

За сравнительно небольшой промежуток времени количество пользователей сети Интернет в Республике Беларусь 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. Количество абонентов сотовой связи продолжает увеличиваться и в 2016 году достигло 11,4 миллиона человек.

Указанные темпы проникновения информационных технологий во все сферы жизнедеятельности человека наряду с имеющей место некачественностью определенной части пользователей являются предпосылкой возрастающего количества компьютерных инцидентов.

Особо проблемной видится ситуация использования возможностей компьютерных технологий и сети Интернет наиболее неподготовленными категориями пользователей, такими как дети и подростки, а также лица преклонного возраста.

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

Во-первых, необходимо обратить внимание на особенности развития психологии ребенка, наивность его мышления, отсутствие критического подхода к фактам и событиям.

Во-вторых, следует отметить тот факт, что пользователями компьютерной техники (компьютерами, планшетами, смартфонами, телевизорами с функциями SmartTV и т.д.) становятся дети с младшего школьного возраста, наряду с этим отсутствует какая-либо система их подготовки к этому. Преподавание информатики в школе начинается с 6 класса и вопросам безопасного использования компьютера и сети Интернет в программе уделено неоправданно мало внимания.

Таким образом, мы находимся в ситуации, когда ребенку с учетом его психофизиологических особенностей предоставляется неограниченный доступ к мощному инструменту обработки и обмена информацией, при этом отсутствуют системные механизмы обучения эффективному и безопасному использованию этого инструмента.

Ведение профилактической работы среди детей сотрудниками образовательных учреждений, представителями иных заинтересованных субъектов профилактики, может иметь определенный эффект в отношении детей старшего школьного возраста, но когда мы говорим о

детях, делающих первые шаги в глобальной паутине, нужна постоянная индивидуальная работа с ребенком.

В данной ситуации единственным эффективным средством профилактики является планомерная работа родителей с ребенком.

Определим 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 *заражения компьютера* при работе в сети Интернет вредоносными программами;
 - возможность ознакомления ребенка с *нежелательной информацией*;
 - возможность вовлечения в *незаконный оборот наркосодержащих и психотропных веществ* в сети Интернет;
 - возможность вовлечения в *сообщества деструктивного толка*;
 - *группинг*;
 - *секстинг*;
 - *кибербуллинг*;
 - возможность возникновения *Интернет-зависимости*. Рассмотрим их подробнее.
1. При использовании сети возможно совершение ребенком правонарушений в сфере информационной безопасности.

Уголовным кодексом предусмотрен ряд преступлений, имеющих отношение к сфере высоких технологий.

Статья 212. Хищение имущества путем модификации компьютерной информации

1. Хищение имущества путем модификации компьютерной 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, -

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 ограничением свободы на срок от двух до пяти лет или лишением свободы на срок от двух до семи лет со штрафом или без штрафа 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 пяти до двенадцати лет со штрафом и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

Примером такого преступления может быть хищение денежных средств с найденной либо похищенной банковской платежной карточки с использованием банкомата, платежного терминала либо с использованием её реквизитов при осуществлении Интернет-платежей, а также завладение денежными средствами, хранящимися на счетах различных электронных платежных систем и сервисов.

Статья 349. Несанкционированный доступ к компьютерной информации

1. Несанкционированный доступ к компьютерной информации, сопровождающийся нарушением системы защиты (несанкционированный доступ к компьютерной информации), совершенный из корыстной заинтересованности либо повлекший по неосторожности причинение существенного вреда, -

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.

2. Несанкционированный доступ к компьютерной информации либо самовольное пользование компьютерной системой или сетью, 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.

Например, это несанкционированный доступ к электронной почте, учетным записям на различных сайтах, в том числе в социальных сетях, содержащейся на компьютере, в смартфоне и защищенной от доступа третьих лиц.

Статья 350. Уничтожение, блокирование или модификация компьютерной информации

1. Умышленное уничтожение, блокирование, приведение в непригодное состояние компьютерной информации, разрушение, блокирование либо нарушение работы компьютерной системы, сети или машинного носителя либо модификация компьютерной информации при отсутствии признаков преступления против собственности, повлекшие причинение существенного вреда, -

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. Те же деяния, совершенные повторно либо группой лиц по предварительному сговору, -

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

3. Деяния, предусмотренные частями 1 или 2 настоящей статьи, повлекшие по неосторожности последствия, указанные в [части 2 статьи 349](#) настоящего Кодекса, -

наказываются лишением свободы на срок от трех до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

В качестве примера можно привести произведенные изменения компьютерной информации: переписка в электронной почте, в социальной сети, в мессенджере с правами другого пользователя; изменение текстовой, графической и иной информации; внесение изменений в защищенные базы данных и т.д.

Так же здесь мы говорим об умышленном уничтожении (удалении, приведении в непригодное состояние) компьютерной информации либо ее блокировании (например путем смены пароля доступа, изменении графического ключа и т.д.).

Статья 352. Неправомерное завладение компьютерной информацией

1. Умышленные несанкционированное копирование, перехват компьютерной информации либо иное неправомерное завладение компьютерной информацией, повлекшие причинение существенного вреда, -

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 срок до двух лет.

2. Те же деяния, совершенные повторно либо группой лиц по предварительному сговору, -

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

3. Деяния, предусмотренные частями 1 или 2 настоящей статьи, повлекшие по неосторожности последствия, указанные в [части 2 статьи 349](#) настоящего Кодекса, -

наказываются лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

В данном случае учитываются действия, связанные с копированием какой-либо значимой информации, повлекшие причинение существенного вреда. К примеру – копирование писем из электронной почты, личной переписки из социальных сетей, закрытых для просмотра третьими лицами фотографий с компьютера.

Статья 354. Разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств

1. Разработка, использование, распространение либо сбыт компьютерной программы или специального программного или аппаратного средства, заведомо предназначенных для нарушения системы защиты, несанкционированного доступа к компьютерной системе, сети или машинному носителю, несанкционированного уничтожения, блокирования, модификации компьютерной информации или неправомерного завладения компьютерной информацией либо нарушения работы компьютерной системы, сети или машинного носителя, -

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

2. Те же действия, совершенные группой лиц по предварительному сговору, -

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

3. Действия, предусмотренные частями 1 или 2 настоящей статьи, повлекшие по неосторожности последствия, указанные в [части 2 статьи 349](#) настоящего Кодекса, -

наказываются лишением свободы на срок от трех до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

К уголовной ответственности по данной статье могут быть привлечены лица за разработку вредоносного программного обеспечения, а также разработку и использование вирусов, например, блокирующих смартфоны либо шифрующих компьютерную информацию на серверах.

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 причинение 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, повлекшее по неосторожности последствия, указанные в [части 2 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.

Указанная статья применяется к лицам, имеющим доступ к компьютерным сетям и системам, в которых хранится значимая информация, халатные действия которых привели к нарушению функционирования таких систем.

При этом необходимо отметить, что ответственность за деяния, предусмотренные *ст.212*, наступает с *14-летнего* возраста, а *ст.ст.349- 355* - с *16-летнего* возраста.

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

Статья 23.4. 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 тридцати 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 учащихся ответственности за совершение противоправных деяний в сфере информационной безопасности, а также разъяснение им сути криминализованных деяний, приведение понятных примеров может свести риск совершения преступлений данной категорией лиц до минимума.

1. 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.

1. 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. Одновременно и ребенок должен быть проинструктирован на случай совершения в отношении него каких-либо противоправных деяний в сети.

1. Возможность заражения компьютера при работе в сети Интернет вирусами. Вредоносные программы – различное программное обеспечение (вирусы, черви, «троянские кони», шпионские программы, боты и др.), которое может нанести вред компьютеру и нарушить конфиденциальность хранящейся в нем информации. Подобные программы чаще всего снижают скорость обмена данными с интернетом, а также могут использовать ваш компьютер для распространения своих копий на другие компьютеры, рассылать от вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети. Вредоносное программное обеспечение использует множество методов для распространения и проникновения на компьютеры, не только через внешние носители информации, но и через электронную почту посредством спама или скачанных из интернета файлов.
1. 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 и учения, аборты, азартные игры, порнография, знакомства, оружие, половое воспитание, алкоголь, табак и т.д.

1. 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.

1. 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.

1. Груминг – это установление дружеского и эмоционального контакта с ребенком в Интернете для его дальнейшей сексуальной эксплуатации. Работают преступники по следующей схеме: лицо, заинтересованное в интимной связи с несовершеннолетним, представляется в сети другим человеком, зачастую сверстником, втирается в доверие к ребенку и настаивает на личной встрече. Последствия для поддавшегося на уговоры ребенка могут быть очень плачевны.
1. Секстинг – пересылка личных фотографий, сообщений интимного содержания посредством сотовых телефонов, электронной почты, социальных сетей. Опасны возможные последствия участия детей в таких действиях. Переписка с неизвестным пользователем, которым может оказаться взрослый человек, страдающий педофилией, чревата совершением в отношении ребенка преступлений на сексуальной почве. Распространение интимных фотографий зачастую используется преступниками для шантажа, известны случаи детских суицидов на данной почве.
1. Кибербуллинг, или Интернет-травля – намеренные оскорбления, угрозы и сообщение другим компрометирующих данных с помощью современных средств коммуникации, как правило, в течение продолжительного периода времени. При этом такие действия могут совершаться сообщая членами какого-либо Интернет-сообщества, в котором состоит ребенок, либо лицами, преследующими хулиганские мотивы. Проблемой в данном случае являются последствия психологического воздействия на ребенка.
1. Интернет-зависимость – навязчивое желание войти в Интернет, находясь офлайн и неспособность выйти из Интернета, будучи онлайн. По своим симптомам Интернет-зависимость ближе к зависимости от азартных игр. Для этого состояния характерны следующие признаки: потеря ощущения времени, невозможность остановиться, отрыв от реальности, эйфория при нахождении за компьютером, досада и раздражение при невозможности выйти в Интернет.

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 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 объяснять, 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 родителями (иным доверенным лицом, обладающим достаточным опытом и познаниями, например, старшим братом или сестрой) 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.

Далее кратко изложим рекомендации для выработки родителями стратегии проведения воспитательной работы в части использования сети Интернет с детьми различных возрастных групп.

Для детей от 7 до 10 лет.

Оптимальной формой ознакомления ребенка в таком возрасте с сетью Интернет будет совместная работа с ребенком за компьютером.

Приучите детей:

- посещать только те сайты, которые Вы разрешили;
- советоваться с Вами, прежде чем совершить какие-либо новые действия, раскрыть личную информацию;
- сообщать Вам, если ребенка что-то встревожило либо было непонятно при посещении того либо иного сайта.

Запретите:

- скачивать файлы из Интернета без Вашего разрешения;
- общаться в Интернете с незнакомыми Вам людьми;
- использовать средства мгновенного обмена сообщениями без Вашего контроля.

Постоянно беседуйте с детьми на тему использования ими сети Интернет: о действиях, посещенных сайтах, возможных новых знакомых.

Для детей от 10 до 13 лет.

В данном возрасте ребенок уже обладает определенными навыками и познаниями о работе в сети, не готов к постоянному личному контролю со стороны взрослых, однако все еще требует контроля.

Рекомендации:

- создайте ребенку на компьютере собственную учетную запись с ограниченными правами;
- используйте средства фильтрации нежелательного контента;
- напоминайте о конфиденциальности личной информации;
- приучайте ребенка спрашивать разрешение при скачивании файлов из Интернета, при скачивании и установке программного обеспечения;
- поощряйте желание детей сообщать Вам о том, что их тревожит или смущает в Интернете;
- настаивайте на том, чтобы ребенок позволял Вам знакомиться с содержимым его электронной почты, учетных записей в социальных сетях, перепиской в средствах мгновенного обмена сообщениями;
- расскажите об ответственности за недостойное поведение в сети Интернет.

На данном этапе могут активно использоваться программные средства родительского контроля, к которым можно отнести следующие инструменты:

- услуга родительского контроля провайдера, оказывающего услугу доступа в сеть Интернет, позволяющая ограничить доступ к Интернет сайтам, содержащим нежелательный контент;
- функции родительского контроля, встроенные в операционную систему (ограничение времени работы компьютера, ограничение запуска программ, в том числе игр);

- функции родительского контроля, встроенные в некоторые антивирусы (например Kaspersky Internet Security, Norton Internet Security), позволяющие контролировать использование компьютера, запуск

различных программ (попытки запуска запрещенных программ блокируются), использование Интернета (ограничение по времени), посещение веб-сайтов в зависимости от их содержимого, загрузку файлов из Интернета, переписку с определенными контактами через Интернет- мессенджеры и социальные сети, пересылку персональных данных, употребление определенных слов и словосочетаний в переписке через мессенджеры;

- специализированное программное обеспечение, предназначенное для выполнения функций родительского контроля, например КиберМама, KidsControl, TimeBoss и другие.

дети;

Подростки в возрасте 14-17 лет.

Рекомендации:

- интересуйтесь, какими сайтами и программами пользуются Ваши
- настаивайте на том, чтобы подросток не соглашался на встречу с

друзьями из Интернета без Вашего ведома;

- напоминайте детям о необходимости обеспечения конфиденциальности личной информации;
- предостерегайте детей от использования сети для хулиганства либо совершения иных противоправных деяний, разъясните суть и ответственность за совершение преступлений против информационной безопасности;
- обсудите с ребенком возможные риски при осуществлении покупок в сети.

В сети Интернет на сайтах провайдеров, производителей антивирусного программного обеспечения, а также на специализированных ресурсах можно найти рекомендации по обеспечению защиты детей от различных типов киберугроз. Также значимой для родителей может быть размещенная в сети информация о действиях, если ребенок уже столкнулся с какой-либо интернет-угрозой.

В случае установления фактов совершения противоправных деяний в сети Интернет в отношении детей рекомендуем родителям не умалчивать данные факты, а сообщать о них в зависимости от ситуации классному руководителю, социальному педагогу учебного заведения, в правоохранительные органы по месту жительства либо Национальный центр реагирования на компьютерные инциденты Республики Беларусь.

Управление по противодействию

киберпреступности КМ УВД Гродненского облисполкома