Аналитический обзор об актуальных способах совершения киберпреступлений на территории Минской области

Стремительное развитие цифровых технологий, переход к безналичным расчетам, размещение в глобальной компьютерной сети Интернет персональных данных при достаточно низкой цифровой грамотности граждан, сопряженной с беспечным отношением к защите собственной информации, стали следствием увеличения количества регистрируемых киберпреступлений.

Злоумышленники активно используют в своей деятельности новейшие достижения науки и техники, применяют всевозможные компьютерные устройства и новые информационные технологии для совершения и сокрытия преступлений.

По итогам семи месяцев 2024 года, в сравнении с аналогичным периодом прошлого года (далее – АППГ), количество зарегистрированных киберпреступлений на территории Минской области увеличилось на 35,2 % (с 1048 до 1417), что является каждым пятым (21 %) уголовным делом на Минщине. Число тяжких киберпреступлений возросло в 2 раза (с 45 до 160, или на 201,9 %).

Необходимо отметить, что если в предыдущие периоды большинство киберпреступлений, относились к хищениям имущества путем модификации компьютерной информации (ст. 212 Уголовного кодекса),

то в текущем году в связи с отнесением к компетенции подразделений по противодействию киберпреступности (далее – ПК) мошенничеств и вымогательств, совершенных с использованием информационно-коммуникационных технологий, тенденция изменилась.

Так, в январе-июле 2024 года совершено 814 мошенничеств (ст. 209 Уголовного кодекса) (АППГ – 43), или 57,4 %, от общего числа зарегистрированных киберпреступлений.

Структурный анализ совершенных в текущем году мошенничеств свидетельствует о явном преобладании таких способов завладения деньгами потерпевших, как:

1. Продажа несуществующего товара, на различных Интернет-ресурсах.

Очень часто жертвами мошенников становятся пользователи сети Интернет, желающие приобрести различные товары в социальной сети Instagram – 333 преступления, или 41 %. Продавцы, как правило, просят предоплату за товар, однако такие истории заканчиваются одним – граждане перечисляют предоплату, а в дальнейшем связь с продавцом теряется, не получив долгожданный товар.

Для примера можно рассмотреть следующие мошеннические учетные записи: original_brand.by, edelweis.resort, fox.store.by, EUROSHINA_BY, @airmac_by, flowerslovers.by, _belbet_off, happysale.by.

2. Обман граждан под предлогом вложения средств в криптовалюту либо сделок с ней на несуществующих биржах и иного заработка в сети Интернет 110 преступлений, или 13,5 %. Несуществующие инвестиционные проекты и мошеннические биржи — это обманные схемы, в которых инвесторам предлагается вложить средства в вымышленные или несуществующие бизнес-проекты, или финансовые инструменты с обещаниями высокой прибыли, которая на самом деле не может быть достигнута. Мошеннические биржи, предлагающие несуществующие инвестиционные проекты, обычно используют различные хитрости и тактики, чтобы привлечь потенциальных инвесторов. Вот несколько типичных характеристик таких мошеннических схем:

1. Обещания высокой доходности при минимальных рисках: Мошеннические биржи обычно привлекают внимание инвесторов, обещая очень высокие доходы при минимальном или даже отсутствующем риске. Это является привлекательным для людей, желающих получить быструю и легкую прибыль, однако на самом деле такие обещания часто оказываются ложными.

2. Неясные условия инвестирования и вывода средств: Мошеннические биржи часто предлагают инвесторам неясные и запутанные условия инвестирования и вывода средств. Это может включать в себя скрытые комиссии, высокие пороги для вывода средств или даже отсутствие возможности вывода вложенных денег вовсе.

3. Использование лживой информации и фальшивых отзывов: Для привлечения новых клиентов мошеннические биржи часто создают ложные отзывы, поддельные рекомендации и искаженные данные о своей деятельности. Это создает иллюзию успешной и надежной компании, призванной убедить инвесторов вложить свои деньги. Для примера можно рассмотреть следующие мошеннические виды мошеннических проектов:

1. Пирамиды.

Пирамидные схемы являются одними из самых распространенных форм финансового мошенничества. Они предлагают инвесторам «легкую» прибыль за счет привлечения новых участников. Основная идея заключается в том, что старшие участники выигрывают за счет взносов новичков. Такие схемы неустойчивы и, когда приток новых участников замедляется, они обречены на крах, оставляя большинство участников без вложенных средств.

2. Фейковые криптопроекты.
В связи с возросшим интересом к криптовалютам, мошенники также начали использовать криптопространство для своих незаконных целей. Они предлагают ложные криптовалютные проекты с обещаниями быстрой и легкой прибыли. Однако за ними стоят скрытые мотивы и планы, которые могут привести к убыткам для инвесторов. К примеру таких проектов, можно привести пример «https://tradestrike.net/», с помощью которого мошенники ввели в заблуждение жителя г. Молодечено и завладели 160009 белорусскими рублями.
3. Звонки мошенников в месенджерах (Viber, Telegram, WhatsApp) под видом сотрудников правоохранительных органов либо специалистов банковских и иных учреждений, вынуждающих потерпевших под различными предлогами получать кредиты и переводить денежные средства либо сбережения на подконтрольные злоумышленниками счета – 357, или 43,9 %.
В текущем году наиболее актуальная схема – побуждение открыть кредит. Злоумышленники сообщают жертве о том, что якобы кто-то посторонний пытается открыть кредит на ее имя, поэтому для деактивации таких действий необходимо самостоятельно обратиться в банк и открыть кредит, и в дальнейшем перевести денежные средства на сберегательные счета. Как правило после перевода денежных средств связь с злоумышленников прекращается.
Наряду с этим в текущем году зарегистрировано: 36 вымогательств (ст. 208 Уголовного кодекса), 9 заведомо ложных сообщений об опасности (ст. 340 Уголовного кодекса), 51 факт незаконного оборота средств платежа и (или) инструментов (ст. 222 Уголовного кодекса), 449 хищений имущества путем модификации компьютерной информации (ст. 212 Уголовного кодекса) и 58 преступлений против компьютерной безопасности (глава 31 Уголовного кодекса).
Основными способами совершения хищений имущества путем модификации компьютерной информации (ст. 212 Уголовного кодекса), являются:
1. Также звонки мошенников в мессенджерах под видом сотрудников правоохранительных органов либо специалистов банковских и иных учреждений, в ходе которых злоумышленники получают доступ к банковским реквизитам граждан (59,9 %). Такой способ называется «Вишинг» – это один из методов мошенничества с использованием социальной инженерии (социальная инженерия – это совокупность способов психологического воздействия на поведение человека с целью получения выгоды), который заключается

в том, что злоумышленники, используя телефонную коммуникацию и играя определенную роль, под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию, или побуждают, убеждают вероятную жертву к совершению определенных действий со своей банковской платежной картой.
Он заключается в том, что злоумышленники, используя телефонную связь и, выдавая себя за сотрудников банка или правоохранительных органов, под различными предлогами вводят в заблуждение потерпевших, выясняя сведения о наличии банковских платежных карточках, их реквизитах, паспортных данных с целью последующего хищения денежных средств.
В большинстве случаев при совершении звонков мошенники используют интернет-телефонию, которая позволяет маскировать телефонные номера под номера белорусских операторов связи.
При этом всем известные мессенджеры Viber, Telegram и WhatsApp имеют возможность использования виртуальных номеров.
К примеру, злоумышленники звонят жертве от имени банковского работника и сообщают, что необходимо осуществить какие-либо действия с банковской платежной карточкой, так как кто-то либо пытается похитить с нее денежные средства, либо оформляет кредит, либо проводит подозрительную оплату.
Для большей достоверности в качестве имени пользователя они указывают официальный номер банка либо его название, а для «аватарки» используют логотип или эмблему банковского учреждения.
При этом зачастую они уже владеют минимальной информацией о лицах, которым звонят (имя, отчество, дата рождения, последние цифры банковской карты и др.), что способствует повышению доверия к звонящему и производит на него определенное впечатление.
В дальнейшем преступник просит сообщить информацию о банковской карте – номер, срок действия, трехзначный код на ее обороте, содержание СМС-сообщения, которое в ходе разговора поступает
на мобильный телефон, либо устанавливает мобильное приложение, позволяющее злоумышленнику получить удаленный доступ к мобильному телефону, в котором сегодня фактически у каждого имеется интернет-банкинг и, соответственно, доступ к банковскому счету.
2. Использование фишинговых Интернет-ресурсов (25,6 %).
Фишинг – вид мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам, паролям, данным лицевых счетов и банковских карт с использованием поддельных интернет-ресурсов, контролируемых злоумышленниками, внешне схожих с настоящими (например, поддельные страницы услуги

«Интернет-банкинг» различных банков).
К примеру в прошлом году житель нашей области, при попытке совершить платёж за коммунальные услуги посредством системы Интернет-банкинга, воспользовался поисковой строкой сайта Google и перешёл, как оказалось, по ложной ссылке для оплаты. Злоумышленникам стали известны реквизиты банковской карты и в результате с его карт-счета было похищено почти 35 тысяч рублей.
Также в социальных сетях появилась реклама, обещающая «призы от Белагропромбанка». Переходя по ссылке, жертва попадает на поддельную банковскую страницу, на которой мошенники выманивают номера телефонов и иные личные данные, что дает им полный доступ к счетам обманутых и даже возможность оформления онлайн-кредитов.
Распространены кибермошенничества от имени «Белпочты». Схема довольно проста – злоумышленники присылают потенциальной жертве сообщение через интернет-мессенджер. В нем сообщают о необходимости уточнения адреса доставки почтового отправления и предлагают перейти по ссылке в Интернете. Невнимательный человек, не проверив адрес, по которому ему предлагают перейти, попадает на фейковый сайт, стилизованный под официальный сайт «Белпочты». Там клиента просят ввести свой адрес, якобы для доставки некоего почтового отправления, и оплатить тариф за услугу «Белпочты» прямо на этой странице, введя реквизиты банковской карты.
Появились случаи мошенничеств, связанных с созданием фейкового аккаунта в мессенджерах от имени руководителя учреждения, где работает потенциальная жертва.
Злоумышленники осуществляют рассылку сообщений с указанием того, что в скором времени гражданину позвонит или напишет сотрудник вышестоящей инстанции (Министерства образования, МВД, КГБ, КГК, СК, ОВД). Как правило, пугаясь, граждане говорят любую информацию, которую требует сотрудник. Далее просят установить удаленное программное обеспечение, позволяющее получить ему доступ к устройству, либо вести видеозапись с демонстрацией экрана мобильного телефона.
Преступления против компьютерной безопасности (глава 31 Уголовного кодекса) в большинстве случаев возбуждаются по фактам неправомерного завладения учетными записями мессенджеров и социальных сетей, таких как (Telegram (31), WhatsApp (3), Instagram (7), Facebook (1) и Вконтакте (12)).
Основные способы совершения вымогательств (ст. 208 Уголовного кодекса), можно разделить на три основные категории:
1) связаны с угрозой распространения личной информации

потерпевших, которые последние желали сохранить в тайне (20, или 55,6 %), как правило-фотографий и видеозаписей интимного характера, которые, в большинстве случаев, потерпевшие самостоятельно пересылали злоумышленникам, полагая, что общаются с потенциальным партнером противоположного пола для знакомства.
2) связаны с блокированием компьютерной информации физических лиц (13 или 36,1 %). При этом в подавляющем большинстве случаев отмечается блокирование учетных записей Apple ID посредством ввода авторизационных данных, предоставленных злоумышленниками под благовидными предлогами, что в последующем не позволяет потерпевшим полноценно использовать свои мобильные устройства.
3) связаны с угрозой применения насилия (3 или 8,3 %).
Основными факторами, способствующими совершению киберпреступлений, являются халатность, излишняя доверчивость граждан, мнимая возможность быстрого обогащения, получение крупных сумм денежных средств, а также недостаточное информирование населения о способах и методах применяемыми преступниками при совершении указанных преступлений.
Знание основных схем и способов обмана позволяет гражданам быть более внимательным и осторожным, что, в свою очередь, помогает предотвратить случаи совершения киберпреступлений.