЙ** категории относят эротику и порнографию, материалы, содержащие насилие, убийства, агрессию, жестокость, пропаганду нездорового образа жизни, а также материалы, оправдывающие насилие и противоправное поведение.

Информация такого рода может повысить у ребенка тревожность, расстроить его, вызвать страх, ужас, панику.



Для детей и подростков в силу их неопытности угрозу представляет информация, содержащая:

- ложные, вводящие в заблуждение рекомендации (например, об употреблении БАД и лекарственных средств, приемов похудения и др.),
- пропаганду опасных для жизни и здоровья увлечений, азартных игр, соревнований,
- неэтичный контент (например, поданная под особым ракурсом или недостоверная информация о некоторых людях и событиях, нецензурная лексика и др.).



Контентные Интернет-риски и законодательство РФ

ЗАПРЕЩЕННАЯ ИНФОРМАЦИЯ

ЗАПРЕЩЕННАЯ ДЛЯ РАСПРОСТРАНЕНИЯ СРЕДИ ДЕТЕЙ

ИНФОРМАЦИЯ, РАСПРОСТРАНЕНИЕ КОТОРОЙ СРЕДИ ДЕТЕЙ ОПРЕДЕЛЕННЫХ ВОЗРАСТНЫХ КАТЕГОРИЙ ОГРАНИЧЕНО

ИНФОРМАЦИЯ НЕЖЕЛАТЕЛЬНОГО ХАРАКТЕРА
(иной опасный или вредоносный контент)

Контентные Интернет-риски

К **опасному или вредоносному контенту** относятся материалы ненавистнического и экстремистского характера, детская порнография, информация, пропагандирующая суицид, азартные игры и нанесение себе вреда, информация о том, как сделать или где приобрести наркотические вещества и др.

ЗАПРЕЩЕННАЯ ИНФОРМАЦИЯ — запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, пропагандирующая потребление и изготовление наркотиков, азартные игры, изготовление взрывчатых веществ, а также иная информации, за распространение которой предусмотрена уголовная или административная ответственность.

Распространение информации, распространение которой в РФ ограничивается, преследуется по закону.

В Российском законодательстве есть возможность в соответствии со КоАП РФ и УК РФ привлечь к административной и уголовной ответственности за распространение данной информации, как владельцев сайтов, на которых размещается данная информация, так и ее авторов, и распространителей.

По положению **№ 436-ФЗ,** к информации, **причиняющей вред здоровью и (или) развитию детей**, относится:

ЗАПРЕЩЕННАЯ для распространения среди детей

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

2) способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную 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;

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;

8) о несовершеннолетнем, пострадавшем в результате противоправных действий, позволяющая прямо или косвенно установить личность такого несовершеннолетнего.

По положению **№ 436-ФЗ,** к информации, **причиняющей вред здоровью и (или) развитию детей**, относится:

Распространение которой среди детей определенных возрастных категорий **ОГРАНИЧЕНО**

1) 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 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.

Неэтичная, противоречащая принятым в обществе нормам морали и социальным нормам, информация не запрещена к распространению, но может содержать информацию, способную оскорбить пользователей и оказать на них вредоносное воздействие, в частности манипулировать сознанием и действиями отдельных граждан или даже групп людей.

Изготовление и распространение подобной информации не попадает под действие КоАП РФ и УК РФ, однако может повлечь ***санкции со стороны владельцев сайта****, на которых пользователь размещает такую информацию, или* ***со стороны организаций****, имеющих возможность ограничить доступ к сайту, содержащего такую информацию.*

Контентные Интернет-риски

Полностью оградить детей от негативной информации невозможно!

Никакие ограничения не помогут, если подросток всерьез намерен что-то отыскать в Интернете: он просто пойдет к другу или воспользуется своим смартфоном.

Однако ответственное и осознанное отношение родителей и учителей х к этой проблеме может значительно снизить риск столкновения детей и подростков с опасной информацией.

С учетом трудностей, связанных с запрещением всех форм потенциально опасного контента для детей, применяются разнообразные стратеги и методы регулирования на различных уровнях.

Государственное регулирование.

Саморегулирование IT-индустрии.

Саморегулирование в школах.

Коммуникационные Интернет-риски

Опасные контакты Агрессия в Интернет

Коммуникационные риски

Связаны с межличностными отношениями Интернет- пользователей и включают в себя незаконные контакты (например с целью встречи), киберпреследования, киберунижения, груминг и др.

Коммуникационные Интернет-риски

Умение распознавать потенциальные риски в процессе *on-line* общения, предотвращать их и справляться при столкновении с ними, то есть обеспечивать безопасность своей коммуникации в Интернет, — важная составляющая коммуникативной компетентности цифрового гражданина.

Некоторые ошибки, совершаемые детьми и подростками в процессе коммуникации и способные привести к возникновению нежелательной (опасной) ситуации:

- предоставление конфиденциальной информации (личная, интимная информация, личная переписка, ПДн и персональные данные родственников и др.),
- открытость профилей социальных сетей,
- публикация материалов, способных навредить репутации.

Особое внимание необходимо обратить на ключевые коммуникационные риски, связанные с взаимодействием между подростками и другими пользователями в Интернете.

Коммуникационные Интернет-риски

К коммуникационным интернет-рискам относят:

- контакты с незнакомцами (онлайн-груминг, вербовка),
- сексуальные домогательства, шантаж (секстинг),
- киберагрессию (троллинг, хейтинг, флейминг, кибersталкинг, кибербуллинг).

Для подобных целей используются чаты, онлайн-мессенджеры (*Viber*, *WhatsApp*, *Skype* и др.), социальные сети, игры, сайты знакомств, форумы, блоги и т.д.

Коммуникационные

Интернет-риски

Общение с незнакомцами (ГРУМИНГ)

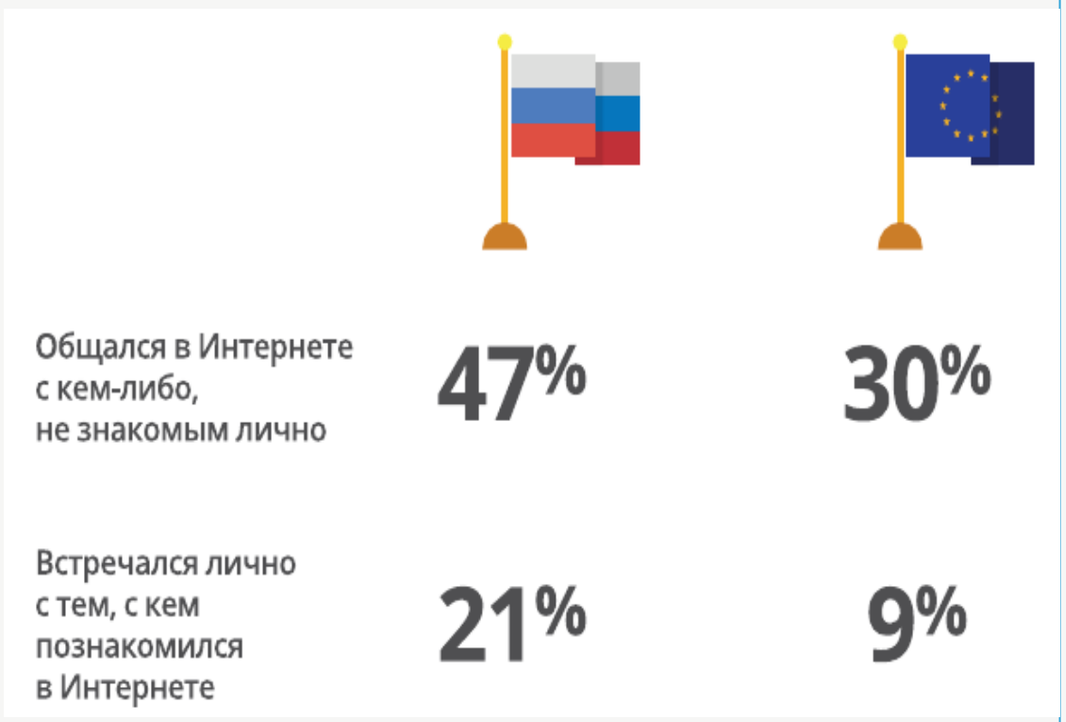
Коммуникационные Интернет-риски

Общение с незнакомцами (**груминг**)

Как показало исследование «Дети России онлайн», большинство российских школьников общаются в Интернете с людьми, которых они знают в реальной жизни.

Причем с возрастом количество таких контактов значительно вырастает.

Чаще всего такие контакты дети заводят в социальных сетях, онлайн-играх и *IM*.



Большое количество «френдов» в социальных сервисах работает на популярность подростка, поэтому многие знакомятся и добавляют в списки друзей **всех подряд**. Таким образом, они допускают незнакомых людей к своей личной информации и могут подвергнуть себя риску.

Помимо возможностей накопления социального капитала в виде интернет-знакомых, такая практика может быть довольно рискованной.

Коммуникационные Интернет-риски

Общение с незнакомцами (**груминг**)

Груминг — это формирование доверительных отношений (дружеского и эмоционального контакта) с ребенком в Интернете с целью его дальнейшей сексуальной эксплуатации (сексуального насилия).

Груминг происходит от английского слова ***grooming***, которое переводится как "уход" или "забота", что передает основную суть метода: создать у ребенка ощущение заботы и вызвать состояние устойчивой психологической связи для совершения последующих преступлений.

Основная цель груминга - получение интимные фото/видео ребенка для последующего шантажа и вымогательства у него денег/более интимных материалов или встреч.

Анонимность интернет-пространства дает для этого множество возможностей. Человек может поставить детское изображение на фото профиля и подружиться с ребенком в социальной сети или в игре. Он может рассказать интересную историю или болтать об общих интересах и увлечениях, то есть вызвать доверие и начать выстраивать отношения.

Коммуникационные Интернет-риски. Интернет Груминг

Сначала злоумышленник тщательно ищет и выбирает подходящую жертву, используя поиск по учетным записям детских форумов или социальных сетей.

Затем он старается выяснить как можно больше данных о ребенке, прочитав его персональную страницу, блог и посетив страницы его друзей.

Знакомство обычно начинается с личного сообщения с содержанием, которое заведомо заинтересует ребенка.

Грумер предлагает ребенку дружбу и внимание, продолжая общение на интересные для него темы, подменяя функции родителей до установления прочных доверительных отношений.

Предлагает встречу, на которой пытается совратить малолетнего или совершить над ним незаконные насильственные действия сексуального характера.

Коммуникационные Интернет-риски

Общение с незнакомцами (**Груминг**)

Треть детей, встречавшихся с незнакомцами из Интернета, довольно активны в поиске новых друзей в Сети. Причем большинство этих новых знакомых никак не связаны с реальным кругом общения ребенка.

Каждый третий ребенок из тех, кто ходил на личные встречи, пережил негативный опыт разочарования.

Большинство этих детей рассказывали о том, что собирались на встречу и даже брали с собой сопровождающего. Но чаще всего это были их сверстники, только каждый десятый ребенок говорил взрослым о том, что идет на встречу с интернет-знакомым, и единицы брали с собой взрослого.

Подавляющая часть детей не знает, как поступать, если на встрече с интернет-знакомым произошло что-то плохое. Мало кто пытается предпринять какие-либо действия, чтобы впоследствии оградить себя от обидчика. Половина детей обращаются за социальной поддержкой, но чаще всего к друзьям. В этой ситуации **именно взрослые — родители и учителя** — должны объяснять детям, каким образом нужно вести себя с людьми, с которыми они знакомятся в Интернете.

Коммуникационные

Интернет-риски

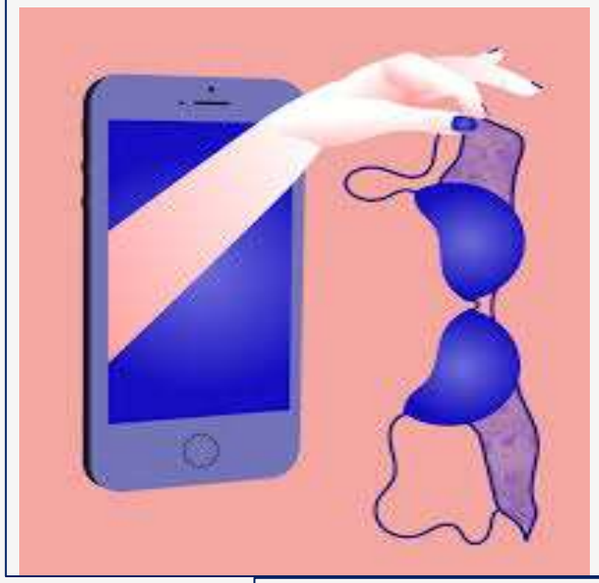
Общение на тему секса (СЕКСТИНГ)

Коммуникационные Интернет-риски

Секстинг

Груминг сейчас прямо связывают с другой современной интернет-угрозой — **секстингом**.

Злоумышленники понимают, что встречаться с несовершеннолетним в реальном мире слишком опасно. Поэтому они придумывают новые схемы, в числе которых использование **секстинга** — переписки на эротические темы.



Слово «секстинг» (от англ. *sex* и *texting*) означает общение на тему секса посредством мобильного телефона или через Интернет.

Преступники находят контакты подростка и связываются с ним, чтобы получить эротические фотографии или видео.

Интернет-среда способствует растормаживанию и дает выход типичному для подростков интересу к общению на сексуальные темы. Сегодня практически в любом устройстве есть камера, фото или видео можно отправить через мессенджер или социальную сеть. Это позволяет легко получать от детей интимные снимки, не вступая с ними в контакт в реальной жизни.

Злоумышленники неплохо понимают детскую психологию и могут убедить ребенка, что все, что он делает, якобы безобидно.

Коммуникационные Интернет-риски

Секстинг

Столкнувшиеся с секстингом подростки, как правило, остаются один на один с этой ситуацией: большинство из них ничего не предпринимает и никому ничего не рассказывает — ни родителям, ни друзьям.

Таким образом, старшие и более опытные люди, которые могли бы поддержать ребенка, помочь решить проблему и дать объективную оценку ситуации, ничего не знают.

Чаще всего подростки используют выжидательную стратегию.

Каждый четвертый из пострадавших детей ждет, что проблема решится сама собой. Значительно реже подростки пробуют решить проблему сами или пытаются заставить другого человека оставить их в покое.

Треть детей рассказывает о секстинге кому-либо из своего близкого окружения либо обращается в специальные службы. Дети не склонны рассказывать о своих переживаниях специалистам, другим взрослым, учителям.

В России подростки, защищаясь от нежелательной сексуальной переписки, чаще всего блокируют возможность человека общаться с ними, меняют настройки безопасности.

Линия помощи

«Здравствуйте, меня зовут Алиса, мне 15 лет, и у меня такая проблема. У меня каждый день запрашивают авторизацию мужчины и рассказывают про свои сексуальные наклонности, и показывают мне по веб-камере свои интимные места. Скажите, пожалуйста, что мне делать и куда обращаться?»

«Здравствуйте, меня зовут Лена, мне 14 лет! Пару месяцев назад связалась в популярной социальной сети с парнем. Он втерся мне в доверие, называл меня милой, делал комплименты. Позже он попросил меня сделать интимные фотки, и я, как дура, согласилась. Потом попросил показывать интимные места по видеосвязи, я тоже согласилась. Согласилась только на один раз. Позже он отстал от меня, но через пару дней написал, что записал это на видео и разошлет его всем моим друзьям, если я не буду продолжать демонстрировать себя по видеосвязи. Пару раз я так и делала, так как боялась, что он разошлет это друзьям, что я опозорюсь. Потом мне это надоело, и я решила действовать. Заблокировала его, кинула в черный список. Пару недель ничего не происходило, я и забыла об этой истории, но потом он выложил и отправил видео паре моих друзей. Я очень испугалась и добавила его обратно, он сказал, что еще пару раз покажу по видеосвязи, и он отстанет навсегда и удалит видео. Так я и сделала, и он отстал. Но сегодня он вновь написал что соскучился, и что хочет еще и что у него осталось видео и фотки, он выложит все, если я откажусь. Помогите, пожалуйста, я не знаю что делать! Это же педофилия! Я ужасно боюсь позора перед друзьями, но в милицию тоже боюсь идти. Помогите, пожалуйста! Мне страшно!»

Коммуникационные Интернет-риски

Агрессия в Интернет

Коммуникационные Интернет-риски

ВИДЫ АГРЕССИИ В ИНТЕРНЕТЕ:

ФЛЕЙМИНГ – разжигание спора, публичные оскорбления и эмоциональный обмен репликами в интернете между участниками в равных позициях.

ТРОЛЛИНГ – размещение в интернете провокационных сообщений с целью вызвать негативную эмоциональную реакцию или конфликты между участниками.

ХЕЙТИНГ – негативные комментарии и сообщения, иррациональная критика в адрес конкретного человека или явления, часто без обоснования своей позиции.

КИБЕРСТАЛКИНГ – использование электронных средств для преследования жертвы через повторяющиеся сообщения, вызывающие тревогу и раздражение.

КИБЕРБУЛЛИНГ - агрессивные, умышленные, повторяющиеся и продолжительные во времени действия, совершаемые группой лиц или одним лицом с использованием электронных форм контакта в отношении жертвы, которой трудно защитить себя.

Коммуникационные

Интернет-риски

Экспрессивные формы Интернет-взаимодействия

Коммуникационные Интернет-риски

Другой вид коммуникационных рисков — это вероятность столкновения **с агрессией в Интернет**. Иллюзия анонимности и безнаказанности приводит к тому, что некоторые пользователи дают выход агрессии в социальных сетях, форумах или иных площадках сети Интернет, оскорбляя других пользователей или провоцируя их на конфликт.

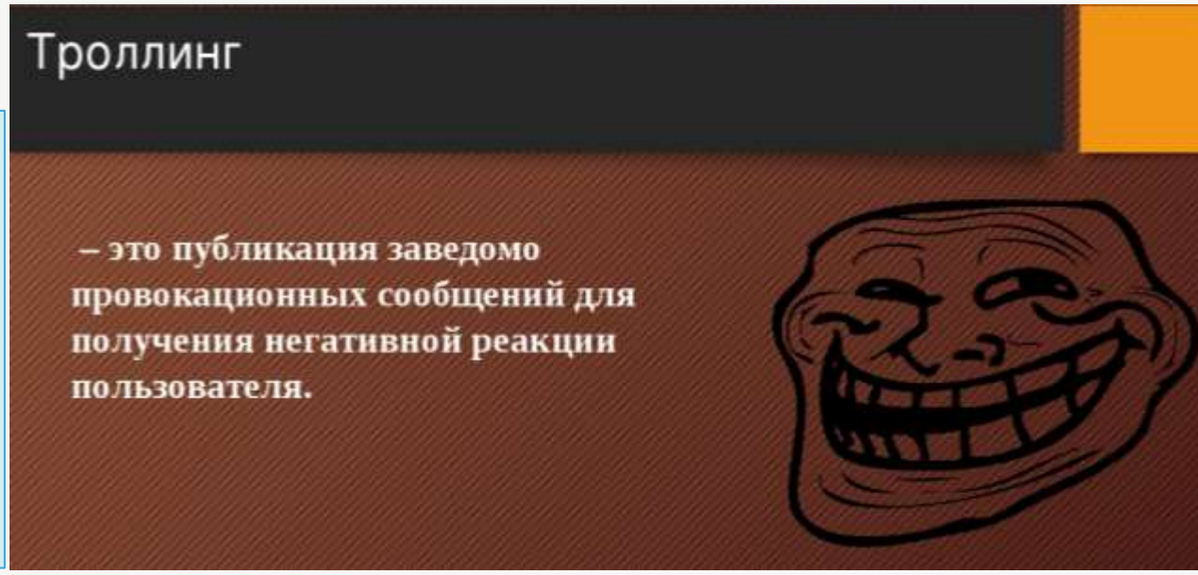
В связи с этим возникли такие экспрессивные формы Интернет-взаимодействия,
как **ТРОЛЛИНГ** и **ФЛЕЙМИНГ**.

Общение в Интернете – очень сложное и многоаспектное явление. Это объясняется невозможностью установить полноценный вербальный контакт с собеседником, а эмоции, чувства, желания и пр. передаются при помощи слов и специальных символов.

*Проблемам **троллинга** и **флейминга** в современном праве пока еще не уделяется должного внимания, хотя оба явления имеют много общего с вопросами оскорбления и клеветы.*

ЧТО ТАКОЕ ТРОЛЛИНГ?

ТРОЛЛИНГ (от англ. ***trolling*** — «ловля рыбы на блесну») — вид виртуальной коммуникации с нарушением этики сетевого взаимодействия, выражающейся в виде проявления различных форм агрессивного, издевательского и оскорбительного поведения.



Интернет-троллинг *— интереснейшее социально-психологическое явление, зародившееся в 0-х годах и достигшее максимального развития в конце первого десятилетия XXI века. Термин «**троллинг**» происходит из сленга участников виртуальных сообществ.*

Троллинг используется как персонифицированными участниками, заинтересованными в большей узнаваемости, публичности либо эпатаже, так и в процессе анонимного взаимодействия пользователей, осуществляемой без возможности идентификации с реальным субъектом виртуальной коммуникации.

Основными местами осуществления троллинга могут выступать различные тематические форумы, конференции, социальные сети, порталы, чаты и новостные сайты. Основными «площадками» для троллинга в Рунете служат - Живой Журнал (ЖЖ), Вконтакте, Одноклассники и др.

Лицо, которое занимается троллингом, принято называть «***ТРОЛЛЕМ***», что символично совпало с названием мифологического существа, характеризующимся вредным характером и скверными привычками.

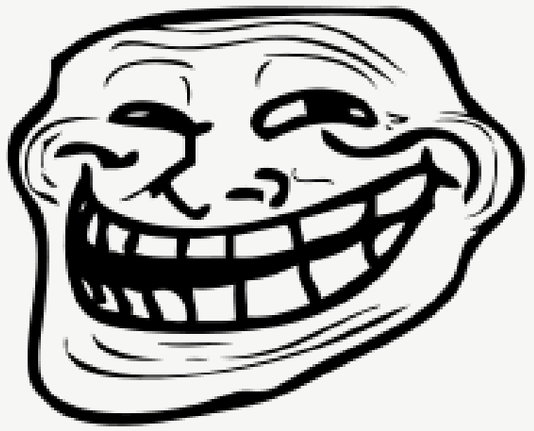
КАКОВЫ ОСОБЕННОСТИ ТРОЛЛИНГА?

Троллинг, как форма агрессии, обладает характерными особенностями:

1. возможность существования троллинга исключительно в виртуальных сообществах.

2. наличие у троллинга специфических механизмов быстрого высвобождения лавинообразной агрессии, которая мгновенно распространяется на большинство участников виртуального сообщества.

3. невозможность потенциальной жертвы конфликта вступить в физический или визуальный контакт с инициатором самой конфликтной ситуации (троллем).



Изображение trollface, созданное в 2008 году художником для веб-комикса, часто используется для обозначения троллинга в современной интернет-культуре

В последнее время троллинг всё шире используется как PR-технология в коммерческой и политической сфере. Эксперты утверждают, что использование этой технологии даёт такие преимущества, как создание ложных эффектов массовости и общественного мнения, возможность повысить доверие к источнику информации, а также увеличение охвата аудитории получателей информации. При этом троллинг относится к числу «грязных» технологий.

КАКИЕ СУЩЕСТВУЮТ ВИДЫ ТРОЛЛИНГА?

В целом в литературе троллинг, которому посвящено в настоящее время большое количество публикаций, рассматривается как негативное явление, которое препятствует установлению и воспроизводству этических норм сетевого взаимодействия и конструктивной работе групп.

В современных публикациях можно найти и множество условных классификаций троллинга, что говорит об интересе к теме и распространенности явления в современном Интернете

Тролль-комментатор, Тролль-провокатор,

Тролль-эгоцентрик, Тролль-советчик,

Троль-герой-любовник,

С начала XXI века интернет-троллями начали создаваться **собственные сетевые сообщества** и организации для обмена опытом по наиболее эффективному разжиганию конфликтов. А позднее и по развитию новых скрытых форм — это называемый **«тонкий троллинг»**. Явная провокация — «**толстый троллинг**».

Тролль-провокатор

- **Офтопик -** сообщения, которые являются несоответствующими направленности форума/темы;
- **Медиа-атака -** раздражающие слух звуковые файлы, шокирующие изображения в сообщении или ссылки на ресурсы с подобным содержанием. Зачастую ссылки замаскированы;
- **Подстрекание/провокация.** Может содержать комментарии экстремистского и расистского содержания;
- **Обвинение** оппонентов в троллинге;
- **Самоуверенные утверждения -** выражение собственного мнения без аргументации или анализа, как общепринятого факта, разжигание «***холиваров».***
- **Спойлеринг -** Преднамеренная публикация деталей, развязки популярного фильма или романа («спойлеринг», от англ. ***spoil*** – «наносить ущерб, портить»);
- **Политически заведомо спорные сообщения;**
- **Некропостинг** - возобновление (или перефразирование) очень спорной прошлой темы, особенно в небольших сообществах;
- **Преднамеренное и повторное неправильное написание ников** (имён, псевдонимов) других пользователей с целью оскорбить их или вызвать у них раздражение

Тролль-эгоцентрик

Этот тип стремится получить как можно больше ответов на свои сообщения и завоевать чрезмерное внимание в коллективе:

- Преднамеренно наивные вопросы;
- Сообщения, содержащие очевидный недостаток или ошибку;
- Просьба о помощи с неправдоподобной или неблаговидной задачей или проблемой;
- Тщательно сконструированные и чётко аргументируемые размышления и теории, базирующиеся на явно неверном утверждении или выдуманном факте.
- Предложение решить «занимательную задачу» с заведомо некорректно или неполно сформулированным условием, порождающее обширные дискуссии по поводу интерпретации.
- Офтопик-жалобы на личную жизнь или угрозы самоубийства;
- Обобщающие параноидальные ответы на личные мнения, выраженные людьми;
- Умышленная игра на чувствах людей в связи с направленностью сообщества;
- Мультиак - одновременное использование нескольких ников для раздувания споров с самим собой, искусственное подогревание темы.

Тролли-советчики

Это особый вид троллинга, который заключается в том, что тролль под видом помощи или совета жертве начинает писать на форумах разную ерунду и абсурдные сообщения.

Такой вид троллинга популярен на музыкальных, компьютерных и технических форумах, где тролль обычно проходит по всем веткам и в каждой из них отписывается якобы желая помочь жертве.

Но на самом деле при виде глупого ответа на свой вопрос, пользователь фактически ведется на провокацию тролля, начинается «флейм» и жертву блокируют («банят») на форуме или в чате.

Также возможна комбинация любых приемов.

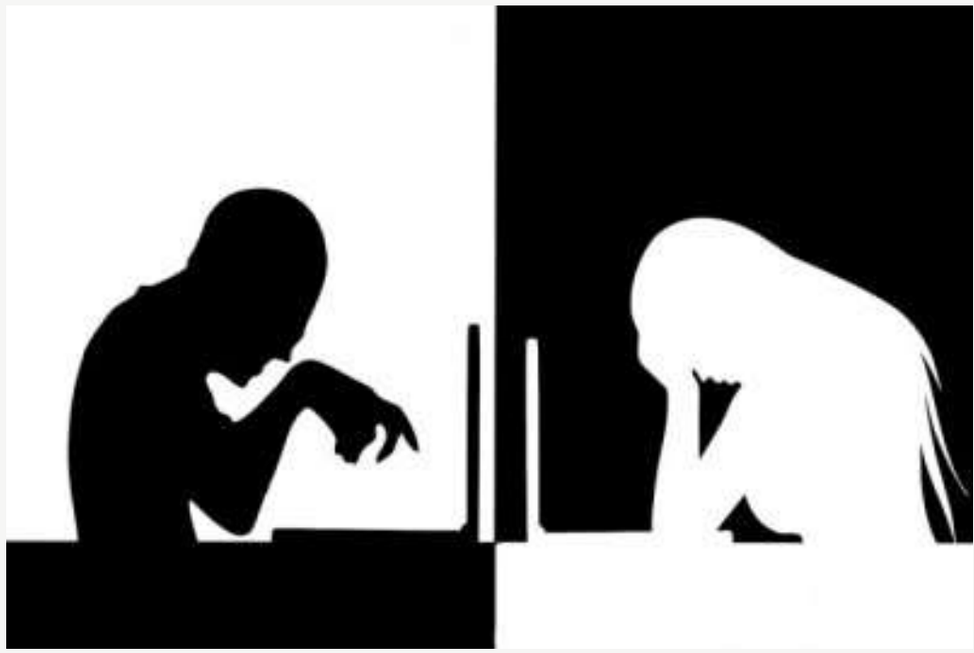
В соответствии с перечисленными видами троллинга можно говорить о целях данного вида речевого взаимодействия

1. **Эксперимент.** Возможность испытать терпение людей и нарушить правила Интернет-этикета без глобальных последствий;
2. **Развлечение.** Некоторых людей забавляет мысль, что человека могут задеть слова совершенно незнакомых людей;
3. **Гнев.** Использование троллинга с целью выражения враждебности группе лиц или какой-то точке зрения (как правило, «переход на личности»);
4. **Трата времени других людей** – это одна из самых желаемых целей троллинга — заключается в том, чтобы другие люди бессмысленно потратили еще больше времени и сил, чем сам «тролль»;
5. **Самоутверждение.** Преодоление комплекса неполноценности или беспомощности путём получения опыта управления окружающей средой, пускай даже виртуальной.
6. **Медиа-война.** Данный вид троллинга чаще всего относят к теме политики и религии, где человек может выдавать себя за неправильно понятого политического комментатора.

Если при обсуждении не удается достигнуть желаемого результата («затроллить»), то троллинг может перейти в более резкую форму спора – флейминг.

Флейминг (от англ. flame — огонь, пламя) *— «спор ради спора», процесс обмена агрессивными сообщениями в местах многопользовательского сетевого общения (чаты, Интернет-форумы, социальные сети и др.).*

Данное явление представляет собой словесную войну, которая зачастую не имеет отношения к первоначальной причине дискуссии, спора. Иногда применяется в контексте троллинга, но чаще всего флейм вспыхивает из-за недоразумения, обиды на виртуального собеседника



Лицо, занимающееся флеймингом (флеймер) ценит вседозволенность и безнаказанность, которыми характеризуется общение в Интернете. При флейминге выбор между логическими доводами/аргументами и оскорблением делается в пользу последнего.

Можно выделить следующие виды флейминга в Интернет-коммуникации:

1. Прозрачные намеки, двусмысленные шутки.

2. Грубые высказывания в адрес собеседника и неаргументированная критика:

3. Каламбуризация и абсурдизация высказывания.

4. Претензии личного характера, критика умственных способностей собеседника.

Ярких различий между троллингом и флеймингом, на первый взгляд, не наблюдается. Однако, отношение участников Интернет-коммуникациик этим двум явлениям абсолютно разное.

Троллинг преследует идею словесного издевательства над окружающими, наслаждения от этого процесса(а порой и откровенного «словесного садизма»).

Флейминг возникает, когда в дискуссии человек прибегает к использованию ненормативной лексики и оскорбительных изречений.

Троллинг может переходить во флейминг в случае, если все аргументы исчерпаны, но индивид хочет показать свое превосходство любыми методами.

КАК БОРОТЬСЯ С ТРОЛЛЯМИ?

До сих пор в Интернете не существует действенных способов борьбы с участниками коммуникации, занимающимися троллингом и флеймингом.

Превентивные действия ограничиваются:

- удалением сообщений,
- словесным предупреждением,
- включением в «бан-лист» (список заблокированных пользователей) на различный срок.

Заставить таких индивидов отвечать за свои действия в Интернете затруднительно.

КАК БОРОТЬСЯ С ТРОЛЛЯМИ?

Защита от троллей

ЛУЧШЕЙ ЗАЩИТОЙ ОТ ТРОЛЛИНГА ЯВЛЯЕТСЯ ИГНОРИРОВАНИЕ !

Поведение тролля является аналогом «энергетического вампиризма». Лучший метод борьбы с троллями — это игнорировать их и удалять их комментарии.

Среди пользователей Интернет принято отвечать сообщениями «*Толсто!*» или «*троль детектед*», а также размещать картинки с изображением тролля или картинки с *troll spray* («очищающая» пространство от троллей).

Тролль наслаждается процессом, а не результатом. Делает это он потому, что ругань и несдерживаемые потоки эмоций являются его «пищей».

В интернет-культуре часто употребляется фраза:

«Не кормите троллей»

(«*Do not feed the troll*»)

Коммуникационные

Интернет-риски

Травля средствами Интернет

Коммуникационные Интернет-риски

Агрессия в Интернете: **кибербуллинг**

Под **буллингом** обычно понимается запугивание, унижение, травля, физический или психологический террор, направленный на то, чтобы вызвать у другого страх и тем самым подчинить человека себе. Во все времена это была одна из серьезных проблем подростковой среды.

Развитие инфокоммуникационных технологий привело к распространению **кибербуллинга.**

КИБЕРБУЛЛИНГ – это вид травли с применением интернет-технологий, включающий оскорбления, угрозы, клевету, компромат и шантаж, с использованием личных сообщений или общественного канала.

Если при обычном буллинге используются вербальные и физические акты насилия, в том числе и психологического, то для кибербуллинга нет необходимости личного присутствия. Все действия совершаются с использованием сообщений электронной почты, сообщений в меседжерах и соцсетях, а также посредством выкладывания фото и видео-материалов, содержащих губительную для репутации жертвы информацию, в общественную сеть.

Коммуникационные Интернет-риски

Агрессия в Интернете: **кибербуллинг**

Кибербуллинг в социальных сетях и на других ресурсах осуществляется регулярно и довольно длительное время.

Единичные случаи конфликтов и оскорблений не могут расцениваться, как кибербуллинг.

Проявления могут включать оскорбления в комментариях, личных сообщениях и публичных беседах. Домогательства интимного, материального или любого другого характера могут исходить от реального ближайшего окружения, а также от совершенно незнакомых людей, случайно заметивших профиль жертвы.

Подобному террору характерна настойчивость, вмешательство в личное время, особенно по ночам и наличие угроз. Для того чтобы скомпрометировать человека могут создаваться страницы, копирующие его личную информацию, для дальнейшего оскорбления (например, учителей, родителей или друзей) якобы от его лица.

С этой же целью может подбираться пароль к реальной странице человека.

Коммуникационные Интернет-риски

Агрессия в Интернете: **кибербуллинг**

Жертвы кибербуллинга обычно более уязвимы, чем те, кто подвергается непосредственным нападкам (буллингу).

Это объяснимо самими особенностями травли в интернет-пространстве, происходящей постоянно.

Нет защиты в виде прекращения учебного дня – в личную жизнь могут вмешиваться постоянно, в любое время суток и по всевозможным источникам.

Конечно, с одной стороны, агрессора можно заблокировать, добавить в черный список, однако это не дает гарантии, что человек не станет использовать другой аккаунт или другую сеть общения. Спрятаться дома не получится, точно так же, как и попросить защиты у старших или руководящих – регламент общения онлайн не подразумевает вмешательства других людей.

Коммуникационные Интернет-риски

Агрессия в Интернете: **кибербуллинг**

Жертвы кибербуллинга обычно более уязвимы, чем те, кто подвергается непосредственным нападкам (буллингу).

Еще одна особенность, делающая кибербуллинг более мощным оружием, чем нападки в реальной жизни – это скорость распространения информации.

В интернете информация распространяется в секунды, и компрометирующее видео может быть просмотрено всеми общими знакомыми и сотней посторонних людей в течение десяти минут после съемки. Кроме того ширина задействованной аудитории при использовании не личных сообщений достигает колоссальных размеров. Все файлы хранятся в сети и могут быть вновь подняты даже после того, как первая волна улеглась. Удалить полностью информацию, попавшую в сеть практически невозможно и требует больших затрат, как времени, так и сил. Кроме этой сложности противостоять кибератакам мешает возможность анонимности.

В большинстве случаев для травли создаются искусственные страницы и адреса, человек не выдает своей личности и продолжает нервировать жертву, не раскрывая своей личности.

Жертвы кибербуллинга могут впадать в состояние страха, достигающего параноидального из-за незнания личности преследователя.

Коммуникационные Интернет-риски

Агрессия в Интернете: **кибербуллинг**

Подвергаются такому нападению те, кто является жертвой и в реальной жизни. Чтобы человек ни разу не подвергся издевательству в школе, но страдал от атак в интернете, не бывает.

Категория риска – подростки, для которых крайне важна оценка окружающих и собственная внешняя презентация в мире. Это повышает чувствительность к любым высказывания, начиная от характеристик личности и ума и заканчивая комментариями аватарки.

В интернете также возможна социальная изоляция, являющаяся одним из вариантов буллинга, только проявляется она исключением из игровых и профессиональных сообществ или в ограничении доступа и прав в них.

Но помимо пассивных форм в виде игнорирования существуют и активные жестокие варианты, способные довести человека до психического расстройства – прямые угрозы физического насилия, избиения или угрозы смерти.

Они могут распространяться не только на саму жертву, но также и на ее близких.

Коммуникационные Интернет-риски

Виды кибербуллинга

Кибербуллинг включает целый спектр форм поведения, на минимальном полюсе которого — шутки, которые не воспринимаются всерьез, на радикальном же — психологический виртуальный террор, который наносит непоправимый вред, приводит к суицидам и смерти.

буллицид — гибели жертвы вследствие буллинга.

Американские исследователи выделили основные типы кибербуллинга:

- Перепалки, или флейминг

- Нападки, постоянные изнурительные атаки (harassment)

- Клевета (denigration)

- Самозванство, перевоплощение в определенное лицо (impersonation)

- Надувательство, выманивание конфиденциальной информации и ее распространение (outing & trickery)

- Отчуждение (остракизм, изоляция).

- Киберпреследование

- Хеппислепинг (Happy Slapping — счастливое хлопанье, радостное избиение)

- Хейтинг (hate)

- Грифинг (griefers)

- Секстинг (sexting)

Коммуникационные Интернет-риски

Агрессия в Интернете: **кибербуллинг**

Чем отличается кибербуллинг от реального?

Различия кибербуллинга от традиционного реального обусловлены особенностями интернет-среды:

- анонимностью;

- возможностью фальсификации;

- наличием огромной аудитории;

- возможностью воздействовать на жертву в любом месте и в любое время.

Коммуникационные Интернет-риски

Агрессия в Интернете: **кибербуллинг**

Серьезность кибербуллинга

Кибербуллинг на первый взгляд может показаться менее серьезным явлением, чем реальная агрессия.

Но последствия кибербуллинга бывают очень тяжелыми, в их список могут входить не только негативные эмоции (стыд, страх, тревога), но и суицидальные попытки и завершенные суициды.

Еще одна сложность — отсутствие обратной связи. В эпизодах «очного» буллинга агрессор видит уязвимость жертвы и может в какой-то момент остановиться, не доводить до самоубийства и других разрушительных последствий. А в интернете не видно, что происходит с другой стороны, и агрессор не знает, когда нужно вовремя прекратить.

Поэтому агрессия онлайн может быть чрезмерной и более опасной.

Коммуникационные Интернет-риски

Коммуникационная компетентность — это не только знание и умение разрешать ситуации, возникающие при столкновении с перечисленными выше Интернет - рисками, но также способность и готовность эффективно использовать весь спектр коммуникативных возможностей, предоставляемых Интернетом.

Интернет изменил процессы коммуникации, сделав ее непрерывной, безграничной, доступной и персональной.

Интернет-сервисы для коммуникации складываются в единое коммуникативное пространство, управляя которым цифровые граждане могут общаться с кем угодно и где угодно, презентовать себя, создавать и развивать свой социальный капитал, обучаться и расширять свои возможности.