БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ

Безопасный интернет: профилактика административных правонарушений, совершаемых в глобальной сети

В связи с развитием новых технологий в области виртуального пространства, в том числе с распространением сети Интернет, возникла проблема, связанная с доступом несовершеннолетних к информации сомнительного содержания и противоречащей общепринятой этике.

Интернет является прекрасным источником для новых знаний, помогает в учебе, занимает досуг. Но в то же время сеть таит в себе много опасностей. Обязательно нужно знать, что могут возникать различные неприятные ситуации и то, как из них лучшим образом выходить. Помните, что безопасность в сети Интернет на 90% зависит от вас, что каждый компьютер, ноутбук имеет персональный IP-адрес, поэтому всегда очень легко установить адрес и данные пользователя.

Как защитить себя от негативной информации?

Отсутствие контроля со стороны родителей за использованием сети Интернет - одна из причин доступности негативной информации несовершеннолетним .Следует понимать, что, подключаясь к сети Интернет, Вы можете встретиться с целым рядом угроз, о которых он может даже и не подозреваете.

Какие угрозы встречаются наиболее часто? Прежде всего:

- ***Доступ к нежелательному содержимому.***

Ведь сегодня дела обстоят таким образом, что любой человек, выходящий в Интернет, может просматривать любые материалы. А это насилие, наркотики, страницы, подталкивающие молодежь к противоправным действиям и многое-многое другое. Ведь все это доступно в Интернет без ограничений. Часто бывает так, что просмотр этих страниц даже не зависит от ребенка, ведь на многих сайтах отображаются всплывающие окна, содержащие информацию, которая не способствует нравственному воспитанию молодёжи.

- ***Контакты с незнакомыми людьми с помощью чатов или электронной почты.***

Все чаще и чаще злоумышленники используют эти каналы для того, чтобы заставить детей выдать личную информацию. В других случаях это могут быть «плохие люди», которые ищут новые жертвы. Выдавая себя за сверстника жертвы, они могут выведывать личную информацию и искать личной встречи.

- ***Всегда ли правдивая информация в сети Интернет?***

Следует знать, что нужно критически относиться к полученным из сети Интернет материалам, ведь опубликовать информацию может абсолютно любой человек. Знайте, что сегодня практически каждый человек может создать свой сайт, и при этом никто не будет контролировать, насколько правдива размещенная там информация. Научитесь проверять все то, что вы видите в сети Интернет.

- ***Оскорбления в сети Интернет.***

Часто бывает такое, что подростки выясняют отношения в сети, при этом употребляя оскорбительные слова и нецензурную брань в адрес друг друга. За такие деяния согласно ст. 9.3 Кодекса Республики Беларусь об административных правонарушениях предусматривается наложение штрафа в размере до двадцати базовых величин.

- ***Можно ли за фото или запись в социальных сетях привлечь к уголовной ответственности?***

И снова ответ утвердительный. *21-летний военнослужащий срочной службы из г. Ганцевичи оказался на скамье подсудимых за распространение или рекламирование порнографических материалов в глобальной компьютерной сети Интернет. Судебное заседание по ч. 2 ст. 343 УК Республики Беларусь прошло в суде Ганцевичского района 23 октября.* Судебный процесс проходил в закрытом режиме, в присутствии присяжных заседателей, так как обвиняемый совершил вменяемое ему преступление, будучи еще несовершеннолетним. *Санкция статьи предусматривает только лишение свободы – на срок от двух до четырех лет. Однако суд Ганцевичского района был снисходителен и назначил наказание в два года лишения свободы с отсрочкой приговора сроком на один год.*

Компьютерная зависимость. Эта новая болезнь поражает молодую часть населения, преимущественно подросткового возраста. Хоть заболевание не имеет ничего общего с инфекцией, но оно распространяется по миру со скоростью эпидемии. Очень много сообщений в прессе о том, что тут и там агрессивное поведение подростка привело к трагическим последствиям. Выводы экспертов не утешительны. Опасность стать зависимым от компьютерной игры грозит каждому, кто проводит за видеоиграми более двух часов в день.

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. Указанные темпы проникновения информационных технологий во все сферы жизнедея-

тельности человека наряду с имеющей место не квалифицированностью 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.

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

2. 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 непозволительно 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.

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;
- грумминг;
- секстинг;
- кибербуллинг;
- возможность возникновения *Интренет-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 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 пятна-*

дцати 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 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 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 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.*

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.

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.*

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

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. 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 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.*

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 уничтожение, блокирование, модификацию компьютерной информации, нарушение работы компьютерного оборудования либо причинение иного существенного вреда, — наказы-*

вается 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.*

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 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 статистическим данным 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.

Совершение в отношении ребенка правонарушений в сфере информационной безопасности.

Каждый пользователь компьютерной техники, сети Интернет автоматически становиться 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.

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.

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 ин-

формации, но и через электронную почту посредством спама или скачанных из интернета файлов.

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 физическому здоровью, а также в некоторых случаях и жизни ребенка.

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.

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.

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 сообща членами какого-либо Интернет-сообщества, в котором состоит ребенок, либо лицами, преследующими хулиганские мотивы. Проблемой в данном случае являются последствия психологического воздействия на ребенка.

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.

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.

Рекомендации родителям

Подростки в возрасте 14-17 лет

Рекомендации:

- интересуйтесь, какими сайтами и программами пользуются Ваши дети;
- 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, педагогу социальному учреждения образования, в правоохранительные органы по месту жительства.

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.