Современное общество живет в эпоху беспрецедентного распространения технологий, ввиду которого цифровизация становится одной из основных движущих сил развития различных сфер деятельности. Наряду с совершенствованием технологических процессов получают развитие электронные сервисы: финансовые услуги, дистанционное управление устройствами, удаленная работа и учеба, интернет-торговля, социальные и нейросети. Они прочно вошли в повседневную жизнь, упрощая быт, повышая комфорт, улучшая качество жизни граждан.

Наряду с безграничными возможностями всеобщая цифровизация несет новые вызовы и угрозы. Глобальная компьютерная сеть Интернет, созданная как платформа для свободного обмена информацией и сотрудничества, все чаще становится полем для преступной деятельности. Киберпреступность представляет собой одну из наиболее серьезных опасностей современности, являясь организованной, высокотехнологичной и финансово мотивированной системой, способной наносить колоссальный ущерб. Зачастую она направлена на одну из наиболее уязвимых категорий – несовершеннолетних.

Так, по итогам января т.г. количество несовершеннолетних, признанных потерпевшими от киберпреступлений, возросло (+39,0% с 41 до 57). В основном дети пострадали от вымогательств (рост в 3,4 раза; с 9 до 31) и уничтожения, блокировки или модификации компьютерной информации в сети Интернет (рост с 0 до 3).

Одним из распространенных механизмов вымогательства у детей денег является блокировка «Apple ID» их мобильных устройств: пострадало 28 подростков, 3 – в результате угрозы распространения фотографий интимного характера, изготовленных и высланных несовершеннолетними злоумышленникам в ходе знакомства.

От мошеннических действий потерпевшими признано 16 подростков (АППГ – 17), из которых 13 пытались приобрести на онлайн-площадках товары по цене ниже рыночной (в основном это были мобильные телефоны марки «Iphone»), 3 – от действий телефонных мошенников по «декларированию» денежных средств родителей.

Необходимо отметить, что в феврале т.г. появилась новая схема преступных действий с использованием информационно-коммуникационных технологий (далее – ИКТ) в отношении несовершеннолетних. Она выглядит следующим образом.

Ребенку в мессенджере («Telegram», «WhatsApp», «Viber» и др.) поступает звонок от якобы курьера «Wildberries», который сообщает о поступившей посылке. Под предлогом уточнения адреса ее доставки он просит продиктовать ему данные личной электронной почты и код из сообщения. После этого с потенциальной жертвой связывается «псевдоправоохранитель», который сообщает подростку, что от его имени производятся незаконные переводы денежных средств за границу. Также несовершеннолетнего информируют, что за это родителям грозит

уголовная ответственность, а его самого направят в приют.

Чтобы этого избежать, ребенку предлагается передать преступникам имеющиеся в доме денежные средства. Действия по поиску сбережений необходимо снимать на камеру мобильного телефона и высылать подтверждающие видеозаписи злоумышленнику.

Если несовершеннолетний не может найти деньги, ему предлагают поучаствовать в «специальной операции» по изобличению преступников. Чтобы последние не смогли прослушать его телефонные разговоры, подростку рекомендуется выключить мобильный телефон, извлечь и уничтожить (сломать) сим-карту оператора связи и идти по указанному мошенниками адресу, как правило, удаленному от места жительства, где «будет проходить спецоперация». После этого мошенники пишут родителям, что их ребенок похищен, и предлагают им перевести денежные средства, которыми они располагают, на электронный кошелек. Для убедительности законным представителям высылают видеоматериалы и персональные фотографии из квартиры (дома), предоставленные преступникам путем пересылки самим же подростком. В связи с ликвидацией сим-карты телефон подростка становится недоступным, что не дает возможность связаться с ним и установить его реальное местонахождение.

Кроме того, распространена следующая схема хищения денежных средств с использованием ИКТ на торговой площадке «Kufar». Так, мошенниками размещается информация о продаже товаров, пользующихся спросом у подростков (телефоны марки «Iphone», брендовые вещи, платья для бальных танцев и др.) по цене в разы ниже рыночной стоимости. Ребенок, видя выгодное предложение, направляет продавцу сообщение, в котором уточняет интересующие его вопросы относительно товара и способ его получения. В случае договоренности, продавец предлагает покупателю оформить доставку товара через почтовое отправление (Белпочта, Европочта и др.), предварительно оплатив услуги доставки. Для этого ребенку в мессенджер высылается ссылка на мошеннический (фишинговый) сайт, который визуально схож с официальным сайтом сервисов доставки товаров и почтовых отправлений (Белпочта, Европочта и др.). Однако, в его названии, как правило, заменен один или два символа. В данной ссылке указывается сумма оплаты и необходимость обязательного введения номера банковской платежной карты (далее – БПК) и трехзначного CVV кода, размещенного на оборотной ее стороне. Кроме этого, необходимо заполнить специальную графу «Остаток денежных средств, имеющихся на БПК». Выполнив указанные требования, подростку-покупателю направляется код авторизации, который он сообщает мошеннику, тем самым предоставляет удаленный доступ к денежным средствам, имеющимся на БПК. Далее злоумышленник с БПК покупателя переводит их на свой счет. После совершение хищения товар не высылается, а покупателя блокируют.