УО «БГУ»
пр-т Независимости, 4
220030, г.Минск

ИНФОРМАЦИОННОЕ ПИСЬМО

О вопросах профилактики преступлений против собственности и информационной безопасности

За истекший период 2026 года Первомайским (г. Минска) районным отделом Следственного комитета Республики Беларусь возбуждено более 350 уголовных дел о хищениях имущества путем обмана или злоупотребления доверием (ст. 209 УК), о хищениях имущества путем модификации компьютерной информации (ст. 212 УК), о вымогательстве (ст. 208 УК), в том числе уголовное дело №26121060786, возбужденное 17.07.2026 по ч. 1 ст. 212 УК.

В Республике Беларусь все чаще становятся актуальными проблемы преступности в сфере высоких технологий. Активизация киберпреступлений происходит на фоне ежегодного роста числа абонентов сотовой электросвязи, держателей банковских платежных карт (далее – БПК), а также пользователей сети Интернет.

Участились случаи хищения денежных средств с банковских счетов, доступ к которым обеспечивается при использовании БПК, после передачи либо завладения информацией о реквизитах БПК злоумышленниками.

Современные методы оплаты в сети Интернет позволяют совершать платежи без знания пин-кода карты, путем введения в компьютерную систему сведений о номере карты, сроке ее действия, владельце, а также коде безопасности – CVC (как правило, трехзначный код, находящийся на оборотной стороне карты). Данные обстоятельства позволяют злоумышленникам, завладевшим указанными реквизитами БПК, совершать платежи в сети Интернет без ведома владельца, обладая всей необходимой для этого информацией.

Вместе с тем интернет-банкинг постепенно завоевывает статус основной платформы для заказа банковских услуг, осуществления денежных переводов и управления открытыми расчетными счетами. Для доступа к системе виртуального банкинга клиент должен установить мобильное приложение или зарегистрироваться на официальном сайте финансового учреждения. Авторизация производится с привязкой

к номеру телефона. Часто пользователи интернет-банкинга указывают пароль, который совпадает с логином пользователя в учетной записи, то есть номером телефона клиента, что позволяет методом подбора осуществлять вход в личные кабинеты пользователей.

Следует отметить, что в последнее время участились случаи противоправных действий в сфере информационных технологий, а именно хищений с БПК и счетов физических и юридических лиц, примеры подобных фактов приведены далее.

1. Злоумышленник после несанкционированного доступа к страницам пользователей в социальных сетях рассылает пользователям, находящимся в разделе «Друзья», сообщения с просьбой об оказании помощи в переводе денежных средств под различными предлогами: «Привет, не мог ли ты одолжить мне денег, отдам через пару дней», «Привет, положи, пожалуйста, 10 рублей на телефон, я отдам», «Привет, можно я переведу тебе на карту свои деньги, а то у меня закончился срок действия карты (или не получается перевести на свою)». Далее входит в доверие к неравнодушным пользователям и, якобы для перевода им денежных средств, просит сообщить реквизиты БПК и коды из смс-сообщений. Пользователь, введенный в заблуждение относительно лица, осуществившего указанную рассылку, и не догадываясь о преступности намерений, сообщает ему указанные сведения, ввиду чего злоумышленник получает доступ к денежным средствам пользователя и совершает их хищение.

Проведя несанкционированную операцию по переводу денежных средств, злоумышленник часто сообщает пользователю, что по техническим причинам не может осуществить операцию и просит повторить указанные действия с какой-либо другой картой (родственников или знакомых).

Справочно: в производстве Первомайского (г.Минска) районного отдела Следственного комитета (далее – Первомайского РОСК) находится уголовное дело по факту совершения преступления, предусмотренного ч. 1 ст. 212 УК по факту хищения денежных средств путем модификации компьютерной информации. Установлено, что в ходе личной переписки мессенджере Telegram потерпевшей от знакомой поступила просьба о покупке услуги в онлайн-игре, для чего был предоставлен QR-код. Перевести денежные средства самостоятельно потерпевшей не удалось, после чего от знакомой поступила просьба предоставить конфиденциальные данные выпущенной на ее имя банковской платежной карты для самостоятельной покупки услуги, а также сообщить поступившие проверочные коды, в результате чего произошло хищение всех денежных средств, находившихся на счете потерпевшей.

2. На торговых площадках «Куфар», «Барахолка» и других правонарушитель находит объявление, размещенное пользователем

о продаже какого-либо имущества, после чего в различных мессенджерах пишет данному пользователю о том, что хотел бы приобрести его имущество, указанное в объявлении, однако по различным причинам не имеет возможности за ним приехать. Он предлагает произвести оплату путем перевода денежных средств на БПК пользователя и, после того как пользователь соглашается, высылает в его адрес ссылку с фишинговой страницей сайта какого-либо банковского учреждения (страница может быть визуально схожа со страницей интернет-банкинга и отличаться только символом в адресной строке доменного имени сайта). Переходя по указанной ссылке, пользователь не замечает, что находится не на действующей странице интернет-банкинга определенного банка. В открывшемся окне на указанном сайте пользователю, как правило, предлагается ввести свой логин и пароль от интернет-банкинга либо паспортные данные, а также коды из смс-сообщений. Введя указанную информацию пользователю, как правило, сообщается об ошибке либо отсутствии платежа. В это время всю введенную информацию видит злоумышленник и вводит на действительном сайте банка, получая тем самым доступ к денежным средствам пользователя и совершая их хищение. Проведя несанкционированную операцию по переводу денежных средств, правонарушитель нередко сообщает пользователю, что по техническим причинам не может осуществить операцию, и просит повторить указанные действия с какой-либо другой картой (родственников или знакомых).

Справочно: в производстве Первомайского (г. Минска) РОСК находится уголовное дело по факту совершения преступления, предусмотренного ч. 1 ст. 212 УК по факту хищения денежных средств потерпевшей в сумме 205 рублей путем модификации компьютерной информации. Установлено, что потерпевший на торговой площадке «Куфар» разметил объявление о продаже автомобильных дисков, указав свои контактные данные. В последующем на абонентский номер потерпевшего в мессенджере «Viber» поступило сообщение от «Ивана», который изъявил желание приобрести вышеуказанный товар, предложив продавцу воспользоваться услугой доставки, которую «Иван» обязался оплатить самостоятельно. Для получения денежных средств, отправленных в качестве оплаты товара, «Иван» отправил потерпевшему ссылку, перейдя по которой последний ввел номер выпущенной на его имя банковской платежной карты, а также пришедший в смс-сообщении проверочный код.

В дальнейшем, в считанные минуты после предоставления указанных сведений, со счета банковской платежной карты потерпевшего были списаны все имеющиеся денежные средства в сумме 205 рублей.

4. На мобильный телефон физического лица поступает входящий звонок от злоумышленника. Как правило, данным способом злоумышленник пользуется сервисом по подмену номера телефона и указывает абонентский номер, принадлежащий какому-либо банку,

организации (например УП «А1», «Энергосбыт», «Беллифт», «БелГИЭ») или схожий с ним. Далее он представляется сотрудником названной организации либо сотрудником органов внутренних дел (может назвать пользователя по имени и отчеству, а также назвать часть номера банковской карты либо информацию о недавно совершенных оплатах). Злоумышленник сообщает о подозрительных операциях по переводу денежных средств в крупных суммах на карт-счета иностранных банков, на финансирование каких-либо операций. Когда пользователь сообщает, что никаких операций он не производил, злоумышленник сообщает, что указанные операции необходимо заблокировать, в связи с чем просит пользователя сообщить отдельные реквизиты БПК либо паспортные данные, и сообщает, что в адрес пользователя высылает смс-сообщения с кодами, которые необходимо назвать после звукового сигнала.

Предлог может быть иной: злоумышленник, представляясь близким родственником, сообщает, что он стал виновником ДТП, и ему срочно требуются денежные средства для компенсации морального вреда пострадавшему для избежания наказания в виде лишения свободы.

В дальнейшем, после распространения кода, пришедшего на мобильный телефон, независимо от предшествующего этому предлога, под видом работников контролирующих и правоохранительных органов злоумышленник уговаривает последних оформить на свое имя кредиты либо задекларировать имеющиеся денежные средства. При этом полученные деньги предлагается передать лже-работникам службы безопасности банка или лже-работникам правоохранительных органов для последующего задержания «преступников»,/ помощи родственникам/декларирования, либо же перевести самостоятельно, в том числе посредством международных переводов «Юнистрим», «Золотая Корона».

Для подтверждения своих слов телефонные мошенники могут прислать через мессенджеры фотографии фальшивых служебных удостоверений работников правоохранительных органов, в том числе с указанием данных действующих работников. Злоумышленник выходит на связь с потерпевшим посредством видеозвонка, на котором изображен человек в фальшивой форме правоохранительных органов, чем еще сильнее входит в доверие потерпевшего.

Таким образом, злоумышленник вынуждает последнего передать все имеющиеся у него наличные денежные средства для их легализации/проверки/помощи родственнику, после чего не выходит на связь.

Справочно: В производстве Первомайского РОСК находится уголовное дело по факту совершения преступления, предусмотренного ч. 1 ст. 209 УК по факту завладения путем мошенничества денежными средствами потерпевшей в сумме 114560 рублей. Установлено, потерпевшей с абонентского номера российского оператора связи поступил звонок неустановленного лица, представившегося работником домофонной службы, который предложил оформить услугу по замене домофона, для чего необходимо продиктовать код доступа, пришедший на мобильный телефон потерпевшей.

Сразу после этого, в мессенджере «Viber» с абонентского номера белорусского оператора связи потерпевшей поступил звонок от неустановленного лица, представившегося сотрудником правоохранительных органов, который сообщил, что только что потерпевшая предоставила удаленный доступ к своим личным данным мошенникам, в связи с чем те намереваются похитить ее денежные средства и перевести на территорию Украины. Для обеспечения сохранности денежных средств, потерпевшая сняла денежные средства со своих банковских счетов и в этот же день нарочно передала их лже-курьеру Национального Банка Республики Беларусь, прибывшему к ней домой.

5. В мессенджере «Telegram» и на сайтах знакомств злоумышленник осуществляет общение с потенциальным потерпевшим. Злоумышленник изъявляет желание познакомиться и ближе узнать друг друга. После того как он втирается в доверие к потерпевшему просит оказать ему помощь. Так как его мобильный телефон (iPhone) сломался, то он теперь не может войти в свой ICloud и скачать свою личную информацию, в связи с чем просит потерпевшего выйти из своего ICloud и войти в его аккаунт. При этом он направляет потерпевшему логин и пароль для входа. Потерпевший, доверившись злоумышленнику делает то, что он ему говорит. После ввода чужих данных для входа мобильный телефон потерпевшего блокируется и на экране появляется иконка «Телефон утерян. Для разблокировки писать @аккаунт». После чего потерпевший пишет указанному аккаунту, чтобы ему разблокировали мобильный телефон, однако ему выставляют требование, чтобы он оплатил данную услугу. Суммы варьируются от 100 до 300 долларов США. После всех произведенных действий потерпевший более не может вернуть свой мобильный телефон к обычным настройкам и более не может им пользоваться. Таким же образом происходят действия, когда потерпевшему необходимо скачать какое-либо приложение и он просит помощи в установке приложения у неустановленных лиц в различных группах в мессенджерах.

Справочно: В производстве Первомайского РОСК находится уголовное дело по факту совершения преступления, предусмотренного ч. 1 ст. 208 УК по факту вымогательства. Установлено, что потерпевший в группе по поиску работы мессенджера «Telegram» начал диалог якобы с нанимателем, в ходе личной переписки с которым по его просьбе осуществил выход со своего аккаунта iCloud для входа на iCloud организации, в которую желал устроиться. В последующем

злоумышленник посредством переписки в указанном мессенджере сообщил, что для разблокировки мобильного устройства потерпевшего ему необходимо произвести оплату в размере 13000 российских рублей.

6. В сети Интернет размещают рекламу якобы инвестиционных платформ, которых на самом деле не существует, чтобы заманить вкладчиков и похитить их деньги. Первым шагом для связи с куратором является заполнение формы, где необходимо оставить свои имя и телефон. Далее с заинтересовавшимся связывается так называемый куратор, под руководством которого в надежде заработать легкие деньги потенциальная жертва сама переводит деньги на электронный кошелек. Чтобы получить хотя бы вложенные деньги обратно, злоумышленники требуют заплатить комиссии, взносы и т.д. Некоторое время они рисуют жертве их прибыль, пока у обманутого человека не закончатся деньги, потом связь с ним прекращается. Деньги остаются на счетах злоумышленников.

Справочно: в производстве Первомайского РОСК находится уголовное дело по факту совершения преступления, предусмотренного ч. 3 ст. 209 УК по факту хищения денежных средств под предлогом инвестирования в криптовалюту. Установлено, что потерпевший зарегистрировался на инвестиционной платформе «MorganMetrics.com», введя свои паспортные данные. Спустя некоторое время в мессенджере Telegram ему поступило сообщение от пользователя «@Demin_Alexa», который, представившись брокером, на протяжении нескольких дней указывал потерпевшему на необходимость покупки различной валюты на криптобиржах и ее перевода на личный счет вышеуказанной платформы. Когда потерпевший захотел вывести денежные средства, ему сообщили, что для их вывода необходимо пополнить баланс счета указанной платформы на 6000 долларов США, только после чего вывод денежных средств станет возможен. В ходе инвестирования потерпевший осуществил покупку криптовалюты и перевод ее на счет, данными которого владел злоумышленник, на сумму 4092,7 долларов США, что в эквиваленте составило 16 813 белорусских рублей.

Таким образом, необходимо резюмировать, что вся запрашиваемая преступником указанная в вышеобозначенных ситуациях информация **известна сотрудникам банка, которые не устанавливают ее в ходе телефонного разговора**.

Для того чтобы обезопасить себя и свои денежные средства от подобных способов хищения, необходимо:

не разглашать логины, номера телефонов, пароли, ПИН-коды, реквизиты расчетных счетов, секретные CVC/CW коды, сведения о последних платежах и сроке действия пластиковых карт третьим лицам;

в ходе использования карты подключить и использовать технологию «3D Secure». На настоящий момент это самая современная технология обеспечения безопасности платежей по карточкам в сети Интернет. Позволяет однозначно идентифицировать подлинность держателя карты,

осуществляющего операцию, и максимально снизить риск мошенничества по карте. При использовании этой технологии держатель банковской карты подтверждает каждую операцию по своей карте специальным одноразовым паролем, который он получает в виде SMS-сообщения на свой мобильный телефон;

исключить передачу посторонним лицам полученных в SMS-сообщениях временных паролей для подтверждения операций, а также своих банковских карт, каким бы то ни было способом;

вводить секретные данные только на сайтах, защищенных сертификатами безопасности и механизмами шифрования. Доменные имена этих ресурсов в адресной строке каждого браузера начинаются с https://;

производить регулярный мониторинг выполненных операций, используя раздел с историей платежей;

не отказываться от дополнительного уровня безопасности (системы многоуровневой аутентификации);

подобрать сложный пароль, используя набор цифр, заглавных и строчных букв, который будет понятен лишь владельцу аккаунта. Менять пароль каждые 2 – 4 недели, если пользуетесь чужими компьютерами для входа в систему интернет-банкинга;

не применять автоматическое запоминание паролей в браузере, если к персональному компьютеру открыт доступ посторонним лицам или для входа на сайт используется компьютер общего доступа;

в ходе использования интернет-банкинга устанавливать антивирусную защиту, своевременно обновляя базы данных вирусов и шпионских утилит;

вход в личный кабинет на сайте интернет-банкинга привязать к MAC или IP-адресу. Это действие обеспечит максимальный уровень безопасности;

использовать для оплаты товаров и услуг в сети Интернет банковские платежные карты, которые не являются зарплатными/пенсионными;

установить лимит на количество и сумму транзакций снятия наличных денежных средств и безналичной оплаты.

В случае обнаружения утерянной кем-либо БПК не стоит выкладывать ее фотографию в сети Интернет с целью поиска владельца. Информации, имеющейся на изображении БПК, достаточно для совершения операций с использованием этих данных без ведома владельца банковской карты, чем и пользуются злоумышленники.

В целях устранения причин и условий, способствовавших совершению преступления, руководствуясь статьей 4 Закона Республики

Беларусь от 13.07.2012 № 403-З «О Следственном комитете Республики Беларусь», прошу: рассмотреть информационное письмо с сотрудниками Вашей организации с целью недопущения совершения преступлений в отношении сотрудников Вашей организации; **в соответствии** с требованиями Закона Республики Беларусь от 04.01.2014 № 122-З «Об основах деятельности по профилактике правонарушений» **на системной основе проводить информирование сотрудников о проявлении осторожности и бдительности, соблюдении установленных правил безопасности пользования персональными БПК,** предупредить о недопустимости игнорирования и пренебрежения действенных требований, направленных на сохранение благосостояния граждан.

С учетом темпа развития информационных систем, внедрения новых цифровых технологий принимать дополнительные меры по безопасности использования банковских продуктов.

О принятых мерах прошу уведомить Первомайский (г. Минска) районный отдел Следственного комитета в месячный срок.

С уважением,

Следователь
Первомайского (г. Минска) районного отдела
Следственного комитета Республики Беларусь Е.В.Рудомина
8017-280-22-95