Угрозы цифрового мира.

В настоящее время мы наблюдаем стремительное развитие средств вычислительной техники различного назначения. Компьютеры все сильнее интегрируются в нашу повседневную деятельность. Все сильнее мы связаны с компьютерами в бытовой сфере и личной жизни. Средства связи уже предоставляют не только голосовые услуги, но и обмен фотографиями, видеороликами. Мы уже не представляем свою жизнь без различных соцсетей и мессенджеров. Различные сферы деятельности человека стремительно захлестывает волна цифровизации. Можно даже говорить, что часть жизни современного человека проходит в некоем цифровом (виртуальном) пространстве. Огромный, разносторонний цифровой мир наряду с благами приносит нам различные трудности и проблемы. Из-за скрытых, недокументированных возможностей информационных систем появляются сложности в управлении ими, а зачастую преступники, пользуясь недостаточной грамотностью людей в сфере информационных технологий наносят им материальный и моральный вред. Чтобы обезопасить себя в современной жизни, надо понимать какие угрозы таит в себе современный цифровой мир. Итак, рассмотрим виды угроз цифрового мира, преступные методы использования информационных технологий, а также какие угрозы подстерегают один из менее защищенных слоев нашего общества - детей.

Виды угроз цифрового мира.

- **Манипуляция сознанием**

  Кроме классических средств массовой информации все больше появляется информационных ресурсов в сети Интернет. Это различные соцсети, мессенжеры и т.п., информация в которых распространяется очень быстро, подобно лавине. Пользователями этих ресурсов в большинстве своем является подрастающее, молодое поколение людей. Поэтому различные методы манипулирования сознанием с использованием Интернет могут быть более эффективными для данной категории людей. Нужно всегда помнить, что манипуляция сознанием через средства массой информации может иметь как положительные так и негативные последствия.

- **Информационный коллапс**

  Большие данные (Big Data). Классическими источниками больших данных являются интернет вещей и социальные медиа. Также источниками возникновения больших данных считаются непрерывно поступающие данные с измерительных устройств, события от радиочастотных идентификаторов, потоки сообщений из социальных сетей, метеорологические данные, данные дистанционного зондирования Земли, потоки данных о местонахождении абонентов

сетей сотовой связи, устройств аудио- и видеорегистрации. Ожидается, что развитие и начало широкого использования этих источников инициирует проникновение технологий больших данных как в научно-исследовательскую деятельность, так и в коммерческий сектор и сферу государственного управления. Чтобы правильно и безопасно управлять такими большими потоками данных требуется развитие специальных методов и технологий их обработки и хранения. Иначе возникает угроза управлению производственными процессами, научной деятельностью, а также сложность государственного управления.

- **Кража цифровой личности**
  Сейчас интенсивно развиваются технологии виртуальной реальности. Они прочно входят в сферу развлечений. Технология «Дип-фейк», например, которая широко используется в кинематографе. Это когда черты лица человека преобразуются по определенному алгоритму. Эта технология приходит и в повседневную жизнь, когда замена внешности используется для шутки в видеочатах. Но эти игры могут легко «перейти» в угрозы морального, репутационного, материального характера по отношению к людям, чьё изображение используется в качестве подмены. А при злонамеренном использовании технологии «Дип-фейк» в видеоконференциях и новостных выпусках можно добиться негативного влияния на достаточно большую аудиторию.
  Не стоит забывать и о биометрических персональных данных, которые все чаще применяются в различных сферах для идентификации человека. Утечка этих данных из мест хранения и их несанкционированное использование может привести к очень негативным последствиям.

- **Управление поведением человека**
  Комплексное использование цифровых технологий может применяться для достижения желаемого результата в социальном управлении целыми регионами. Это так называемые агитационные методы. Используя соцсети и информационные Интернет-каналы, манипуляторы добиваются участия людей в несанкционированных мероприятиях. При этом часто используются методы социальной инженерии основанные, например, на обещаниях получения человеком «лёгкого заработка». На начальном этапе для сбора «толпы» манипуляторы могут пропагандировать вполне положительные цели (улучшение качества жизни, экономического благосостояния и т.п.). Но затем с использованием цифровых технологий происходит массовый «вброс» лживой информации, приводя массу людей к агрессивному состоянию. Эта угроза очень опасна тем, что наряду со значительным материальным ущербом может возникнуть даже угроза целостности государства.

- **Онлайн мошенничество**
  Развитие разнообразных цифровых технологий помогает людям решать многие повседневные задачи. Это банковские платежи, онлайн покупки, запись к специалистам в различных учреждениях и т.п. При этом многие не задумываются о том, что из-за собственной невнимательности и неосторожности могут пострадать от действий мошенников. Рассмотрим самые распространенные методы, которыми для достижения своих (в основном корыстных) целей пользуются мошенники.
  Фальшивые сайты и страницы. Мошенники изготавливают так называемые сайты «двойники» (копии), банков, онлайн магазинов, государственных учреждений и сервисов. При этом сайты визуально очень похожи на настоящие. «Двойники» регистрируются на доменные имена (интернет адреса) также похожие на оригинальные, но отличающиеся на какую-нибудь букву, символ и т.п. Пользователь вводит фальшивый адрес сайта (но как ему кажется оригинальный) и попадает на фальшивый сайт «двойник». Далее пользователь на фальшивом сайте вводит логин и пароль, которые похищают мошенники и затем от имени пользователя могут совершать злонамеренные действия.
  Фишинг. Для получения доступа к логинам и паролям мошенники проводят рассылки сообщений по электронной почте, в соцсетях, мессенджерах от имени популярных брендов, банков. Эти сообщения содержат ссылки на фальшивые сайты, переходя на которые пользователь вводит логин и пароль, которыми завладевают мошенники и используют в корыстных целях.

Угрозы информационной безопасности детей

Дети наиболее подвержены риску негативного влияния в цифровой информационной среде ввиду недостаточного жизненного опыта и знаний. Важна комплексная работа среди детей нескольких институтов: правительственные программы, семейное воспитание, работа образовательных и культурных учреждений. Немалое значение имеет и правильно организованная работа поисковых интернет-систем.
К наиболее распространенным угрозам информационной безопасности детей можно отнести следующие:

- **Вредоносные программы, спам;**
- **Контентные риски, неподобающий контент;**
- **Кибермошенничество;**
- **Киберпреследования: кибербуллинг, груминг;**
- **Интернет-зависимость.**

Вредоносные программы, спам. Вредоносные программы могут проникать на устройства ребенка разными способами, порой даже ребенок не замечает, что допустил «заражение» устройства вирусом. Вредоносные программы могут не только вывести устройства из нормального работоспособного состояния, но и передать персональные данные ребенка мошенникам. Противодействовать вирусам помогут антивирусные программы. Но наилучший эффект достигается в комплексе с осторожными действиями ребенка. Спам или навязчивая реклама может вызвать у ребенка ложное представление, что он обязан следовать рекламным призывам. Опять же на помощь могут прийти специальные программы: спам-фильтры, которые с помощью настраиваемых алгоритмов предотвращают появление нежелательной рекламы.

Контентные риски, неподобающий контент. Эта угроза возникает при неконтролируемом посещении ребенком сайтов, которые содержат информацию, запрещенную для распространении среди детей. А именно это информация:

- побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;
- способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;
- обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных законом;
- отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;
- оправдывающая противоправное поведение;
- содержащая нецензурную брань;
- содержащая информацию порнографического характера.

Защитить ребенка от нежелательного контента в Интернете можно соблюдая следующие правила:

- Необходимо приучить ребенка советоваться со взрослыми и немедленно сообщать о появлении нежелательной информации подобного рода;
- Необходимо объяснить детям, что далеко не все, что они могут прочесть или увидеть в Интернете – правда. Приучите их спрашивать о том, в чем они не уверены;

- Необходимо спрашивать ребенка об увиденном в Интернете. Зачастую, открыв один сайт, ребенок захочет познакомиться и с другими подобными ресурсами.

Кибермошенничество. Подростки уже самостоятельно могут совершать покупки товаров и услуг в Интернет-магазинах. При этом возникают указанные выше риски, связанные с похищением материальных средств и конфиденциальной информации. Не стать жертвой кибермошенников можно если проинформировать ребенка о самых распространенных методах мошенничества и научить его советоваться со взрослыми перед тем, как воспользоваться теми или иными услугами в Интернете. Необходимо установить на устройства антивирус или, например, персональный брандмауэр. Эти приложения наблюдают за трафиком и могут быть использованы для предотвращения выполнения множества действий на зараженных системах, наиболее частым из которых является кража конфиденциальных данных.
Для безопасного совершения покупок в интернет-магазинах надо следовать следующим правилам:

- Прежде чем совершить покупку в интернет-магазине, удостоверьтесь в его надежности;
- Необходимо вместе с ребенком познакомиться с отзывами покупателей;
- Проверьте реквизиты и название юридического лица – владельца магазина;
- Уточните, как долго существует магазин. Посмотреть можно в поисковике или по дате регистрации домена (сервис Whois);
- Поинтересуйтесь, выдает ли магазин кассовый чек;
- Сравните цены в разных интернет-магазинах;
- Позвоните в справочную магазина;
- Обратите внимание на правила интернет-магазина;
- Выясните, сколько точно вам придется заплатить (могут быть «скрытые» платежи);

Кибербуллинг. Это травля в Интернете. Это могут быть оскорбления и злые шутки в сообщениях или в комментариях, публикация личной информации (например, вашего адреса, номера телефона, интимных фотографий), посты с угрозами. Наиболее распространенные виды травли:

- Игнорирование жертвы в соцсетях или обрывание связи с ней;
- Агрессор регулярно угрожает жертве в Интернете, задаёт неприятные, личные вопросы или шантажирует;
- Высмеивание при помощи оскорблений;
- Публикация личной информации без разрешения её владельца;
- Публикация личной информации, которая может навредить репутации жертвы или разрушить её.

Если у ребенка наблюдается беспокойное поведение, неприязнь к Интернету, нервозность при получении новых сообщений, то вероятно он стал жертвой кибербуллинга. Ребенок может стать не только жертвой, но и инициатором кибербуллинга. Для предупреждения кибербуллинга необходимо следовать следующим правилам:

- Необходимо объяснить детям, что при общении в Интернете они должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов – читать грубости также неприятно, как и слышать;
- Необходимо научить детей правильно реагировать на обидные слова или действия других пользователей;
- Необходимо объяснить детям, что нельзя использовать Интернет для хулиганства, распространения сплетен или угроз;
- Необходимо следить за тем, что ребенок делает в Интернете, а также следить за его настроением после пользования Интернетом.

Груминг. Груминг это установление взрослыми дружеских отношений с несовершеннолетними через Интернет для вступления с ними в интимную связь, запугивания и шантажа. Для груминга злоумышленники используют социальные сети, электронную почту, текстовые сообщения, чаты в онлайн-играх, а также различные интернет-ресурсы для общения между пользователями. Избежать груминга по отношению к ребенку можно следуя следующим правилам:

- Необходимо выяснить, с кем контактирует в Интернете ребенок, стараться регулярно проверять список контактов детей, чтобы убедиться, что они лично знают всех, с кем они общаются;
- Необходимо объяснить ребенку, что нельзя разглашать в Интернете информацию личного характера (номер телефона, домашний адрес, название или номер школы и т.п.), а также пересылать интернет-знакомым свои фотографии;
- Если ребенок интересуется контактами с людьми намного старше его, следует провести разъяснительную беседу;
- Нельзя позволять ребенку встречаться с онлайн-знакомыми без разрешения или в отсутствии взрослого человека. Если ребенок желает встретиться с новым интернет-другом, следует настоять на сопровождении ребенка на эту встречу;
- Необходимо интересоваться тем, куда и с кем ходит ребенок.

Интернет-зависимость. «Путешествия» по бескрайним просторам Интернета позволяет почерпнуть много интересных знаний, которыми делятся люди. Но иногда они могут переступить ту незаметную черту, когда окажется, что влечение провести время в Интернете превратилось в зависимость. Чаще всего это игровая зависимость. Но и обычный серфинг может завоевать практически все время досуга человека, ограничивая

возможность заниматься другими делами. При этом может ухудшаться общее психоэмоциональное состояние и как следствие – возникновение различных заболеваний. Дети, ввиду не богатого жизненного опыта могут неправильно оценить тяжесть чрезмерного времяпровождения в Интернете, перерастающее в зависимость. Основными предвестниками появления интернет-зависимости являются:

- навязчивое стремление постоянно проверять электронную почту и другие онлайн сервисы;
- предвкушение следующего сеанса онлайн;
- увеличение времени, проводимого в Интернете;
- увеличение количества денег, расходуемых онлайн.

Обезопасить ребенка от интернет-зависимости можно жестко ограничив время пользования Интернетом. Но нельзя ограничиваться только этой мерой. Необходимо в освободившееся время заинтересовать ребенка заниматься другими полезными делами: занятием спортом, в различных кружках и мастер-классах, поездках и походах выходного дня, различные игры и занятия в семейном кругу. Важно научить ребенка пользоваться Интернетом как инструментом для своих полезных занятий (например, кулинарные рецепты или как смастерить что-либо полезное для семьи, друзей).

Стремительное развитие цифровых технологий в современном мире позволяют человеку достичь значительных успехов в различных сферах деятельности. Необходимо постоянно совершенствовать свои знания, чтобы противостоять угрозам, которые таит в себе богатый мир цифровых технологий.