*Дополнительный материал к единому дню информирования населения 18.08.2022*

**Об эффективности принимаемых мер, направленных на профилактику и противодействие киберпреступности, выявление причин и условий, способствующих совершению киберпреступлений**

Интернет и компьютерные технологии стремительно проникают во все сферы жизнедеятельности человека. Однако технологии порождают и новые виды преступной деятельности.

Основными факторами, способствующими совершению киберпреступлений являются:

низкая правовая культура пользователей, недостаточные знания большинства населения в области информационной и финансовой безопасности;

количество пользователей;

анонимная связь;

отсутствие условий для повышения эффективности деятельности правоохранительных органов;

отсутствие единой правоприменительной практики;

международные мосштабы;

недостаточный уровень возможностей международного сотрудничества.

В целом на территории района к аналогичному периоду прошлого года отмечается значительное снижение зарегистрированных преступлений по линии ˮпротиводействия киберпреступности“ – с 17 до 6 преступлений. В 2021 году таких преступлений было зарегистрировано – 24, а в 2020 – 38.

В основном, более 80 % - это хищение имущества путем модификации компьютерной информации, т.е. преступления, направленные на совершение хищений денежных средств с банковских счетов граждан. В среднем по области регистрируется более 20 преступлений ежедневно. Причиненный ущерб по Витебской области составил сумму чуть менее 600 тысяч рублей.

Из 6 преступлений по линии противодействия киберпреступности, зарегистрированных на территории Сенненского района, все предусмотренные статьёй 212 Уголовного кодекса Республики Беларусь (ˮХищение путем использования компьютерной техники“),

Причиненный ущерб от таких преступлений жителям Сенненского района составил 5 824 рубля 68 копеек.

При этом на территории района зарегистрировано 2 преступления, предусмотренные статьей 209 Уголовного кодекса Республики Беларусь (ˮМошенничество“), где также способ преступления – с использованием компьютерной техники.

Встречаются примеры преступления против информационной безопасности, взломы игровых аккаунтов и социальных сетей, которые тоже направлены на получение денежных средств путем выманивания у онлайн-друзей либо владельца аккаунта; также использование вредоносного программного обеспечения; заведомо ложное сообщение об опасности, так называемое ложное минирование.

Преступлений против информационной безопасности (по главе 31 Уголовного кодекса Республики Беларусь) в текущем году не зарегистрировано (за аналогичный период 2021 – не зарегистрировано). Однако на территории области (53) и Республики борьба (419) с такими преступлениями актуальна, в связи с чем сотрудниками правоохранительных органов проводится работа по их выявлению и установлению виновных лиц. Снижение количества преступлений против информационной безопасности обусловлено перепрофилированием киберпреступников и сокращением фактов несанкционированного доступа к страницам пользователей социальных сетей с целью завладения реквизитами банковских платежных карт в ходе переписки с друзьями владельцев страниц.

Анализ совершенных за 6 месяцев текущего года хищений путем использования компьютерной техники (статья 212 Уголовного кодекса Республики Беларусь) указывает на то, что из 6 преступлений, зарегистрированных в отделе внутренних дел райисполкома, только 1 совершено на территории Республики Беларусь (с использованием белорусских банкоматов и платежных терминалов), в остальных случаях электронный след ведет за пределы страны.

*Справочно: проведен анализ сведений о потерпевших от хищений путем использования компьютерной техники за текущий период 2022 года:*

*66 % потерпевших – женщины, 33% – мужчины;*

*среднее специальное образование у 66%, высшее – у 33% потерпевших;*

*50,0% потерпевших – рабочие;*

*пенсионеры – 34%;*

*временно не работают и не учатся – 16%.*

*Денежные средства у потерпевших похищены со счетов в ОАО* ˮ*АСБ Беларусбанк*“ *по 4 фактам, в ОАО* ˮ*Белагропромбанк*“ *– по 1 факту, в ЗАО* ˮ*МТБанк*“ *по 1 факту.*

Наиболее актуальные виды киберпреступлений совершаемые способом **вишинга** и **фишинга**.

**Вишинг –** это звонок мошенников, которые под видом работников банков или правоохранительных органов выманивают у доверчивых граждан персональные данные – номер банковской карты, ее секретный трехзначный цифровой код с оборотной стороны, код из SMS, логин и пароль доступа к интернет банкингу.

После получения мошенниками заветных цифр, они под различными предлогами выманивают еще и цифровой код из SMS от банка для совершения перевода денежных средств с карты владельца на иную карту.

Мошенники развивают свои технологии и предлагают не только передать номер и код карты, но и под предлогом отмены якобы совершаемой операции по карте предлагают установить мобильное приложение на телефон либо другое устройство. На самом деле это приложение и переданный код его регистрации предоставляет мошенникам возможность управления устройством, на котором оно установлено. Т.е. потерпевший, доверившись якобы сотруднику банка, по его «совету» для отмены расходной операции по карте или сохранения денежных средств установил приложение, например из Play Market для системы Адроид, передал код его регистрации – тем самым предоставил звонящему доступ к своему устройству. Далее мошенники уже сами видят все, что происходит на экране телефона, в том числе и происходящие от банка СМС коды, а также введенный в интернет банкинг пароль. Далее уже дело техники. Сами мошенники уже имеют возможность перевести деньги с карты владельца на свои счета и даже открыть кредит. В Республике зарегистрированы факты через вышеуказанный удаленный доступ завладение преступниками крупными денежными средствами государственных учреждений, когда имея доступ к компьютерной технике организации в том числе к электронной почте организации, через которую осуществляется оформление договоров и сделок купли продажи, преступники заключают дополнительные соглашения на подставные счета.

Иногда к разговору подключается еще один соучастник, представляющийся сотрудником правоохранительных органов либо представитель службы безопасности, предлагает участие в «спецоперации» по разоблачению недобросовестного работника банка, который, используя свое служебное положение, оформил на ваше имя кредит либо осуществляет незаконный перевод денежных средств. Для его уличения необходимо перевести деньги на безопасный счет или оформить другой кредит и перевести полученные деньги на специально созданный для спецоперации защищенный счет. После разоблачения банковского работника обещают вернуть деньги.

***К примеру: случай*** ***произошел в Новополоцке. Местная жительница в ходе телефонной беседы с якобы сотрудником банка передала ему секретные сведения о реквизитах карты, своем идентификационном номере паспорта и коды из смс-сообщений от банка для подтверждения операций. В итоге женщина лишилась суммы денег эквивалентной более 30 тысяч долларов.***

Еще одним из предлогов для совершения преступления может быть сообщение о том, что недобросовестный сотрудник банка разгласил ваши личные данные, вследствие чего несколько банков одновременно оформили заявки на открытие кредитной линии. Для аннулирования этих кредитов необходимо обратиться в банки с заявлением на кредит, а полученные деньги нужно будет перевести на указанный специально созданный счет (злоумышленнику) для закрытия случайно оформленного кредита, чтобы не портить кредитную историю.

***Такой пример имеется и в нашем районе. Женщина лишилась пособия на рождение ребенка, после беседы с так называемым себя представителем службы безопасности банка, при чем ее не смутило, что звонок осуществлялся по мессенджеру Вайбер и уведомление в приложении банкинг о том, что перевод ею денег может быть кражей.***

Второй способ Фишинг. Мошенники составляют короткий разговор, либо осуществляют переписку с продавцами на площадке объявлений по поводу покупки товара, а потом под разными предлогами убеждают получить оплату за продаваемый товар. Для этого переводят разговор в любой мессенджер и направляют в виде ссылки поддельную форму для оформления доставки товара и якобы получения оплаты. Продавец желая получить деньги, не обратив внимания на адрес ссылки и доменное имя, вводит реквизиты своей карты и секретный трехзначный код на ее обороте, тем самым передавая свои персональные данные, которыми можно воспользоваться для хищения средств.

***При продаже детских вещей на торговой площадке «КУфар» находящаяся в отпуске по уходу за ребенком до 3 лет молодая женщина перешла по присланной потенциальным «покупателем» ссылке, ввела реквизиты свой банковской карты, включая трёхзначный код на ее обороте, в результате чего передала персональные данные мошенникам и лишилась почти 13 тысяч рублей.***

***В январе девушка после переписки с покупателем товара в***

На территории Сенненского района в 2022 году зарегистрировано 2 преступления, предусмотренные статьей 209 УК (мошенничество):

***Два жителя района решили приобрести мобильные телефоны Айфон через объявления размещенные на интернет площадке «Телеграмм» и «Инстаграмм» в результате чего перевели денежные средства общей суммой более 2 000 рублей на счет продавца, однако так свой товар и не получили.***

Жители Витебска, а так же других населенных пунктов области, сталкиваются с угрозами о минировании. В результате проведенных совместных оперативных мероприятий с правоохранительными

***Девятиклассник, 15 летний житель Витебской области, познакомился в социальной сети с ровесницей. На свидание вживую у парня не хватало смелости. Однажды ему захотелось доказать, что он способен на многое. Узнал где учится его подруга и когда у нее контрольная по математике. В намеченный день учреждение образования на электронную почту получило заведомо ложное сообщение об опасности – о минировании школы. В отношении несовершеннолетнего возбуждено 4 уголовных дела. Устанавливается причастность к аналогичным деяниям на территории России и других стран.***

Здесь перед нами стоит задача обезопасить наших детей. Ведь возраст привлечения к уголовной ответственности за совершение хищения путем использования компьютерной техники, предусмотренного статьей 21 УК наступает с 14 лет, а наказание вплоть на срок лишения свободы до 3 лет.

Те же действия, совершенные повторно или группой лиц по предварительному сговору, наказываются лишением свободы на срок до 5 лет.

Если хищение крупное, то предусмотрено наказание в виде лишения свободы на срок до 7 лет.

За хищение, совершенное организованной группой или в особо крупном размере, грозит до 12 лет лишения свободы.

Действенным методом работы по раскрытию и противодействию киберпреступности является внесение информации о почтовых ящиках, IP-адресах, банковских платежных картах, электронных кошельках, аккаунтах пользователей социальных сетей, фишинговых ресурсах и иных криминалистических идентификаторов в базу данных ˮЦифровой след“. Путем дальнейшей проверки, мониторинга и анализа имеющихся сведений в базе данных ˮЦифровой след“ обнаруживаются совпадения идентификаторов (номера телефонов, электронных кошельков, банковских карт или счетов), таким образом, устанавливаются подозреваемые по аналогичным фактам совершенных преступлений.