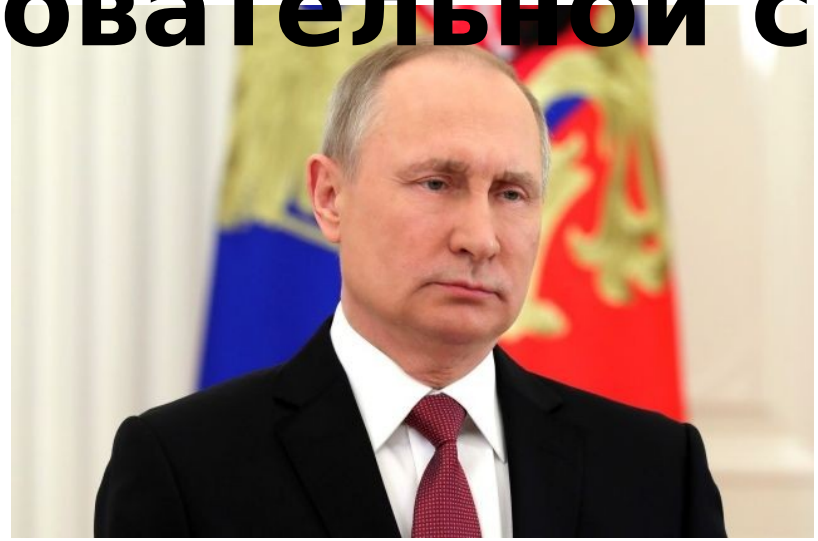
Информационная безопасность образовательной среды



Необходимым условием решения стоящих перед страной задач является надежная безопасность России…

В.В.Путин

(Из Послания Федеральному Собранию РФ)

Доктрина информационной безопасности Российской Федерации представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

Доктрина информационной безопасности РФ

Понятие «Безопасность»

отсутствие какого-либо риска, в случае реализации которого возникают негативные последствия (внутренних и внешних угроз) в отношении кого-либо или чего-либо.

Безопасность образовательной среды

состояние защищенности информационного пространства образовательной среды от внешних и внутренних угроз при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан…

Безопасность образовательного учреждения (ОУ)

это условия сохранения жизни и здоровья обучающихся, воспитанников и работников, а также материальных ценностей образовательного учреждения от возможных несчастных случаев, пожаров, аварий и других чрезвычайных ситуаций;

это система мер, принятых администрацией учреждения и государством, для защиты детей и имущества от внутренних и внешних угроз с учетом фактического состояния, технического состояния ОУ, условий организации учебно-воспитательного процесса, криминальной и техногенной обстановки, природной территории, предупреждения, пресечения и ликвидации последствий террористических акций.

Информационная безопасность

Раньше…– защита информации, в первую очередь, защита государственной тайны, криптография (наука о методах обеспечения конфиденциальности, или «тайнопись») и компьютерная безопасность

Теперь…–добавляется «защита от информации» и «аналитическое обеспечение информационной безопасности»

Основой организации обеспечения безопасности образовательной среды является анализ реальных и потенциальных внешних и внутренних угроз, кризисных ситуаций, а также прочих неблагоприятных факторов

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 № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" **).**

Социологические исследования

95% детей России посещают интернет ресурсы ежедневно, причем размер населенного пункта практически не влияет на процент активных пользователей.

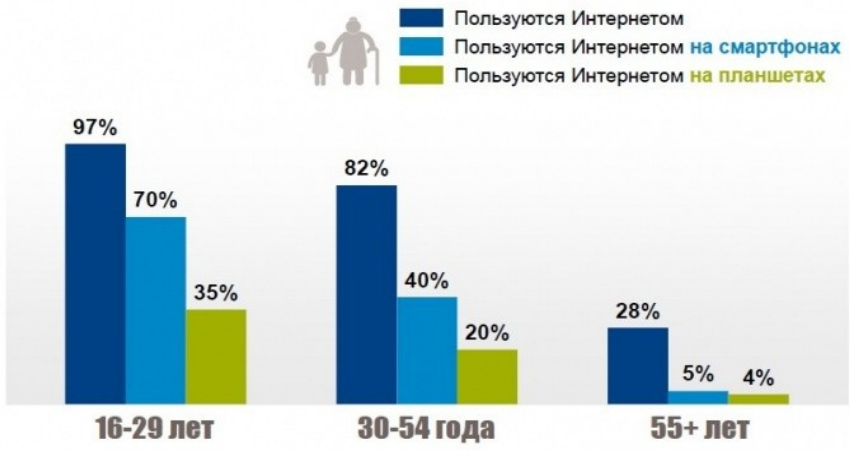
Неожиданное открытие, сделанное учеными: подавляющее большинство детей в Интернете не интересуется порнографией, насилием и наркотиками.

На первый план среди всех интернет-угроз сегодня выходят такие проблемы, как формирование потребительского отношения к жизни и кибер-преследование, когда подростки сводят друг с другом счеты с помощью современных технологий (компрометирующие видеоролики, «фэйковые» странички в соцсетях и на сайтах знакомств, «фотожабы», публичные оскорбления, коллективные бойкоты и т.д.)

Актуальность обеспечения медиабезопасности детей и подростков

Проблема обеспечения информационной безопасности детей в сети Интернет становится все более актуальной в связи с существенным возрастанием численности несовершеннолетних пользователей.

За последние годы в результате значительного повышения обеспеченности компьютерами россиян и подключения в рамках национального проекта практически всех школ к Интернету пользовательская активность российских школьников резко возросла. *Данные исследований Фонда Развития Интернет свидетельствуют о высокой степени контакта детей и подростков с негативным контентом и другими рисками интернет-среды.*



Помимо звонков и коротких сообщений телефоны используются для выхода в интернет, загрузки изображений, музыки, видео, игр.

При этом несовершеннолетние меньше, чем взрослые, подготовлены к проблемам, с которыми могут столкнуться в сети, и нередко остаются беззащитными перед ними. Именно дети и подростки сегодня менее всего защищены от потока негативной информации в Сети.

ВИДЫ ОН-ЛАЙН УГРОЗ, ПРЕДСТАВЛЯЮЩИХ ОПАСНОСТЬ ДЛЯ ЖИЗНИ, ФИЗИЧЕСКОГО, ПСИХИЧЕСКОГО И НРАВСТВЕННОГО ЗДОРОВЬЯ И ПОЛНОЦЕННОГО РАЗВИТИЯ РЕБЕНКА

1. Обилие откровенных материалов сексуального характера.

Многочисленные видеоролики и снимки могут дезориентировать ребенка, ранить его психику, вызвать нарушения психосэксуального и нравственно-духовного развития, воспрепятствовать построению нормальных социальных, в том числе межполовых и семейных отношений в будущем.

2. Виртуальные знакомые *и друзья*.

Кроме своих сверстников и интересных личностей, общение с которыми пойдет на пользу, ребенок может завязать знакомство не только с педофилом и извращенцем, но и с мошенником и хулиганом. Виртуальное хамство и розыгрыши часто заканчиваются киберпреследованием и кибернижением, доставляя объекту травли множество страданий. Для ребенка такие переживания могут оказаться критичными, поскольку он более раним, чем взрослые люди.

ВИДЫ ОН-ЛАЙН УГРОЗ, ПРЕДСТАВЛЯЮЩИХ ОПАСНОСТЬ ДЛЯ ЖИЗНИ, ФИЗИЧЕСКОГО, ПСИХИЧЕСКОГО И НРАВСТВЕННОГО ЗДОРОВЬЯ И ПОЛНОЦЕННОГО РАЗВИТИЯ РЕБЕНКА

В последние годы получили распространение такие общественно опасные посягательства на личность несовершеннолетнего в сети, как ***кибербуллинг*** – подростковый виртуальный террор, получил свое название от английского слова bull — бык, с родственными значениями: агрессивно нападать, бередить, задирать, придираться, провоцировать, донимать, терроризировать, травить.

Кибербуллинг — это травля, оскорбления или угрозы, высказываемые жертве с помощью средств электронной коммуникации, в частности, сообщений в социальных сетях, мгновенных сообщений, электронных писем и СМС. С каждый годом стремительно увеличивается количество трагедий, к которым приводит кибербуллинг.

Наиболее опасными видом кибербуллинга считаются ***киберпреследование*** — скрытое выслеживание жертвы с целью организации нападения, избиения, изнасилования и т.д.

Для безопасности несовершеннолетнего особую угрозу представляют личные встречи с виртуальными знакомыми в реальной жизни, о которых родители могут ничего не знать. Ребенку необходимо объяснить правила безопасного общения в сети

ВИДЫ ОН-ЛАЙН УГРОЗ, ПРЕДСТАВЛЯЮЩИХ ОПАСНОСТЬ ДЛЯ ЖИЗНИ, ФИЗИЧЕСКОГО, ПСИХИЧЕСКОГО И НРАВСТВЕННОГО ЗДОРОВЬЯ И ПОЛНОЦЕННОГО РАЗВИТИЯ РЕБЕНКА

3. Опасная для детей информация, способная причинить серьезный вред их здоровью, развитию и безопасности может содержаться на электронных ресурсах, содержащих материалы экстремистского и террористического характера.

Федеральным законом от 25.07.2002 № 114-ФЗ "О противодействии экстремистской деятельности запрещены возбуждение социальной, расовой, национальной или религиозной розни; пропаганда исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии; пропаганда и публичное демонстрирование нацистской атрибутики или символики либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения; публичные призывы к осуществлению указанных деяний либо массовое распространение заведомо экстремистских материалов, а равно их изготовление или хранение в целях массового распространения.

В случаях, предусмотренных законодательством Российской Федерации, производство, хранение или распространение экстремистских материалов является правонарушением и влечет за собой ответственность (ст. 12, 13 Федерального закона от 25.07.2002 № 114-ФЗ "О противодействии экстремистской деятельности").

ВИДЫ ОН-ЛАЙН УГРОЗ, ПРЕДСТАВЛЯЮЩИХ ОПАСНОСТЬ ДЛЯ ЖИЗНИ, ФИЗИЧЕСКОГО, ПСИХИЧЕСКОГО И НРАВСТВЕННОГО ЗДОРОВЬЯ И ПОЛНОЦЕННОГО РАЗВИТИЯ РЕБЕНКА

Даже случайный клик по всплывшему баннеру или переход по ссылке может привести на сайт с опасным содержимым!

4. Особую опасность представляют для незрелой психики несовершеннолетних электронные ресурсы, созданные и поддерживаемые деструктивными религиозными сектами.

Главная проблема деструктивных сект в сети – это предоставление ложной информации. Попасть под негативное влияние секты через сайт очень легко – если ребенок читает в сети соответствующий материал, смотрит видео и фото-информацию, то он уже вступает во взаимодействие с вербовщиком секты, невольно участвует в психологической игре организаторов секты, нередко попадая от них в зависимость.

Вовлечение малолетних в религиозные объединения, а также обучение малолетних религии вопреки их воле и без согласия их родителей или лиц, их заменяющих, запрещены (ст. 5 Федерального закона от 26.09.1997 № 125-ФЗ "О свободе совести и о религиозных объединениях"). Запрещается также создание и деятельность религиозных объединений, цели и действия которых противоречат закону (ст. 6 указанного Федерального закона).

ВИДЫ ОН-ЛАЙН УГРОЗ, ПРЕДСТАВЛЯЮЩИХ ОПАСНОСТЬ ДЛЯ ЖИЗНИ, ФИЗИЧЕСКОГО, ПСИХИЧЕСКОГО И НРАВСТВЕННОГО ЗДОРОВЬЯ И ПОЛНОЦЕННОГО РАЗВИТИЯ РЕБЕНКА

5. Доверчивость и наивность детей нередко используют в своих целях компьютерные мошенники, спамеры, фишеры.

Несовершеннолетние нередко переходят по присланным им злоумышленниками ссылкам без подозрений, скачивают неизвестные файлы, которые могут оказаться вирусами или содержать незаконную информацию.

Недостаточно информированный об опасностях в сети ребенок может сообщить злоумышленнику номер кредитной карточки родителей, пароль от электронного кошелька, свой настоящий адрес и многое другое.

Несовершеннолетнего пользователя взрослые преступники могут с использованием электронных ресурсов втянуть *в совершение антиобщественных, противоправных, в том числе уголовно-наказуемых деяний*. При этом следует иметь в виду, что привлечение к уголовной ответственности взрослого лица за вовлечение несовершеннолетнего в совершение преступления не исключает уголовной ответственности и самого подростка в случаях, когда он достиг установленного уголовным законом возраста.

RG.RU Специальный редакционный проект

СПАМ KASPERSKY lab

Доля спама в интернет-трафике РФ в 2018 году превысила мировой уровень.

В российском трафике доля спама в 2018 году составила 53 процента. Во всем мире - около 50 процентов. За спам-сообщениями может скрываться не только назойливая реклама, но и мошеннические рассылки, вредоносное программное обеспечение.

По словам специалистов ЛК, в 2018 году предотвратили свыше 89 миллионов попыток перехода пользователей на фишинговые сайты. Среди типов организаций, чьи пользователи были атакованы фишерами, наиболее часто встречались банки, платежные системы, глобальные интернет-порталы и социальные сети.

ВИДЫ ОН-ЛАЙН УГРОЗ, ПРЕДСТАВЛЯЮЩИХ ОПАСНОСТЬ ДЛЯ ЖИЗНИ, ФИЗИЧЕСКОГО, ПСИХИЧЕСКОГО И НРАВСТВЕННОГО ЗДОРОВЬЯ И ПОЛНОЦЕННОГО РАЗВИТИЯ РЕБЕНКА

Фи́шинг — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом.

После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

ВИДЫ ОН-ЛАЙН УГРОЗ, ПРЕДСТАВЛЯЮЩИХ ОПАСНОСТЬ ДЛЯ ЖИЗНИ, ФИЗИЧЕСКОГО, ПСИХИЧЕСКОГО И НРАВСТВЕННОГО ЗДОРОВЬЯ И ПОЛНОЦЕННОГО РАЗВИТИЯ РЕБЕНКА

6. Пропаганда наркотиков, насилия и жестокости, суицидального поведения, абортов, самоповреждений может быть весьма опасной для неокрепшей детской психики. СНИФФИНГ

Ребенок на веру принимает многие сомнительные идеи, особенно если они грамотно изложены. Например, о том, как лучше покончить с собой или от приема каких таблеток «станет веселее», как без обращения ко врачу избавиться от нежеланной беременности и т.д. Этим пользуется немало людей, использующих детей в корыстных и иных личных целях. Согласно Конвенции ООН о правах ребенка такие действия есть не что иное, как *криминальная, в том числе коммерческая эксплуатация ребенка*.

Результатом пропаганды агрессии, насилия и жестокости становятся омоложение и феминизация контингента несовершеннолетних правонарушителей:

- **в 2018 году выявлено более 38 тыс. правонарушителей, не достигших 18 летнего возраста;**
- **за последние 4 года доля несовершеннолетних девочек, помещенных в Центры временного содержания несовершеннолетних правонарушителей, возросла с 18,5% до 20,4%, а состоящих на учете в ПДН – с 19,9 до 23%;**
- **в контингенте несовершеннолетних преступников доля девочек за последние 5 лет возросла с 17,9% до 23,0%.**

ПОРТАЛ ПРАВОВОЙ СТАТИСТИКИ

ВИДЫ ОН-ЛАЙН УГРОЗ, ПРЕДСТАВЛЯЮЩИХ ОПАСНОСТЬ ДЛЯ ЖИЗНИ, ФИЗИЧЕСКОГО, ПСИХИЧЕСКОГО И НРАВСТВЕННОГО ЗДОРОВЬЯ И ПОЛНОЦЕННОГО РАЗВИТИЯ РЕБЕНКА

7. Помимо указанной выше информации в Сети есть немало сомнительных развлечений, таких как онлайн-игры, пропагандирующие секс, жестокость и насилие, требующие немалых финансовых вложений. Дети бывают вовлечены в азартные игры в сети.

В соответствии с п. 3 ст. 14 Закона «Об основных гарантиях прав ребенка» в целях обеспечения безопасности жизни, охраны здоровья, нравственности ребенка, защиты его от негативных воздействий предусмотрено проведение экспертизы (социальной, психологической, педагогической, санитарной) предназначенных для детей: настольных, компьютерных и иных игр, игрушек и и игровых сооружений.

	**Bad Language - Ненормативная лексика** **Игра содержит грубые и непристойные выражения.**
	**Discrimination - Дискриминация** **Присутствие в продукте сцен или материалов, которые могут порочить или дискриминировать некоторые социальные группы.**
	**Fear - Страх:** **Материалы игры могут оказаться страшными и пугающими для маленьких детей.**
	**Gambling - Азартные игры** **В игре есть возможность сыграть в азартные игры и сделать ставку, в том числе — реальными деньгами.**
	**Sexual Content – Непристойности** **В игре присутствует обнажение и/или встречаются сцены с сексуальными отношениями.**
	**Violence - Насилие** **Игра изобилует сценами с применением насилия.**

ВИДЫ ОН-ЛАЙН УГРОЗ, ПРЕДСТАВЛЯЮЩИХ ОПАСНОСТЬ ДЛЯ ЖИЗНИ, ФИЗИЧЕСКОГО, ПСИХИЧЕСКОГО И НРАВСТВЕННОГО ЗДОРОВЬЯ И ПОЛНОЦЕННОГО РАЗВИТИЯ РЕБЕНКА

8. Психологами отмечается распространенность в среде пользователей, в том числе несовершеннолетних, случаев болезненного пристрастия к участию в сетевых процессах, так называемой "Интернет-зависимости", (навязчивое желании неограниченно долго продолжать сетевое общение. Интернет-зависимыми сегодня являются около 10 % пользователей во всём мире.

Выделяется 5 основных типов интернет-зависимости:

1. **Навязчивый веб-серфинг** — бесконечные путешествия по Всемирной паутине, поиск информации.
2. **Пристрастие к виртуальному общению и виртуальным знакомствам** — большие объёмы переписки, постоянное участие в чатах, веб-форумах, избыточность знакомых и друзей в Сети.
3. **Игровая зависимость** — навязчивое увлечение компьютерными играми по сети.
4. **Навязчивая финансовая потребность** — игра по сети в азартные игры, ненужные покупки в интернет-магазинах или постоянные участия в интернет-аукционах.
5. **Пристрастие к просмотру фильмов через интернет**, когда больной может провести перед экраном весь день не отрываясь из-за того, что в сети можно посмотреть практически любой фильм или передачу.

О ***клиническом феномене зависимости от игр и ПК*** (***лудомания, игромания, гэмблинг***) говорят с конца 1980-х годов, сначала за рубежом, теперь, по мере продвижения информационных технологий, и в России.