МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ БЕЛАРУСЬ

УПРАВЛЕНИЕ ВНУТРЕННИХ ДЕЛ ГРОДНЕНСКОГО ОБЛИСПОЛКОМА

КРИМИНАЛЬНАЯ МИЛИЦИЯ

ОТДЕЛ ПО РАСКРЫТИЮ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

МАТЕРИАЛЫ

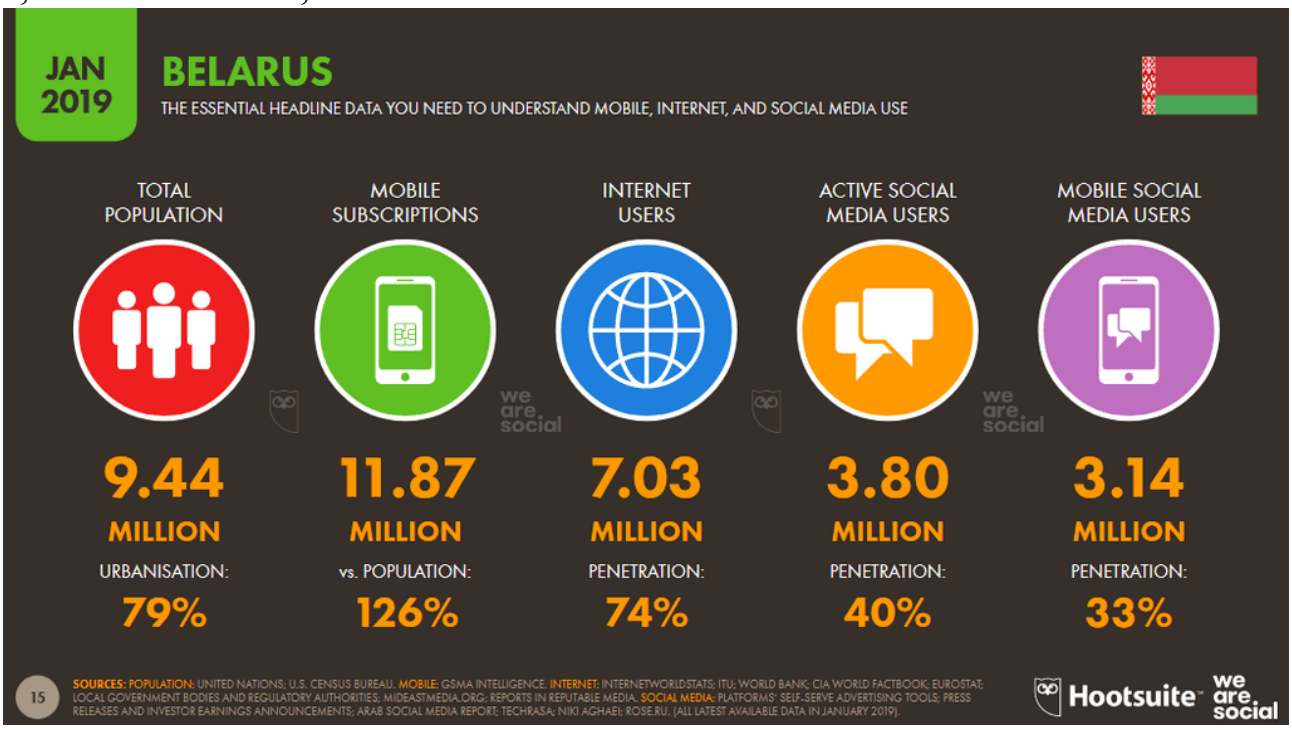
для ведения профилактической работы с учащимися учреждений образования и их родителями

Тема: «Профилактика преступлений в сфере высоких технологий среди несовершеннолетних»»

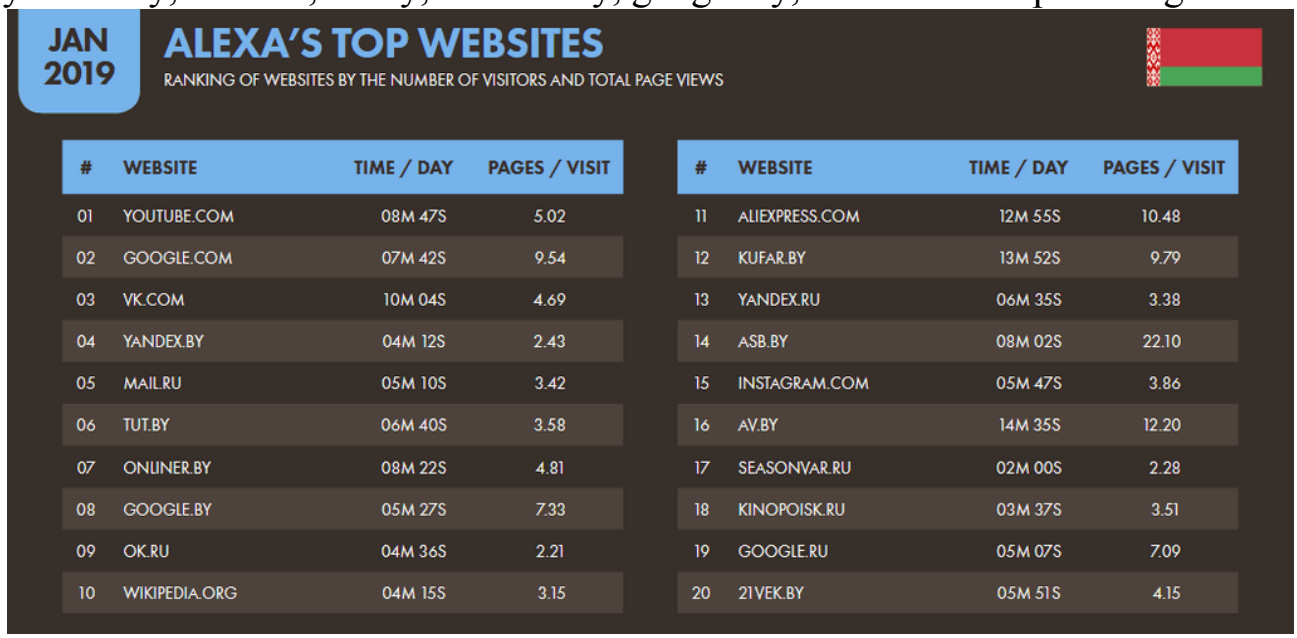
г. Гродно
2019

Количество пользователей сети интернет в Республике Беларусь и их сетевая активность имеют устойчивую тенденцию роста. Приведем некоторые статистические данные из открытых источников сети интернет.

К январю 2019 года на 9,44 млн. жителей Беларуси приходилось 11,87 млн. абонентов мобильной связи, за год прирост составил 3,1%. Количество интернет-пользователей также показало рост 4,5% и равняется 7,03 млн. человек, или 74% населения.



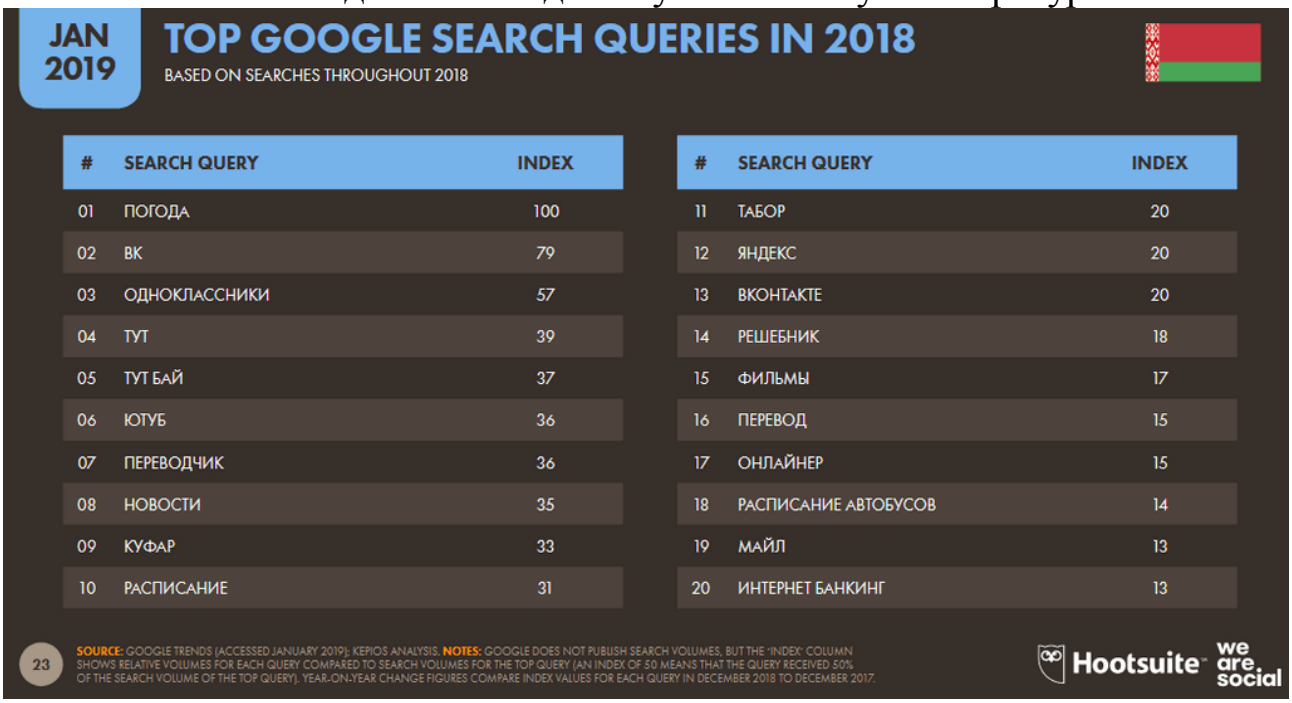
Самым популярным сайтом является YouTube, в среднем в день пользователь проводит на нём примерно 8 минут 47 секунд. На втором месте google.com – 7 минут 42 секунды, на третьем – сайт соцсети «ВКонтакте» с результатом 10 минут 4 секунды. В топ-10 попали yandex.by, Mail.ru, tut.by, Onliner.by, google.by, OK.ru и Wikipedia.org.



#	WEBSITE	TIME / DAY	PAGES / VISIT
01	YOUTUBE.COM	08M 47S	5.02
02	GOOGLE.COM	07M 42S	9.54
03	VK.COM	10M 04S	4.69
04	YANDEX.BY	04M 12S	2.43
05	MAIL.RU	05M 10S	3.42
06	TUT.BY	06M 40S	3.58
07	ONLINER.BY	08M 22S	4.81
08	GOOGLE.BY	05M 27S	7.33
09	OK.RU	04M 36S	2.21
10	WIKIPEDIA.ORG	04M 15S	3.15

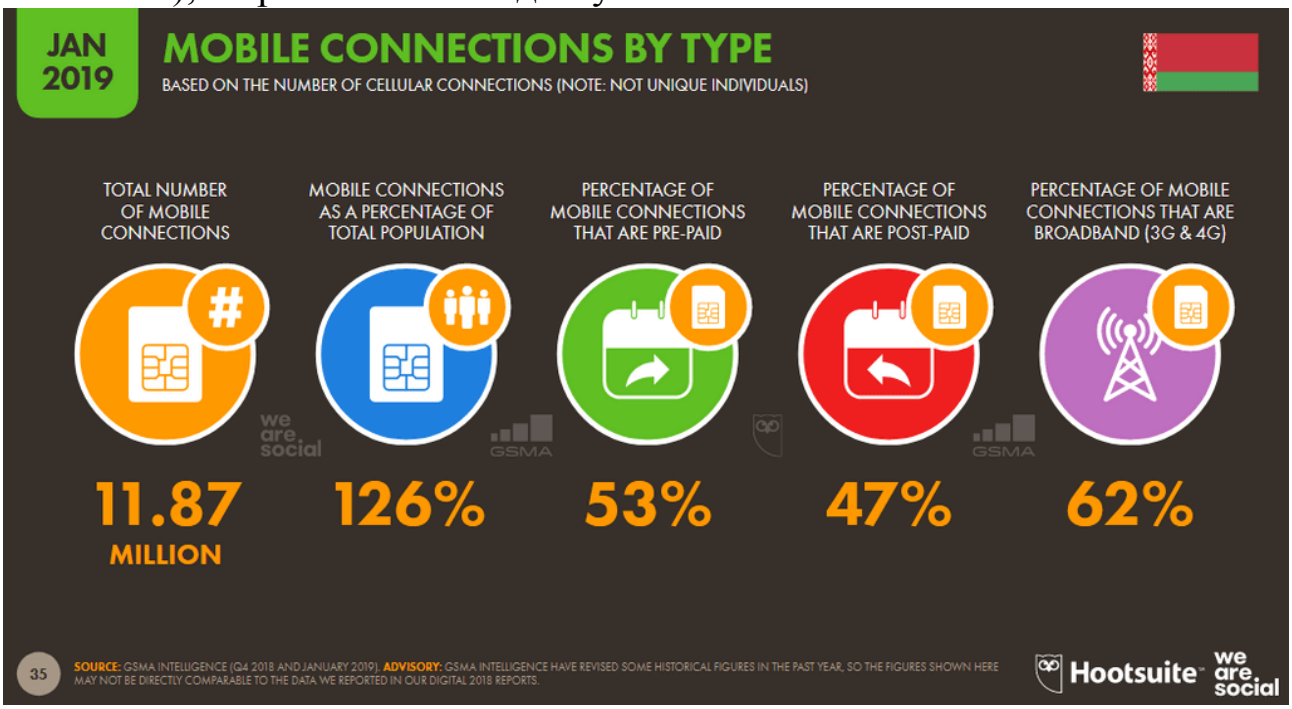
#	WEBSITE	TIME / DAY	PAGES / VISIT
11	ALIEXPRESS.COM	12M 55S	10.48
12	KUFAR.BY	13M 52S	9.79
13	YANDEX.RU	06M 35S	3.38
14	ASB.BY	08M 02S	22.10
15	INSTAGRAM.COM	05M 47S	3.86
16	AV.BY	14M 35S	12.20
17	SEASONVAR.RU	02M 00S	2.28
18	KINOPOISK.RU	03M 37S	3.51
19	GOOGLE.RU	05M 07S	7.09
20	21VEK.BY	05M 51S	4.15

Топовым поисковым запросом Google в 2018 году была «погода». Несколько реже белорусы искали «вк» и «одноклассники». При этом специфика поисковых запросов показывает, что пользователи не запоминают адреса полюбившихся сайтов, а ищут их в поисковике, что может повлечь попадание на подложную копию нужного ресурса.



Активные пользователи соцсетей составили 3,8 млн. человек, из них почти 83 процента пользуются соцсетями с мобильных устройств. Например, количество белорусских посетителей ВКонтакте оценивается в 3,5 млн., Одноклассников – около 2,7 млн., рекламная аудитория Instagram составляет 2,1 млн. пользователей, Facebook – 1 млн.

В Беларуси около 11,87 млн. мобильных абонентов (126% населения), широкополосный доступ имеют 62% абонентов.



Согласно исследованиям, 81% белорусов имеет счёт в банке, 46% делают покупки или оплачивают счета через интернет. Количество выданных банковских платежных карточек на конец 2018 года по данным Национального банка Республики Беларусь превысило 15 млн., инфраструктура их обслуживания включает более 121 тыс. объектов торговли и сервиса, более 4200 банкоматов, 3100 инфокиосков.

Указанные темпы проникновения информационных технологий и безналичных платежей во все сферы жизнедеятельности человека наряду с имеющей место неквалифицированностью и неосмотрительностью определенной части пользователей являются предпосылкой возрастающего количества киберинцидентов.

В том числе наблюдается высокая активность в сети интернет со стороны детей и подростков. Доступом в глобальную паутину, возможностью общения с использованием мессенджеров и социальных сетей пользуются дети начиная с младшего школьного возраста.

В данной ситуации значимой проблемой является *недостаточная подготовленность детей и подростков* к безопасному использованию информационных технологий. При этом стоит выделить три аспекта такой неподготовленности: *технологический*, выражающийся в недостаточной осведомленности о специфике информационного обмена в сети интернет, технологических аспектов создания, хранения и передачи информации и мер по обеспечению безопасности указанных процессов, *психологический*, проявляющийся в излишней наивности, доверчивости, отсутствии критического подхода к фактам и событиям, а также *организационный*, в соответствии с которым при использовании детьми и подростками информационных технологий не обеспечивается достаточный уровень контроля со стороны взрослых, а также не предпринимается мер по разъяснению им алгоритмов поведения при возникновении определенных проблемных ситуаций.

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 индивидуальная постоянная работа с ребенком, как правило со стороны родителей.

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;
- груминг;
- 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.

Уголовным кодексом предусмотрен ряд преступлений, отнесенных к компетенции подразделений по раскрытию преступлений в сфере высоких технологий. Рассмотрим их подробнее.

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.

Необходимо отметить, что ответственность за деяния, предусмотренные *ст.212*, наступает *с 14-летнего возраста*.

Примером такого преступления может быть хищение денежных средств с найденной либо похищенной банковской платежной карточки с использованием банкомата, платежного терминала. В последнее время наиболее актуальны факты хищений с использованием реквизитов карт 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 – несанкционированный доступ (открытие и просмотр файлов, писем, переписки) к электронной почте, учетным записям на различных сайтах, в том числе в социальных сетях, к информации, 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 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, шифровании) 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 и применяется при разработке, изготовлении и сбыте специальных программ и устройств, предназначенных для осуществления несанкционированных доступов, например поддельных смарт-карт для просмотра закодированных каналов спутникового телевидения.

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, -

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.

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

Ответственность за деяния, предусмотренные *ст.ст.349-355,* наступает *с 16-летнего возраста*.

Необходимо отметить, что количество преступлений в сфере высоких технологий имеет устойчивую тенденцию к росту. Так, в 2017 году на территории Гродненской области зарегистрировано 266 уголовных дел (Республика Беларусь – 3099), в 2018 – 300 (4741), а за 2,5 месяца 2019 года уже более 200 (1803).

В 2018 и начале 2019 года на территории Гродненской области наблюдается преобладание среди совершаемых преступлений противоправных деяний в сети Интернет, которые выражаются, с одной стороны, во «взломе» и несанкционированном использовании учетных записей пользователей в социальных сетях с целью выманивания реквизитов банковских платежных карточек, а с другой стороны – в совершении хищений с карт-счетов граждан путем использования компьютерной техники либо мошенничества.

Несмотря на предпринимаемые меры профилактического характера, продолжают регистрироваться преступления в сфере высоких технологий, совершаемые несовершеннолетними.

Так, в 2017 году к уголовной ответственности за совершение преступлений рассматриваемой категории в стране было привлечено 34 несовершеннолетних лица, из них 4 – в Гродненской области, в 2018 – 35 и 2 соответственно, за 2,5 месяца 2019 года – 9 и 1 соответственно. При этом количество фактов совершенных данными лицами преступлений в разы выше.

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 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, родители заказывают в банках дополнительные карточки для детей для осуществления платежей в объектах торговли и сервиса. 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.

К таким преступлениям могут быть отнесены следующие статьи Уголовного кодекса Республики Беларусь:

– мошенничество (ст.209 УК);

– причинение имущественного ущерба без признаков хищения (ст.216 УК);

– изготовление и распространение порнографических материалов или предметов порнографического характера (ст.343 УК, ст.343-1 УК);

– клевета (ст.188 УК);

– оскорбление (ст.189 УК);

– разжигание расовой, национальной или религиозной вражды или розни (ст.130 УК) и иные.

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 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 в компьютеры, не только через внешние носители информации, но и через электронную почту посредством спама или скачанных из интернета файлов.

5. *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.

6. *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.

7. *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. В качестве примеров таких сообществ можно привести группы, содержащие в своем наименовании фразы «синий кит», «колумбайн», «страх как он есть», «strax kak on est», «fear it self» и иные. Необходимо понимать, что основной критерием отнесения сообщества к деструктивным является не наименование группы, которое можно изменить в любой момент, а ее информационное наполнение и умысел администратора.

8. *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.

9. *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.

10. *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.

11. *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.

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 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.

- С ребенком необходимо установить доверительные отношения и положительный эмоциональный контакт в вопросе использования сети интернет. Необходимо оговорить с ребенком критический уровень опасности, когда решение в возникшей проблемной ситуации должно приниматься родителем (либо 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 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 межсетевой 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. Использование лицензионного программного обеспечения, полученного из доверенных источников, повышает безопасность работы в сети.

- 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 (напимер 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 интернет-пейджеры;

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

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 новыми 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 либо в правоохранительные органы по месту жительства.

ОРПСВТ КМ УВД Гродненского облисполкома