Тема: «Профилактика преступлений, совершаемых с применением информационно-телекоммуникационных технологий»

Информационно-телекоммуникационные технологии (ИТТ) играют огромную роль в современном обществе и оказывают значительное влияние на различные аспекты жизни людей.

Во-первых, ИТТ позволяют существенно улучшить доступ к информации. С появлением Интернета и широкого распространения цифровых технологий стало возможным получать информацию из разных источников по всему миру всего лишь за несколько кликов. Это создает безграничные возможности для образования, самообразования, профессионального развития и культурного обогащения.

Во-вторых, ИТТ играют важную роль в коммуникации и обмене информацией. Они упрощают и ускоряют передачу сообщений, позволяют общаться с людьми по всему миру через электронную почту, социальные сети, видео- и аудиозвонки.

Тем не менее, следует отметить, что интенсивная цифровизация общества и связанное с ним расширение сфер применения ИТТ создают «благоприятную» среду для возникновения новых способов совершения преступлений, таких как:

1. Кибермошенничество: различные схемы обмана и мошенничества: фишинговые сообщения, ложные звонки «служб поддержки» и т.д.

2. Киберпроникновение (хакинг): проникновение в компьютерные системы или сети для получения незаконного доступа к данным, вреда или кражи информации для вымогательства денег, блокировки доступа к компьютеру или файлам, шифрование данных или угрозы публикации скомпрометированной информации.

3. Кибербуллинг: использование ИТТ для травли, угроз или домогательств в сети Интернет: публикация негативных сообщений, клеветы, манипуляция фотографиями и другие формы психологического насилия.

4. Кибертерроризм: использование ИТТ для создания паники, страха и нарушения общественной безопасности.

Виртуальное пространство предоставляет пользователям возможность взаимодействовать и общаться в онлайн-среде без раскрытия своей реальной личности, что приводит к возникновению ложного чувства анонимности и способствует проявлению негативных поведенческих тенденций, обусловленных ощущением «свободы выражать свои мысли без последствий», особенно подвержена «эффекту анонимности» молодежная среда в силу возрастных особенностей.

В контексте ложного чувства анонимности, подростки могут проявлять более агрессивное и провокационное поведение, чем в реальной жизни: безнаказанным может считаться распространение оскорблений, провоцирование конфликтов или онлайн-травля других людей, а в стремлении заработать «легкие деньги», осознавая противозаконность своих действий, они игнорируют неизбежность наступления общественно опасных последствий.

Кроме того, причинами совершения несовершеннолетними и в отношении них киберпреступлений могут послужить:

- низкий уровень критического мышления и правовой грамотности: дети и подростки зачастую не задумаются и не осознают потенциальных рисков, связанных с их действиями в сети, способных привести к нарушению законодательства и причинению материального ущерба;

- социальное давление и влияние сверстников: нередко несовершеннолетние втягиваются в киберпреступную деятельность под влиянием сверстников, желания быть "популярными" или из-за давления в круге общения;

- отсутствие контроля со стороны родителей: зачастую родители не осознают риски, связанные с использованием сети Интернет и не обеспечивают должный контроль над действиями своих детей в онлайн-пространстве.

В современных реалиях необходимо развивать у детей навыки цифровой гигиены, соблюдение базовых принципов которой позволит минимизировать уровень негативного влияния медиапространства, что является важным аспектом благополучия.

Одной из основных составляющих цифровой гигиены является поддержание электронной безопасности. Это включает в себя использование надежных паролей и их регулярное обновление, а также активацию двухфакторной аутентификации для защиты личных данных от несанкционированного доступа, также следует воздержаться от общения с неизвестными пользователями, от распространения информации личного характера о себе и своих близких, не ставить отметки о геолокации, относиться с подозрением к электронным сообщениям, требующим немедленно перейти по ссылке, позвонить или открыть вложение, перевести деньги или оплатить выигрыш и помнить, что Интернет — это публичное пространство, и вести себя в нем нужно точно также, как в любом другом общественном месте.

По информации ОУУП и ПДН УМВД России по Калининградской области

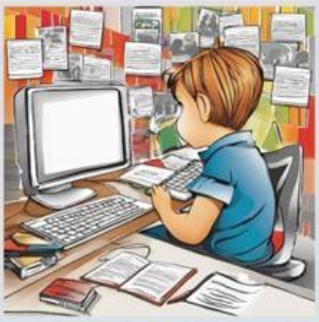
1. Защита паролей:
- Создавай сложные пароли, состоящие из различных символов и цифр.
- Никогда не используй один и тот же пароль для разных аккаунтов.
- Не сообщай свои пароли другим людям, даже друзьям.
- Регулярно меняй пароли.

2. Безопасность в онлайн-играх:
- Не доверяй незнакомым игрокам, не делись с ними личными данными.
- Никогда не указывай личные данные в игровых чатах.
- Если кто-то пытается тебя запугать или просит совершить что-то неправильное в игре, сообщи об этом родителям или учителям.

3. Осторожное поведение в социальных сетях:
- Не добавляй в друзья незнакомых пользователей.
- Не публикуй личные данные.
- Будь осторожен с тем, что ты публикуешь в Интернете.
Даже удалённые сообщения и фотографии могут быть сохранены и распространены другими людьми.

4. Защита от вредоносного ПО:
- Устанавливай антивирусное программное обеспечение на свои устройства.
- Не открывай подозрительные ссылки или вложения.
-Избегай открытых и ненадежных Wi-Fi сетей, так как они могут быть небезопасными.

5. Сообщение о подозрительной активности:
- Если ты видишь что-то подозрительное или странное в Интернете или в своих устройствах, сообщи об этом своим родителям.
- Если тебя пытаются шантажировать или запугать в Интернете, незамедлительно обратитесь за помощью к взрослым.



1. Кибербуллинг: дети могут стать жертвами онлайн-травли, угроз и неприятностей со стороны других детей через социальные сети, электронные сообщения или онлайн-игры.

2. Неподходящий контент: Дети могут натолкнуться на нежелательный или неподходящий контент в интернете, такой как насилие, порнография, наркотики или экстремистские идеологии.

3. Фишинг: Дети могут быть мишенью мошенников, которые могут отправлять им поддельные электронные сообщения или создавать фальшивые веб-сайты, чтобы получить их личную информацию.

4. Онлайн-мошенничество: Дети могут стать жертвами интернет-мошенничества, к огда им предлагают поддельные товары, у слуги или розыгрыши с целью выманивания денег или личных данных.

5. Утечка личной информации: Дети могут случайно или небрежно раскрыть свою личную информацию в интернете, что может привести к нежелательным последствиям.

6. Подделка личности: Дети могут столкнуться с ситуацией, когда кто-то создает фальшивые аккаунты или п редставляется ими в интернете, чтобы навредить им или другим людям.

Важно обучать детей основам безопасности в интернете и поддерживать открытую коммуникацию, чтобы они могли обратиться за помощью или советом, если столкнутся с киберрисками.