УДК 343.97

МОШЕННИЧЕСТВО, СОВЕРШЕННОЕ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ, КАК ОДНА ИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ

А. Ю. Сологубов
слушатель 5 курса
факультета подготовки сотрудников полиции и следователей
Барнаульского юридического института МВД России
Научный руководитель: ***И. В. Ботвин****,*
начальник кафедры уголовного права и криминологии
Барнаульского юридического института МВД России,
кандидат юридических наук, доцент

В настоящее время научно-технический прогресс шагнул стремительно вперед, из индустриального общества в общество информационное. Отличительной особенностью информационного общества является развитие информационных технологий, массовое включение в работу множества высоких технологий во всех сферах жизни человека.

Как правило, преступников интересуют персональные данные жертв. Именно их современный человек должен беречь особенно тщательно. Зачастую жертвами мошенников становятся и продавцы, и покупатели на известных сайтах «Авито» и «Юла» [1].

Для защиты от нового вида мошенничества нужно с осторожностью относиться к оплате и озвучиванию своих паролей или пин-кодов от карт. При любых подозрениях нужно самостоятельно перезвонить человеку по знакомому номеру. Нельзя не согласиться с тем, что «самое уязвимое место в защите информационной системы от мошенничества — это человек, никакие программно-аппаратные средства не защитят вас, если вы будете неосторожны и невнимательны» [2].

Стоит упомянуть и про необходимость введения двухфакторной аутентификации. При осуществлении переводов через онлайн-кошельки/карты подтверждением данного перевода является смс-код, который приходит на номер, зарегистрированный в мобильном банке. Но если злоумышленник завладел сим-картой и может перехватывать все приходящие смс-коды? Наше предложение состоит в том, что, к примеру, при переводе сумм, начинающихся с 5 тысяч рублей, стоит вводить проверку на безопасность данного платежа, то есть сотрудники банка должны будут проверить все данные платежа: как и откуда

он был отправлен, его назначение, возможно, комментарии, которые были указаны к платежу.

Со стороны государства необходимо ввести уроки цифровой грамотности, заручившись тем, что информационная гигиена — это не техническая информация, а этическая проблема. Необходимо говорить о повышении грамотности населения. Основными субъектами профилактики в данном случае служат сами граждане, которые должны вдумчиво относиться к любым звонкам по поводу их денежных средств или иных материальных ценностей. Таким образом, на основании нашего предложения может быть снижен риск потери личных денежных средств у граждан не только в России, но и в Беларуси, будут пресечены мошеннические посягательства на имущество граждан.

1. Сологубов А. Ю. Мошенничество в период пандемии COVID-19 // Молодежь — Барнаулу : материалы XXII гор. науч.-практ. конф. молодых ученых, Барнаул, 2–9 нояб. 2020 г. / Алтайский гос. ун-т ; под ред. Ю. В. Анохина. Барнаул : Алтайский гос. ун-т, 2021. С. 903–904. Вернуться к статье

2. Дьяков Н. В. Применение методов социальной инженерии в социальных сетях // Общество. 2020. № 2 (17). С. 126–128. Вернуться к статье