Государственное бюджетное учреждение культуры
Ставропольского края
«Ставропольская краевая детская библиотека им. А.Е. Екимцева»

Информационная безопасность детей: технологии и рекомендации

Информационный сборник по итогам краевой конференции

19 октября 2023 года

Информационная безопасность детей: технологии и рекомендации. Информационный сборник по итогам краевой конференции 19 октября 2023 года / ГБУК «СКДБ им. А. Е. Екимцева», НМО. – Ставрополь, 2024. – 51 с. – Текст: электронный.

В пособии представлена информация о путях формирования информационной культуры и информационной безопасности детей и подростков в библиотеках края согласно утвержденной Распоряжением правительства от 28 апреля 2023 г. № 1105-р Концепции информационной безопасности детей, заменившей аналогичный документ от 2015 года. В приложениях к сборнику представлен сценарный материал для проведения разноплановых мероприятий для младшего, среднего и старшего школьного возраста.

Оглавление

Формирование культуры информационной безопасности детей в библиотеках Ставропольского края: технологии и рекомендации

Кононова Ирина Геннадьевна, директор краевой детской библиотеки им. А.Е. Екимцева

Распоряжением правительства от 28 апреля 2023 г. № 1105-р утверждена концепция информационной безопасности детей, заменившая аналогичный документ от 2015 года.

Главная цель концепции – защитить детей от информационных угроз и рисков в современной цифровой среде.

В настоящее время несовершеннолетних жителей России - 30,2 миллиона человек (20,6% населения), в СК детей от 0 до 14 лет – 492027, из них 89,4% являются активными пользователями Интернета.

Современные дети - первое поколение, чье взросление происходит на фоне стремительно развивающихся информационно-коммуникационных технологий. В своих привычках, ценностях и поведении в сети "Интернет" эта группа принципиально отличается от представителей более старшей аудитории (18 - 45 лет). Их основными интересами являются общение в социальных сетях, просмотр видео и онлайн-игры.

Вместе с тем указанная аудитория является крайне уязвимой с точки зрения информационной безопасности.

В интернете дети могут столкнуться с разными опасностями, например, со злоумышленниками, которые под видом сверстников могут расспрашивать о личных данных ребёнка и его семье. Затем эта информация может использоваться для шантажа, угроз или манипуляций, а также для вовлечения детей в деструктивные организации.

В области виртуальной коммуникации дети подвержены рискам стать жертвой компьютерного мошенничества и вымогательства, вовлечения в сексуальную эксплуатацию, террористическую и экстремистскую деятельность, распространение наркотических средств, психотропных веществ, посредством игровых активностей, а также в сообщества с нарушением общепринятых норм морали.

Широкое распространение в цифровой среде получили деструктивные молодежные субкультуры, включая движения, связанные с вооруженным нападением на образовательные организации, популяризацией деятельности криминальных сообществ, продвижением преступных и антиобщественных действий, в том числе агрессивного, насильственного, суицидального, экстремального и экстремистского характера.

Все большее распространение получает задействование сетевых платформ и мессенджеров для вовлечения детей в несогласованные публичные мероприятия (включая протестные акции), поскольку несовершеннолетние не только легче поддаются идеологическому и психологическому воздействию, но и при определенных обстоятельствах не подлежат уголовной ответственности.

Несформированность критического мышления обусловливает особую уязвимость детей перед воздействием такой информации, оказывает на несовершеннолетних психотравмирующее воздействие, способствует вовлечению в деструктивную деятельность, усвоению ими антисоциальных ценностей и норм, неправильному восприятию традиционных российских духовно-нравственных ценностей, провоцирующего «психологический слом», побуждает их к совершению общественно опасных действий, способных причинить вред как самому ребенку, вызвать депрессивное состояние, проявление девиантного поведения, повышенной агрессии к окружающим, так и его окружению.

Причем проблема обеспечения безопасности несовершеннолетних читателей в инфосфере не ограничивается вопросами их защиты в информационно-телекоммуникационной сети Интернет. На основе Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию» **информационная среда** как часть инфраструктуры библиотечного учреждения может быть определена как совокупность следующих компонентов: продукция средств массовой информации, печатная продукция, аудиовизуальная продукция на любых видах носителей, зрелищные мероприятия. Таким образом, с учетом новой концепции необходимо в комплексе рассматривать **все существующие угрозы.**

На основании принятой концепции, в которой существенно изменились приоритеты в целях и задачах, рассмотрим основные моменты **по обеспечению информационной безопасности детей в библиотечном учреждении**, которые необходимо учитывать в работе.

Первое: правовая защита детей, заключающаяся в создании нормативно-правовой базы регулирования отношений читателя и библиотеки в области обеспечения информационной безопасности.

Предполагается усиление контроля за противоправным контентом. При этом нужно понимать, что международное право в сфере защиты прав человека гарантирует ребенку ряд прав, связанных так или иначе с информацией. Этому вопросу посвящены ст. ст. 13-17 Конвенции о правах ребенка. В частности, в п. 1 ст. 13 Конвенции о правах ребёнка указано, что ребенок имеет право свободно выражать свое мнение. Это право состоит из нескольких частей и, помимо прочего, «включает свободу искать, получать и передавать информацию и идеи любого рода, независимо от границ, в устной, письменной или печатной форме, в форме произведений искусства или с помощью других средств по выбору ребенка». Право на доступ к информации является неотъемлемым аспектом свободы выражения мнения, поскольку оно позволяет гражданам иметь адекватное представление и формировать критическое мнение о состоянии общества, в котором они живут. Для этого право на доступ к информации включено в состав права на свободу выражения своего мнения, которое, помимо прочего, включает в себя право на поиск, получение и передачу информации. При этом предполагается, что получение информации возможно из любого источника и в любой форме: устной, письменной, печатной и др.

Таким образом, во всех ограничительных мероприятиях должны быть разумные границы.

Второе: технологическая защита, направленная на создание технических способов блокировки нежелательного контента, ограничения доступа к отрицательной информации, технические возможности осуществления библиотечными специалистами контроля за временем пребывания ребёнка в сети и качественный анализ сайтов и интернет-сообществ, посещаемых несовершеннолетними.

Третье: психолого-педагогические методы, направленные на работу с читателями-детьми по формированию их медиа и компьютерной грамотности, критического мышления по отношению к информации, получаемой в сети, стратегий поведения при встрече с нежелательным интернет-контентом.

Ежегодный анализ работы по созданию безопасной информационной среды в детских и общедоступных библиотеках, работающих с несовершеннолетним населением региона, позволяет построить пошаговый алгоритм действий:

– изучение руководителями библиотечных учреждений и библиотечными специалистами нормативно-правовых основ обеспечения информационной безопасности детей;

– разработка необходимых локальных актов по вопросам информационной безопасности несовершеннолетних читателей в библиотечном учреждении (**Положение** о защите детей от информации, причиняющей вред их здоровью и развитию, **Положение** об ограничении доступа читателей к видам информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей целям и задачам библиотечного учреждения);

– проведение самоаудита и последующее повышение компетентности библиотечных специалистов в решении задач обеспечения информационной безопасности детей и подростков;

– оценка безопасности информационной среды библиотечного учреждения, обслуживающего детского пользователя;

– проведение с читателями и родителями (законными представителями) просветительской работы, нацеленной на повышение культуры информационной безопасности. В концепции особо указывается о существующих возможностях услуги «Родительский контроль». В том числе проводить на постоянной основе **просветительские мероприятия** для родителей и для специалистов, которые связаны с воспитанием, обучением и организацией досуга детей, направленные на информирование **о правилах безопасного пользования** детьми сетью «Интернет», средствах защиты несовершеннолетних от доступа к информации, наносящей вред их здоровью, нравственному и духовному развитию.

Необходимо на постоянной основе **проводить мероприятия, направленные на повышение уровня грамотности** детей по вопросам

информационной безопасности, формирование критической оценки получаемых сведений, на таких уроках ребятам нужно объяснять, например, как распознавать мошенников и как правильно поступать, когда незнакомцы начинают выяснять личные данные ребёнка или спрашивать о его семье.

Ожидается, что в результате реализации концепции у детей:

повысится уровень информационной безопасности и цифровой грамотности детей;

увеличится устойчивый спрос на получение высококачественной информационной продукции;

повысится охват специалистов, работающих с детьми, мероприятиями в области обеспечения безопасности и развития детей в информационном пространстве;

увеличится число родителей (законных представителей), проинформированных о существующих возможностях услуги «Родительский контроль»;

сократится число детей, пострадавших от жестокого обращения и травли, в том числе в сети «Интернет»;

снизится вовлеченность несовершеннолетних в деструктивные группы с использованием сети «Интернет»;

сократится количества информации, причиняющей вред здоровью и (или) развитию детей;

в сети появится больше контента, направленного на формирование у детей традиционных ценностей.

Концепция будет действовать бессрочно и может служить методологической основой разработки комплекса нормативно-правовых и организационно-методических документов, регламентирующих деятельность библиотек в области информационной безопасности детей.

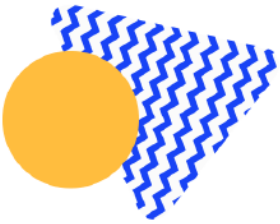
Региональным властям рекомендовано учитывать её положения при формировании перечней региональных мероприятий по обеспечению информационной безопасности детей.

Как научить детей кибербезопасности: образовательные проекты от «Ростелеком»

Шкурдзе Татьяна Сергеевна, пресс-секретарь Ставропольского филиала ПАО «Ростелеком»

Хартия «Цифровая этика детства»

«Ростелеком» как один из учредителей Альянса по защите детей в цифровой среде считает важной подготовку детей к жизни в современных условиях. Для этого необходимо развивать безопасное интернет-пространство, в котором дети, независимо от возраста и места проживания, смогут общаться, учиться, развиваться и открывать для себя новые возможности. Хартия призвана объединить и скоординировать соответствующие усилия представителей общественности, государства и профессионального сообщества.



Присоединиться к хартии:
https://internetforkids.ru/

Кибербезопасность детей – наша общая задача

Исследования

Компания анализирует риски, с которыми сталкиваются дети в интернете и предлагает свои методы защиты в онлайн-среде

Проекты

«Ростелеком» партнер и инициатор всероссийских и региональных проектов, направленных на повышение цифровой грамотности

Материалы

«Ростелеком» разработал пакет методических материалов, которые распространяются бесплатно (брошюры, видеоуроки, фильмы)

Мероприятия

В регионах сотрудники «Ростелекома» постоянно проводят уроки по кибербезопасности и присоединяются к активностям

Издания

В 2021 году при поддержке провайдера издана книга по кибербезопасности, которая распространяется в библиотеках

Ростелеком

Исследование киберрисков

Исследование «Технологии защиты детей в интернете» проводилось с октября 2021 года по март 2022 года. Выводы получены с применением интеллектуальной аналитической системы на основе выборки, включающей более 21 тысяч научных работ. С помощью анализа было выявлено 23 риска, разработана брошюра с рекомендациями.

Скачать исследование
Скачать брошюру

Материалы

«Ростелеком» разработал собственный пакет методических материалов, которые доступны всем желающим

Фильмы

В популярном видеосервисе Wink доступна серия фильмов для детей и взрослых

Лекции

Онлайн-курс для родителей «Как защитить ребенка от рисков в интернете?» с видеоуроками

Викторины

Онлайн-платформа, которая пополняется новыми тестами и опросами

Вебинары

Вебинары с участием экспертов «Ростелеком - Солар» (г. Москва)

Лицей

В онлайн-сервисе содержатся развивающие программы в сфере цифровой грамотности

Практические знания

- Подробно разбираются правила кибергигиены, применение которых сделает пользование интернетом максимально безопасным;
- На реальных примерах разъясняется, как защищать цифровые ценности, как правильно придумывать, менять и запоминать пароли;
- Описана зависимость детей от соцсетей и лайков, а также рассказано о пользе пабликов и опасностях, которые в них подстерегают;
- Даны четкие рекомендации как вести себя, если ребенок стал жертвой кибербуллинга, куда обратиться за помощью.

Скачать книгу

Ростелеком

Проекты

Изучи интернет – управляй им

Всероссийский онлайн-чемпионат «Изучи интернет – управляй им» – соревнования по цифровой грамотности для школьников и студентов до 18 лет. Регистрация продлится до 1 ноября 2023 года

Премия «За безопасное цифровое детство»

Проект Альянса, нацеленный на поддержку инициатив по развитию безопасной цифровой среды. Лауреатами премии могут стать дети от 14 до 18 лет, родители, а также школьные учителя

Проекты МинЦифры РФ и «Ростелеком – Солар»

Спецпроекты «КиберЗОЖ», «Кибербуллинг», «Выучи свою роль», «Прокачай скиллы защиты» адресованы разным аудиториям. Последний предназначен для юных геймеров и рассказывает о защите ПО в игре

Семейный IT-марафон

За шесть лет участниками IT-марафона стали больше 570 семейных команд со всей страны — несколько тысяч детей, их родителей и друзей. 7-й марафон прошел со 2 марта по 25 апреля 2023 года

Онлайн-проект «DigitaLogia»

Образовательный онлайн-проект «Ростелекома» и Центра «Кванториум». Цель проекта – рассказать школьникам о цифровых технологиях, развитии телекоммуникаций и кибербезопасности

Классный журнал

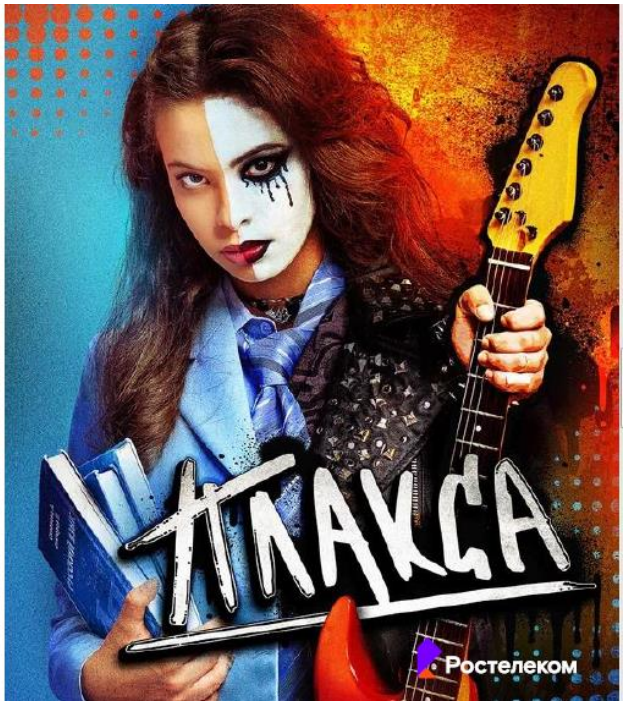
Для развития безопасного детского и подросткового сегмента интернета «Ростелеком» и интерактивный «Классный журнал» публикуют на страницах издания и на сайте полезные интернет-ссылки

Ростелеком

Кино
против буллинга

«Плакса» — 8-серийный проект из линейки Wink Originals. Цифровая премьера сериала состоялась на платформе Wink 28 сентября 2023 года, в новом сезоне сериал покажет телеканал СТС. В рамках проекта заработала платформа «Я не Плакса» — специальный сайт, где собрана информация о видах буллинга, его последствиях и способах борьбы с ним.

Смотреть сериал



Вместе мы сможем больше

Привлекайте партнеров, организации и лидеров мнений (блогеров) для реализации проектов по кибербезопасности для детей

Сотрудничество

Специалисты «Ростелекома» тесно сотрудничают с детской библиотекой, Центром «Поиск», технопарком «Кванториум»

Интеграции

«Ростелеком» – постоянный партнер всероссийской акции «Библионочь», в рамках которой делает цифровые интеграции

Новые форматы

На базе краевой детской библиотеки «Ростелеком» впервые провел игровой урок с реквизитом и аниматорами

Ростелеком

Реальные риски в виртуальной реальности

Призова Анна Владимировна, методист Центра психолого-педагогической помощи населению «Альгис»

Сегодня сложно представить повседневную жизнь без существования Интернета. Отвечая требованиям времени, практически каждый человек является активным пользователем всемирной Сети. Особенно активными потребителями интернет-контента являются дети и подростки. Так, процесс цифровизации повседневной жизни продиктован вызовами современных реалий: чтобы ребенок был в безопасности, он должен быть на связи; чтобы он развивался, он должен использовать цифровые возможности (посмотреть значение слова в поисковике, состоять в чате класса, подготовить доклад и так далее). В связи с этим актуальным представляется вопрос обеспечения интернет-безопасности.

В первую очередь, стоит обратить внимание на тот контент, который просматривает ребенок, какими ресурсами пользуется. Чаще всего – это игры, которые привлекают ребенка быстрым достижением успеха. В игре можно быстро проходить с уровня на уровень, «прокачивать» героев и все это сопровождается наградой. В реальной жизни все иначе: чтобы заслужить похвалу и признание, необходимо прилагать усилия, тратить время и другие ресурсы. Поэтому игры дают ребенку ощущение собственной значимости без значимых вложений. Таким образом, происходит подмена личных успехов виртуальными, а в отдаленной перспективе – несформированность навыков, необходимых для реальной жизни.

Еще одним негативным проявлением активного пользования интернетом является навязывание идеи о супергероях и супервозможностях. Данный контент формирует у ребенка представление о себе как о заурядной личности, не обладающей выдающимися талантами и способностями. Как следствие – низкая самооценка при высоком уровне притязаний, разочарование от осознания, что реальность не соответствует ожиданиям.

В настоящее время одним из самых популярных контентов среди пользователей стал просмотр видеоблогов различной тематики, а также коротких видеороликов. Данный контент может носить и познавательно-развивающий характер, но чаще дети выбирают легкий в восприятии и не несущий смысловой нагрузки.

Следствием такого «бездумного» использования интернет-ресурсов становится изменение паттернов обучения. Дети больше не стремятся запомнить факты, формулы или даты, если их легко можно найти в интернете. Еще одним изменением является формирование «клипового мышления» – современные дети могут быстро переключаться, распределять внимание, просматривать информацию «по диагонали», но при этом сложно сосредотачиваются на чем-то одном и навык вдумчивого изучения информации уходит на второй план.

К настоящему времени проблема кибербуллинга выходит на первый план в вопросе безопасности нахождения в интернете. Травля в цифровом

пространстве может приобретать различные формы (оскорбления, злые шутки в сообщениях или комментариях, публикация личной информации, посты с угрозами). Жертвой кибербуллинга может стать любой человек, поэтому одним из важных аспектов является формирование основ безопасного общения в интернете, информирование детей и подростков о необходимости соблюдения правил поведения в цифровом пространстве.

Таким образом, можно сделать вывод, что помимо неограниченной базы информации и разнообразия форм времяпрепровождения, интернет, как таковой, несет в себе и массу опасностей, о которых необходимо помнить не только активным пользователям, но и их окружению. Выделяют следующие:

– коммуникативные навыки: детям и подросткам все сложнее общаться в реале, страдает грамотность речи, способность оформления мыслей в словесную форму;

– высок риск возникновения отчужденности и социальной изолированности, повышения агрессивности;

– формирование основ зависимости от интернета и гаджетов;

– высокий уровень эгоцентризма и низкий уровень эмпатии: детям сложно поставить себя на место другого, они не понимают, зачем это делать.

С точки зрения психологии все проблемы, связанные с длительным пребыванием ребенка в виртуальном пространстве, основываются на тех сложностях, которые существуют у него в реальной жизни. И в первую очередь это сложности внутрисемейных отношений. Отсутствие или недостаточность внимания, поддержки, полноценного общения со стороны близких провоцирует желание «уйти» от столь некомфортных условий. Ребенок стремится самоутвердиться и поддержать свою самооценку там, где он может быть сильным, уверенным, успешным, достигать новых вершин при минимуме усилий. Также формированию интернет-направленности личности способствуют сложности социального взаимодействия в среде сверстников. Именно в детском возрасте на первом плане стоит стремление занять значимое место в коллективе, быть принятым, разделять интересы большинства, не быть «белой вороной». В связи с этим в рамках психологической работы с детьми и подростками, имеющими признаки интернет-зависимости, ведущей становится психокоррекционная работа, направленная на установление конструктивных отношений внутри семьи, коррекция эмоционально-волевой сферы ребенка (развитие эмоционального интеллекта, навыков эмпатии и саморефлексии). Как альтернативный способ проведения досуга все чаще психологами организуются не только индивидуальные занятия, но и групповые формы работы с детьми, призванные обеспечить психологически безопасное пространство для самопрезентации, командного взаимодействия, формирования мотивации на самопознание и интерес к личности другого, развитие копинг-стратегий поведения.

В заключение стоит отметить, что влияние сети Интернет на современное общество нельзя оценить однозначно. Интернет, информационные технологии, компьютеры и социальные сети оказывают давление на всех. Современные технологии и интернет стали одним из самых важных изменений в обществе в данный момент развития человечества. Они трансформируют повседневную жизнь человека, поэтому так важно соблюдать баланс между жизнью реальной и жизнью виртуальной.

Через видеоигру – на страницы книг

Коновалова Анна Петровна, библиотекарь Кочубеевской ЦБС им. А.В. Рубеля

Идея создания проекта «Через игру – на страницы книг» пришла не сразу. Все началось с небольшой рекламы в соцсетях серии книг Оливера Боудена «Assassin’s Creed». Книги были написаны на основе одноименной компьютерной игры.

У нас в фонде имеется этот цикл, и мне показалось хорошей идеей создать небольшой промо-ролик «Ассасины против Тамплиеров», где я рассказала историю создания этого цикла и его суть.

Хорошим подспорьем стало то, что незадолго до этого вышел одноименный фильм по компьютерной игре, и этот фильм моментально приобрел огромную популярность среди молодежи. Поэтому и промо-ролик получил большой отклик от наших юных читателей. Он был запущен на всех социальных медиа-площадках нашей библиотеки как реклама книжной версии популярной компьютерной игры. Давайте взглянем на отрывок, чтобы лучше понимать, о чем конкретно идет речь.

Возросшая активность посещений и внезапный интерес молодых читателей показал, что короткометражный клип на актуальную для подростков тему гораздо эффективнее, чем банальный текстовый анонс или статья о содержании фонда библиотеки. Многие даже не подозревали, что у их любимых игр есть книжные версии. Поэтому было принято решение развить эту идею и создать полноценный, интересный проект.

В результате долгой и плодотворной работы специалистами библиотеки были разработаны мини-фильмы по книгам из серии: «Ведьмак», «Сталкер», «Ассасины» и «Метро», по которым были созданы популярные компьютерные игры.

Ролики были размещены на всех медиаплощадках библиотеки для ознакомления, а также специалистами библиотеки были проведены интерактивные мероприятия для молодежи по этим книгам: «Книжный респаун», «Вселенная игр и книг» и многие другие.

Задания, которые выполняли участники, были связаны и с книгами, и с современными гаджетами. Учитывая то, сколько времени подростки

проводят в соцсетях и на других интернет-площадках, этот проект стал одним из самых успешных за последние годы с точки зрения привлечения молодого поколения конкретно в нашу библиотеку и в мир чтения в целом.

За два года работы над проектом были созданы 4 фильма и проведено более 10 мероприятий с привлечением школ и различных культурных объединений. Специфика каждой игровой вселенной предполагает, что на создание и верстку каждого фильма уходит от 1 до 3 месяцев, в зависимости от количества исходного материала.

Например, вселенная «Ведьмака» включает в себя 7 отдельных авторских повестей и около 10 второстепенных произведений, вроде фанфиков и сборников рассказов. В то время как вселенная «Сталкера» - это огромное собрание сочинений разных авторов общим количеством более 300 книг.

Почему же для привлечения молодежи все-таки были выбраны именно видеоигры? Ответ очень простой – воздействовать нужно, используя то, что интересно и актуально именно для этой категории читателей. А молодежь интересуется прежде всего современными технологиями, медиаконтентом и всем, что связано с интернет-пространством. Соответственно, эта самая молодежь, когда любимая игра подходит к концу, ищет способ вернуться в любимый виртуальный мир. Вот тут-то на помощь и приходят книги. Молодые люди обожают всё, что связано с их увлечением – сувенирную продукцию, кастомную одежду, постеры по мотивам популярной игры, и при умелом подходе этот интерес можно переориентировать на книгу. Итогом этого проекта стало увеличение количества молодых читателей и привлечение их к совместной реализации проекта, а также внедрение различных виртуальных сервисов в работу библиотеки для привлечения подписчиков в социальных сетях.

Медиабезопасность детей и подростков на примере работы клуба «Смайлик»

Шмакова Наталья Сергеевна, библиотекарь медиацентра ЦГБ г. Невинномысска

Интернет стал неотъемлемой частью нашей жизни. Но безопасность в глобальной сети касается всех, как взрослых, так и детей.

На базе детского Медиацентра в Невинномысской Центральной библиотеке создан компьютерный клуб «Смайлик» в помощь формированию и воспитанию информационной культуры детей и подростков. Возрастная категория участников клуба от 7 до 14 лет. Занятия клуба «Смайлик» направлены на достижение следующих целей:

- формирование читателя информационного века, информационного общества;

- помощь ребёнку-читателю в освоении технических средств, способствующих быстрому и полному удовлетворению его информационных потребностей;
- помощь в написании рефератов и домашнего задания.

Мероприятия проводятся с учетом возрастных особенностей детей. Посещая занятия клуба, дети обучаются основам компьютерной грамотности, учатся сосредотачиваться, мыслить самостоятельно, развивать внимание, расширяют свой кругозор. А использование элементов игры для детей младшего возраста позволяет повысить интерес к занятиям, развить и реализовать их творческий потенциал.

В наши дни мы все проводим много времени в Интернете, в том числе дети и подростки. Каждый родитель хочет, чтобы дети чувствовали себя в безопасности, находясь в сети, ведь в Интернете есть вещи, которых следует опасаться. В последнее время Интернет-угрозы приобрели вполне реальные очертания и урон, который они способны причинить, это оборачивается материальными потерями, физическим вредом здоровью или даже угрозой для жизни. Опасны не только вирусы и хакеры, которые могут украсть личную информацию; помимо них существует кибербуллинг (травля), неприемлемый контент и онлайн-хищники, нацеленные на детей и подростков. Поэтому основной целью работы клуба «Смайлик» является проведение бесед, занятий по медиабезопасности, т.е. обеспечение информационной безопасности детей и подростков путем привития им навыков ответственного и безопасного поведения в Интернете.

Ежегодно в клубе проводится Неделя Безопасного Рунета, приуроченная к Международному Дню безопасного Интернета. В течение всей недели проводились для читателей клуба интерактивные познавательные программы, викторины, беседы, практикумы, выставки. Были проведены следующие мероприятия: Web-путешествие «Вебландия - виртуальный детский мир»; урок-путешествие по безопасным сайтам «Kinder-Inter.net»; урок интернет-этикета «Интернет: интересно, полезно, безопасно». Были оформлены выставки: «Книги, Интернет и я – вместе лучшие друзья», «Интернет: безопасный, интересный, познавательный», а также стенд, посвященный Неделе безопасного Рунета. В рамках Недели читатели обсуждали вопросы защиты персональных данных, знакомились с полезными ресурсами, учились совершать безопасные онлайн-покупки, демонстрировали навыки безопасного поведения в Сети.

Для всех детей и родителей были подготовлены видео-ролики по безопасности Интернета для детей и подростков. Для пользователей была подготовлена слайд-презентация «Безопасные и полезные сайты для детей и родителей». На ролике представлены такие сайты как Портал "Чудо-юдо"; сайт "Развитие ребенка"; сайт "По складам" и «МААМ» - учебные материалы для детского сада и школы.

В настоящее время созданы и развиваются огромное количество ресурсов, призванных предупредить об Интернет-угрозах и научить грамотному поведению в сети. Например, «Лига безопасного Интернета».

Основная его цель - создание безопасного пространства Интернета на территории Российской Федерации. Этот сайт содержит большое количество материалов, в том числе методических, которые мы используем для проведения занятий с детьми, а также выпускаем буклеты для родителей.

Вместе с членами клуба «Смайлик» мы выпустили интернет-библиографию «Полезные сайты для детей». Предлагаем познакомиться с наиболее интересными на наш взгляд сайтами Интернета, которые могут быть полезны детям и взрослым в выборе детской художественной литературы. Многие из них содержат, как библиографическую, так и полнотекстовую информацию. Большинство сайтов для детей обладают хорошо разработанной системой поиска и путеводными знаками. В оформлении сайтов используются разнообразные красочные иллюстрации, звуковые и мультимедийные фрагменты. Они очень удобны в использовании. Это такие сайты, как:

- «Дом сказки» (здесь можно почитать и послушать в авторской озвучке современные сказки для детей, увлекательные истории и захватывающие приключения);
- «Почитай-ка» (сказки, загадки, курьезы, необычные рассказы, стихи, факты из жизни великих сказочников);
- «Добрые сказки» (уникальная методика - образование и воспитание через сказки. Сказки о семье, буквах, словах, искусстве, родном языке, музыке, природе, науке, овощах и фруктах и многом другом);
- «Солнышко» (был отмечен Интернет-премиями «Награда.ру». Здесь собрано более полутора сотен произведений: сказки народов мира, авторские сказки, детские повести и рассказы на любой вкус);
- «Обучалки-развивалки» (посвящен детям, их развитию, воспитанию и обучению, а также творчеству. Здесь вы найдете статьи о детях, обучающие и развивающие программы для малышей и школьников, которые можно скачать бесплатно, а ребенок непременно захочет посмотреть детское обучающее видео).

Эта Интернет-библиография пользуется большим спросом у наших читателей.

Как мы понимаем, полностью оградить детей от опасного и нежелательного сетевого контента не могут ни родители, ни учителя, ни программно-технические средства, используемые для этого. Поэтому так важно сформировать у детей навыки грамотного поведения в сети Интернет, вооружить их средствами защиты от Интернет-угроз, самым главным среди которых является внимательное, доверительное отношение между взрослыми и детьми.

Финансовое мошенничество. Социальная инженерия.

Кошелев Виталий Викторович, главный экономист Отделения Ставрополь Южного ГУ Банка России

Банк России

ЭМОЦИИ, КОТОРЫЕ ВЫЗЫВАЕТ ИНФОРМАЦИЯ ОТ ТЕЛЕФОННЫХ МОШЕННИКОВ

ПОЛОЖИТЕЛЬНЫЕ

- РАДОСТЬ
- НАДЕЖДА
- ЖЕЛАНИЕ ПОЛУЧИТЬ ДЕНЬГИ

ОТРИЦАТЕЛЬНЫЕ

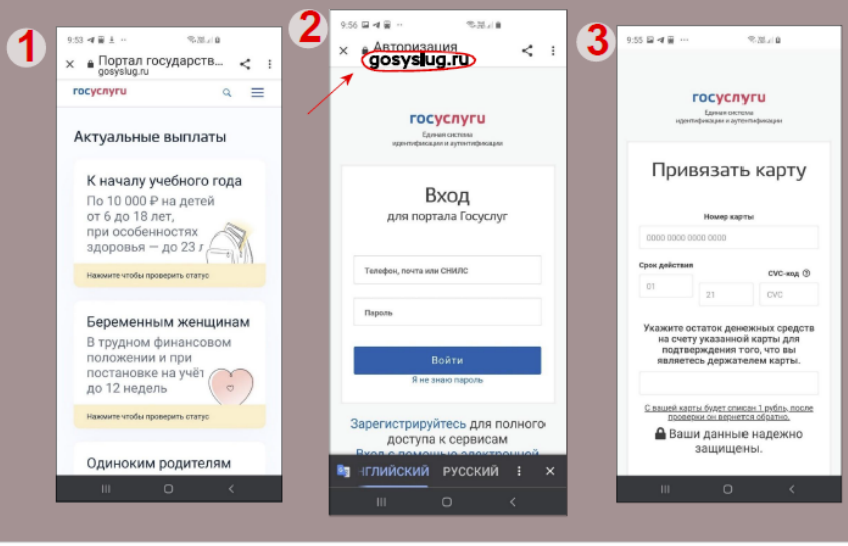
- СТРАХ
- ПАНИКА
- ЧУВСТВО СТЫДА

«Вы выиграли крупную сумму денег»
«Вам положены социальные выплаты»
«Пенсионный фонд рад сообщить вам о перерасчете вашей пенсии, вам положена выплата в размере…»

«С вашего счета списали все деньги»
«Ваш родственник попал в аварию и сбил человека»
«Вас беспокоит следователь Следственного комитета, вы участник уголовного дела»

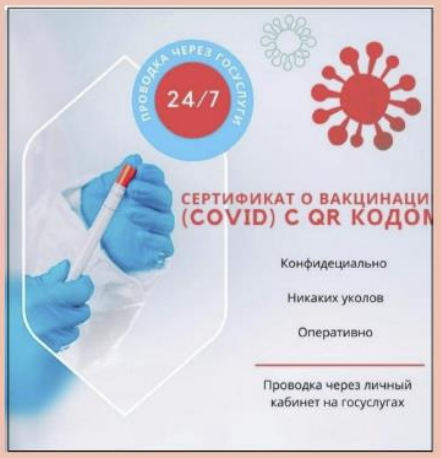
Банк России

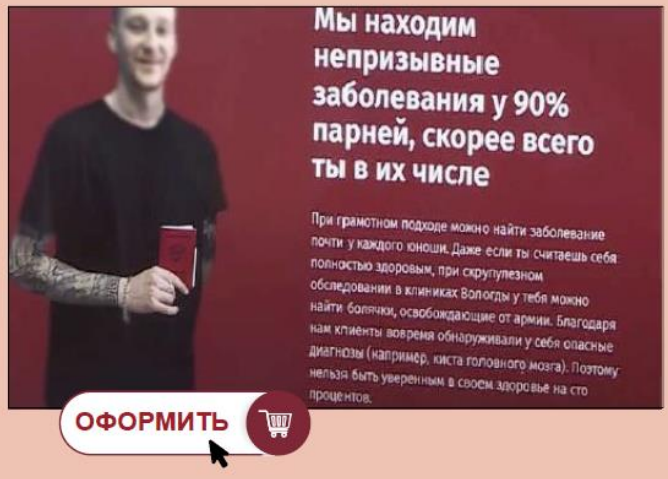
САЙТЫ, МАСКИРУЮЩИЕСЯ ПОД «ГОСУСЛУГИ»



Банк России

НОВОСТНОЙ ФИШИНГ





Банк России

ОБЩИЕ ПРАВИЛА ПОВЕДЕНИЯ С КИБЕРМОШЕННИКАМИ

- Не сообщайте никому личную и финансовую информацию (данные карты)
- Установите антивирусные программы на все свои гаджеты и регулярно обновляйте их
- Не читайте сообщения и письма от неизвестных адресатов и не перезванивайте по неизвестным номерам
- Не переходите по сомнительным ссылкам и не скачивайте неизвестные файлы или программы
- Заведите отдельную банковскую карту для покупок в Интернете

Будьте бдительны: не действуйте второпях и проверяйте информацию!

Расскажите эти правила поведения своим друзьям и знакомым!

Банк России

ОБЩИЕ ПРАВИЛА ПОВЕДЕНИЯ С КИБЕРМОШЕННИКАМИ

Самостоятельно звоните в свой банк по номеру телефона, указанному на обратной стороне карты или на официальном сайте банка

Установите двухфакторный способ аутентификации – например, логин и пароль + подтверждающий код из СМС

Официальные сайты финансовых организаций в поисковых системах (Яндекс, Mail.ru) помечены цветным кружком с галочкой

Будьте бдительны: не действуйте второпях и проверяйте информацию!

Расскажите эти правила поведения своим друзьям и знакомым!

Банк России

КАК ПРОТИВОСТОЯТЬ ТЕЛЕФОННЫМ МОШЕННИКАМ

1. Не отвечайте на звонки с незнакомых номеров
2. Прервите разговор, если он касается финансовых вопросов
3. Не торопитесь принимать решение
4. Проверьте информацию в Интернете или обратитесь за помощью к близким родственникам

5. Самостоятельно позвоните близкому человеку / в банк / в организацию
6. Не перезванивайте по незнакомым номерам

Возьмите паузу и спросите совета у родных и друзей!

Банк России

ПРИЗНАКИ ФИШИНГОВЫХ САЙТОВ

- Ошибки в адресе сайта
- Сайт состоит из 1 страницы (только для ввода данных)
- В адресной строке отсутствует замочек
- В названии сайта нет https
- Ошибки в тексте и дизайне
- Побуждают ввести свои личные / финансовые данные
- Предлагают скачать файл, установить программу

Относитесь с подозрением к письмам (сообщениям) с неизвестными ссылками и файлами для скачивания!

Банк России

ПОПУЛЯРНЫЕ УЛОВКИ МОШЕННИКОВ В ИНТЕРНЕТЕ

- Интернет-магазины и аукционы
- Восстановление кредитной истории
- Сообщение о крупном выигрыше или выплате от государства
- Заманчивое предложение о работе
- Льготные кредиты
- Туристические путевки со скидкой
- Сбор «пожертвований» для детей, больных, животных и др.
- Предложение вложиться в высокодоходные инвестиции

Не верьте слепо предложениям в Интернете — проверяйте информацию на достоверность!

Информационная грамотность в медиа: как отличить истину ото лжи?

Чернышева Марина Борисовна, директор АНО ИРЦ «Гражданское партнерство», учредитель и редактор портала sk-news.ru

КАК РАСПОЗНАТЬ ФЕЙК?

- Читайте не только заголовок.
- Кто автор?
- Проверьте дату и время публикации.
- Проверьте какой новостной сайт это опубликовал.
- Проверьте ссылки и источники указанные в посте.
- Проверьте сомнительные цитаты и фотографии.
- Будьте осторожнее с предвзятыми постами.
- Убедитесь что об этом пишут и другие новостные порталы.
- Подумайте прежде чем поделиться!

ПРИ ПОДДЕРЖКЕ ПРЕЗИДЕНТСКОГО ФОНДА КУЛЬТУРНЫХ ИНИЦИАТИВ

А ЧТО СКАЖЕТ НЕЙРОСЕТЬ?

1. Оценка нескольких источников: перекрестные ссылки на информацию из разных надежных источников для проверки точности и последовательности.
2. Проверьте достоверность источников. Изучите репутацию, опыт и предвзятость источников, чтобы оценить их надежность.
3. Ищите доказательства и ссылки. Подлинная информация обычно включает цитаты или ссылки, подтверждающие утверждения.
4. Проверка фактов с помощью веб-сайтов надежных организаций.
5. Будьте осторожны с предвзятостью. Активно ищите разные точки зрения, чтобы не попасть в эхо-камеру.
6. Учитывайте намерения и тон автора: оцените мотивы информации и наличие тенденций к сенсационности или кликбейту.
7. Используйте навыки критического мышления. Анализируйте контекст и подвергайте сомнению утверждения, которые кажутся слишком хорошими, чтобы быть правдой, или чрезмерно сенсационными.
8. Помните: хотя эти шаги могут помочь, важно сохранять бдительность и постоянно обновлять свои знания, чтобы ориентироваться в постоянно меняющемся информационном пространстве.

ПРИ ПОДДЕРЖКЕ ПРЕЗИДЕНТСКОГО ФОНДА КУЛЬТУРНЫХ ИНИЦИАТИВ

КОНТРВЕРСИЙНОСТЬ

ЗАДУМАЙТЕСЬ, ЕСЛИ:

- Автор явно проявляет симпатию к одной из сторон конфликта и антипатию к другой
- Эксперты поддерживают одну и ту же точку зрения
- Не представлена точка зрения человека или стороны которую обвиняют
- Тон подачи информации эмоционален и тенденциозен.

ПРИ ПОДДЕРЖКЕ ПРЕЗИДЕНТСКОГО ФОНДА КУЛЬТУРНЫХ ИНИЦИАТИВ

ТАКТИКА ДЕЗИНФОРМАЦИИ

1. Фальсификация: Создание полностью ложной информации или историй.
2. Искажение фактов с целью создания ложного впечатления.
3. Информация вне контекста с целью ввести в заблуждение или исказить факты.
5. Выдача себя за другое лицо: фейковые аккаунты для распространения ложной информации.
6. Астротурфинг: создание искусственного массового движения или фальшивых онлайн-персонажей для продвижения определенной повестки дня.
7. Сатира или пародия: представление ложной информации в виде юмора или сатиры с целью ввести людей в заблуждение или сбить с толку.
8. Заголовки-кликбейты. Использование сенсационных или вводящих в заблуждение заголовков
9. Манипулирование изображениями или видео: изменение визуального контента для создания ложных повествований или введения зрителей в заблуждение.
10. Сети ботов: использование автоматических учетных записей или ботов для распространения дезинформации и манипулирования онлайн-дискуссиями.

!!! Важно критически оценивать источники информации и знать об этих тактиках.

ФОНД ПРЕЗИДЕНТСКИХ ГРАНТОВ

Приложение 1

Календарь безопасного Интернета

ЯНВАРЬ

Последнее воскресенье января (28 января 2024 года) – Международный день БЕЗ интернета, главная цель которого – отвлечь людей от компьютеров и глобальной сети хотя бы на один день. Свою историю этот праздник ведет с начала 2000-х годов, его организаторами стали активные интернет-пользователи. Для библиотек день без интернета становится поводом для организации дискуссий и бесед о пользе и вреде интернета, его значении в жизни человека.

28 января – Международный день защиты персональных данных. Этот день был учрежден в 2007 году для того, чтобы напомнить пользователям сети о соблюдении правил поведения в интернете, которые помогут обезопасить виртуальную и реальную жизнь.

ФЕВРАЛЬ

Второй месяц года проходит под знаком безопасного интернета, этим мероприятиям посвящена целая неделя. Неделя безопасного Рунета – крупнейшая российская серия мероприятий по проблемам детской контентной цифровой безопасности, проходящая в нашей стране ежегодно с 2008 года.

Ежегодно во второй день второй недели второго месяца года отмечается Международный день безопасного интернета, который в России впервые был проведен в 2007 году. Безопасный интернет – это обилие позитивного контента, знания обычных пользователей об основах безопасности, общественный договор относительно норм поведения в Сети, а также интернет-возможности и сервисы, приходящие на помощь людям практически в любой проблемной ситуации.

МАРТ

1 марта – день хостинг-провайдера в России. В 2011 году у людей и организаций, чья деятельность связана с интернетом, появился новый праздник, получивший название «День хостинг-провайдера». Хостинг – услуга по хранению информации, а организация, занимающаяся предоставлением такого рода услуг на своих технических площадках, называется хостинговой компанией или хостинг-провайдером. Праздник является данью уважения тем, кто трудится над усовершенствованием систем хранения и передачи информации.

12 марта – день свободы слова в Интернете. Отмечается по инициативе международной организации «Репортеры без границ» (под патронатом ЮНЕСКО) с 2008 года.

АПРЕЛЬ

4 апреля – день веб-разработчика. Веб-разработчики занимаются созданием кода страниц сайтов, приложений, проверяют их работоспособность, наполняют информацией. Веб-сайт – это интернет-ресурс, имеющий свое название, определенное место среди остальных

сайтов, и состоящий из различного рода электронных страниц с текстовым, графическим или иным медийным содержанием. Дата 4.04. как 404 — код ошибки клиента, который означает, что файл или страница не найдены.

7 апреля – день рождения Рунета. В этот день в 1994 году для России был зарегистрирован домен – .Ru – и внесен в международную базу данных национальных доменов верхнего уровня. С этого момента Россия была официально признана государством, представленным в интернете. Сегодня в России введен еще один домен – .рф – национальный домен верхнего уровня для Российской Федерации – первый в интернете домен на кириллице.

МАЙ

17 мая – Всемирный день электросвязи и информационного общества. Цель данного Дня – способствовать повышению уровня осведомленности о возможностях, которые может принести обществу и странам использование интернета и информационно-коммуникационных технологий.

28 мая – День оптимизатора Рунета (День SEO-оптимизатора). Впервые отмечался в 2006 году. Аббревиатура SEO (Search Engine Optimization, поисковая оптимизация) обозначает различные методы работы с поисковыми системами – с целью роста позиций ресурса в поисковой выдаче по определенным запросам пользователей.

ИЮНЬ

14 июня интернет-сообщество отмечает Международный день блогера. Идея проведения этого праздника родилась в 2004 году, когда 500 человек из более чем 40 стран, объединившись, решили, что им нужен свой день – своего рода символ дружеских отношений между сетевыми блогерами всего мира. Блогер – человек, который самостоятельно ведет и администрирует свой интернет-дневник, где регулярно рассказывает о событиях своей жизни, делится фотографиями, мыслями и идеями.

ИЮЛЬ

17 июля – Всемирный день эмоджи (эмодзи). Смайлики, пиктограммы, идеограммы, образующие графический язык, часто используемый в системе электронного обмена информацией, стали неотъемлемой частью нашего общения в сети.

26 июля 2024 года (ежегодно в последнюю пятницу месяца) проходит День системного администратора. Реалии сегодняшнего дня таковы, что с представителем данной профессии имеет перспективу столкнуться практически каждый из нас. Системные администраторы создают и поддерживают работоспособность компьютерных сетей, серверов, периферийного оборудования, программ – всем этим оборудованы и классы в школе, и магазины, и банки, и многие другие общественные учреждения.

АВГУСТ

31 августа – День блога. В 2005 году активные пользователи LiveJournal заметили, что слово blog очертаниями похоже на цифры 3108 – так родилась идея праздновать День блога (Blog Day). Инициаторы Дня блога призывают посвятить его знакомству с блогерами из разных стран и с

разными интересами. В 2007 году в связи с этой датой начался конкурс лучших блогов Best of Blogs, в котором могут принимать участие публикации на десяти языках, в том числе, и на русском.

СЕНТЯБРЬ

9 сентября – День тестировщика. Ежедневно программистами создается не одна тысяча программ для электронных устройств: начиная с простых калькуляторов и заканчивая искусственным интеллектом для высокотехнологических машин. Каждый из этих программных продуктов должен пройти этап тестирования. О том, что тестировщиком быть небезопасно, напоминает печальный факт, благодаря которому и появился в календаре этот памятный день: 9 сентября 1945 г. ученые Гарвардского университета, тестировавшие вычислительную машину Mark II Aiken Relay Calculator, нашли мотылька, застрявшего между контактами электромеханического реле.

13 сентября /если год високосный — 12 сентября, отмечается День программиста в России (празднуется в 256-й день года). Число 256 выбрано потому, что это количество целых чисел, которое можно выразить с помощью одного восьмиразрядного байта, а также это максимальная степень числа 2, которая меньше количества дней в году — 365.

19 сентября – день рождения «Смайлика». История празднования этого дня такова: 19 сентября 1982 года профессор Университета Карнеги-Меллона (штат Пенсильвания, США) Скотт Фалман впервые предложил использовать три символа, идущие подряд – двоеточие, дефис и закрывающую скобку :-), для обозначения «улыбающегося лица» в тексте, который набирается на компьютере. Это было серьезным пополнением электронного лексикона.

30 сентября – день интернета в России. Инициатива праздника принадлежит московской фирме IT Infoart Stars, которая 1998 году разослала предложение назначить 30 сентября «Днем интернета» и провести «перепись населения русскоязычного интернета». По данным аналитической компании GfK, к началу 2019 года аудитория интернет-пользователей в России среди населения старше 16 лет составила 90 миллионов человек – почти 75,4% взрослого населения страны.

ОКТЯБРЬ

2 октября – день рождения электронной почты. Эта дата считается условной, потому что изобретатель первой почтовой программы Рэй Томлинсон не помнит точный день, когда было отправлено первое письмо, но это произошло в 1971 году. Рэй Томлинсон стал известным не только благодаря первой электронной почте, но и изобретению символа @ – известной всему миру «собаки».

10 октября – День рождения социальной сети «ВКонтакте». Дата приурочена ко дню рождения основателя сети – Павла Дурова. Первый раз день рождения «ВКонтакте» отпраздновали 10 октября 2006 года, когда Павлу Дурову исполнилось 22 года. Даже его выход из числа владельцев компании, не повлиял на то, что его имя прочно ассоциируется с названием одной из самых популярных в России социальных сетей в России и мире.

29 октября – день рождения интернета. Точкой отсчета для этого праздника стала первая передача данных между двумя компьютерами, которая состоялась 29 октября 1969 года. Как гласит история, случилось это Калифорнийском университете Лос-Анджелеса (UCLA) и в Стэнфордском исследовательском институте (SRI) (находящимися на расстоянии в 640 км) – именно между ними был впервые проведен сеанс связи. В первый раз удалось отправить всего три символа «LOG» – часть слова LOGIN (команды входа в систему).

НОЯБРЬ

30 ноября – Международный день защиты информации. Отмечается с 1988 г. по инициативе американской Ассоциации компьютерного оборудования. В 1988 г. была зафиксирована первая массовая эпидемия червя, получившего название по имени своего «творца» – Морриса. Наступило время задуматься о необходимости комплексного подхода к обеспечению информационной безопасности.

ДЕКАБРЬ

4 декабря – день рождения отечественной информатики. В августе 1948 года член-корреспондент АН СССР Исаак Брук совместно с инженером Баширом Рамеевым представил проект автоматической вычислительной машины. 4 декабря 1948 года Государственный комитет Совета Министров СССР по внедрению передовой техники в народное хозяйство зарегистрировал это изобретение под названием «Цифровая электронная вычислительная машина».

Материал переработан с сайта https://rodb-v.ru/safe-Internet/kalendar-bezopasnogo-interneta/?ysclid=lr1xo7tt77711246777

Приложение 2

Сценарий мероприятия по теме «Безопасность в сети Интернет» для младших школьников

Ведущий: сейчас я предлагаю вам отгадать загадки, чтобы понять, о чем пойдет речь на нашей встрече.

Игра «Угадай-ка».

Что за чудо-агрегат
Может делать все подряд -
Петь, играть, читать, считать,
Самым лучшим другом стать? (компьютер.)

На столе он перед нами, на него направлен взор,
подчиняется программе, носит имя... (монитор).

Не зверушка, не летаешь, а по коврику скользишь
и курсором управляешь. Ты – компьютерная... (мышь).

Нет, она – не пианино,
только клавиш в ней – не счесть!
Алфавита там картина, знаки, цифры тоже есть.
Очень тонкая натура. Имя ей ... (клавиатура).

Сохраняет все секреты «ящик» справа, возле ног,
и слегка шумит при этом. Что за «зверь?» (системный блок).

Есть такая сеть на свете
Ею рыбу не поймать.
В неё входят даже дети,
Чтоб общаться, иль играть.
Информацию черпают,
И чего здесь только нет!
Как же сеть ту называют?
Ну, конечно ж... (Интернет)

Ведущий: Как вы думаете, о чём мы сегодня будем говорить?

Правильно, мы с вами поговорим об интернете, точнее о безопасности в интернете. Мы живём в эпоху Интернета, без которого, увы, сейчас трудно справиться. Интернет заменил у нас многое. Это нам облегчило жизнь. Сейчас всего лишь при помощи одного небольшого устройства мы можем обмениваться мгновенными сообщениями, покупать книги или музыку, получать любую необходимую информацию и многое другое. Интернет ворвался в нашу жизнь.

У кого дома есть компьютер?

Как вы им пользуетесь?
А у кого дома есть Интернет?
А как вы думаете, какая опасность может подстерегать пользователей интернета? (ответы детей).

Мы можем найти в интернете любую информацию, но некоторые сайты могут быть заражены, и наш компьютер может «заболеть».

Поэтому постарайтесь запомнить основные правила безопасного интернета.

Просмотр социального ролика от следственного комитета РФ «Твой безопасный Интерент»

https://youtu.be/estdGAd5SRc?si=EDuqmYPYhDGEGKVJ

Ведущий: А сейчас послушайте сказку о золотых правилах безопасного поведения в Интернет.

СКАЗКА

В некотором царстве, Интернет - государстве жил-был Смайл-царевич-королевич, который правил славным городом. И была у него невеста – прекрасная Смайл-царевна-Королевна, день и ночь проводившая в виртуальных забавах.

Сколько раз предупреждал её царевич об опасностях, подстерегающих в сети, но не слушалась его невеста. Не покладая рук трудился Смайл-царевич, возводя город, заботился об охране своих границ и обучал жителей города основам безопасности жизнедеятельности в Интернет-государстве. И не заметил он, как Интернет-паутина всё-таки затянула Смайл-царевну в свои коварные сети.

Погоревал – да делать нечего: надо спасать невесту. Собрал он королевскую дружину. Стали думать головы мудрые, как вызволить царевну из плена виртуального. И придумали они «Семь золотых правил безопасного поведения в Интернет», сложили их в котомку Смайл-царевичу, и отправился он невесту искать.

Вышел на поисковую строку, кликнул по ссылкам поганым, а они тут как тут: сообщества Змея-искусителя-Горыныча, стрелялки-убивалки Соловья-разбойника, товары заморские купцов шаповских, сети знакомств - зазывалок русалочьи… Как же найти-отыскать Смайл-царевну?

Крепко задумался Смайл-королевич, надел щит антивирусный, взял в руки меч-кладенец кодовый, сел на коня богатырского и ступил в трясину непролазную. Долго бродил он и остановился на распутье игрища молодецкого трёхуровневого, стал читать надпись на камне: на первый уровень попадёшь – времени счёт потеряешь, до второго уровня доберёшься – от родных-близких отвернёшься, а на третий пойдёшь - имя своё забудешь. И понял Смайл-царевич, что здесь надо искать невесту.

(Ведущий: как вы думаете, ребята, о чем здесь говорится? Что происходит с человеком, если он сильно увлекается виртуальным миром?)

Взмахнул он своим мечом праведным и взломал код игрища страшного! Выскользнула из сетей разомкнувшихся Смайл-царевна, осенила себя паролем честным и бросилась в объятия своего суженого. Обнял он

свою невесту горемычную и протянул котомочку волшебную со словами поучительными: «Вот тебе оберег от козней виртуальных, свято соблюдай наказы безопасные!»

1. Спрашивай взрослых

Если что-то непонятно, страшно или неприятно,
Быстро к взрослым поспеши,
Расскажи и покажи.

Всегда спрашивай родителей о незнакомых вещах в Интернете. Они расскажут, что безопасно делать, а что нет.

2. Установи фильтр

Как и всюду на планете,
Есть опасность в интернете.
Мы опасность исключаем,
Если фильтры подключаем.

Чтобы не сталкиваться с неприятной и огорчительной информацией в интернете, установи на свой браузер фильтр, или попроси сделать это взрослых – тогда можешь смело пользоваться интересными тебе страничками в интернете.

3. Не открывай файлы

Не хочу попасть в беду –
Антивирус заведу!
Всем, кто ходит в интернет,
Пригодится наш совет.

Не скачивай и не открывай неизвестные тебе или присланные незнакомцами файлы из Интернета. Чтобы избежать заражения компьютера вирусом, установи на него специальную программу – антивирус!

4. Не спеши отправлять SMS

Иногда тебе в сети,
Вдруг встречаются вруны.
Ты мошенникам не верь,
Информацию проверь!

Если хочешь скачать картинку или мелодию, но тебя просят отправить смс - не спеши! Сначала проверь этот номер в интернете – безопасно ли отправлять на него смс и не обманут ли тебя. Сделать это можно на специальном сайте.

5. Осторожно с незнакомцами

Злые люди в Интернете,
Расставляют свои сети.
С незнакомыми людьми
Ты на встречу не иди!

Не встречайся без родителей с людьми из Интернета вживую. В Интернете многие люди рассказывают о себе неправду.

6. Будь дружелюбен

С грубиянами в сети,
Разговор не заводи.

Ну и сам не оплошай –
Никого не обижай.

Общаясь в Интернете, будь дружелюбен с другими. Не пиши грубых слов! Ты можешь нечаянно обидеть человека, читать грубости так же неприятно, как и слышать.

7. Не рассказывай о себе
Чтобы вор к нам не пришёл,
И чужой нас не нашёл,
Телефон свой, адрес, фото,
В интернет не помещай,
И другим не сообщай.

Никогда не рассказывай о себе незнакомым людям: где ты живешь, учишься, свой номер телефона. Это должны знать только твои друзья и семья!

Залилась совестливыми слезами дева красная, дала своему наречённому слово честное, что не будет пропадать в забавах виртуальных, а станет трудиться на благо народа, города своего, сама начнёт обучаться и помогать будет люду заблудшему и погрязшему в трясине сетевой. И зажили они дружно и счастливо с мечтою расширить границы образования.

Тут и сказочке конец, а кто слушал - МОЛОДЕЦ!

Какова мораль этой сказки?

А сейчас немного отдохнём и поиграем.

Игра «Вирусы»

Цель игры: Эмоциональная разрядка, снятие напряжения.

Вспомогательные материалы: Листы А4 двух цветов и лента, которой можно будет обозначить линию, разделяющую две команды.

Процедура проведения: Листы А4 нужно скомкать и сделать из них снежки двух разных цветов. Снежки одного цвета обозначают, например, вирусы, спам, зараженные файлы, снежки другого цвета – безопасная информация, безопасные файлы. Участники делятся на две команды так, чтобы расстояние между командами составляло примерно 3 м. В руках каждой команды снежки двух цветов, которые они, по команде ведущего, бросают другой команде. Задача: как можно быстрее закидать противоположную команду снежками, при этом успевая откидывать все «опасные» снежки и сохранять у себя все «безопасные». Ведущий засекает 30 секунд и, услышав команду «Стоп!», участники должны прекратить игру.

Выигрывает та команда, на чьей стороне оказалось меньше «опасных» и больше «безопасных» снежков. Перебегать разделительную линию запрещено.

Ведущий: Ребята, давайте попробуем почувствовать на себе вирусную атаку и постараться защититься от нее! Правила будут такие. Вам нужно разбиться на 2 команды. Но сначала из листочков бумаги черного и белого цвета сделаем снежки! Каждый должен сделать по 2 снежка белого и черного цвета. Черные снежки – «опасные», а белые – «безопасные». По моей

команде начинаем бросать друг в друга снежки! Задача одной команды – как можно быстрее закидать противоположную команду снежками.
Также задача каждой команды – успеть откидывать все черные снежки и сохранять у себя белые.
Ведущий: Сейчас я вручу каждому памятку с правилами. Прочитайте правила и постарайтесь их выполнять (вручение памяток).
Подведём итоги нашей встречи. Прочитайте предложение и продолжите.
Мне было интересно узнать…
Мне понравилось…
Меня удивило…
Мне захотелось…

Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями. Но – как и реальный мир – Сеть тоже может быть опасна!

Желаю, чтобы и в жизни, и на просторах Интернета у вас было всё просто отлично!

Памятки о правилах безопасного пользования интернетом остаются вам.

Памятка по безопасному поведению в Интернете

Это важно знать!

- Я не скажу о себе ничего (ни адреса, ни телефона, ни других сведений) без разрешения родителей.
- Я никогда не передам по Интернет своей фотографии.
- Я никогда не встречусь ни с кем, кого знаю только по Интернет, без разрешения родителей. На встречу я пойду с отцом или с матерью.
- Я никогда не отвечу на сообщение, которое заставляет меня краснеть, будь то электронное письмо или общение в чате.
- Я буду разговаривать об Интернет с родителями.
- Я буду работать только тогда, когда они разрешат мне, и расскажу им обо всем, что я делал в Интернет.

Материал переработан по материалам книги: Классные часы, посвященные безопасности в сети Интернет: сборник методических разработок. – Бугуруслан. –2019.

Приложение 3

Сценарий киберурока для младших школьников «Как Ваня понял, что онлайн-игра до добра не доведет»

Ход киберурока:

Чтение и обсуждение истории

Ведущий: здравствуйте, ребята. Послушайте сказку «Как Ваня понял, что онлайн-игра до добра не доведет» и подумайте, о чем мы сегодня будем говорить на занятии.

Ведущий рассказывает историю.

Сегодня я расскажу вам историю про мальчика Ваню, который очень любил играть в онлайн-игры.

"И зачем вы только этот планшет ему купили! Ещё больше играть будет!", – возмущалась бабушка. "Планшеты сейчас у каждого ребёнка сейчас есть, и ничего...", – возражал папа. "А в телефоне всё мелкое, со своими игрушками он зрение испортит!", – добавляла мама.

Бабушка только вздыхала и уходила на кухню. Вначале Ваня играл в игры нечасто, учил уроки, помогал прибираться по дому. Но потом в его любимой игре начался сезон турниров. Вот тут и началось самое интересное! "Ваня, а ты слышал, что скоро в нашей игре турнир будет?", – возбуждённо крикнул Павлик, подбежав к другу.

"Нет, а что такое турнир?" . "Ну ты и тундра!", – удивился Павлик. "Это чемпионат, здесь можно стать мега крутым бойцом!"

" Эх, у меня, наверно, не получится поучаствовать. Не разрешит мне мамка столько играть! А долго надо играть?", – с интересом спросил Ваня.

"Не меньше пяти часов! Дня два будут состязания идти. Надо во всех битвах победить. А это трудно: знаешь, какие там бойцы!", – заявил Павлик.

Ваня пришёл домой с мыслями только об одном: что бы такое придумать, чтоб ему разрешили турнир этот пройти. Ваня даже обещания маме и папе заготовил: хорошо учиться, прибираться в комнате, всегда помогать и всё такое.

Дома была только бабушка. Тётя приболела, и родители уехали её проведать. Два дня их не будет! Ваня был счастлив: бабушка не такая строгая, как мама и папа. Уж теперь турнир точно будет его!

После вкусного обеда Ваня вымыл за собой тарелку и, заглядывая бабушке в глаза, тихо спросил: "Бабуля, можно?"

"Что можно?", – спросила бабушка. Ваня отвечал: "Ну, поиграть немного на планшете... У меня турнир сегодня". "Ну, если турнир, то конечно! Но только немного", – улыбнулась бабушка. "Конечно, конечно!", – Ваня, схватив планшет, удобно устроился на диване.

Игра захватила мальчика, он ничего вокруг не видел и не слышал. Битва была сложной. Он осилил только троих бойцов и начал игру сначала, а в дверях детской уже появилась бабушка: "Ванечка, ты же просил немного, а уже целый час прошёл! Ну всё, заканчивай!"

"Бабуля, милая, ну минуточку, последний бой!" – попросил Ваня.

"Пять минут, Ваня, пять минут!" – ответила бабушка.

Но через пять минут Ваня даже и не подумал убрать планшет. Он снова проиграл бой и очень разозлился: он хотел стать победителем, но, увы, не получалось.

И когда бабушка снова заглянула в комнату, мальчик сделал вид, что не слышит её замечания. Да, он знал, что бабушка обидится, но он потом извинится, а сейчас битва – вот самое главное! Бабушка заходила несколько раз, но Ваня или молчал, или просто махал рукой: некогда мне.

В конце концов бабушка не выдержала и спросила: "Ваня, я устала тебе говорить, что пора прекращать свою игру! У тебя уже глаза квадратные! Ты меня слышишь?"

Мальчик сказал: "Да, отстань, ты от меня! «Ваня, Ваня»..."

"Да как ты разговариваешь со мной", – дрожащим голосом заговорила бабушка.

"Как хочу, так и разговариваю! Это моя квартира, и я здесь хозяин! Не нравится – уходи!", – последние слова мальчик громко выкрикнул, а потом вскочил с дивана и захлопнул дверь своей комнаты перед лицом бабушки.

Он думал, что сейчас бабушка зайдёт его снова ругать, но услышал только тихие шаги за дверью. "Наверно, на кухню пошла, – подумал он, – вот и хорошо. Я как раз доиграю, а потом извинюсь. А сейчас не до этого: битва есть битва!"

Ваня весь ушёл в игру. Сколько прошло времени – он не знал. Турнир все ещё не заканчивался, а у планшета села батарея. Мальчик вспомнил, что оставил зарядное устройство в большой комнате.

"Ну и ладно, – сказал сам себе Ваня, – схожу за зарядным устройством, зайду на кухню к бабушке, извинюсь и продолжу!"

Ваня потянулся: все мышцы из-за того, что он долго сидел в одной позе, затекли. Он открыл дверь своей комнаты и удивился: в коридоре были другие обои, да и всё было по-другому.

"Бабуля здесь за пару часов всё переклеила что ли?", – удивился Иван.

Но когда мальчик вошёл на кухню, то никакой бабушки не было. А была только девочка лет восьми. Она сидела за столом и за обе щёки уплетала конфеты.

"Ты кто?" – спросил Ваня.

"Оля", – сказала девочка, – а вы, дядя, наверно, водопроводчик?

"Какой водопроводчик? Да и какой я тебе дядя, я тебя только на пару лет старше!", – ответил Ваня.

"Ха-ха! Ну вы и шутник! Я что, похожа на бабушку?". – весело рассмеялась девочка.

"Хватит мне морочить голову, – Ваня разозлился, – ты кто такая, и где моя бабушка?"

"Какая бабушка?" – поинтересовалась девочка.

"Инга Андреевна – моя бабушка! Ты мне объясни, ты как сюда попала, тебя бабушка впустила?", – спросил удивленно Ваня.

"Я здесь живу!". – девочка обиженно поджала губки. Затем, что-то припоминая, добавила: "Инга Андреевна, – где-то я это слышала... А, вспомнила! Мне папа рассказывал. Это моя прабабушка. Он ещё говорил, что она пропала до его рождения. Внук её старший обидел. Он так заигрался на планшете в игру, что никого не видел и не слышал. Его родители – мои бабушка и дедушка – пытались его привести в чувства, врачей вызывали, но всё бесполезно. Даже новую болезнь открыли – «зомбикомп» называется. С тех пор к этому мальчику, а он, кстати, мой дядя, перестали заходить. Врач сказал, что ему даже еда не нужна, ведь он переселился в виртуальный мир. На двери его комнаты даже табличку повесили: «Не входить!».

Ваня пришёл в ужас: "А бабушка, куда она пропала?". – спросил Ваня.

"Никто не видел её с того вечера. Стоп, а вы не из той комнаты с табличкой? Вы – мой дядя и виртуального мира?", – удивленно спросила Оля. Ваня ничего не ответил. Он выбежал из кухни и влетел в свою комнату. Взглянув на себя в зеркало, он не увидел мальчишку. На него из зеркала смотрел усталый бледный дедушка. "Что я натворил! – закричал Ваня. "Из-за какой-то глупой игры бабушка пропала! Бабушка, моя милая бабушка." – сквозь слезы бормотал Ваня. Ваня, рыдая, упал в кровать и от своего бессилия уснул. Ваня, Ваня. Кто-то осторожно трогал его за плечо. Открыв глаза, Ваня увидел свою бабушку.

"Бабушка, милая, ты вернулась!?", – спросил Ваня.

"Да я, никуда и не уходила, на кухне посидела, чтоб тебе не мешать...", – ответила бабушка.

"Ты мне не мешаешь. Бабушка, прости меня, я не хотел тебя обидеть, честно!", – извиняясь, проговорил Ваня.

Бабушка улыбнулась и ответила: "Я не сержусь на тебя, Ваня".

А мальчик подумал: «Как хорошо, что это был сон!».

Ваня, бывает, и сейчас может поиграть в какую-нибудь игру. Но теперь он помнит, что это всего лишь игра, а реальный мир намного интересней!

Вопросы для обсуждения:

- *Сравните отношение Вани до ... и после...*
- *Как отнеслась бабушка к поведению Вани?*
- *Для чего нужно слушаться и прислушиваться к словам старших?*

Дети обсуждают варианты поведения в этой ситуации.

Подведение итогов

Ведущий еще раз акцентирует внимание детей на ситуации, делает выводы:

1. Слушаться взрослых.
2. Словом и поступком можно обидеть человека.
3. Игры на компьютере, планшете, в телефоне должны быть дозированными по времени

Сценарий переработан по материалам книги: Уроки безопасности в школе (КИБЕРуроки). Сборник методических разработок. Материалы опубликованы на сайте Муниципального бюджетного учреждения «Центр психолого-педагогической, медицинской и социальной помощи» г. Перми

Приложение 4

Сценарий игры для учащихся средних и старших классов по теме «КИБЕРБЕЗОПАСНОСТЬ»

Сценарий занятия. ВАРИАНТ №1.

Часть 1. Мотивационная (до 5 минут).

Ведущий: Ребята, сегодня наше занятие посвящено кибербезопасности. Жизнь современного человека трудно представить без цифровых сервисов и приложений. Мы используем их для решения самых разных повседневных задач. При этом онлайн-среда связана не только с массой полезных возможностей, но и с рисками для безопасности пользователя. Именно поэтому так важно развивать собственную цифровую грамотность, знать о возможных рисках и владеть разными методами защиты, в том числе и технологическими. Также сфера кибербезопасности активно развивается, поэтому это ещё и перспективное направление для профессионального развития. О том, почему важно быть внимательными в цифровом мире, вам расскажет Наталья Ивановна Касперская – глава компании InfoWatch

Демонстрация видео с Н. И. Касперской.
https://www.youtube.com/watch?v=bWjO164NGN0

В продолжение занятия предлагаю вам погрузиться в настоящее состязание кибермошенников и специалистов по информационной безопасности. Мы проведем командную игру и научимся противостоять киберугрозам, разберём типичные сценарии атак и узнаем, как пользователи могут себя защищать.

Часть 2. Основная (до 20 минут).

Описание игры «Кибербезопасность».

Класс делится на две команды - «Кибермошенники» и «Специалисты по информационной безопасности» (как вариант, можно предложить разделить класс на несколько команд - специалистов по информационной безопасности; в этом варианте ведущий сам озвучивает все карточки с киберугрозами).

Каждая команда получает набор карточек с возможными действиями (см. дополнительные материалы).

Механика игры:

1. Ведущий выбирает одну из карточек-угроз (в любой последовательности) и озвучивает её.
2. Задача команды «Кибермошенники» – подобрать из набора карточек с действиями те, что злоумышленники типично используют в такой ситуации.
3. Задача команды «Специалисты по информационной безопасности» – оставить план защиты из своего набора карточек-действий и описать модель поведения пользователя.

На обсуждение отводится 3-5 минут.

4. «Кибермошенники» презентуют свой вариант плана «нападения», а «специалисты по информационной безопасности» - план защиты.

5. Ведущий оценивает, отражена ли атака (при необходимости используя ключи к ситуациям, в которых представлены примерные планы атаки и защиты), если да, то присваивает балл команде «специалистов по ИБ». Возможен вариант выбора команды экспертов из числа детей, которые будут качественно оценивать планы действий команд и при необходимости дополнять их.

Тематики заданий из сферы кибербезопасности, которые встречаются в игре:

- фишинговые ссылки;
- социальная инженерия;
- защита личной информации;
- защита профиля.

Пример проведения одного тура игры «Кибербезопасность».

Ведущий: Итак, герой нашей истории молодой ученый Алексей, который давно ведёт свой профиль, у него много подписчиков, интересные и полезные научно-популярные публикации – потерять аккаунт для него будет обидно.

Первая угроза: кибермошенники пытаются совершить кражу профиля Алексея через взлом логина/пароля. Команда «Кибермошенников» из своих карточек-действий составляет план атаки. Вам нужно отобрать те действия, которые злоумышленники типично используют в такой ситуации (можете добавить свои варианты действий). Команда «Специалистов по информационной безопасности» составляет из своих карточек план защиты. Ваша задача - собрать эффективную при такой угрозе модель поведения для пользователя (можете добавить свои варианты действий). Работа в группе 3-5 минут.

Ведущий: Время для обсуждения закончилось, давайте дадим слово каждой группе и узнаем, какие планы получились у команд. Слово команде «кибермошенников».

(Ответ представителей команды «кибермошенников».)

Теперь время ответить на атаку, вторая команда, вам слово.

(Ответ представителей команды «специалистов по информационной безопасности».)

С учетом планов команд я могу объявить победителей этого тура

(Ведущий комментирует ответы команд, при необходимости используя ключ с примерными планами атак и защиты, и называет команду-победителя первого тура.).

Следующие туры проходят по такой же схеме. Количество туров ведущий определяет самостоятельно.

Методический комментарий.

Игра может проходить и в формате, когда все обучающиеся играют роль специалистов по информационной безопасности. В таком варианте ведущий озвучивает угрозу и выводит на экран примерный план атаки кибермошенников (из ключа к ситуациям, представленным в приложении).

Задача – всем вместе найти вариант отражения атаки и обезопасить профиль молодого ученого Алексея.

Ведущий: Теперь вы знаете чуть больше о том, как действуют мошенники онлайн и как можно предусмотреть риски. Это была отличная тренировка для вас.

Предлагаю вам из тех полезных правил для пользователя, что мы сегодня услышали и из тех, что вы можете назвать самостоятельно, составить список - топ-5 полезных привычек кибербезопасности, которые каждый из нас может начать придерживаться с сегодняшнего дня.

Обучающиеся предлагают полезные привычки кибербезопасности, ведущий модерирует составление списка.

Ведущий: Спасибо вам за ваши идеи и комментарии, предлагаю подвести итоги занятия.

Часть 3. Заключение (до 5 минут).

Ведущий: Сегодня мы рассмотрели ситуации, когда пользователи не задумываются о последствиях своих действий и сами ставят себя под угрозу. Наша ответственность как пользователей цифровых сервисов – быть внимательными и стремиться повышать уровень своей цифровой грамотности. Теперь мы можем соблюдать простые правила и внедрять в свою жизнь полезные привычки кибербезопасности.

Сценарий занятия. ВАРИАНТ №2.

Часть 1. Мотивационная (до 5 минут).

Ведущий. Ребята, сегодня мы с вами поговорим о том, с чем постоянно сталкивается современный человек – это использование Интернета для решения повседневных задач: для учебы, общения, творчества, профессиональной деятельности. Возможности, доступные нам благодаря подключению к сети, могут принести много пользы, но там же можно столкнуться и с разными угрозами. Важно использовать доступ в Интернет с умом, эффективно и безопасно. Как и в реальной жизни, в Интернете стоит придерживаться некоторых правил, именно их мы сегодня с вами обсудим. О том, почему важно быть внимательными в цифровом мире, вам расскажет Наталья Ивановна Касперская – глава компании InfoWatch.

Демонстрация видео с Н. И. Касперской.

В продолжение занятия предлагаю вам разобрать несколько ситуаций, которые иногда случаются в сети. Вы выступите в роли сторонних наблюдателей и предложите свои решения.

Часть 2. Основная (до 20 минут).

Методический комментарий. В основной части представлено два вида заданий.

1. Интерактивное задание в форме анимационных фрагментов.

Рекомендуется групповой вариант работы, но возможен и фронтальный.

Порядок работы с каждой ситуацией-кейсом строится по следующему алгоритму:

- просмотр первой части видеофрагмента;

- обсуждение ситуации в группе и формулировка правил-выводов безопасного поведения;
- обсуждение правил-выводов безопасного поведения;
- проверка правила-вывода на основе просмотра второй части ролика.

2. Работа с заданиями-карточками, описывающими конкретные ситуации, с которыми обучающиеся могут столкнуться в реальной жизни.

Предложена следующая тематика ситуаций-кейсов:

1) фишинговые ссылки;
2) социальная инженерия;
3) защита личной информации;
4) защита профиля.

Ведущий: Мы посмотрим небольшой ролик с ситуацией, которая знакома каждому из вас, ведь все мы общаемся с друзьями и заводим новые знакомства. Смотрим первую часть ролика, думаем, что случилось и как можно было бы предотвратить эту ситуацию.

Видео-кейс № 1. Фишинговые ссылки. Видео с сайта: https://razgovor-cdn.edsoo.ru/media/ie/media-1/index.html?back_url=/topic/34/grade/1011/

Друзья, предлагаю вам разделиться на группы и попробовать сформулировать правила, при соблюдении которых можно было бы избежать подобной ситуации.

(Ребята делятся на мини-группы по 4 человека и обсуждают возможные правила. На эту работу отводится 1-2 минуты.)

А теперь давайте обсудим получившиеся у вас правила. Что вы можете посоветовать делать в подобных ситуациях?

(От каждой группы один обучающийся предлагает одно правило. Ведущий фиксирует на доске.)

Мы с вами обсудили, что пошло не так в ситуации Вани, теперь давайте досмотрим ролик и узнаем, какие цифровые привычки и правила нам предлагают создатели ролика, чтобы не попасться на удочку мошенников.

Продолжение демонстрации видео-кейса № 1. Фишинговые ссылки.

Методический комментарий. Дополнительно в этом кейсе можно обсудить значение слова «фишинговая» ссылка. Действия мошенников называют «фишингом» из-за английского слова «фиш», что означает «рыба» или «рыбачить», то есть буквально мошенники стараются «выудить» информацию у пользователя.

Есть ещё одна ситуация, которую описывает в своем блоге герой мультфильма. Давайте посмотрим его, следите за сюжетом и поведением персонажей.

Видео-кейс № 2. Социальная инженерия.

Как вы считаете, какую ошибку допустил герой мультфильма? Каких правил надо придерживаться, чтобы не попадать в ловушки, в которые попала Кира? Давайте, как и в предыдущем случае, сначала обсудим это в группах, а потом все вместе.

(Работа в группах, обсуждение и последующие ответы обучающихся.)

Вы отлично справились, давайте досмотрим видео и узнаем, какие правила поведения в интернете мы с вами должны запомнить.

Продолжение демонстрации видео-кейса № 2. Социальная инженерия.

Методический комментарий. Социальная инженерия – разные виды манипуляций и обмана, цель которых заставить человека раскрыть личные данные, получить доступ к его личной и финансовой информации.

Я предлагаю вам посмотреть другую ситуацию, которая произошла с любительницей классического искусства Ариной. Как и в прошлый раз, будьте внимательны и отмечайте поведение персонажей, чтобы ответить на мой вопрос. Смотрим.

Видео-кейс № 3. Защита личной информации.

Как думаете, что произойдет дальше? Что в этой ситуации в поведении Арины вы считаете опасным? Есть ли здесь ошибка? На что мы должны обращать внимание, чтобы не попасть в такие же ситуации, как Арина? Поработайте, пожалуйста, в тех же группах, а потом мы обменяемся с вами мыслями.

(Работа в группах, обсуждение, ответы обучающихся.)

Ребята, вы молодцы, сейчас мы посмотрим развязку, узнаем не только, что случилось с Ариной, но и то, как обезопасить свою личную информацию и какие правила в этом помогут.

Продолжение демонстрации видео-кейса № 3. Защита личной информации.

Сейчас мы посмотрим ещё один ролик, где рассказывается история Жанны. Предлагаю узнать, что с ней приключилось и как друзья смогли прийти на помощь. Следите за сюжетом, у меня будет вопрос для вас.

Видео-кейс № 4. Защита профиля.

Как вы считаете, почему в аккаунте появилась такая информация? Как друзья Жанны поступят дальше? Что важно помнить и соблюдать, чтобы сохранить свой профиль в безопасности? Попробуйте составить правила, которые помогут вам обезопасить ваш профиль в социальной сети.

(Работа в группах, обсуждение, ответы обучающихся.)

Вы хорошо справились с заданием. Теперь время узнать, как правильно защищать свой профиль, какие правила для этого нужно знать.

Продолжение демонстрации видео-кейса № 4. Защита профиля.

Ребята, давайте ещё раз назовем правила, которые мы узнали на нашем занятии сегодня? Почему важно их соблюдать, как вы думаете?

(Ответы обучающихся, обсуждение.)

Работа с заданиями-карточками

Ведущий: Ребята, предлагаю вам посмотреть на знакомые действия и ситуации со стороны. Сыграем в игру и проверим, как хорошо вы умеете пользоваться цифровыми сервисами и приложениями.

Методический комментарий. Ведущий делит обучающихся на команды (3-4 команды). Каждая команда получает карточку с описанием ситуации, дополнительно карточка выводится на экран (при наличии технических условий). Также возможен и фронтальный формат работы.

Командам необходимо ответить на два вопроса:

1. Какую ошибку герой или герои ситуации допустили?
2. Какие правила для пользователя можно вывести из этой ситуации?

На обсуждение каждой ситуации дается 3 минуты. Дальше каждая группа представляет результаты обсуждения.

Ведущий сверяет полученные результаты с ключом к заданию.

Карточка-задание №1

Ваша одноклассница Катя ведет видеоблог про образ жизни, увлечения, учебу. Она делится всем тем, чем живет современный школьник. Катя выкладывает на свой канал рассказы о своей жизни, увлечениях, занятиях. В очередном выпуске своего блога Катя решает попробовать один из популярных форматов – прямой эфир с обзором комнаты. В начале эфира Катя сообщает, что сегодняшнюю встречу она ведет из дома, называя свой адрес. В одном из кадров она показывает, что есть у неё в комнате, как она всё украсила к Новому году, где делает уроки, какие у неё хобби, заходит в комнату к брату, который с друзьями разучивает на гитаре новую песню. Во время эфира в кадр попадает фамильная реликвия – шкатулка с уникальными украшениями.

Ведущий: Подумайте, в чем могли быть ошибки Кати? Что она сделала не так, и о чем нужно помнить, когда что-то выкладываешь в сеть?

Работа обучающихся в группах.

Ведущий: Время для обсуждения закончилось, давайте обсудим, какие ошибки совершила Катя и что можно ей посоветовать?

Ответы обучающихся (по одному пункту поочерёдно от каждой группы), комментарии и дополнения педагога в соответствии с ключом к заданию.

Ключ к заданию.

- не оставляйте информацию о себе и родственниках в открытом доступе: домашний адрес, телефоны, номер школы, свой возраст, геолокации;
- в прямом эфире, где у вас нет заранее подготовленного текста и сценария вы говорите все, что придет в голову и ненамеренно можете сообщить информацию потенциально опасную;
- не размещайте фото или видео, на которых видно обстановку вашей квартиры, все то, что может притягивать мошенников;
- не выкладывайте фото или видео с участием ваших родственников, друзей без их разрешения;
- используйте настройку «для близких друзей», чтобы контролировать доступ к своему профилю и информации о себе.

Ведущий: Отлично, спасибо за ваши ответы! На данном примере стало понятно, что даже в таких знакомых ситуациях могут быть подводные камни.

Дополнительно к этому заданию обучающимся можно предложить набор фотографий и обсудить, стоит ли размещать их в социальных сетях, и объяснить почему.

Карточка-задание №2.1

(команды получают разные варианты карточек).

Аня, ученица 6 класса, недавно ей исполнилось 11 лет. У Ани есть любимый пес Джек и кот Персик. Аня регистрирует новую страничку в социальной сети, т. к. старая была захвачена злоумышленниками. Она решает, какой пароль поставить для своего нового аккаунта в этой социальной сети. Вот варианты, из которых она выбирает:

1. persik1234
2. ANNall
3. A!-2na1234

Аня останавливается на первом варианте пароля и отказывается от опции установить дополнительное подтверждение входа по почте или номеру телефона.

Карточка-задание №2.2

Аня, ученица 6 класса, недавно ей исполнилось 11 лет. У Ани есть любимый пес Джек и кот Персик. Аня регистрирует новую страничку в социальной сети, т. к. старая была захвачена злоумышленниками. Она решает, какой пароль поставить для своего нового аккаунта в этой социальной сети. Вот варианты, из которых она выбирает:

1. Jack4321
2. ANNall
3. A!-7n9aj234

Аня останавливается на втором варианте пароля и отказывается от опции установить дополнительное подтверждение входа по почте или номеру телефона.

Карточка-задание №2.3

Аня, ученица 6 класса, недавно ей исполнилось 11 лет. У Ани есть любимый пес Джек и кот Персик. Аня регистрирует новую страничку в социальной сети, т. к. старая была захвачена злоумышленниками. Она решает, какой пароль поставить для своего нового аккаунта в этой социальной сети. Вот варианты, из которых она выбирает:

1. 123456789
2. ANNA_JACK
3. A!-2na1234

Аня останавливается на первом варианте пароля и отказывается от опции установить дополнительное подтверждение входа по почте или номеру телефона.

Карточка-задание №2.4

Аня, ученица 6 класса, недавно ей исполнилось 11 лет. У Ани есть любимый пес Джек и кот Персик. Аня регистрирует новую страничку в социальной сети, т. к. старая была захвачена злоумышленниками. Она выбирает, какой пароль поставить для своего нового аккаунта в этой социальной сети. Вот варианты, из которых она выбирает:

1. 123456789
2. ANNAPERSIK
3. A!-7n9aj234

Аня останавливается на втором варианте пароля и отказывается от опции установить дополнительное подтверждение входа по почте или номеру телефона.

Ведущий: Обсудите, какие из вариантов паролей надежные, какие нет, и почему? Надёжный ли пароль выбрала Аня? Сформулируйте правила, о которых нужно помнить при создании паролей.

Работа обучающихся в группах.

Ведущий: Время для обсуждения закончилось, давайте обсудим надежность паролей, представленных на карточках, и выбор Ани.

Ответы обучающихся, комментарии и дополнения учителя в соответствии с ключом к заданию.

Ключ к заданию.

- на всех карточках последний пароль подходит под критерии надежного пароля: содержит специальные знаки, заглавные буквы, цифры, при этом комбинация не связана с пользователем;
- не следует использовать общеизвестные факты для создания паролей (ваши имя, возраст, дату рождения, клички животных, имена близких родственников и т. п.);
- легко взломать пароли, состоящие только из цифр или букв;
- не следует использовать элементарные пароли типа 123456..., абвгд...;
- подключайте дополнительное подтверждение входа — двухфакторную аутентификацию.

Проверить надежность пароля можно на сайте 2ip.ru/passcheck. Предлагаю проверить, за какой период можно взломать пароли, которые были представлены у вас на карточках.

Обучающиеся проверяют надежность паролей persik1234 - ненадежный, возможно взломать за 254 часа ANNal 1 – ненадежный, возможно взломать за 14 секунд Jack4321 – ненадежный, возможно взломать за 910 минут 123456789 – ненадежный, возможно взломать за 0 секунд ANNA_JACK - ненадежный, возможно взломать за 1889 часов ANNAPERSIK - ненадежный, возможно взломать за 588 минут A!-2na1234 – надежный, может быть взломан за 6810 лет A!-7n9aj234 – надежный, может быть взломан за 544770 лет

Часть 3. Заключение (до 5 минут).

Ведущий: Сегодня мы рассмотрели ситуации, когда пользователи не задумываются о последствиях своих действий и сами ставят себя под угрозу. Наша ответственность как пользователей цифровых сервисов – быть внимательными и стремиться повышать уровень своей цифровой грамотности. Теперь мы можем соблюдать простые правила и внедрять в свою жизнь полезные привычки кибербезопасности.

Приложение

Карточки-угрозы

- кража профиля пользователя через взлом логина/пароля
- манипуляция, чтобы пользователь самостоятельно передал свои данные

- получение доступа к сохраненным личным данным/данным банковской карты
- продуманное мошенничество на основе доступной информации о человеке
- мошенничество через подменные/анонимные профили
- мошенничество на основе утечки данных пользователя на сторонних ресурсах

Набор карточек для группы «Специалисты по информационной безопасности»

- Проверьте профиль человека, действительно ли такой человек существует? Попросите незнакомца поподробнее рассказать о себе.
- Запросите больше информации о том, что вам предлагают. Проверьте официальный сайт компании, от лица которой вам пишут, и уточните информацию о контактах службы поддержки.
- Воспользуйтесь функцией «Пожаловаться» на комментарий, человека, пост в службу модерации в социальной сети или «Добавить в спам» в своем почтовом ящике.
- Авторизуйтесь через свои аккаунты и вводите данные только на официальных сайтах.
- Прежде чем знакомиться в социальных сетях, внимательно изучите страницу пользователя. Есть ли у него друзья, посты, отметки на странице? Или аккаунт выглядит подозрительно?
- Не переходите по ссылкам от малознакомых людей.
- Проверьте адресную строку сайта. Внимательно изучайте любой сайт, на котором вам предлагается ввести какие-либо конфиденциальные данные.
- Сравните предлагаемую цену с другими сайтами: обычно цены на поддельных сайтах подозрительно низкие.
- Не публикуйте персональные данные – например, домашний адрес, телефон, геолокации.
- Используйте разные пароли на различных сервисах. Выбирайте сложные пароли, не используйте ваши имя и дату рождения при создании пароля.
- Не поддавайтесь агрессии и не ведитесь на провокации.
- Настройте двухфакторную аутентификацию в соцсетях, чтобы аккаунт не перешел в руки недоброжелателей. Привяжите актуальный номер вашего телефона к профилю, а также укажите ваши настоящие имя, фамилию, установите реальное фото: так восстановить профиль в случае взлома будет проще.
- Выделите время и разберитесь в настройках приватности своего профиля во всех соцсетях.
- Защищайте всю информацию, даже если думаете, что она не важна.
- Делясь важной или личной информацией, используйте фильтр «Только для друзей». Не делитесь в интернете важной информацией: фото паспорта и других документов, билетов, посадочных талонов и др.

Набор карточек для группы «Кибермошенники»

- Проследить за открытой информацией в профиле, изучить подробности жизни человека.
- Спровоцировать на эмоции, вызвать интерес у пользователя, использовать приём ограниченного времени.
- Начать торопить пользователя, чтобы не дать разобраться в происходящем.
- Разослать спам-сообщение друзьям пользователя.
- Создать и оформить сайт так, чтобы он был очень похож на официальный, где пользователю предлагается оплатить штраф или просто купить какой-то товар или услугу.
- Создать копию хорошо известного официального сайта, но в адресной строке использовать буквы, схожие по написанию с настоящим адресом.
- Создать профиль, похожий на официальный профиль администрации сайта. Выдать себя за администраторов и модераторов сайта, чтобы получить данные или пароль пользователя.
- Отправить человеку сообщение якобы от лица организации (создать копию профиля этой организации) о серьезной проблеме: например, сообщить о штрафе или о том, что родственник попал в беду.
- Представиться сотрудником технической поддержки и выманить конфиденциальные данные или склонить к выполнению сомнительных действий.
- Предложить продолжить знакомство офлайн и отправить ссылку для покупки билетов на мероприятие – например, в кино.
- Поставить на поддельном сайте низкую заманчивую цену на популярный товар, чтобы побудить ввести данные банковской карты.
- Совершить покупки с аккаунта пользователя, если данные банковской карты сохранены в профиле и не требуют дополнительного подтверждения (двухфакторной аутентификации).

Ключи к ситуациям угрозы (примерные планы атаки и защиты)

Угроза: кража профиля пользователя через взлом логина/пароля.

Пример атаки:

1. Создать профиль, похожий на официальный профиль администрации сайта. Выдать себя за администраторов и модераторов сайта, чтобы получить данные или пароль пользователя.
2. Начать торопить пользователя, чтобы не дать разобраться в происходящем.
3. Спровоцировать на эмоции, вызвать интерес у пользователя, использовать прием ограниченного времени.
4. Совершить покупки с аккаунта пользователя, если данные банковской карты сохранены в профиле и не требуют дополнительного подтверждения (двухфакторной аутентификации).

Пример защиты:

1. Запросите больше информации о том, что вам предлагают. Проверьте официальный сайт компании, от лица которой вам пишут и уточните информацию о контактах службы поддержки.
2. Воспользуйтесь функцией «Пожаловаться» на комментарий, человека, пост в службу модерации в социальной сети или «Добавить в спам» в своем почтовом ящике.
3. Используйте разные пароли на различных сервисах. Выбирайте сложные пароли, не используйте ваши имя и дату рождения при создании пароля.
4. Настройте двухфакторную аутентификацию в соцсетях, чтобы аккаунт не перешел в руки недоброжелателей. Привяжите актуальный номер вашего телефона к профилю, а также укажите ваши настоящие имя, фамилию, установите реальное фото: так восстановить профиль в случае взлома будет проще.

Угроза: манипуляция, чтобы пользователь самостоятельно передал свои данные.

Пример атаки:

1. Создать и оформить сайт так, чтобы он был очень похож на официальный, где пользователю предлагается оплатить штраф или просто купить какой-то товар или услугу.
2. Поставить на поддельном сайте низкую заманчивую цену на популярный товар, чтобы побудить ввести данные банковской карты.
3. Спровоцировать на эмоции, вызвать интерес у пользователя, использовать прием ограниченного времени.

Пример защиты:

1. Проверьте адресную строку сайта. Внимательно изучайте любой сайт, на котором вам предлагается ввести какие-либо конфиденциальные данные.
2. Сравните предлагаемую цену с другими сайтами: обычно цены на поддельных сайтах подозрительно низкие.
3. Авторизуйтесь через свои аккаунты и вводите данные только на официальных сайтах.

Угроза: получение доступа к сохраненным личным данным/данным банковской карты.

Пример атаки:

1. Предложить продолжить знакомство офлайн и отправить ссылку для покупки билетов на мероприятие – например, в кино.
2. Создать копию хорошо известного официального сайта, но в адресной строке использовать буквы, схожие по написанию с настоящим адресом.
3. Совершить покупки с аккаунта пользователя, если данные банковской карты сохранены в профиле и не требуют дополнительного подтверждения (двухфакторной аутентификации).

Пример защиты:

1. Прежде чем знакомиться в социальных сетях, внимательно изучите страницу пользователя. Есть ли у него друзья, посты, отметки на странице? Или аккаунт выглядит подозрительно?

2. Проверьте профиль, человека, действительно ли такой человек существует? Попросите незнакомца поподробнее рассказать о себе.
3. Не переходите по ссылкам от малознакомых людей.
4. Защищайте всю информацию, даже если думаете, что она не важна.

Угроза: продуманное мошенничество на основе доступной информации о человеке.

Пример атаки:

1. Создать профиль, похожий на официальный профиль администрации сайта. Выдать себя за администраторов и модераторов сайта, чтобы получить данные или пароль пользователя.
2. Проследить за открытой информацией в профиле, изучить подробности жизни человека.
3. Разослать спам-сообщение друзьям пользователя.

Пример защиты:

1. Не публикуйте персональные данные – например, домашний адрес, телефон, геолокации.
2. Делясь важной или личной информацией, используйте фильтр «Только для друзей». Не делитесь в интернете важной информацией: фото паспорта и других документов, билетов, посадочных талонов и др.
3. Настройте двухфакторную аутентификацию в соцсетях, чтобы аккаунт не перешел в руки недоброжелателей. Привяжите актуальный номер вашего телефона к профилю, а также укажите ваши настоящие имя, фамилию, установите реальное фото: так восстановить профиль в случае взлома будет проще.
4. Не поддавайтесь агрессии и не ведитесь на провокации.

Угроза: мошенничество через подменные/анонимные профили.

Пример атаки:

1. Проследить за открытой информацией в профиле, изучить подробности жизни человека.
2. Отправить человеку сообщение якобы от лица организации (создать копию профиля этой организации) о серьезной проблеме: например, сообщить о штрафе или о том, что родственник попал в беду.
3. Создать и оформить сайт так, чтобы он был очень похож на официальный, где пользователю предлагается оплатить штраф или просто купить какой-то товар или услугу.
4. Начать торопить пользователя, чтобы не дать разобраться в происходящем.

Пример защиты:

1. Запросите больше информации о том, что вам предлагают. Проверьте официальный сайт компании, от лица которой вам пишут и уточните информацию о контактах службы поддержки.
2. Не поддавайтесь агрессии и не ведитесь на провокации.
3. Делясь важной или личной информацией, используйте фильтр «Только для друзей». Не делитесь в интернете важной информацией: фото паспорта и других документов, билетов, посадочных талонов и др.

4. Выделите время и разберитесь в настройках приватности своего профиля во всех соцсетях.
5. Воспользуйтесь функцией «Пожаловаться» на комментарий, человека, пост в службу модерации в социальной сети или «Добавить в спам» в своем почтовом ящике.

Угроза: мошенничество на основе утечки данных пользователя на сторонних ресурсах.

Пример атаки:

1. Совершить покупки с аккаунта пользователя, если данные банковской карты сохранены в профиле и не требуют дополнительного подтверждения (двухфакторной аутентификации).
2. Разослать спам-сообщение по друзьям пользователя.

Пример защиты:

1. Авторизуйтесь через свои аккаунты и вводите данные только на официальных сайтах.
2. Не переходите по ссылкам от малознакомых людей.
3. Проверьте адресную строку сайта. Внимательно изучайте любой сайт, на котором вам предлагается ввести какие-либо конфиденциальные данные.
4. Используйте разные пароли на различных сервисах. Выбирайте сложные пароли, не используйте ваши имя и дату рождения при создании пароля.
5. Защищайте всю информацию, даже если думаете, что она не важна.

Информация переработана с сайта
https://razgovor.edsoo.ru/topic/34/grade/1011/

Приложение 5

Памятка для родителей об информационной безопасности детей в возрасте от 13 до 15 лет

1. Создайте список домашних правил посещения Интернета при участии подростков и требуйте безусловного его выполнения. Обговорите с ребенком список запрещенных сайтов («черный список»), часы работы в Интернете, руководство по общению в Интернете (в том числе в чатах).
2. Компьютер с подключением к сети Интернет должен находиться в общей комнате.

3. Не забывайте беседовать с детьми об их друзьях в Интернете, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы.
4. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
5. Необходимо знать, какими чатами пользуются Ваши дети. Поощряйте использование модерируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.
6. Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из сети Интернет.
7. Приучите детей не выдавать свою личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.
8. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
9. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами рассказали вам, о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.
10. Расскажите детям о порнографии в Интернете. Помогите им защититься от спама. Научите подростков не выдавать в Интернете своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.
11. Приучите себя знакомиться с сайтами, которые посещают подростки.
12. Научите детей уважать других в интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде – даже в виртуальном мире.
13. Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.

14. Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.

Если вы еще не знаете, как поговорить с ребенком об Интернете, обращайтесь на линию помощи «Дети Онлайн».