**Дети и Интернет. Профилактика правонарушений в сети Интернет**

За сравнительно небольшой промежуток времени количество пользователей сети Интернет превысило пять миллионов человек. Сегодня по плотности проникновения широкополосного доступа на 100 человек Беларусь вышла на среднеевропейские показатели, а по скорости – на третье место в мире.

Когда мы говорим о такой категории пользователей, как дети, необходимо констатировать ряд причин, по которым именно они могут стать участниками (жертвами, виновниками, соучастниками) совершения правонарушений в сети Интернет.

Основные риски и угрозы, которые могут возникнуть при использовании сети Интернет ребенком:

-вероятность совершения ребенком правонарушений в сфере информационной безопасности;

-вероятность совершения в отношении ребенка правонарушений в сфере информационной безопасности;

-вероятность совершения ребенком либо в отношении ребенка иных преступлений с использованием сети Интернет;

-возможность ознакомления ребенка с нежелательной информацией;

-возможность вовлечения в незаконный оборот наркосодержащих и психотропных веществ в сети Интернет;

-возможность вовлечения в сообщества деструктивного толка.

***1.Вероятность совершения ребенком правонарушений в сфере информационной безопасности.***

**Статьи уголовного кодекса Республики Беларусь, имеющие отношение к сфере высоких технологий:**

Статья 212. Хищение путем использования компьютерной техники

1. Хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации -

наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

2. То же деяние, совершенное повторно, либо группой лиц по предварительному сговору, либо сопряженное с несанкционированным доступом к компьютерной информации, - наказывается штрафом, или исправительными работами на срок до двух лет, или арестом, или ограничением свободы на срок от двух до пяти лет, или лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

3. Деяния, предусмотренные частями 1 или 2 настоящей статьи, совершенные в крупном размере, -

наказываются лишением свободы на срок от двух до семи лет со штрафом или без штрафа с конфискацией имущества или без конфискации и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

4. Деяния, предусмотренные частями 1, 2 или 3 настоящей статьи, совершенные организованной группой либо в особо крупном размере, - наказываются лишением свободы на срок от шести до пятнадцати лет с конфискацией имущества и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

Статья 349. Несанкционированный доступ к компьютерной информации

1. Несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты (несанкционированный доступ к компьютерной информации), повлекший по неосторожности изменение, уничтожение, блокирование информации или вывод из строя компьютерного оборудования либо причинение иного существенного вреда, - наказывается штрафом или арестом.

2. Несанкционированный доступ к компьютерной информации, совершенный из корыстной или иной личной заинтересованности, либо группой лиц по предварительному сговору, либо лицом, имеющим доступ к компьютерной системе или сети, -

наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

3. Несанкционированный доступ к компьютерной информации либо самовольное пользование электронной вычислительной техникой, средствами связи компьютеризованной системы, компьютерной сети, повлекшие по неосторожности крушение, аварию, катастрофу, несчастные случаи с людьми, отрицательные изменения в окружающей среде или иные тяжкие последствия, -

наказываются ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет.

Статья 350. Модификация компьютерной информации

1. Изменение информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо внесение заведомо ложной информации, причинившие существенный вред, при отсутствии признаков преступления против собственности (модификация компьютерной информации) -

наказываются штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

2. Модификация компьютерной информации, сопряженная с несанкционированным доступом к компьютерной системе или сети либо повлекшая по неосторожности последствия, указанные в части 3 статьи 349 настоящего Кодекса, -

наказывается ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

Статья 351. Компьютерный саботаж

1. Умышленные уничтожение, блокирование, приведение в непригодное состояние компьютерной информации или программы, либо вывод из строя компьютерного оборудования, либо разрушение компьютерной системы, сети или машинного носителя (компьютерный саботаж) - наказываются штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до пяти лет, или лишением свободы на срок от одного года до пяти лет.

2. Компьютерный саботаж, сопряженный с несанкционированным доступом к компьютерной системе или сети либо повлекший тяжкие последствия, - наказывается лишением свободы на срок от трех до десяти лет.

Статья 352. Неправомерное завладение компьютерной информацией

Несанкционированное копирование либо иное неправомерное завладение информацией, хранящейся в компьютерной системе, сети или на машинных носителях, либо перехват информации, передаваемой с использованием средств компьютерной связи, повлекшие причинение существенного вреда, - наказываются общественными работами, или штрафом, или арестом, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

Статья 353. Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети

Изготовление с целью сбыта либо сбыт специальных программных или аппаратных средств для получения неправомерного доступа к защищенной компьютерной системе или сети - наказываются штрафом, или арестом, или ограничением свободы на срок до двух лет.

Статья 354. Разработка, использование либо распространение вредоносных программ

1. Разработка компьютерных программ или внесение изменений в существующие программы с целью несанкционированного уничтожения, блокирования, модификации или копирования информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо разработка специальных вирусных программ, либо заведомое их использование, либо распространение носителей с такими программами -

наказываются штрафом, или арестом, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

2. Те же действия, повлекшие тяжкие последствия, -

наказываются лишением свободы на срок от трех до десяти лет.

Статья 355. Нарушение правил эксплуатации компьютерной системы или сети

1. Умышленное нарушение правил эксплуатации компьютерной системы или сети лицом, имеющим доступ к этой системе или сети, повлекшее по неосторожности уничтожение, блокирование, модификацию компьютерной информации, нарушение работы компьютерного оборудования либо причинение иного существенного вреда, - наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или исправительными работами на срок до двух лет, или ограничением свободы на тот же срок.

2. То же деяние, совершенное при эксплуатации компьютерной системы или сети, содержащей информацию особой ценности, - наказывается лишением права занимать определенные должности или заниматься определенной деятельностью, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, повлекшие по неосторожности последствия, указанные в части третьей статьи 349 настоящего Кодекса, - наказываются ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

При этом необходимо отметить, что ответственность за деяния, предусмотренные ст.212, наступает с 14-летнего возраста, а ст.ст.349-351 – с 16-летнего возраста.

Кодексом об административных правонарушениях также предусмотрена ответственность за совершение несанкционированного доступа к компьютерной информации, не повлекшего существенного вреда.

Статья 22.6. Несанкционированный доступ к компьютерной информации

Несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты, - влечет наложение штрафа в размере от двадцати до пятидесяти базовых величин.

Согласно статистических данных в 2016 году к уголовной ответственности за совершение преступлений рассматриваемой категории было привлечено 34 несовершеннолетних лица, из них 3 – в Гродненской области.

Своевременное доведение учащимся ответственности за совершение противоправных деяний в сфере информационной безопасности, а также разъяснение им сути криминализированных деяний, приведение понятных примеров может свести риск совершения преступлений данной категорией лиц до минимума.

***2. Совершение в отношении ребенка правонарушений в сфере информационной безопасности.***

Каждый пользователь компьютерной техники, сети Интернет автоматически становится обладателем определенной компьютерной информации, которая хранится на жестких дисках компьютеров, в памяти мобильных телефонов на съемных носителях, в облачных хранилищах, которая содержится в учетных записях пользователей на различных Интернет-сайтах, например в электронной почте, в социальных сетях, Интернет-дневниках. Все активнее в нашу жизнь входят электронные платежи в сети Интернет. При небрежном подходе к организации безопасности хранения и использования такой информации, ее владелец, в данном случае ребенок, может стать жертвой противоправных деяний третьих лиц, направленных на завладение и совершение неправомерных деяний по отношению к этой информации.

***3. Совершение ребенком либо в отношении ребенка иных преступлений с использованием сети Интернет.***

Необходимо понимать, что компьютер и Интернет – это всего лишь инструмент, в том числе используемый для совершения противоправных деяний. Такие давно известные правонарушения, как мошенничество, распространение клеветнических сведений, оскорбление, распространение материалов порнографического содержания, информации экстремистского содержания, разжигание межнациональной, межрасовой, межконфессиональной вражды и т.д. в настоящее время достаточно часто совершаются с использованием сети Интернет, что в некоторых случаях является дополнительным квалифицирующим признаком совершаемого преступления.

Дети, пользуясь сетью Интернет и находясь в состоянии мнимой анонимности, умышленно либо по незнанию могут совершать такие деяния. Также ребенок должен быть проинструктирован на случай совершения в отношении него каких-либо противоправных деяний в сети.

**4. Возможность ознакомления ребенка с нежелательной информацией.**

Сеть Интернет является источником огромного количества информации, как полезной для ребенка, так и нежелательной, способной нанести непоправимый вред находящейся на этапе становления психике. К такой информации относят следующую тематику: наркомания, ярко выраженное насилие, экстремизм, жестокое обращение с детьми, оккультные и псевдорелигиозные организации, аборты, азартные игры, порнография, знакомства, оружие, половое воспитание, алкоголь, табак и т.д.

**5. Вовлечение детей в незаконный оборот наркосодержащих и психотропных веществ в сети Интернет.**

В настоящее время Интернет стал основной площадкой нелегального оборота наркотических средств и психотропных веществ. Он предоставляет возможность ребенку как получить большой объем информации о наркотиках, так и практически не выходя из дома на условиях анонимности приобрести наркотики, психотропные вещества, курительные смеси. Также не исключена возможность вовлечения детей в преступные схемы распространения таких веществ.

**6. Возможность вовлечения детей в сообщества деструктивного толка.**

В сети Интернет активно ведут деятельность различные оккультные и псевдорелигиозные организации, сообщества пользователей деструктивной направленности. Неокрепшая психика ребенка зачастую является целью их деятельности. Периодически появляются сообщества в социальных сетях, ориентированные исключительно на детей, предлагающие в игровой форме осуществлять определенные действия, которые в итоге могут привести к угрозе психическому и физическому здоровью, а также в некоторых случаях и жизни ребенка.

**Статья 130.**Разжигание расовой, национальной или религиозной вражды или розни

1. Умышленные действия, направленные на возбуждение расовой, национальной, религиозной вражды или розни, на унижение национальной чести и достоинства, – наказываются штрафом, или арестом на срок до шести месяцев, или ограничением свободы на срок до пяти лет, или лишением свободы на тот же срок.

2. Те же действия, соединенные с насилием либо совершенные должностным лицом с использованием своих служебных полномочий, – наказываются лишением свободы на срок от трех до десяти лет.

3. Действия, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц либо повлекшие по неосторожности смерть человека либо иные тяжкие последствия, – наказываются лишением свободы на срок от пяти до двенадцати лет.

Как видим, представленный и далеко не исчерпывающий список угроз в сети позволяет констатировать, что неподготовленному ребенку при работе в сети Интернет может быть причинен существенный вред.

Встает вопрос, каким образом этот вред можно предотвратить. И здесь необходимо сделать вывод, что основным инструментом профилактики является планомерная и целенаправленная работа родителей с детьми с момента, когда они делают первые шаги в глобальную паутину, до момента, когда знания и психика детей достигают того уровня, позволяющего обеспечить самоконтроль.

Здесь необходимо отметить, что и родители должны обладать достаточным уровнем подготовки в части пользования компьютером, а также методикой воспитания подрастающего пользователя сети Интернет.

**На различных этапах становления личности и с приобретением опыта работы в сети используются различные подходы к обеспечению безопасности детей в Интернете, при этом необходимо учитывать следующие основные положения:**

- Интернет – не отдельный виртуальный мир, а всего лишь составляющая часть реальности, соответственно в сети Интернет действуют те же моральные и правовые ограничения, что и в повседневной жизни. В сети недопустимы поступки, которые непозволительны в реальности.

- Анонимность в сети Интернет, во-первых, является мнимой, поскольку личность любого пользователя сети может быть установлена. Во-вторых, ребенку необходимо понимать, что его собеседник также находится в состоянии такой анонимности, поэтому к указанным им сведениям о себе, выложенным фотографиям, текстам сообщений всегда необходимо относиться критично.

- Использование сети Интернет может нести некоторые опасности (вредоносные программы, небезопасные сайты, Интернет-мошенники и др.), поэтому каждое действие должно быть подкреплено соображениями безопасности. Недопустимо совершение действий, в безопасности которых ребенок не уверен.

- Установите с ребенком доверительные отношения и положительный эмоциональный контакт в вопросе использования сети Интернет. Оговорите с ребенком критический уровень опасности, когда решение в возникшей проблемной ситуации должно приниматься родителем (либо иным доверенным лицом, обладающим достаточным опытом и познаниями, например, старший брат или сестра) либо по согласованию с ними.

- Установленные для ребенка правила работы в сети Интернет должны соответствовать возрасту и развитию Вашего ребенка. Применение слишком мягких правил на начальном этапе освоения сети ребенком может повысить риск возникновения у ребенка различных угроз. В то же время слишком жесткие правила либо запреты для ребенка, обладающего достаточным опытом и знаниями, могут повлечь игнорирование им всяких правил и использование выхода в сеть Интернет без какого-либо контроля родителей.

- Ребенку для работы в сети Интернет должен быть предоставлен в пользование компьютер со специфически настроенными параметрами. Он должен быть оснащен поддерживаемой производителем версией операционной системы с установленными актуальными обновлениями. В обязательном порядке на компьютере должно быть установлено и настроено актуальное антивирусное программное обеспечение, установлен и настроен сетевой экран. Родителями должен контролироваться перечень установленного на компьютере программного обеспечения и его настройки. При необходимости на компьютере должно быть установлено специальное программное обеспечение, позволяющее контролировать и ограничивать деятельность ребенка в Интернете. Используйте лицензионное программное обеспечение.

- В настоящее время наблюдается бурный рост информационных технологий и сети Интернет в частности. В связи с этим программные, организационные меры обеспечения безопасности постоянно развиваются. Родители должны быть нацелены на саморазвитие в данной сфере и корректировать поведение детей в соответствии со складывающимися условиями.