ПАРЛАМЕНТАРИЗМ
ИНСТИТУТЫ

СБОРНИК
материалов круглого стола: «Защита и безопасность детей в интернете», проведенного 25 июля 2025 года

г. Астана, 2025 год

Содержание

Сулеймен Ляззат Жанылыскызы,
заместитель директора Института парламентаризма

ПРИВЕТСТВЕННОЕ СЛОВО

Құрметті әріптестер,
қадірлі қонақтар мен дөңгелек үстелге қатысушылар!

Бүгінгі басқосуымыз – қоғам назарындағы өзекті әрі маңыздылығы күн санап артып келе жатқан мәселеге арналған. Балаларды интернет кеңістігінде қорғау – заманауи цифрлық дәуірдің алдыңғы қатарлы тақырыптарының бірі.

Технологиялық дамудың қарқыны балалық шақтың сипатына да ықпал етуде: бүгінде виртуалды орта баланың күнделікті өмірінің бір бөлшегіне айналды. Бұл – бала білім алатын, өсіп-өнетін, қарым-қатынас жасайтын және өзін танып-білетін орта. Алайда интернет тек игіліктер алаңы ғана емес, сонымен бірге баланың әлсіздеу психикасына түрлі қауіп төндіруі мүмкін орта болып отыр. Өкінішке орай, бұл қауіп-қатерлерге қарсы тұратын табиғи қорғаныс жүйесі балаларда әлі толық қалыптаспаған.

Цифрлық мүмкіндіктер кеңейген сайын, біз алаңдатарлық құбылыстармен де жиі бетпе-бет келіп отырмыз: кибербуллинг, психологиялық қысым, балаларды қауіпті әрекеттерге тарту, жеке шекаралардың бұзылуы мен құпиялықтың жоғалуы. Мұның бәрі бізден — ересектерден, мамандар мен заң шығарушы қауымнан — жай ғана үстірт әрекет емес, терең пайым мен шынайы ізгілікке негізделген саясат жүргізуді талап етеді.

Қазақстан Республикасының Президенті Қасым-Жомарт Кемелұлы Тоқаевтың дәл атап көрсеткеніндей, «Балалардың үйлесімді және жан-жақты дамуы үшін жағдай жасау, жас азаматтардың құқықтарын қорғау және денсаулығын қорғау әрқашан мемлекетіміздің басты басымдығы болып қала бермек...».

Соңғы жылдары Қазақстан осы бағытта берік нормативтік-құқықтық негіз қалыптастырды. 2018 жылы балаларды денсаулығы мен дамуына зиян келтіретін ақпараттан қорғау туралы заң қабылданып, цифрлық қауіпсіздікке жүйелі түрде қарауға негіз қалады. Контентті саралау тетіктері әзірленді, жас ерекшелігіне сай шектеулер енгізілді, ақпараттық гигиена стандарттары бекітілді.

Дегенмен, заман тынысы жылдам өзгеріп жатыр. Пандемия кезіндегі қашықтан оқытуға көшу балаларды одан әрі осал етті. UNICEF Kazakhstan Kids Online зерттеуіне сәйкес, әр алтыншы бала жағымсыз контентке тап болса, әр бесінші бала — кибербуллингтің құрбанына айналған. Осы сын-қатерлерге жауап ретінде заңнама нақтыланды: 2022 жылы «кибербуллинг» ұғымы енгізілді, 2023 жылы — тиісті өтініштерді беру тетігі пайда болды, ал 2024 жылы — жәбірлеу үшін әкімшілік жауапкершілік қарастырылды. Бұл өзгерістердің дайындалуына Парламентаризм институты да белсенді атсалысты: ол заңнамалық бастамаларды сүйемелдеп қана қоймай, ведомствоаралық диалог алаңы ретінде де қызмет етіп келеді.

Алайда, біздің басты мақсатымыз — баланы шектеу немесе оны виртуалды кеңістіктен оқшаулау емес. Керісінше, оның еркін дамуына мүмкіндік беретін, қауіпсіз, ашық әрі қолдау көрсететін орта қалыптастыру. Мұндай ұстаным халықаралық тәжірибеде де көрініс табуда: Ұлыбританиядағы жас ерекшелігіне сай дизайн кодексінен бастап, ЕО, АҚШ, Жапония мен Финляндияға дейін көптеген елдерде цифрлық сауаттылықты арттыру, алгоритмдердің ашықтығы мен зиянды контенттің алдын алу мәселелері мемлекеттік стратегияның ажырамас бөлігіне айналған.

Бұл мысалдар бізге маңызды бір ақиқатты көрсетеді: цифрлық қауіпсіздік — бұл тыйым салу емес, бұл — мәдениет, жүйелі көзқарас және өзара сенім. Қазақстан да дәл осы бағытты таңдады.

Бүгінгі талқылаудың құндылығын арттырып тұрған тағы бір жайт — оның әр тарапты қамтыған, кешенді форматы. Бұл залда мемлекеттік органдардың өкілдері, халықаралық ұйымдар, IT саласының мамандары, педагогтер, заңгерлер және, ең бастысы — балалармен күнделікті жұмыс істеп жүрген жандар жиналып отыр. Осындай ашық пікір алмасу арқылы біз жай проблемаларды тізбектеумен шектелмей, нақты шешімдерге қадам жасай аламыз: заңнаманы жетілдіруден бастап, ерте анықтау, алдын алу және психологиялық қолдау тәжірибелерін енгізуге дейін.

Парламентаризм институты үшін балалардың цифрлық қауіпсіздігі — жай ғана зерттеу бағыты емес, күн тәртібіндегі нақты әрі өзекті міндет. Бұл — отбасының, мектептің, мемлекеттің, бизнестің және балалардың өздерінің күш біріктіруін қажет ететін ортақ іс. Біз бала технологиялар дамыған әлемде қауіп-қатермен бетпе-бет келмей, сол технологиялар оның тұлғалық қалыптасуы мен еркін дамуына қызмет етуі тиіс екендігін терең сезінеміз. Оның құқықтары тек көшеде ғана емес, интернет кеңістігінде де толық қорғалу керек.

Баршаңызға шынайы жанашырлықтарыңызға, кәсіби белсенділіктеріңізге және балалар тағдырына бейжай қарамай, терең ой қосу үшін келгендеріңізге алғыс айтамын. Бүгінгі пікірлер, ұсыныстар мен идеялар — қамқорлық қағидаға, ал қауіпсіздік қалыпты өмір сүру нормасына айналған болашақтың қауіпсіз цифрлық кеңістігін қалыптастыруға бағытталған нақты үлес болатынына кәміл сенемін.

Летисия Баззи-Вейл,
Заместитель представителя
Детского фонда ООН (ЮНИСЕФ)
в Казахстане

ПРИВЕТСТВЕННОЕ СЛОВО

Уважаемые участники, коллеги!

Для меня большая честь обратиться к вам сегодня на этом важном круглом столе, посвящённом вопросам защиты детей и безопасности в Интернете.

Я сердечно приветствую каждого из вас и выражаю благодарность Институту парламентаризма за инициативу и проведение столь значимого диалога.

По мере того, как Казахстан продолжает цифровую трансформацию, мы наблюдаем впечатляющие возможности для инноваций и расширения связей. Однако эти достижения сопровождаются новыми и постоянно меняющимися рисками — особенно для детей и подростков. Рост киберпреступности и онлайн-эксплуатации детей представляет собой серьёзный вызов, требующий комплексного, устойчивого и основанного на фактах законодательного и политического реагирования.

Позвольте привести лишь несколько тревожных фактов:

Каждую секунду в мире фиксируется случай сексуального насилия над ребёнком в Интернете. Только в 2024 году было удалено 300 000 веб-страниц с материалами, связанными с сексуальным насилием над детьми. Это на 5% больше по сравнению с 2023 годом.

Кроме того, недавние исследования, в том числе проведённое при поддержке ЮНИСЕФ исследование Kazakhstan Kids Online (2023), демонстрируют тревожный уровень кибербуллинга, пересечения с сексуальным контентом, а также случаи онлайн-эксплуатации.

Эти цифры — не просто статистика. Это призыв к действию для всех нас, кто работает над защитой прав и благополучием детей.

Казахстан уже предпринял важные шаги. В частности, создание специализированного Департамента по борьбе с киберпреступностью в структуре Министерства внутренних дел — это значимое достижение. Однако противодействие онлайн-угрозам для детей требует также прочной нормативной правовой базы, межсекторальной координации и активного участия законодательных органов.

Именно здесь ключевую роль играет Институт парламентаризма. Будучи ведущим центром исследований, анализа политики и наращивания потенциала законодательных структур Казахстана, ваша вовлечённость имеет решающее значение для разработки мер реагирования на цифровые риски, пересмотра национального законодательства и продвижения его соответствия международным стандартам.

Для ЮНИСЕФ большая честь сотрудничать с Правительство Республики Казахстан в рамках двухлетней программы «Защита детей от онлайн насилия, жесткого обращения и эксплуатации в Казахстане», реализуемой при поддержке глобальной инициативой Safe Online. Программа нацелена на повышение осведомлённости для профилактики онлайн насилия в отношении детей, укрепление законодательства и институциональных механизмов защиты детей от онлайн-угроз.

ЮНИСЕФ готов и далее поддерживать усилия страны, предоставляя доступ к лучшим международным практикам, способствуя укреплению нормативно-правовой базы по защите детей в цифровой среде, а также усилению экспертного потенциала законотворческих органов в области цифровой безопасности и прав ребёнка.

Только вместе мы сможем обеспечить, чтобы законодательство и политика Казахстана поспевали за стремительно меняющимся цифровым миром, ставя безопасность и благополучие детей в центр внимания.

Ещё раз благодарю Институт парламентаризма за вашу приверженность и лидерство в вопросах защиты детей в цифровой среде. Мы высоко ценим наше партнёрство и с нетерпением ждём продолжения сотрудничества.

КӨП РАХМЕТ! Благодарю вас.

Саин Аружан,
Эксперт в сфере защиты прав детей, общественный деятель, руководитель общественного фонда «Добровольное общество «Милосердие»

СОЦИАЛЬНЫЕ СЕТИ И ДЕТИ: РИСКИ, ВОЗМОЖНОСТИ И БАЛАНС ИНТЕРЕСОВ

Уважаемые коллеги, дорогие друзья!

Я очень рада приветствовать всех участников круглого стола и особенно наших соратников по делу защиты прав детей. Тема сегодняшнего обсуждения чрезвычайно актуальна, ведь цифровая среда стала частью жизни каждого ребёнка. Интернет открывает перед ними огромные возможности: образовательные, познавательные, развивающие. При правильном подходе он может стать большим помощником в обучении и познании мира.

Но мы не можем забывать, что вместе с этим интернет несёт и серьёзные угрозы. Дети могут подвергаться риску вовлечения в опасные игры, контактировать с недобросовестными взрослыми или просто бесцельно проводить часы за короткими роликами, теряя интерес к реальной жизни. Эти риски сегодня обсуждаются во всём мире, и задача каждого государства — выработать такие механизмы, которые позволят сохранить баланс: дать доступ к полезному и одновременно защитить от опасного.

Позвольте подчеркнуть: мы должны сосредоточиться не только на том, чтобы «тушить пожары», когда беда уже случилась. Нам нужно действовать профилактически. Я глубоко убеждена: если ребёнок занят в реальной жизни, если у него есть кружки, спортивные секции, любимое дело, то времени и потребности уходить в виртуальное пространство у него просто не остаётся.

Именно поэтому я считаю реформу, инициированную президентом Касым-Жомартом Токаевым в 2020 году, одной из самых важных для будущего детей. Тогда в закон о культуре и спорте были внесены изменения, появился государственный заказ на кружки и секции. За первый год около 500 тысяч детей получили возможность бесплатно заниматься спортом и творчеством. Более того, по статистике МВД подростковая преступность за этот же период сократилась в два раза. Это наглядное доказательство того, что вовлечение детей в полезные занятия реально снижает риски, в том числе связанные с интернетом.

Однако мы видим и сопротивление этой реформе, ведь речь идёт о перераспределении значительных бюджетов. Но я убеждена: именно такие вложения в человеческий капитал — это лучшая инвестиция государства в своё будущее.

Отдельно хочу подчеркнуть роль родителей. Сегодня многие из них не знают о тех возможностях, которые предлагают IT-компании для ограничения и контроля доступа ребёнка к интернету. Образование родителей в этой сфере не менее важно, чем просвещение самих детей. Мы должны объяснять им, какие существуют риски, и давать инструменты для их предотвращения.

Наконец, хочу сказать о роли общества и СМИ. Очень важно показывать детям, что их реальные достижения — спортивные, творческие, научные — ценятся и признаны. Это даёт им стимул реализовывать себя в жизни, а не искать сомнительное внимание в виртуальном пространстве.

Подводя итог, хочу отметить: защита детей в интернете невозможна без комплексного подхода. Это и государственные реформы, и поддержка родителей, и образовательные программы, и внимание общества. Если мы создадим условия, при которых детям будет интереснее жить в реальном мире, чем в виртуальном, мы сможем свести к минимуму все цифровые риски.

Спасибо за внимание!

Герко Василий Сергеевич,
Директор Представительства АО «Национальные информационные технологии» по г. Астана

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДЕТЕЙ: ОТ АНАЛИЗА УГРОЗ К ПЕРВЫМ ЦИФРОВЫМ РЕШЕНИЯМ

Цифровизация и новые вызовы

С 2023 года в Казахстане активно реализуется курс на цифровизацию жизненных ситуаций: более 250 инициатив упростили и защитили ключевые процессы в жизни граждан — от рождения ребёнка и получения социальных выплат до медицины и бизнеса.

Но вместе с возможностями цифровая среда принесла и новые угрозы. На Национальном курултае Глава государства отдельно остановился на пяти вызовах современного общества:

— лудомания;
— наркомания;
— вовлечение подростков в криминальные схемы;
— информационные атаки;
— снижение моральных ориентиров.

Самой уязвимой группой здесь остаются дети. Интернет усиливает каждую из этих угроз и становится катализатором негативных процессов.

Анализ рисков для детей

Сегодня дети — одни из самых активных пользователей интернета. Но именно они чаще всего сталкиваются с:

— кибербуллингом и травлей;
— вовлечением в деструктивные сообщества;
— риском попасть в цепочки наркокурьеров;
— доступом к порнографии и экстремистским материалам;
— азартными играми;
— случаями склонения к насилию и даже суициду.

По данным исследования *Kazakhstan Kids Online*:

— каждый **четвёртый ребёнок** сталкивался с кибертравлей,
— каждый **третий** — с агрессивным контентом,
— сотни детей участвовали в закрытых сообществах с признаками деструктивного влияния.

Мы имеем дело с новой формой уязвимости, требующей проактивного реагирования.

Международный опыт и подход Казахстана

Мировая практика показывает: цифровая безопасность должна быть встроена в инфраструктуру с самого начала — на уровне оператора связи, школы и семьи. Этот принцип работает в Великобритании, Японии, Южной Корее, США.

Изучив лучшие кейсы, мы пришли к выводу: Казахстан также может построить собственную модель цифровой защиты детей.

SIM KIDS: первые шаги

Так родилась инициатива **«Детские тарифы»**, трансформировавшаяся в проект **SIM KIDS**. Это специальная SIM-карта, которая позволяет:

— ограничивать доступ к вредному контенту;
— уведомлять родителей о рисках;

— отслеживать геолокацию ребёнка;
— блокировать подозрительную активность.

Весной 2025 года в Алматы был запущен пилот совместно с прокуратурой и операторами Tele2/Altel.

Результаты пилота:

— 94% родителей отметили снижение тревожности и усиление контроля;
— зафиксированы сотни попыток доступа к запрещённым ресурсам;
— число жалоб на онлайн-угрозы снизилось почти на треть.

SIM KIDS стал первым реальным инструментом, показавшим эффективность цифровых решений в защите детей.

Формирование экосистемы защиты

SIM KIDS — лишь часть общей системы. Параллельно ведётся работа по:

— фильтрации по умолчанию на детских тарифах и блокировке запрещённого контента;
— обязательной регистрации SIM-карт по ИИН с согласием родителей;
— внедрению цифровой гигиены в школах;
— мониторингу деструктивных групп и работе горячей линии «111».

Эта экосистема формируется совместно с Министерством просвещения, МВД, операторами связи и другими партнёрами.

Дальнейшие шаги

Следующий этап — масштабирование SIM KIDS на национальном уровне, интеграция в школьную инфраструктуру и расширение функционала. Также необходимо закрепить работу законодательно и использовать технологии искусственного интеллекта для проактивного выявления угроз.

Заключение

Цифровая безопасность детей — это не запреты, а разумные рамки, позволяющие ребёнку развиваться без страха. Интернет должен быть пространством знаний и доверия, а не агрессии и угроз.

Казахстан имеет все шансы стать **первой страной в Центральной Азии**, где цифровая безопасность детей станет частью системной инфраструктуры. Пилот SIM KIDS доказал: мы на правильном пути.

Ускембаев Аслан Алданулы,
Заместитель начальника Департамента по противодействию киберпреступности МВД РК

ЗАЩИТА ДЕТЕЙ В ЦИФРОВОМ ПРОСТРАНСТВЕ

Уважаемые коллеги, участники круглого стола!

В мире, где цифровые технологии проникают в каждый аспект нашей жизни, безопасность детей в Интернете становится особенно актуальной. К сожалению, цифровое пространство, несмотря на свои огромные возможности для обучения и развития, часто становится ареной для различных видов насилия, как психологического, так и физического. Сталкиваясь с угрозами в интернете, дети могут испытать сильный стресс, потерять чувство безопасности, а порой это может привести к трагическим последствиям.

Безопасность детей в сети – это не просто обязанность, это наша ответственность.

Перед нами стоят актуальные задачи, с которыми сталкиваются дети и их родители в цифровом мире. Мы должны подумать о механизмах профилактики, о том, как обеспечить защиту детей от вредоносного контента, а также о том, какие меры нужно принять на уровне общества, государства и образовательных учреждений.

Проблема сексуальных преступлений, затрагивающих права детей, особенно в цифровой среде, является одной из самых острых и требует комплексного подхода со стороны правоохранительных органов, правозащитников, государственных структур и общества в целом.

В последние годы наблюдается рост преступлений сексуального характера, совершенных в отношении детей в Интернете. Это включает в себя как создание и распространение порнографических материалов с участием несовершеннолетних, так и сексуальные домогательства, сексуальное манипулирование детьми в социальных сетях, а также онлайн-сексуальные преступления, связанные с видеоконференциями и мессенджерами.

Интернет создает уникальные условия для совершения подобных преступлений. Анонимность и отсутствие географических ограничений делают преступников менее уязвимыми. Кроме того, дети, имеющие доступ к сети, часто не понимают всей опасности цифрового мира и могут стать жертвами манипуляций со стороны преступников.

Одной из главных проблем, с которой сталкиваются правоохранительные органы при расследовании преступлений сексуального характера в Интернете, является сложность сбора доказательств. В отличие от традиционных преступлений, где материалы преступления могут быть физически изъяты, в цифровой среде доказательства могут быть быстро удалены или зашифрованы. Преступники, как правило, обладают высокими техническими навыками, что позволяет им скрывать свою личность и избегать задержания.

Ключевым моментом является использование технологий для обеспечения доказательной базы: поиск цифровых следов, анализ жестких дисков, мобильных устройств, логов и данных, переданных через Интернет. Но даже в случае изъятия доказательств в сети Интернет необходимо учитывать юридические и правовые сложности, такие как международная юрисдикция, защита данных и права детей.

Одним из главных вызовов является необходимость создания эффективных законодательных механизмов для борьбы с преступлениями сексуального характера в цифровой среде.

Как Вам известно 16 июня 2024 года введено в действие уголовное наказание за приставание сексуального характера к несовершеннолетним, в том числе с использованием сети Интернет.

*Справочно: в текущем году уже зарегистрировано **57** фактов контактного приставания к несовершеннолетним (окончено – 57, прервано - 0).*

Борьба с преступлениями сексуального характера в Интернете невозможна без активного международного сотрудничества. Преступники часто используют международные каналы для обмена информацией и распространения материалов, что затрудняет их задержание в рамках одной юрисдикции. Важнейшим шагом в борьбе с этой проблемой является обмен информацией между государствами, а также использование международных баз данных и механизмов для быстрой и эффективной координации усилий.

Каждое преступление сексуального характера, совершенное в отношении детей, несет за собой долгосрочные психологические и социальные последствия для жертв. В онлайн-среде эта угроза становится еще более опасной, поскольку дети могут столкнуться с насилием, не осознавая его масштаба. Интернет лишает ребенка физического контакта с преступником, что порой затрудняет осознание угрозы.

Также стоит отметить, что в случае с детьми, подвергшимися онлайн-сексуальному насилию, отсутствие поддержки и понимания со стороны окружающих и властей может усугубить проблему. Дети, особенно младшего возраста, не всегда понимают, что стало жертвой преступления, или не могут рассказать о произошедшем.

Наша задача – не только реагировать, но и предупреждать подобные преступления. Профилактика преступлений в отношении детей в интернете требует активной работы с детьми и их родителями. Важно формировать у детей навыки безопасного общения в Интернете, прививать осознание рисков и научить их распознавать угрозы.

Следует усилить программы цифровой грамотности и безопасности, как в школах, так и в социальных учреждениях. Важно также развивать просветительские инициативы, направленные на родителей, чтобы они могли обеспечивать безопасное пространство для своих детей в сети.

Борьба с преступлениями сексуального характера в отношении детей в цифровой среде требует комплексного подхода, который включает не только правовую, но и технологическую, а также образовательную составляющую.

Проблемы расследования преступлений сексуального характера в цифровой среде, затрагивающих права детей, являются вызовом для всего общества. Это задача не только для правоохранительных органов, но и проблема, касающаяся всех нас — родителей, педагогов, законодателей и технологий. Только через комплексный подход, который включает в себя усилия на всех уровнях, можно эффективно бороться с этим злом и защитить детей от угроз, исходящих из цифрового мира.

Благодарю за внимание!

Турабай Кундыз Бакытбеккызы,
Национальный специалист по вопросам защиты ребенка Детского фонда ООН (ЮНИСЕФ) в Казахстане

МЕЖДУНАРОДНЫЕ СТАНДАРТЫ И ПОДХОДЫ ПО ЗАЩИТЕ РЕБЕНКА В ЦИФРОВОЙ СРЕДЕ

Интернет и цифровые технологии в первую очередь открывают перед детьми новые возможности для обучения, творчества и самореализации. Одновременно такие технологии привносят в жизнь детей некоторые риски, связанные с неприемлемым контентом, контактами и поведением, например, кибербуллинг и более серьезные формы насилия. Именно поэтому Детский фонд ООН (ЮНИСЕФ) на глобальном и национальном уровнях разрабатывает и рекомендует комплексные подходы, направленные на профилактику онлайн-рисков, защиту детей в цифровой среде и создание безопасных возможностей для их развития.

Согласно докладу ЮНИСЕФ «Положение детей в мире, 2017 год: Дети в цифровом мире», сегодня каждый третий пользователь Интернета в мире — ребёнок . Всё больше детей начинают пользоваться цифровыми технологиями уже в раннем возрасте: в Казахстане 45% детей выходят в цифровое пространство в возрасте от 5 до 8 лет. Важно подчеркнуть, что цифровая среда становится неотъемлемой частью реализации прав ребёнка. Комитет ООН по правам ребёнка в своём Замечании общего порядка № 25 (2021) отметил, что доступ к цифровым технологиям способствует осуществлению всего спектра прав, включая образование, участие в общественной жизни и право на свободу выражения мнения. Вместе с тем ранняя цифровизация усиливает уязвимость детей перед рисками, требующими системного регулирования и профилактики.

Международный опыт ЮНИСЕФ показывает, что угрозы, с которыми сталкиваются дети в онлайн-среде, тесно взаимосвязаны и охватывают несколько ключевых направлений. Среди них выделяются неприемлемый контент (насилие, материалы сексуального характера, дезинформация, пропаганда нездорового поведения), неприемлемый контакт (груминг, шантаж, домогательства), неприемлемое поведение (буллинг, секстинг, угрозы, распространение интимных изображений,) и коммерческие риски (навязчивая реклама, азартные игры, скрытые платежи, сбор персональных данных и несправедливые условия использования). Международные исследования и практика показывает, что реагирование только на отдельные проявления, например на кибербуллинг, делает систему защиты фрагментарной. Именно поэтому ЮНИСЕФ на глобальном уровне рекомендует комплексный подход, учитывающий весь спектр угроз.

Правовая основа такого подхода формируется рядом ключевых международных документов. Центральное место занимает Конвенция о правах ребёнка (1989) и её Факультативный протокол, касающийся торговли детьми, детской проституции и детской порнографии (2000). Существенное значение имеют Будапештская конвенция о киберпреступности (2001), обеспечивающая международное сотрудничество в расследовании онлайн-преступлений, и Лансаротская конвенция Совета Европы (2007), криминализирующая сексуальную эксплуатацию и злоупотребления в отношении детей, возлагающая на государства обязательства по их предотвращению и защите пострадавших, а также предусматривающая систему мониторинга за исполнением. В последние годы особую актуальность приобретают Руководящие принципы предпринимательской деятельности в аспекте прав человека, разработанные ООН и устанавливающие ответственность ИКТ-компаний за соблюдение прав детей, а также Модель национальных мер реагирования на

онлайн-эксплуатацию детей (WeProtect Global Alliance), применяемая многими странами в качестве практического инструмента выстраивания стратегий. Новейшим международным инструментом стала недавно принятая Конвенция ООН против киберпреступности (2024 г.), которая в перспективе должна стать первым глобальным обязательным стандартом в данной сфере. Из международной практики, к недавно разработанным инициативам относится Детский кодекс Великобритании (2020), регулирующий деятельность цифровых сервисов с учётом возраста пользователей. Все эти документы подчёркивают: цифровые права неотъемлемы от прав человека, а государства несут обязанность обеспечивать безопасную и инклюзивную онлайн-среду для детей.

В 2023 году ЮНИСЕФ совместно с Министерством просвещения РК провёл исследование Kazakhstan Kids Online: Цифровая жизнь детей в Казахстане, которое впервые дало целостную картину цифрового опыта детей. Его результаты легли в основу запуска в 2024 году программы ЮНИСЕФ «Защита детей от онлайн-насилия, жестокого обращения и эксплуатации в Казахстане», поддержанной глобальной инициативой Safe Online. Программа направлена на укрепление систем и потенциала национальных институтов для предотвращения и пресечения онлайн сексуальной эксплуатации и насилия над детьми. Уже сегодня достигнуты значимые результаты, подтверждающие серьёзность намерений Казахстана системно адресовать онлайн риски для детей с учетом международных стандартов.

На Первой глобальной министерской конференции по искоренению насилия в отношении детей, состоявшейся в Колумбии в 2024 году, Казахстан твердо заявил о своём намерении защищать детей в цифровой среде, что показало приоритетность онлайн безопасности детей для Казахстана.

С точки зрения законодательного регулирования ЮНИСЕФ и Международный союз электросвязи рекомендуют минимальные меры, включающие криминализацию всех форм онлайн сексуальной эксплуатации и насилия в отношении детей, разработку процедур расследования и хранения цифровых доказательств, регулирование деятельности цифрового бизнеса, предоставление услуг помощи пострадавшим детям, а также независимый мониторинг соблюдения прав ребёнка онлайн. Важным является принцип: всё, что незаконно в офлайн-среде, должно считаться незаконным и онлайн. При этом необходимо учитывать баланс: меры по защите не должны ограничивать права детей на участие и доступ к позитивным возможностям цифровой среды.

Опыт ЮНИСЕФ, накопленный в рамках глобальных программ по цифровой безопасности детей, подтверждает, что защита детей в онлайн-пространстве возможна только в рамках комплексного межсекторального подхода. Это включает разработку и совершенствование законодательства, создание механизмов межведомственного взаимодействия, мониторинг соблюдения прав детей и учет их мнения, а также образовательные и профилактические программы. Ключевую роль в этом процессе играют законодательные органы, обеспечивающие совершенствование законодательства, надзор за его выполнением и учёт мнения детей и общества.

Казахстан уже сделал важные шаги по защите детей в онлайн среде и важно продолжать укреплять систему, опираясь на международные стандарты и положительные практики. Цель состоит в том, чтобы цифровое пространство было безопасным и развивающим, создавая условия для полноценного роста, образования и благополучия каждого ребёнка.

Касенова Гульнара Пазылжановна,
И.о. Генерального директора
РГКП "Национальный научно-практический, образовательный и оздоровительный центр "Бобек" Министерства просвещения Республики Казахстан

ПСИХОЛОГИЯ ЦИФРОВОГО ВЫБОРА: КАК ПОМОЧЬ РЕБЕНКУ ВЫСТРОИТЬ ЗДОРОВЫЕ ОТНОШЕНИЯ С ИНТЕРНЕТОМ

Воспитание детей в условиях цифровой эпохи стало настоящим вызовом. Родителям всё труднее ориентироваться в онлайн-мире, чтобы обеспечить безопасность своих детей, а также найти баланс между рисками и возможностями, которые несут в себе интернет и гаджеты. Часто взрослые просто не успевают за стремительным развитием технологий и не всегда могут понять, чем именно заняты их дети за экраном компьютера, планшета или телефона.

Интернет – это инструмент с огромными возможностями, но при неправильном использовании он может нести серьёзные риски: от зависимости до кибербуллинга и утраты личной информации.

Наша цель – не запретить интернет, а помочь ребёнку выстроить осознанные, безопасные и сбалансированные отношения с цифровым миром.

БАЗОВЫЕ ПРИНЦИПЫ ЗДОРОВОГО ИНТЕРНЕТ-ПОВЕДЕНИЯ

«Здоровое интернет поведение» - это стиль онлайн жизни, при котором ребёнок:

- защищает себя и свои данные;
- уважает других и следует правилам этики;
- критически мыслит и проверяет информацию;
- соблюдает баланс между онлайном и офлайном;
- умеет действовать при рисках (буллинг, мошенничество, неподходящий контент).

Почему это важно:

- Интернет – это публичное пространство: всё оставляет след и влияет на репутацию.
- Алгоритмы усиливают то, что мы смотрим и пишем: привычки формируют ленту и настроение.
- Непродуманные действия ведут к рискам: утечки данных, кибербуллинг, манипуляции, финансовые потери, проблемы с законом.

12 ключевых принципов *(структура: суть → почему важно → что делать → ошибки и последствия → сигналы риска)*

1) Цифровая гигиена и безопасность устройств

Устройства и аккаунты должны быть защищены и обновлены. Вредоносные программы крадут данные и деньги. Старые версии ПО уязвимы.

Что делать: включить автообновления ОС/приложений, ставить приложения только из официальных магазинов, использовать антивирус, не давать устройству права администратора без необходимости, ограничивать разрешения приложений.

Ошибки и последствия: вирусы, блокировка аккаунтов, утечка фото/переписок.

Сигналы риска: телефон «тормозит», сам открывает окна, тратит аномальный трафик/батарею.

2) Приватность и управление данными

Личные данные – ценность, их раскрывают дозированно.

По открытой информации можно найти человека, взломать аккаунт, манипулировать им.

Что делать:

• настроить приватность соцсетей;
• убрать геометки;
• использовать ник вместо ФИО;
• не публиковать адрес, школу, расписание, финансовые данные, документы.

Ошибки и последствия: доксинг, преследование, кража личности.

Сигналы риска: просьбы выслать «для проверки» фото документа или селфи с паспортом.

3) Надёжные пароли и 2FA

Каждый аккаунт – уникальный пароль + двухфакторная аутентификация.

Один утёкший пароль = доступ ко всем аккаунтам.

Что делать:

• ставить пароли длиннее 12 символов;
• использовать фразы-пароли;
• подключать 2FA через приложение;
• никогда не делиться паролями.

Ошибки и последствия: взлом аккаунтов, шантаж, удаление контента.

Сигналы риска: письма «срочно подтвердите пароль», входы из незнакомых мест.

4) Критическое мышление и проверка информации

Доверяй, но проверяй. Не всё, что написано онлайн, — правда.

Почему важно:

• Фейки воздействуют на эмоции и решения.

Что делать:

• Проверять источник, дату, автора.
• Искать подтверждение информации в нескольких местах.
• Быть осторожным с «сенсациями» и манипулятивными заголовками.

Ошибки и последствия:

• Распространение лжи.
• Репутационные потери.
• Конфликты с другими людьми.

Сигналы риска:

• «Срочно репостни!», «Только сегодня».
• Гиперэмоциональные посты.

5) Этикет и эмпатия онлайн (нетикет)

Общайся уважительно, как вживую. Слова в сети ранят не меньше, чем офлайн.

Почему важно:

• Поддерживает уважительную атмосферу.
• Помогает избежать конфликтов и травли.

Что делать:

• Думать о тоне сообщения.
• Не писать в аффекте.
• Не шеймить, не травить.

• Уважать разные взгляды.
• Не публиковать чужие фото/переписки без согласия.

Ошибки и последствия:

• Конфликты.
• Исключение из сообществ.
• Дисциплинарные меры в школе.

Сигналы риска:

• Поток негативных комментариев.
• «Подстрекатели» в чате.
• Растущая агрессия в переписках.

6) Ответственная публикация и цифровой след

Всё опубликованное может остаться навсегда.

Почему важно:

• Репутация формируется цифровым следом.
• Скриншоты и репосты живут дольше, чем пост.

Что делать:

• Применять «правило бабушки» — не публиковать то, что не показал бы семье или учителю.
• Удалять сомнительные посты.
• Пересматривать старые публикации.

Ошибки и последствия:

• Эффект Стрейзанд — удалённый пост может разойтись ещё шире.
• Репутационные проблемы в будущем (учёба, работа).

Сигналы риска:

• Давление «выкладывай смелее».
• Челленджи с опасными заданиями.

7) Границы общения и незнакомцы

Личная информация и встречи — только с теми, кому доверяешь, и через взрослых.

Почему важно:

• Существует риск грумминга, вымогательства, вовлечения в деструктивные сообщества.

Что делать:

• Не отправлять интимные/личные фото.
• Не соглашаться на тайные встречи.
• Блокировать и жаловаться на нарушителей.

Ошибки и последствия:

• Шантаж.
• Преследование.
• Психологическая травма.

Сигналы риска:

• «Давай без взрослых», «Никому не говори».
• Донаты «за фото».

8) Антибуллинг и безопасная коммуникация

Не будь агрессором. Не поддерживай буллинг наблюдением, защищай жертву.

Почему важно:

• Буллинг разрушает самооценку и атмосферу безопасности.

Что делать:

• Использовать правило 3С: **Стоп – Скриншот – Сообщи взрослому.**

• Поддержать жертву в личных сообщениях.
• Не вступать в перепалки.
• Фиксировать факты буллинга.
Сигналы риска:
• Массовые насмешки в чате.
• «Бан-рейды».
• Травля по фото или внешности.

9) Возрастные ограничения и фильтры контента
Контент должен соответствовать возрасту и задачам.
Почему важно:
• Жёсткий контент и азартные механики вредят развитию.
Что делать:
• Настраивать фильтры контента.
• Разговаривать о причинах запрета, а не просто запрещать.
Ошибки и последствия:
• Страхи, агрессия, нарушение сна.
• Формирование зависимости от запретного контента.
Сигналы риска:
• Ночные просмотры.
• Скрытые вкладки.
• Резкие перепады настроения.

10) Баланс экранного времени и цифровая осознанность
Экран — это инструмент, а не замена реальной жизни.
Почему важно:
• Переизбыток экрана снижает концентрацию, нарушает сон.
Что делать:
• Ввести «экранные правила»:
– Без гаджетов за 60 мин до сна.
– «Экран-паузы» каждые 30–40 мин.
• Фиксировать время в настройках.
• Планировать офлайн-активности.

11) Финансовая и игровая безопасность
Донаты, покупки, лутбоксы — только с разрешения взрослых.
Почему важно:
• Азартные механики и мошенники нацелены на детей.
Что делать:
• Установить запрет на платежи без пароля или биометрии.
• Задать лимиты и семейные правила донатов.
• Быть осторожными с «бесплатными» подарками.
Ошибки и последствия:
• Списания с карты.
• Долги.
• Зависимость от «дропа».
Сигналы риска:
• Тайные траты.
• Продажа игровых предметов.
• Просьбы «оценить аккаунт».

12) Этика и репутация в сети

Почему важно соблюдать этику:

• Репутация и будущее — университеты и работодатели изучают цифровой след.

• Психологическое благополучие — уважительная среда снижает тревогу и одиночество.

• Безопасность — этичные коммуникации уменьшают риск конфликтов и шантажа.

• Культура диалога — учимся спорить аргументами, а не агрессией.

Возможные последствия нарушений:

• **Личные:** стресс, тревога, потеря интереса к учёбе/хобби.

• **Социальные:** конфликты, изоляция, ухудшение отношений с семьёй и друзьями.

Возрастные акценты

7–9 лет. Правила «что такое личное», кто такие незнакомцы, «СТОП СКРИН СООБЩИ», базовый нетикет, семейные таймеры.

10–12 лет. Приватность, критическое мышление, фильтры контента, первые пароли/2ФА с помощью взрослых, правила донатов.

13–15 лет. Цифровой след, репутация, аргументация без хейта, самостоятельная проверка источников, права автора.

16–17 лет. Карьерный бренд, юридические риски, финансовая грамотность онлайн, кибербезопасность аккаунтов.

Ежедневный чек лист для ребёнка

- Я не делился паролями и личной инфой.
- Пост/комментарий: не обижает ли он кого то?
- Проверил источник перед репостом.
- Таймер экрана соблюдён; был офлайн перерыв.
- Не переходил по сомнительным ссылкам.
- Поддержал, если видел чью то травлю.

ЧТО ДОЛЖЕН ДЕЛАТЬ РОДИТЕЛЬ?

1) ИНТЕРЕСОВАТЬСЯ, А НЕ КОНТРОЛИРОВАТЬ

Задавайте вопросы - что смотришь, во что играешь, что нового узнал?

Вовлекайтесь в цифровую жизнь ребёнка – смотрите ролики вместе, играйте, обсуждайте.

2) УСТАНОВИТЬ ПРАВИЛА И ГРАНИЦЫ

Время. Например, не более 1 часа в день для младших школьников.

Место. Без гаджетов за обеденным столом, в спальне перед сном.

Контент. Чёткое понимание, какие сайты разрешены, какие – нет.

3) СОЗДАТЬ “ЦИФРОВОЙ СВОД ПРАВИЛ” ДЛЯ ВСЕЙ СЕМЬИ

Сформулируйте 5-7 правил совместно с ребёнком и соблюдайте их все вместе.

1. После 21:00 гаджеты отдыхают
2. Сначала уроки – потом YouTube
3. Время для живого общения без гаджетов

4) **ИСПОЛЬЗОВАТЬ РОДИТЕЛЬСКИЙ КОНТРОЛЬ**

Настроить фильтры и ограничения на устройствах.

Установить безопасные детские браузеры и видеоплатформы.

Использовать приложения: Google Family Link, Kaspersky Safe Kids и др.

5) **БЫТЬ ДОСТУПНЫМ ДЛЯ РАЗГОВОРА**

Если ребёнок столкнулся с буллингом или нежелательным контентом, он должен знать, что вас можно не бояться – вы не будете кричать, запрещать или наказывать, а поможете.

6) **РОЛЬ ПРЕПОДАВАТЕЛЯ (В ШКОЛЕ ИЛИ КРУЖКЕ)**

7) **ОБУЧАТЬ ЦИФРОВОЙ ГРАМОТНОСТИ**

Что такое фейк, кликбейт, фишинг, манипуляции?

Как распознать опасные ссылки, вредоносные приложения?

Как защитить пароли и личную информацию?

8) **СОЗДАТЬ ПРОСТРАНСТВО ДЛЯ ДИАЛОГА**

Проводить открытые беседы

1. Что делать, если тебя оскорбляют в сети?
2. Какие последствия ожидают тебя, если ты не обратишься к взрослому
3. Давать реальные кейсы - разобрать ситуации, чтобы научить ребёнка реагировать.

9) НАБЛЮДАТЬ ЗА ДЕТЬМИ

Резкое снижение успеваемости, замкнутость, усталость – возможные сигналы цифровой зависимости.

При признаках тревоги – обсуждение с родителями, приглашение школьного психолога.

10) ИНТЕГРИРОВАТЬ ЦИФРОВУЮ ЭТИКУ В ОБУЧЕНИЕ

Не просто рассказывать о безопасности, а преподавать поведенческие нормы в интернете.

Обсуждать, что такое кибербуллинг, троллинг, шейминг, и как вести себя в таких ситуациях.

ПРАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ РОДИТЕЛЕЙ И ПЕДАГОГОВ

- Создайте “интернет-дневник” – куда ребёнок будет записывать, чему научился онлайн.
- Проводите “цифровой детокс” в выходные – вся семья без гаджетов.
- Смотрите вместе полезные ролики: «Уроки цифровой гигиены», мультфильмы про интернет-безопасность.
- Организуйте тематические квесты или игры на тему «Интернет глазами детектива».

Неправильное поведение в интернете, интернет-зависимость или молчание о тревожных ситуациях в сети могут иметь серьёзные последствия для ребёнка – как психологические, так и социальные.

КАКИЕ ИНТЕРНЕТ-РИСКИ СУЩЕСТВУЮТ ДЛЯ ДЕТЕЙ?

1) Кибербуллинг

Оскорбления, травля, унижение в сети

Родители могут долгое время не знать, что ребенка травят в сети. При этом жертва может постоянно получать сообщения с угрозами и оскорблениями. Подобная ситуация может продолжаться долгое время.

В итоге ребенок страдает от кибербуллинга – он может замкнуться, испытывать тревожность, депрессию, стресс.

Последствия: чувство изоляции, снижение самооценки, отказ от общения, иногда – суицидальные мысли.

2) Груминг

Выманивание личной информации или встреч взрослыми под видом подростков

Ребёнок может стать жертвой взрослых, выдающих себя за сверстников.

Последствия. Шантаж, запугивание, вовлечение в сексуальные, криминальные или манипулятивные действия.

3) Контент 18+

Доступ к порно, насилию, пропаганде

Сцены насилия, пропаганда агрессии или деструктивного поведения.

Последствия. Искажение восприятия реальности, эмоциональная перегрузка, чувство страха, копирование вредных моделей поведения.

4) Интернет-зависимость

Потеря контроля над временем в сети

Когда ребёнок:

- Теряет контроль над временем в сети
- Предпочитает онлайн-общение живому
- Раздражается без телефона или Wi-Fi

Последствия: нарушения сна, ухудшение зрения, снижение концентрации, проблемы с учёбой, физическая пассивность, агрессия.

5) Фишинг и мошенничество

Ложные ссылки, сайты, просьбы перевести деньги

Последствия. Потеря денег, взлом аккаунтов

6) Распространение личной информации

Публикация фото, адреса, телефонов

Последствия. Шантаж, травля, привлечение злоумышленников

7) Нарушение цифровой этики

Когда ребёнок:

- Оскорбляет других в сети
- Публикует чужие фото без разрешения
- Распространяет фейки или участвует в травле

Последствия: блокировка аккаунтов, конфликты с друзьями и сверстниками, потеря репутации.

ОСНОВНЫЕ ПРАВИЛА ПОВЕДЕНИЯ РЕБЁНКА В ИНТЕРНЕТЕ

Родители и педагоги должны регулярно напоминать об этих правилах:

1. Не сообщай личную информацию
(ФИО, номер телефона, адрес, фото семьи)
2. Не общайся с незнакомцами
Если кто-то пишет – скажи взрослым. Не встречайся в реальности.
3. Не выкладывай чужие фото и видео без разрешения
4. Не груби и не унижай других в сети
То, что в интернете, остаётся навсегда. Уважай других.
5. Соблюдай режим
Интернет – после уроков и в установленное время
6. Не верь всему в интернете
Проверяй информацию, спрашивай взрослых
7. Если что-то пугает – сразу расскажи взрослым

ЗАКЛЮЧЕНИЕ

Интернет может быть источником знаний, творчества и общения, но при неумелом или чрезмерном использовании он способен нанести вред психическому, эмоциональному и даже физическому здоровью ребёнка.

Этому нужно учить с детства – через доверие, диалог, пример родителей и поддержку педагогов. Интернет не уйдёт из жизни ребёнка. Наша задача – сделать его безопасной и полезной частью этой жизни, научить использовать технологии во благо, а не во вред.

Помните: воспитание здоровых интернет-привычек — это не разовое действие, а постоянный процесс.

Работайте в команде: ребёнок + родитель + педагог. Только так получится вырастить грамотного и безопасного пользователя.

Мини словарь:

Фишинг — обман для кражи данных.

Груминг — завоевание доверия ребёнка для эксплуатации.
Доксинг — публикация личных данных без согласия.
Кибербуллинг — травля онлайн.
Кэтфишинг — подделка личности в сети.
Шейминг — публичное унижение.

Костяная Юлия Сергеевна,
Начальник Центра частного
законодательства Института
парламентаризма при УДП РК

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ ДЕТЕЙ В ИНТЕРНЕТЕ: ВЫЗОВЫ И РЕШЕНИЯ

Введение. Сегодняшние дети растут в быстро развивающемся цифровом мире, где цифровые медиа играют важную роль в их повседневной жизни. Цифровые сервисы предлагают возможности для обучения, развлечений, доступа к информации, открытия новых вещей и общения с другими сверстниками и членами сообщества. Тем не менее, они также создают риски, включая проблемное или чрезмерное использование цифровых медиа, воздействие неприемлемого контента, вредоносное поведение и другие проблемы с безопасностью в Интернете.

Дети повсеместно используют интернет. В Казахстане результаты исследования показали, что 71 % детей пользуются компьютером, ноутбуком либо планшетом. Доля пользователей детей интернета (включая мобильный) в среднем 74%. [1]

Каждый родитель хочет, чтобы дети чувствовали себя в безопасности, находясь в сети, ведь в интернете есть вещи, которых следует опасаться. Опасны не только вирусы и хакеры, которые могут украсть личную информацию; помимо них существует кибербуллинг, неприемлемый контент и онлайн-хищники, нацеленные на детей и подростков.

Одной из актуальных проблем является защита персональных данных в Интернете. Сегодня люди практически на ежедневной основе делятся своими персональными данными в сети. Это происходит при регистрации на различных онлайн-платформах, в социальных сетях, при регистрации в онлайн-играх и массе других интернет-сервисах.

Обсуждение. Дети в силу специфики нынешней цифровой эпохи наравне со взрослыми, если не чаще, активно пользуются различными цифровыми возможностями, но зачастую не совсем понимают какие сайты безопасны для посещения, а какие нет, что можно сообщать о себе, а что нет. Очень часто дети бесконтрольно посещают различные сайты, разрешают алгоритмам сбор cookies, заполняют поля с персональными данными, в общем оставляют свои цифровые следы.

В связи с этим, и детям и взрослым нужно понимать, что такое персональные данные. Согласно подпункту 2) статьи 1 Закона «О персональных данных и их защите», [2] персональные данные - это сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе. Проще говоря, персональные данные - это вся зафиксированная информация о человеке. Если взглянуть на документы (удостоверение личности, паспорт, водительские права, договоры с сотовыми операторами, медицинские карточки, адресная справка, данные с ЕНПФ, электронные документы с eGov и т.д.), то можно отметить следующую зафиксированную информацию: фамилия, имя и отчество, дата рождения, номер документа, ИИН, адрес прописки и адрес проживания, номер телефона и т.д. Вся эта зафиксированная информация на бумажном или электронном носителях является нашими персональными данными. К персональным данным детей также можно отнести сведения о номере школы, в которой ребенок обучается, данные проездной карточки, которая содержит изображение ребенка, ФИО и дату рождения и другое.

Согласно гражданскому законодательству от лица несовершеннолетних в сделках, то есть на действия, направленные на установление, изменение или прекращение гражданских прав и обязанностей, участвуют или могут давать согласие только их опекуны, родители либо законные представители. То же самое касается и предоставления согласия на сбор и обработку персональных данных. Статья 10 Закона Республики Казахстан «Об онлайн-платформах и онлайн-рекламе» [3] обязывает собственников платформ не только

обеспечивать целостность и сохранность обрабатываемых персональных данных, но и запрашивать согласие на размещение таких данных у родителей или законных представителей, когда речь идет о детях. Это подчеркивает особую ответственность онлайн-сервисов в отношении защиты конфиденциальности детских данных.

Естественно, информацию общего доступа, такую, как например свое имя, ребенок имеет полное право распространять самостоятельно, так как ребенок является частью общества, и он имеет право на самовыражение и участие в этом обществе. Однако, при распространении более конфиденциальной информации, такой как адрес проживания или контактные данные, ребенок должен учитывать свою собственную безопасность и обратить внимание на возможные последствия своих действий, особенно если информация может быть использована третьими лицами.

Согласно Конституции Республики Казахстан и Закону Республики Казахстан «О правах ребенка», ребенок обладает теми же правами, что и взрослый человек. В связи с чем, персональные данные ребенка также, как и у взрослого, делятся на данные общего доступа и ограниченного доступа.

Общедоступные персональные данные -это те данные, на которые в соответствии с законами Республики Казахстан не распространяются требования конфиденциальности, доступ к которым является свободным с согласия субъекта. Например, некоторые данные прописанные в вашем резюме и размещенные в общедоступных ресурсах, библиографии, на страницах социальных сетей. Зачастую к ним относятся ФИО, номер телефона и дата рождения, так как, в основном, именно эту информацию мы сами публикуем и тем самым даем согласие на их распространение. Однако следует отметить, что в отношении детей эти данные требуют особой защиты.

Персональные данные ограниченного доступа - это данные, доступ к которым ограничен законодательством. Например, это может быть номер удостоверения личности, паспорта (любого другого удостоверяющего документа), адрес проживания, медицинские сведения, банковские счета и т.д. зачастую являются персональными данными ограниченного доступа, так как эти сведения являются конфиденциальными, должны быть защищены и не подлежат распространению, иначе в обратном случае их доступность может навредить субъекту. Любые лица, получающие доступ к таким данным, согласно статье 11 Закона «О персональных данных и их защите», обязаны соблюдать конфиденциальность данных и не допускать их распространения без согласия субъекта или его законного представителя либо наличия иного законного основания.

В случае утечки персональных данных ребенка, можно обратиться в уполномоченный орган по защите персональных данных, в Управление по защите персональных данных Комитета по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности, через сервис электронных обращений eOtinish. Необходимо указать суть обращения, категории данных, предполагаемого нарушителя, приложить доказательства и документы, подтверждающие статус заявителя (опекун, родитель, законный представитель).

Кроме того, законодательством Республики Казахстан предусмотрена ответственность за нарушение конфиденциальности персональных данных, согласно статье 79 Кодекса об административных правонарушениях Республики Казахстан, [4] штраф за незаконные сбор и обработку персональных данных варьируется от 36 920 тенге (10 МРП) до 3 692 000 тенге (1000 МРП) в зависимости от степени вреда и субъекта персональных данных.

В зарубежных странах также существует наказание за нарушение конфиденциальности. В 2019 году YouTube (Google) был оштрафован Федеральной торговой комиссией США (FTC) на $170 млн за нарушение Закона США о защите конфиденциальности детей в интернете путем сбора данных детей без согласия родителей. [5] Также TikTok был оштрафован FTC на $5.7 млн за нарушение COPPA, поскольку собирала данные детей без согласия родителей и не удаляла аккаунты детей по запросу. [6] В 2018 году компания VTech была оштрафована на $650 000 за неспособность адекватно

защитить данные детей, что привело к утечке. [7] В январе 2025 FTC ужесточила правила COPPA: введён обязательный опт-ин родителей для таргетированной рекламы детям, ограничено хранение данных и расширено понятие «идентифицирующей информации» (включая биометрику). [8]

В целом, можно отметить, что в законодательстве Казахстана есть нормы, регулирующие обработку данных несовершеннолетних, но они носят общий характер и не образуют отдельного комплексного регулирования.

Если обратиться к мировым исследованиям, то они подтверждают высокую уязвимость детской приватности. Согласно отчёту Национального альянса кибербезопасности (США), в 2022 г. каждый 43-й ребёнок пострадал от утечки своих данных. [9] Почти 90 % американцев обеспокоены тем, что соцсети хранят информацию о детях. В Евросоюзе исследователи обращают внимание на преобладание сбора данных: например, консорциум EdTech Exposed (Human Rights Watch) выявил, что более 9 из 10 образовательных приложений отслеживают учеников и передают сведения рекламным фирмам. [10]

По данным Международной образовательной мониторинговой программы ЮНЕСКО (GEM Report 2023), лишь 16 % стран имеют законы, явно гарантирующие приватность учащихся. [11] При этом анализ 163 учебных платформ показал, что 89 % из них могут «слеживать» детей – собирать данные и оценивать интересы ребёнка для таргетинга рекламы. В опросах Kaspersky 50 % детей выкладывают личные фото онлайн, и каждый третий делится данными школы. Исследование Internet Safety Labs в США подтвердило: школы часто внедряют сотни цифровых технологий, и 96 % из них передают данные учеников третьим лицам (даже незаметно для родителей и администраторов). [12] Таким образом, академическая и практическая статистика указывает на тотальную цифровизацию детства, сочетающуюся с массовыми нарушениями приватности и отсутствием адекватных гарантий.

Для решения существующих проблем, в первую очередь следует применять технические меры защиты данных детей в цифровой среде, которые предполагают использование принципа «приватности по умолчанию». Он включает применение шифрования, анонимизации и минимизации данных, а также установку максимально безопасных настроек в детских сервисах и приложениях. Родителям рекомендуется дополнительно использовать приложения родительского контроля, ограничивать автозапуск медиа, закрывать профили в играх и социальных сетях, а также внимательно читать условия пользования онлайн-платформами.

Наряду с техническими мерами особое значение имеют образовательные программы. Школы всё активнее вводят курсы цифровой грамотности и медиаобразования, а международные организации, такие как UNICEF, ООН, реализуют проекты по безопасному интернету в Казахстане и других странах СНГ. Основной акцент делается на обучение детей и родителей распознавать угрозы, не разглашать чувствительные данные, правильно настраивать приватность и критически относиться к онлайн-контенту. Подобные программы включают этические аспекты, а также практические навыки защиты.

Для комплексной защиты необходима согласованная работа всех участников процесса. Государственным органам следует разрабатывать стратегии онлайн-безопасности детей, усиливать контроль за соблюдением возрастных ограничений, создавать межведомственные центры мониторинга рисков и поддерживать международное сотрудничество. Образовательные учреждения должны внедрять политику «безопасной школы», выбирать проверенные платформы и обучать детей навыкам цифровой гигиены. Разработчики обязаны реализовывать принципы «privacy by design» и «privacy by default», обеспечивать прозрачные интерфейсы конфиденциальности и проходить добровольные аудиты безопасности. Родители же остаются первой линией защиты: они должны обучать детей кибергигиене, следить за настройками конфиденциальности, использовать родительский контроль, обсуждать онлайн-опыт ребёнка и подавать личный пример ответственного поведения в сети.

Заключение. Таким образом, защита персональных данных детей в интернете является не просто технической задачей, а комплексной проблемой, требующей постоянного внимания и совместных усилий. Родители, образовательные учреждения, законодатели и технологические компании должны работать сообща, чтобы создать безопасное, этичное и благоприятное цифровое пространство для наших детей. Только через образование, ответственное использование технологий и строгое соблюдение законов мы сможем обеспечить, чтобы интернет оставался источником возможностей, а не угроз для подрастающего поколения.

Список использованной литературы:

1. Бюро национальной статистики Агентства по стратегическому планированию и реформам Республики Казахстан. / https://bala.stat.gov.kz/dolya-detej-v-vozraste-6-15-let---polzovatelej-informatsionno-kommunikatsionnymi-tehnologiyami/ (дата обращения 21 июля 2025 года)
2. Закон Республики Казахстан от 21 мая 2013 года N 94-V. «О персональных данных и их защите» // https://adilet.zan.kz/rus/docs/Z1300000094
3. Закон Республики Казахстан от 10 июля 2023 года № 18-VIII ЗРК. «Об онлайн-платформах и онлайн- рекламе»// https://adilet.zan.kz/rus/docs/Z2300000018
4. Кодекс Республики Казахстан от 5 июля 2014 года № 235-V ЗРК. «Об административных правонарушениях»// https://adilet.zan.kz/rus/docs/K1400000235#z264
5. Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law.// https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law?emc=edit_tu_20190906%3Fcampaign_id%3D26&instance_id=12171&nl=bits&regi_id=91882581&segment_id=16787&te=1&user_id=709dec13c5b831ddfe8ae5bc7e34aea1& (дата обращения 21 июля 2025 года)
6. TikTok will pay $5.7 million over alleged children's privacy law violations // https://www.theverge.com/2019/2/27/18243312/tiktok-ftc-fine-musically-children-coppa-age-gate (дата обращения 21 июля 2025 года)
7. Toy firm VTech fined $650,000 over data breach // https://www.bbc.com/news/technology-42620717? (дата обращения 21 июля 2025 года)
8. FTC Finalizes Changes to Children's Privacy Rule Limiting Companies' Ability to Monetize Kids' Data// https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-changes-childrens-privacy-rule-limiting-companies-ability-monetize-kids-data#:~:text=%2A%20Requiring%20opt,approved%C2%A0%20108%20COPPA (дата обращения 21 июля 2025 года)
9. Protecting Our Kids' Data Privacy is Paramount // https://www.staysafeonline.org/articles/protecting-our-kids-data-privacy-is-paramount (дата обращения 21 июля 2025 года)
10. Remote learning apps shared children's data at a 'dizzying scale'// https://www.washingtonpost.com/technology/2022/05/24/remote-school-app-tracking-privacy/ (дата обращения 21 июля 2025 года)
11. Technology in education// https://gem-report-2023.unesco.org/technology-in-education/ (дата обращения 21 июля 2025 года)
12. Most apps used in US classrooms share students' personal data with advertisers, researchers find// https://cyberscoop.com/apps-expose-student-data-privacy/#:~:text=A%20whopping%2096,to%20a%20study%20published%20Tuesday (дата обращения 21 июля 2025 года)

Акоева Юлия Георгиевна,
Психолог, тренер по детской безопасности
Психологические аспекты информационной безопасности детей и подростков

ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ И ПОДРОСТКОВ

В современном мире невозможно обойтись без использования информационных технологий. Дети очень быстро вовлекаются в цифровую среду, становятся активными пользователями гаджетов и интернета и являются одной из самых уязвимых групп для манипуляций преступников.

Большинство опасностей интернет-пространства сопоставимы с опасностями реального мира:

- Взломы аккаунтов;
- Утечка конфиденциальных данных;
- Вовлечение в мошеннические схемы, под видом заработка;
- Грумминг;
- Кибersталкинг;
- Кибербуллинг;
- Педофилия;
- Группы смерти;
- Потеря интереса к событиям реальной жизни, интернет-зависимость и т.д.

Условно угрозы можно разделить на:

- Угрозы, связанные с контентом – ребенок может потреблять неадекватный его возрасту, потребностям, особенностям контент;
- Угрозы, связанные с покупкой товаров и услуг – ребенок может совершать покупки в интернете, не соответствующие различным критериям безопасности;
- Угрозы, связанные с вредоносным программным обеспечением;
- Угрозы, связанные с общением – ребенок может общаться с опасными людьми, сталкиваться с мошенничеством;
- Угрозы, связанные с зависимостями и проблемами развития когнитивных процессов.

Родители не могут предусмотреть всех угроз, с которыми может столкнуться их ребенок в информационном пространстве, поэтому, очень важно обратить внимание на те аспекты, которые могут повлиять на понимание ребенком проблемы.

1. Низкий уровень осведомленности.

В первую очередь, на поведение ребенка в интернете, влияет уровень его осведомленности – то есть, насколько он понимает, что такое интернет и умеет им пользоваться.

Для того, чтобы понимать, от чего защищать ребенка, осведомленным, в первую очередь, должен быть сам родитель. Часто бывает так, что родители не подозревают о том, каким образом работают фишинговые ссылки, что такое EXIF данные, какие данные являются конфиденциальными, какие пароли являются надежными, как и для чего

совершаются взломы аккаунтов. Соответственно, при низком уровне осведомленности родителей, снижается осведомленность детей, и они легче попадаются на крючки.

Программы родительского контроля до определенной степени могут обезопасить ребенка, но не являются панацеей.

Ограничения, как правило, нужны и действуют до определенного момента, а впоследствии ребенок не учится саморегуляции, у него не формируется критическое мышление и когда ребенку что-то запрещают, он чаще всего не перестает это делать, а начинает тщательнее это скрывать.

Поэтому в вопросах безопасности с детьми необходима разъяснительная работа, для формирования понимания того, как пользоваться интернетом, и чего остерегаться.

2. Зависимость и задержки развития

Проблема современного родительства заключается в том, что многие молодые родители дают гаджеты в очень раннем возрасте, вот мы видим молодую семью на прогулке, ребенок в коляске, смотрит в телефон. Ребенок в это время не познает мир, не бегает босиком по траве, не развивает моторику, а смотрит на быстро сменяющиеся яркие кадры в экране – подобное поведение формирует уже у маленьких детей зависимость, а так же, затормаживает их когнитивное развитие, что впоследствии приводит к более плачевным последствиям. Ребенок, который с маленького возраста привыкает воспринимать информацию в таком формате, впоследствии сталкивается с трудностями в обучении, так как статичные книги и учебники не могут удерживать его внимание, он не может концентрироваться длительное время на том, что ему необходимо. Таким детям сложнее сопоставлять и анализировать информацию.

3. Отсутствие доверительных отношений со взрослым

При нарушенных детско-родительских отношениях, дети, ближе к подростковому возрасту, ищут в интернете отдушину и людей, с которыми они могли бы эмоционально сблизиться, к сожалению, не всегда это оказываются добропорядочные люди. Злоумышленник входит в доверие ребенка и может воспользоваться своим положением.

В моей практике был не один кейс, когда ко мне приводили детей, которые знакомились в интернете с, как они предполагали, сверстниками. Все начиналось с безобидной переписки, затем шел обмен фотографиями, затем просьбы более подробных или откровенных фотографий, потом шантаж и требование откровенных видео, угрозы и требование встретиться. Во всех этих случаях дети боялись рассказать о происходящем родителям или боялись за благополучие родителей и шли на условия, которые выдвигал преступник.

В такой ситуации, ребенок у которого нет доверительного контакта с родителем или другим значимым взрослым, остается один на один со своей проблемой или прямой опасностью

4. Отсутствие критического мышления

Ключевым фактором, на который необходимо делать акцент в обеспечении безопасности детей – это развитие критического мышления.

Критическое мышление – это способность анализировать информацию, идеи и убеждения, тщательно оценивая их достоверность, логичность и обоснованность. Даже мы, взрослые, не всегда способны трезво оценить происходящее и поддаемся на разного рода провокации, детям в этом отношении еще сложнее, так как критическое мышление формируется не сразу, а в процессе взросления личности

В век современных технологий, когда нейросети воспроизводят не только голос, но и внешность человека, важно учить детей правильным алгоритмам действий, в случае если они получают сообщение от якобы близких.

Наверняка, многие помнят истории, в которых детям звонили, говорили, что мама попала в беду, надо собираться, так как сейчас приедет машина, называли цвет, марку и номер или когда ребенку приходит голосовое сообщение с незнакомого номера, в этом сообщении мамин голос сообщает, что у нее разрядился телефон, она взяла телефон коллеги,

чтобы связаться с ребенком и сообщить, что отправила за ним машину с таким-то номером. Водитель привезет ребенка к маме.

Большинство детей, услышав, что родитель в беде или родной голос и, получив более или менее логичное объяснение, не подвергают сказанное сомнению.

Подготовленный же ребенок, может предпринять ряд шагов, чтобы обезопасить себя – перезвонить родителю; если нет возможности связаться с родителем, позвонить кому-то из близких взрослых; сообщить о проблеме; обратиться за помощью.

Помимо того, что дети могут становиться жертвами насилия, в отсутствие критического мышления, они могут распространять заведомо ложную информацию.

Одно время я вела тренинги по безопасности для детей.

Я заранее договаривалась с одним из ребят из группы, что я буду рассказывать о нем другим ребятам, а он не будет сразу опровергать сказанное.

На первом занятии я говорила ребятам, что у этого ребенка дома 8 кошек, приукрашивала факты, они все удивлялись, бурно это обсуждали.

На следующем занятии я спрашивала у ребят, рассказали ли они кому-нибудь о тех 8 кошках, и большинство говорило – да. Затем я признавалась, что это была неправда, и что прежде, чем что-то рассказывать дальше, необходимо проверить достоверность информации.

Затем я спрашивала, знают ли они о том, что у белых медведей черная кожа, возникала пауза и дети в большинстве случаев лезли в телефоны, чтобы проверить, так ли это.

Помимо того, что дети должны учиться анализировать и проверять информацию, их нужно учить тому, как это делать – искать достоверные, авторитетные источники; источников информации должно быть не менее трех.

Наша задача, как взрослых, как родителей, создать здоровую среду для новых поколений.

В условиях, когда дети не понимают, с какими угрозами они сталкиваются, становятся жертвами преступников, очень легко утратить чувство психологической безопасности.

Психологическая безопасность создает условия для нормального функционирования психических процессов и исключает антиобщественное поведение человека.

Также, очень важно делать акцент на понимание морально-этических норм, которые могут размываться при потреблении неадекватного контента.

Соответственно, работа по повышению осведомленности, разъяснительная работа должна вестись не только на уровне детей и подростков, не только на уровне внешней защиты и программного обеспечения, но и на уровне родителей.

В процессе этой разъяснительной работы, должны учитываться различные факторы – у нас может не хватать специалистов, которые могли бы давать исчерпывающую информацию по вопросам детской безопасности. Мышление современной молодежи, ввиду образа жизни и постоянного присутствия в цифровой среде, очень отличается от мышления людей старших поколений.

К моему большому сожалению, внимание современной молодежи удерживать достаточно сложно, если не добавлять в информацию геймификацию и прочие развлекательные составляющие. Мы должны учитывать особенности восприятия современных детей и подростков.

Большая часть способов преподнесения информации, в виде лекций просто пролетает мимо наших детей. Способы должны меняться и адаптироваться под требования современного мира. Но для того, чтобы это происходило, необходима подготовка соответствующих кадров.

Резюмируя вышесказанное, повторюсь, что в вопросах обеспечения детской и подростковой безопасности с психологической точки зрения, на мой взгляд, ключевыми являются:

1. Высокий уровень осведомленности об угрозах информационной среды, как детей, так и родителей. Формирование понимания в первую очередь у родителей, от чего необходимо защитить ребенка, передавая ему в руки гаджет.

2. Детско-родительские отношения – доверительный контакт в семье, либо с другим значимым взрослым.

3. Развитие критического мышления, на практике, регулярно – дети редко хорошо усваивают материал без повторения.

4. Наличие у детей возможности проводить время за интересными занятиями в реальном мире, вне цифровой среды. У детей должно быть живое общение – друзья, игры, познание вне интернета. Но это требует от родителей больших вложений, как сил, времени, так и денег.

5. Адаптация программ под изменяющиеся условия мира, внедрение образовательных программ, создание безопасных онлайн-платформ.