

МАТЕРИАЛЫ
для членов информационно-пропагандистских групп
(март 2021 г.)

**Профилактика преступлений, связанных с неправомерным
завладением реквизитами пластиковых банковских карт и хищением
средств с карт-счетов граждан, а также в сфере высоких технологий**

*Материал подготовлен
управлением Следственного комитета Республики Беларусь
по Гродненской области*

Интернет и компьютерные технологии стремительно проникают во все сферы жизнедеятельности человека, что порождает и новые виды преступной деятельности. Во всем мире сложилась тенденция, когда методы совершения киберпреступлений постоянно совершенствуются и видоизменяются и зачастую опережают развитие систем защиты.

Посредством глобальной компьютерной сети Интернет стали возможными факты вымогательства, мошенничеств, распространения наркотиков и детской порнографии, груминг, кибербуллинг и кибертерроризм, фишинг, вишинг.

Мишенью киберпреступников становятся информационные ресурсы, принадлежащие банковскому сектору, государственным органам и коммерческим организациям, а также конфиденциальная информация, персональные данные и имущество граждан.

Расширение в республике сферы внедрения информационно-коммуникационных технологий (далее – ИКТ) обусловило рост числа угроз и противоправных деяний в области информационной и финансовой безопасности.

Несмотря на принимаемые меры, на протяжении нескольких последних лет наблюдается устойчивый рост количества регистрируемых киберпреступлений.

Изошренность преступников, постоянное совершенствование методов и способов преступной деятельности одновременно с низкой цифровой и финансовой грамотностью населения, недостаточным уровнем систем защиты влекут лавинообразный рост числа регистрируемых хищений с использованием компьютерной техники (статья 212 Уголовного кодекса Республики Беларусь (далее – УК)).

Число зарегистрированных таких хищений в 2020 году (2 466) почти в 4 раза превысило уровень 2019 года (618), что составляет более 90 % от общего количества преступлений в сфере высоких технологий. Причиненный ущерб составил 1 527 371 рубль (ущерб за весь 2019 год -

346 453 рубля). За два месяца 2021 года зарегистрировано уже 447 указанных преступлений с размером ущерба 409 628 рублей.

Отмеченный общий рост числа регистрируемых преступлений, предусмотренных статьей 212 УК, обусловлен увеличением таковых, совершенных посредством глобальной сети Интернет и ИКТ.

Информация о способах совершения хищений с использованием компьютерной техники согласно сведениям Единого государственного банка данных о правонарушениях приведена в таблице:

Способ совершения хищения (ст.212 УК)	2019	2020	2 мес. 2021
Посредством завладения реквизитами доступа и (или) несанкционированного доступа к ресурсам	368	1841	357
Посредством приобретения товаров в Интернете и (или) оплаты услуг	22	61	5
Посредством найденной (украденной) БПК	90	169	33
Путем использования вредоносных программ и (или) модификации компьютерной информации	18	117	18
Иной способ совершения	120	278	34
Общий итог	618	2466	447

Большинство указанных хищений совершено с использованием переданных держателями реквизитов банковских пластиковых карт (далее – БПК), в частности - трехзначного защитного кода (CVV2/CVC2 кода проверки подлинности банковской карты).

Преступному воздействию посредством глобальной компьютерной сети Интернет преимущественно подвергаются информационные ресурсы, принадлежащие банковскому сектору, государственным органам и коммерческим организациям, а также конфиденциальная информация и персональные данные граждан.

При этом меры технической защиты доступа к банковским счетам успешно преодолеваются приемами «социальной инженерии», когда введенные в заблуждение о правильности своих действий клиенты банков предоставляют злоумышленникам реквизиты доступа к своим счетам, что приводит к хищению денежных средств.

Наиболее распространенными способами совершения таких преступлений в настоящее время являются хищения денежных средств граждан, разместивших объявления на торговых интернет-площадках (фишинг), посредством несанкционированного доступа к учетным записям в социальных сетях, а также с использованием реквизитов банковских платежных карточек, полученных в ходе звонков гражданам под видом сотрудника банка, правоохранительного органа (вишинг).

Фишинг – вид Интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным владельца банковской карты. Это достигается путем проведения рассылок СМС-сообщений/электронных писем от имени популярных брендов, внутри различных сервисов и социальных сетей, а также от имени банка.

Одна из наиболее распространенных схем фишинга на территории Республики Беларусь связана с Интернет-ресурсом «Kufar.by». Злоумышленник под предлогом приобретения товара осуществляет переписку, как правило в мессенджере «Viber», в ходе которой отправляет сообщение, содержащее ссылку с адресом фейкового Интернет-ресурса, сходного по содержанию с сайтом одной из служб доставки товара, созданного преступником специально для завладения конфиденциальными данными банковской платежной карты потерпевшего. Пользователь Интернет-ресурса «Kufar.by», думая, что вводит сведения для получения денежных средств за свой товар, предоставляет тем самым злоумышленнику все необходимые платежные данные по карте.

Вишинг – вид интернет-мошенничества, целью которого, как и фишинга, является получение доступа к конфиденциальным данным владельца карты. Основное отличие – использование телефонной связи.

Как правило, мошенники звонят банковским клиентам под видом «службы безопасности банка» или «службы финансового мониторинга» и сообщают о том, что по карте якобы совершена подозрительная операция. Под предлогом спасения денежных средств они заставляют клиента совершить ряд действий, чтобы украсть деньги с его счета. Далее схема мошенничества развивается по нескольким сценариям:

- мошенники выманивают платежные данные карты (16-значный номер, имя владельца, срок действия и трехзначный код на обратной стороне, а также код из СМС от банка) либо обманом узнают данные для входа в личный кабинет;

- мошенники в процессе звонка просят установить на телефон специальное приложение якобы для лучшей защиты – им оказывается программа удаленного доступа и управления (TeamViewer, AnyDesk, RMS, RDP, Radmin, Ammyu Admin, AeroAdmin), с помощью которой можно зайти в личный кабинет онлайн-банка жертвы и перевести оттуда деньги на свой счет;

- во время звонка мошенники убеждают своих жертв снять деньги в банкомате и зачислить их на специальный счет для «спасения средств».

В последнее время стали появляться более сложные схемы: к звонкам от «банковских работников» добавились звонки от «правоохранительных органов», которые «подтверждают», что кто-то

пытается украсть деньги клиента, поэтому их надо спасти путем перевода на «безопасный» счет.

Еще одним способом завладения денежными средствами держателей банковских карт является информирование последних посредством сети Интернет о выигрыше крупной суммы денежных средств. В ходе переписки злоумышленники, под предлогом перечисления выигрыша на банковскую карту, предлагают пройти процедуру регистрации на сайте, где держатель банковской карты указывает фамилию, имя и отчество, а также мобильный телефон. Затем запрашиваются реквизиты банковской карты, на которую якобы будет перечисляться выигрыш.

Мошенники также могут обещать интернет-пользователю крупную сумму выигрыша или выплаты, но перед этим просят заплатить небольшую «комиссию» либо осуществить «закрепительный платеж».

Помимо этого, до настоящего времени злоумышленники совершают хищения денежных средств со счетов пользователей социальных сетей, с которыми они вступили в переписку и последние под воздействием обмана, добровольно предоставили сведения о своей банковской платежной карте либо произвели перечисление денежных средств на подконтрольный преступнику счет.

Потерпевшими от названных уголовно-наказуемых деяний являются все слои населения. В 2020 году их количество составило 2 482 человека, из которых 1 759 женщин и 723 мужчины (за 2 месяца 2021 года – 448, среди которых 287 женщин и 161 мужчина).

Возраст потерпевших от хищений с использованием компьютерной техники составил:

- менее 30 лет – 617 или 24,9% (за 2 месяца 2021 г. – 77 или 17,2%);
- от 30 до 45 лет – 970 или 39,1% (149 или 33,3%);
- от 45 до 60 лет – 569 или 22,9% (137 или 30,6%);
- свыше 60 лет – 326 или 13,1% (85 или 19%).

По социальному положению наибольшее количество потерпевших относятся к следующим группам:

- рабочие – 860 или 34,6% (за 2 месяца 2021 г. – 179 или 39,9%);
- временно не работают и не учатся – 512 или 20,6% (61 или 13,6%);
- пенсионеры – 326 или 13,1% (72 или 16,0%);
- в отпуске по уходу за ребенком до 3-х лет – 254 или 10,2% (30 или 6,6%);
- работники культуры, науки, медицины и образования – 271 или 10,9% (49 или 10,9%);
- служащие – 162 или 6,5% (29 или 6,4%).

По образовательному уровню наибольшее количество потерпевших в 2020 году имели средне-специальное (1 072 или 43,1%) и высшее (987

или 39,7%) образование. Сохранилась данная тенденция и в текущем году, за 2 месяца которого 186 (41,5%) потерпевших имели средне-специальное и 159 (35,4%) высшее образование.

Обращают на себя внимание неединичные факты, когда потерпевшими выступают сотрудники банковских учреждений, а также иные работники различных организаций и предприятий, имеющие, в том числе, специальное экономическое и финансовое образование, обладающие достаточным уровнем знаний, позволяющим исключить передачу посторонним лицам реквизитов своих банковских пластиковых карт.

Например, среди лиц, пострадавших от хищений с использованием компьютерной техники, в 4-м квартале прошлого и за 2 месяца текущего года имелись банковские работники, сотрудники контрольно-ревизионного управления министерства финансов по Гродненской области, финансового отдела Гродненского райисполкома, лица из числа руководителей, а также бухгалтерских работников различных предприятий, учреждений и организаций, кроме того менеджер по информационным технологиям одной из организаций частной формы собственности.

Практика расследования подразделениями Следственного комитета уголовных дел о хищениях денежных средств с банковских счетов граждан Республики Беларусь свидетельствует о том, что основной причиной их совершения является низкий уровень цифровой и финансовой грамотности потерпевших.

В таких условиях внедряемые банками системы и онлайн-приложения с предусмотренной аутентификацией доступа к банковскому счету не в полной мере обеспечивают защиту клиентов банков от хищения денежных средств с банковских счетов.

Меры технической защиты доступа к банковскому счету успешно преодолеваются приемами «социальной инженерии», когда введенные в заблуждение о правильности своих действий клиенты банка передают злоумышленникам реквизиты доступа к своим счетам, что приводит к хищению денежных средств. Завладение реквизитами доступа к банковским счетам граждан в результате использования методов «социальной инженерии» является условием совершения большей части регистрируемых хищений денежных средств с банковских счетов.

Преступления рассматриваемой категории характеризуются высокой степенью латентности, что обусловлено использованием злоумышленниками различного программного обеспечения для сокрытия в сети Интернет своих личных данных и использованием оформленных на подставных лиц, либо приобретенных в сети Интернет аккаунтов,

банковских счетов (электронных кошельков, балансовых номеров телефонов), и, как следствие, крайне низкой раскрываемостью.

Ввиду изложенного, основным способом противодействия совершению рассматриваемых деяний, наряду с иными, является осуществление мероприятий профилактического характера по повышению цифровой и финансовой грамотности граждан, а также внедрение банковскими учреждениями республики механизмов мониторинга и предотвращения несанкционированных операций.