

«Мы имеем дело с целенаправленной идеологической угрозой»

Представители ФСБ на встрече с журналистами, школьниками и студентами в редакции «ОГ» рассказали, кто, как и зачем вербует подростков в Интернете

В редакции «Областной газеты» прошла встреча с официальным представителем УФСБ России по Свердловской области Еленой ДОКУЧАЕВОЙ. Журналисты издания, студенты и юнкоры проектов журфака УрФУ и школьники – участники проекта «ОГ-ого!» узнали, какие схемы сегодня чаще всего используют для вербовки подростков в Интернете и что делать, чтобы невинный диалог в соцсети не обернулся трагедией. Эмоциональное давление, манипуляции и угрозы в мессенджерах – еще не все методы, которые сегодня используют киберпреступники.

Столкнуться с угрозой в Интернете сегодня может любой. Злоумышленники становятся все активнее и все чаще выбирают в качестве жертв детей и подростков. Их ищут по открытым профилям в соцсетях, втягивают в общение через анонимные чаты и игры. Главная цель – подчинить эмоционально, разрушить критическое мышление и заставить действовать по нужному сценарию. Это уже не единичные случаи, а целенаправленная система воздействия. Об этом рассказала Елена Докучаева, которая в ходе беседы ответила на вопросы участников встречи и поделилась конкретными примерами из практики.

«ОГ»:

– Можно ли сегодня говорить о целенаправленной системе влияния на подростков?

– Да, мы наблюдаем именно это – не единичные случаи, а четко выстроенные схемы влияния. На днях ФСБ задержала 57 администраторов неонацистских телеграм-каналов, которые призывали несовершеннолетних к совершению терактов. Были предотвращены попытки нападения на школы в Москве и Тюмени, а также подготовка терактов в Кемерово, Ростове-на-Дону и Йошкар-Оле. У задержанных нашли переписку с кураторами из-за рубежа. Всего под их воздействие попали 305 школьников. Мы имеем дело не просто с кибермошенниками, а с целенаправленной идеологической диверсией.

– По каким критериям вербовщики в Интернете выбирают своих жертв? Как понять, что человек, особенно подросток с еще не окрепшей психикой, находится под угрозой?

– Все начинается с информации, которую мы сами размещаем о себе в Интернете. Открытые страницы в соцсетях, посты, фо-



тографии, комментарии дают злоумышленникам представление о нашей личности, слабостях, интересах. Они собирают данные, изучают психологический портрет и определяют болевые точки. Первый контакт маскируют под дружеское общение. Иногда все начинается с простой фразы: «Привет! Как ты?» Это может быть сообщение в онлайн-игре или приглашение в закрытую группу. Однако никакого внимания от незнакомцев в сети не бывает случайным.

Юлия Казмина, студентка 2-го курса факультета журналистики УрФУ:

– Получается, что не всегда встреча с мошенниками в онлайн начинается с психологического давления с их стороны?

– Они действуют очень тонко. Задача на первом этапе – дать человеку ощутить свою значи-

мость. Подростку, который чувствует себя одиноко, предложить поддержку и участие, и это будет выглядеть очень искренне. Многие, кто позже понял, что стал жертвой, рассказывали, что их просто «спрашивали, как дела», интересовались здоровьем, хвалили. Даже взрослые люди, которые были задержаны за диверсии, признавались, что этого было достаточно, чтобы поверить незнакомцу из соцсети: «ему было не все равно, он спрашивал, держится ли у меня температура...». Это известный способ сделать человека эмоционально зависимым, и вербовщики используют это в своих интересах.

«ОГ»:

– На каких платформах больше всего риска попасть в поле зрения злоумышленников?

– Везде, где есть возможность общения, существует риск быть замеченным. Социальные сети, мессенджеры, форумы, онлайн-игры. Особенно опасны анонимные чаты и закрытые сообщества, где создается иллюзия эксклюзивности. Игровые платформы, где подростки проводят часы, становятся полем для охоты. Вербовщики притворяются друзьями, наставниками и единомышленниками.

– Каким образом преступникам в онлайн становится понятно, что человека можно подтолкнуть к противоправным действиям?

– Они аккуратно прощупывают болевые точки. Это может быть любая идея, которая волнует человека, материальный интерес. В ход идут идеологические тезисы, обсуждение политики, формирование образа врага, создание чувства угрозы. Вместе с «заботой», комплиментами, якобы дружеским интере-

сом это приводит к разрушению критического мышления. Один из фильмов, ярко демонстрирующих возможности внушения, – «Фокус», где главный герой поддается влиянию подсознательных импульсов. Система работает аналогично: визуальные образы, фразы, мемы формируют наше мнение даже тогда, когда мы этого не осознаем.

– С развитием искусственного интеллекта появилось много дипфейков – подделывают не только голоса, но и видео. Есть ли какие-то способы отличить их от настоящих?

– Если полагаться только на свои личные ощущения, то почти нет. Я сама получала фальшивые голосовые от знакомых с просьбой перевести деньги. Все выглядело очень правдоподобно. Нужно понимать: технологии ушли далеко, и это требует еще большей бдительности. Мошенники используют не только подменные фото и номера телефонов, но и видеоизображения. Задавайте контрольные вопросы, ответы на которые знает только ваш реальный знакомый.

Кристина Агранович, студентка 2-го курса факультета журналистики УрФУ:

– А вы сами лично сталкивались с мошенниками в Интернете?

– Да. Мне написал в телеграм якобы бывший директор. Все выглядело достоверно: фото, стиль общения. Но потом он не смог ответить на пару простых проверочных вопросов. Также его номер был скрыт. Сотрудники правоохранительных органов часто становятся мишенью киберпреступников. Вот почему так важно проверять, кто вам пишет и не верить на слово, даже если сообщение приходит от близкого человека. Насторожить должны любые нетипичные и срочные просьбы.

«ОГ»:

– Есть ли какие-то наиболее распространенные схемы обмана и вербовки онлайн?

– Они каждый раз меняются. Преступники разыгрывают целые спектакли. Их цель – вызвать панику, отключить критическое мышление и заставить перевести деньги, предоставить любые личные данные, совершить преступление.

Вам могут писать от имени директора, потом позвонить «сотрудники ФСБ», «банка», «полиции». Были случаи, когда