## [Профилактика правонарушений в сети Интернет](https://gcgdp.by/news/948-profilaktika-pravonarushenij-v-seti-internet.html)

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.

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

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;
* **возможности вовлечения в незаконный оборот наркосодержащих и психотропных веществ в сети Интернет;**
* **возможности вовлечения в сообщества деструктивного толка;**

При использовании сети возможно совершение ребенком правонарушений в сфере информационной безопасности. Уголовным кодексом предусмотрен ряд преступлений, имеющих отношение к сфере высоких технологий:

##### ***Статья 212 УК Республики Беларусь. 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.**

1. 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.

Примером такого преступления может быть хищение денежных средств с найденной либо похищенной. в том числе у родственников, 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 УК Республики Беларусь. 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.

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 352 УК Республики Беларусь. 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.

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 353 УК Республики Беларусь. 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 достаточно специфична, ее использование в отношении несовершеннолетних маловероятно. Применяется при разработке, изготовлении и сбыте специальных программ и устройств, предназначенных для осуществления несанкционированных доступов.

***Статья 226 УК Республики Беларусь. 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 2017 году к уголовной ответственности за совершение преступлений рассматриваемой категории было привлечено 34 несовершеннолетних лица, из них 5 – в Минской 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.

***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.

***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.

***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 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 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, педагогу социальному учреждения образования, в правоохранительные органы по месту жительства.