Управлением Следственного комитета Республики Беларусь по Гродненской области (далее УСК) проанализированы причины и условия, способствовавшие совершению преступлений, связанных с неправомерным завладением реквизитами пластиковых банковских карт и хищением средств с карт-счетов граждан, а также в сфере высоких технологий.

Глобальная всемирная сеть Интернет все чаще используется в преступных целях. Расширяющиеся технические возможности компьютеров, их программного обеспечения, активно развивающиеся сети сотовой связи, возможности хранилищ электронной информации, совершенствующиеся навыки пользователей, а также возрастающие их материальные возможности способствуют созданию новых способов, средств и объектов преступных киберпосягательств.

В связи с динамичным и масштабным ростом киберугроз и киберпреступлений, причиняемого ими ущерба юридическим и физическим лицам, такие угрозы и преступления представляют серьезную проблему для общества, а борьба с ними является актуальной и стратегически важной задачей для правоохранительных органов, особенно в части, касающейся реализации мер, направленных на эффективное противодействие росту киберпреступлений, своевременное установление лиц, совершивших преступные деяния, получение доказательств, подтверждающих совершение преступления.

На протяжении последних лет на территории Гродненской области наблюдается тенденция существенного роста преступности в сфере высоких технологий.

Так, если в 2018 году следственными подразделениями Гродненской области возбуждено 666 уголовных дел в сфере высоких технологий, из которых 382 дела о хищениях, совершенных путем использования компьютерной техники, то уже в 2019 году их количество выросло практически вдвое до 1 311 (802). По итогам 4 месяцев текущего года возбуждено 334 (205) уголовных дела, что свидетельствует о продолжаемой динамике роста такого рода преступлений.

Основная часть таких противоправных деяний связана с несанкционированным доступом к личным страницам граждан в социальных сетях, последующим получением от их имени реквизитов банковских пластиковых карт иных лиц и хищением с карт-счетов граждан денежных средств (статьи 349 и 212 УК).

Регистрируемые преступления в сфере высоких технологий обладают определенной спецификой, при этом отчетливо видна тенденция серийного распространения однотипных преступлений, подходы к документированию и раскрытию которых также идентичны.

Например, еще два-три года назад к таким преступлениям можно было отнести факты перенаправления пользователей на сайты в сети Интернет, содержащие информацию от имени МВД о блокировке компьютера за просмотр материалов порнографического содержания и требованием уплаты «штрафа», которые квалифицировались по ст.351 (компьютерный саботаж) и 209 (мошенничество) УК. До этого аналогичные факты мошенничества были сопряжены с установкой на компьютеры вредоносного программного обеспечения, так называемых «винлокеров». Такие случаи в настоящее время носят уже единичный характер.

Анализ уголовных дел показывает, что в последнее время более широкое распространение получили преступления, совершение которых связано с использованием социальных сетей, в том числе сопряженных с несанкционированным доступом к аккаунтам пользователей такой сети.

Значительно увеличилось количество обращений в правоохранительные органы пользователей социальных сетей, с которыми злоумышленники вступили в переписку и последние под воздействием обмана, добровольно предоставили сведения о своей банковской платежной карте, либо перечислили деньги на указанные номера мобильных телефонов. Также заявителями выступают владельцы взломанных аккаунтов социальных сетей, от имени которых производилась переписка.

Существенно возросло количество хищений денежных средств с использованием полученных в ходе переписки либо звонков гражданам от имени сотрудников банков реквизитов банковских платежных карточек и иной конфиденциальной информации, позволяющей получить доступ к управлению карт-счетом.

В любом случае, традиционно сами потерпевшие предоставляли эту информацию злоумышленникам, которые входили к ним в доверие или обманывали различными способами.

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. После ввода реквизитов банковской карты на мобильный телефон, указанный в анкете, приходит смс-сообщение с кодом подтверждения, при вводе которого с банковской карты автоматически списывается не фиксированная сумма денежных средств. После их списания на сайте появляется сообщение о том, что в системе неполадки и держателю банковской карты предлагается пройти повторно процедуру регистрации и ввода реквизитов банковской карты. В ходе каждой такой процедуры регистрации и ввода реквизитов банковской карты с банковской карты заявителя списываются денежные средства.

Нередко жертвами киберпреступлений становятся различные предприятия и организации.

При таких обстоятельствах, учитывая, что использование служебного компьютера, при помощи которого осуществляется ведение учёта и организация экономической деятельности предприятия, во вне служебных целях, повышает риск его заражения вредоносным программным обеспечением, следствие пришло к выводу, что одним из условий совершения вышеуказанного преступления явилось несоблюдение работниками правил пользования служебным компьютерным оборудованием.

Причинами и условиями, способствующими совершению преступлений, явились наличие несложного пароля к электронному почтовому ящику и его несменяемость, излишняя доверчивость и неосмотрительность бухгалтера предприятия, не убедившегося в личности лица, выдаваемого себя за представителя шведского партнера, и не проверившего информацию об изменении реквизитов банковского счета.

Имеющиеся возможности оперативного взаимодействия с правоохранительными органами иностранных государств, а также механизмы получения международной правовой помощи по уголовным делам не позволяют в полной мере обеспечить принцип неотвратимости наказания. Следует констатировать, что из-за специфики киберпреступлений, их раскрытие и расследование на современном этапе остается сложной задачей. Большая часть таких преступлений в настоящее время остается не раскрытыми.

При таких обстоятельствах на первый план выходит проведение качественной работы всеми заинтересованными субъектами по профилактике наиболее распространенных видов преступлений против информационной безопасности, повышению общей компьютерной и финансовой грамотности работников предприятий области и населения в целом, доведению гражданам информации о вероятных способах совершения в отношении них киберпреступлений, а также выявлению фактов несовершенства применяемых банковскими учреждениями Республики Беларусь финансовых инструментов, а также иных причин и условий, способствующих совершению хищений путем использования компьютерной техники.

Необходимо отметить, что в соответствии с Концепцией информационной безопасности Республики Беларусь, утвержденной Постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1, реагирование на риски и вызовы в информационной сфере осуществляется всеми без исключения государственными органами и организациями в соответствии с областью их деятельности согласно непосредственному предназначению, максимально полно и оперативно.

Такое реагирование предполагает сбор информации об используемых технологиях, способах деструктивных информационных воздействий и совершения киберпреступлений, анализ, оценку и прогнозирование состояния безопасности данной сферы, выявление реализующихся вызовов и угроз, локализацию негативных последствий и восстановление нанесенного вреда (ущерба).

В период январь – май 2020 года на территории Гродненской области совершено 7 преступлений несовершеннолетними. Все противоправные деяния связаны с использованием банковских карт потерпевших, получения незаконного доступа к их данными в мобильном либо интернет-банкинге.

В целях повышения эффективности деятельности всех субъектов профилактики, необходимо:

на системной основе проводить профилактические мероприятия по противодействию киберпреступности, основанных на популяризации среди молодежи, нетерпимости к асоциальному поведению в информационном пространстве, об ответственности за использование банковскими картами, реквизитами банковских и иных счетов.

Сабко 74 33 76