Тема: **Информационная безопасность. Уголовная ответственность в информационной сфере.**

Слайд2

Интернет является прекрасным источником для новых знаний, помогает в учебе, занимает досуг. Через интернет мы заказываем нужные нам товары, делаем покупки, проводим оплату разного рода услуг(жкх, кредиты и т.д.) Но в то же время, в сети Интернета таится много опасностей и много соблазна. (Запретный плод всегда сладок). Первая часть моего выступления озвучила как ***информационная безопасность.***

Слайд3

Информационная безопасность детей это состояние защищенности детей, при котором отсутствует риск, связанный с причинением вреда их здоровью, физическому, психическому, духовному и нравственному развитию.

Слайд4

Хочу напомнить, что в РФ **существует** ***Федеральный закон № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»*** Устанавливает правила медиа безопасности детей при обороте на территории России продукции средств массовой информации, размещаемой в информационно-телекоммуникационных сетях и сетях подвижной радиотелефонной связи.

Но при наличии закона все мы прекрасно знаем о том, что угроз, сопровождающих интернет меньше не становится

Слайд5

Угрозы, подстерегающие ребенка в Глобальной сети .

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

6.Порнография

7. Депрессивные молодежные течения. Ребенок может поверить, что шрамы – лучшее украшение, а суицид – всего лишь способ избавления от проблем. Все помнят сколько горя принес родителям нашумевший «Синий кит» депрессивное молодежное течение, где организаторами раздавались задание приводившие детей к суицидальным действиям.

8.Наркотики. Интернет пестрит новостями о “пользе” их употребления, рецептами и советами изготовления разного вида ПАВ(психоактивных веществ) и подробно рассказывают как пользоваться любыми видами одурманивающих средств. А самое опасное, что через интернет их может приобрести любой желающий.

9.Сайты знакомств, социальные сети, блоги и чаты. Казалось бы, что здесь может представлять опасность? К сожалению уже было много случаев, когда педофилы выдавали себя за одного из подростков или выдумывали несуществующих людей, чтобы войти в доверие к ребенку и завести пошлые или открыто сексуальные беседы с ними, с просьбой выслать фотографии интимного характера или даже договориться о личной встрече.

10.Секты Виртуальный собеседник не схватит за руку, но ему вполне по силам “проникнуть в мысли” и изменить ваш взгляды на мир.

11.Экстремизм, национализм, фашизм. Все широкие возможности Интернета используются представителями экстремистских течений для того, чтобы заманить в свои ряды новичков.

Слайд.12

Общие правила безопасности при работе в Интернете

Ребенок должен понять, что его виртуальный собеседник может выдавать себя за другого. Отсутствием возможности видеть и слышать других пользователей легко воспользоваться. И 10-летний друг Вашего ребенка по чату в реальности может оказаться злоумышленником.

Оградите ребенка от ненадлежащего веб-содержимого. Не следует открывать письма электронной почты, файлы или Web-страницы, полученные от людей, которые не знакомы или не внушают доверия.

Не разрешайте ребенку предоставлять личную информацию через Интернет Ребенку нужно знать, что нельзя через Интернет давать сведения о своем имени, возрасте, номере телефона, номере школы или домашнем адресе, и т.д. Убедитесь, что у него нет доступа к номеру кредитной карты или банковским данным. Научите ребенка использовать прозвища (ники) при общении через Интернет: анонимность - отличный способ защиты. Не выкладывайте фотографии ребенка на веб-страницах или публичных форумах.

Теперь я хочу перейти ко второй части выступления: **Уголовная ответственность в информационной сфере.**

Слайд 13

Здесь работают такие законы как : ФЕДЕРАЛЬНЫЙ ЗАКОН № 149 об ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ

Федеральный закон РФ № **152-ФЗ «О персональных данных»** вступил в силу 26.01.2007. Этот документ определяет требования по работе с **персональными данными** российских граждан, обеспечивает **защиту** их интересов и надлежащий уровень **защиты**. Собирать, обрабатывать и хранить **персональные данные** людей можно (за некоторыми исключениями) **только с их согласия**. Каждый из вас как законный представитель при поступлении в школу дает или не дает согласия на обработку персональных данных своего ребенка.

Часть 1 статьи 137 **Уголовного** кодекса Российской Федерации предусматривает **ответственность за** незаконное собирание или распространение сведений о частной жизни лица, составляющих его **личную** или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении или в средствах массовой информации.

Фейк -Говоря простыми словами, фейк (от английского fake – обман, имитация, фальсификация,подделка, фальшивка) – это то, чего в действительности не существует.

За фейки о ВС РФ могут назначить штраф в размере от 700 тысяч до 1,5 миллиона рублей, исправительные или принудительные работы, наказание в виде лишения свободы на срок до 3 лет. Согласно статье 207.3 УК РФ, если распространение фейка привело к тяжким последствиям, лицо могут осудить на срок от 10 до 15 лет с лишением права занимать определенные должности и заниматься определенной деятельностью на срок до 5 лет.

Президентом внесено дополнение в «Закон о фейках» «Закон о военной цензуре». И здесь надо понимать, что даже поставив лайк под данным видео или фото, связанных с нынешней операцией на Украине или переслав его другим ваш, ребенок не осознавая становится ее распространителем.

Слайд 14

Буллинг — это травля, агрессивное преследование одного человека другим (другими).

Кибербуллинг

- любое унизительное, оскорбительное или угрожающее сообщение, отправленое в эл.форме.
- унизительные фотографии или видео, опублекованные в соц.сетях без вашего согласия
- поддельные профили в соц. сетях или веб-сайты, созданные с целью опорочить жертву.
- Порочащие вас высказывания в соц. сетях и интернете.

Мы доводим до наших учеников, что когда они выставляют фотографии своих одноклассников или знакомых в социальных сетях без их согласия, то это может повлечь за собой административное наказание. И хотели бы чтобы вы со своей стороны тоже говорили об этом со своими детьми.

Мы все родители и наши дети для нас всегда остаются детьми и мы часто не замечаем, когда они достигают возраста после которого наступает уже не административная, а уголовная ответственность. Если еще в 13 лет совершенный им поступок можно рассматривать как оплошность, то в 14 лет за этим может последовать серьезное наказание.

Слайд 15

Неполный перечень преступлений, за которые наступает ответственность с 14 лет является

- убийство (ст. 105 УК РФ)
- умышленное причинение тяжкого вреда здоровью (ст. 111 УК РФ),
- похищение человека (ст. 126 УК РФ),
- изнасилование (ст. 131 УК РФ),
- насильственные действия сексуального характера (ст. 132 УК РФ),
- кража (ст. 158 УК РФ),
- грабеж (ст. 161 УК РФ),
- разбой (162 УК РФ),
- вымогательство (ст. 163 УК РФ)
- угон (ст. 166 УК РФ)

Советы по защите детей в интернете

1.Установите родительский контроль и интернет-фильтры. Они разработаны специально для того, чтобы помочь вам защитить детей в Сети.

Программы-фильтры

Power Spy 2008

Программу удобно использовать, чтобы узнать, чем заняты дети в отсутствие родителей.

Программы-фильтры

iProtectYou Pro

Программа-фильтр интернета,
позволяет родителям ограничивать по разным параметрам сайты,
просматриваемые детьми.

Программы-фильтры

KidsControl

Предназначение KidsControl – контроль времени, которое ребенок проводит в интернете.

Программы-фильтры

CYBERSitter

дает взрослым возможность ограничивать доступ детей к нежелательным ресурсам в Internet.

Программы-фильтры

КиберМама 1.0b

КиберМама проследит за временем работы, предупредит ребенка о том, что скоро ему нужно будет отдохнуть и приостановит работу компьютера, когда заданное вами время истечет.

КиберМама поддерживает следующие возможности:

- Ограничение по суммарному времени работы
- Поддержка перерывов в работе
- Поддержка разрешенных интервалов работы
- Возможность запрета интернета
- Возможность запрета игр/программ

2.Убедитесь, что на устройстве ребенка установлены последние версии антивирусов и программного обеспечения. Антивирусные программы защищают устройства от внешних атак, находят и уничтожают потенциальные угрозы для системы и предупреждают о них. Новые вирусы появляются постоянно, и разработчики регулярно улучшают антивирусы, чтобы они оставались эффективными.

3.Следите за списками друзей ваших детей и блокируйте любые нежелательные или подозрительные контакты.

4.Отключите возможность совершать покупки из приложений, если устройства позволяют это сделать.

5.Сами будьте примером для подражания. Хвалите ребенка за дружелюбное и уважительное отношение к окружающим. Кроме того, обращайте его внимание на то, что может попасть в кадр на заднем плане.

6. Помогите своим детям понять, что они не должны размещать в Сети информацию о себе: номер мобильного телефона, домашний адрес, номер школы, а также помните, что когда вы выкладываете фотографии (свои и семьи) их могут использовать не в ваших интересах.

7.Проследите за тем, чтобы нельзя было определить местоположение ребенка. Попросите детей не добавлять GPS (джи пи ес)-координаты (геометки) к фотографиям

Помните, что безопасность ваших детей в **Интернете**, на **90%** зависит от вас.

Спасибо за внимание!