Периодическое печатное издание Совета депутатов и администрации Целинного сельсовета
Коченевского района Новосибирской области

ВЕСТНИК

№ 8 от 15.06.2023

В номере:

ПРОКУРАТУРА КОЧЕНЕВСКОГО РАЙОНА НОВОСИБИРСКОЙ ОБЛАСТИ ИНФОРМИРУЕТ:

Хищения, совершаемые с использованием современных информационно-телекоммуникационных технологий

Развитие технологий в современном мире обуславливает их повсеместное проникновение во все сферы общественной жизни. Этим пользуются не только добросовестные пользователи информационных сетей, но и злоумышленники, преследующие различные противоправные цели – личное обогащение, дискредитацию граждан и государственных органов, распространение запрещенной информации, идей терроризма и экстремизма.

В Российской Федерации отмечается ежегодный рост таких преступлений. Повсеместно регистрируются преступления, связанные с хищением денежных средств из банков и иных кредитных организаций, физических и юридических лиц, совершаемых с использованием современных информационно-коммуникационных технологий, ответственность за которые в зависимости от способа преступного посягательства предусмотрена ст.ст. 158, 159, 159.3, 159.6 УК РФ.

Федеральным законом от 23.04.2018 № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» введена ответственность виновных лиц по статье 158 УК РФ за кражу, совершенную с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного статьей 159.3 УК РФ).

Аналогичным образом, с целью усиления уголовной ответственности за противоправные действия с использованием электронных средств платежа, изменены диспозиции и санкции статей 159.3 и 159.6 УК РФ.

Зачастую в совокупности с ними совершаются преступления в сфере компьютерной информации или так называемые киберпреступления, которые на практике нередко используются в качестве инструментария завладения чужим имуществом.

В целях борьбы с компьютерной преступностью уголовным законом предусмотрена ответственность за ряд специальных составов, криминализирующих такие деяния, как: неправомерный доступ к охраняемой законом компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ), а также неправомерное воздействие на критическую информационную инфраструктуру РФ (ст. 274.1 УК РФ).

Подавляющее большинство анализируемых хищений совершается с применением методов «социальной инженерии», то есть доступа к информации с помощью телекоммуникационных сетей для общения с потерпевшими (сотовой связи, ресурсов сети Интернет). Технология основана на использовании слабостей человеческого фактора и является достаточно эффективной. Например, преступник может позвонить человеку, являющемуся

пользователем банковской карты (под видом сотрудника службы поддержки или службы безопасности банка), и выведать пароль, сославшись на необходимость решения небольшой проблемы в компьютерной системе или с банковским счетом, зачастую дезинформируя о его блокировке.

Распространенный характер носят хищения, связанные с другим способом обмана доверчивых граждан. Преступники, представляясь близкими родственниками (знакомыми) потерпевших, просят о передаче или перечислении электронным платежом определенной суммы денежных средств для разрешения сложившейся в их жизни неблагоприятной ситуации. К примеру, в связи с необходимостью освобождения их от уголовной ответственности. Нередко злоумышленники сами представляются сотрудниками органа правопорядка.

Дистанционные хищения совершаются посредством размещения на открытых сайтах в сети Интернет заведомо ложных предложений об услугах и продаже товаров за денежное вознаграждение, которое в дальнейшем перечисляется на банковский счет виновного лица.

Денежные средства неправомерно списываются со счетов потерпевших, когда в руки преступников попадают их мобильные телефоны с установленными на них банковскими сервисами. То же самое касается и банковских карт: похитителями совершаются покупки путем оплаты товаров бесконтактным способом, при наличии пароля доступа – деньги снимаются в банкоматах.

Так называемый фишинг - тоже техника «социальной инженерии», направленная на получение конфиденциальной информации. Обычно злоумышленник посылает потерпевшему e-mail, подделанный под официальное письмо – от банка или платежной системы – требующее «проверки» определенной информации, или совершения определенных действий. Это письмо как правило содержит ссылку на фальшивую веб-страницу, имитирующую официальную, с корпоративным логотипом и содержимым, и содержащую форму, требующую ввести необходимую для преступников информацию – от домашнего адреса до пин-кода банковской карты.

Социальная инженерия используется также для распространения троянских коней: эксплуатируется любопытство, либо алчность объекта атаки. Злоумышленник направляет e-mail, sms-сообщение или сообщение в мессенджере, во вложении которого содержится, например, важное обновление антивируса. Также это может быть выгодное предложение о покупке со скидкой или сообщение о фиктивном выигрыше с приложенной ссылкой при переходе по которой на устройство пользователя скачивается вредоносная программа. После чего преступник получает удаленное управление и возможность осуществления перечисления денежных средств со счета привязанной к абонентскому номеру банковской карты.

Такая техника остается эффективной, поскольку многие пользователи, не раздумывая кликают по любым вложениям или гиперсылкам. Особенно это актуально в связи с глобальной цифровизацией общества, которая затрагивает и социально уязвимые слои населения, например, пожилых людей, испытывающих сложности при освоении современной техники, а также страдающих излишней доверчивостью.

Преступники реализуют множество других способов и инструментов для завладения чужими деньгами: используют дубликаты сим-карт потерпевших, а также устройства-скиммеры, считывающие информацию, содержащуюся на магнитной полосе банковской карты для последующего изготовления ее дубликата. Рассылают в социальных сетях со взломанных страниц пользователей сообщения их знакомым с просьбами одолжить деньги, внедряют вредоносные ПО в системы юридических лиц, похищают электронные ключи и учетные записи к нему в офисах организации и т.д.

Необходимо отметить, что криминальные методы «удаленного» хищения денежных средств постоянно эволюционируют, при этом преступниками активно используются современные IT-технологии, которые зачастую просты в использовании и доступны неограниченному числу пользователей глобальной сети.

Для создания препятствий правоохранительным органам для раскрытия подобных преступлений злоумышленники: меняют сотовые телефоны, места своего нахождения; оформляют сим-карты и открывают счета в банках на подставных лиц; используют анонимные электронные кошельки и предоплаченные банковские карты, Proxy-серверы и различные программы, скрывающие фактические IP-адрес и место нахождения, привлекают лиц, не осведомленных о противоправности их действий, применяют другие способы конспирации. Это касается не только хищений, но и преступлений в сфере компьютерной информации. При этом данные преступления носят скоротечный, многоэпизодный (серийный), и трансграничный характер.

Противодействие терроризму – главная цель общества и государства

Основным нормативным правовым актом, регулирующим борьбу с терроризмом, является Федеральный закон от 06.03.2006 № 35-ФЗ "О противодействии терроризму»

Терроризм - это идеология насилия и практика воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий.

Терроризм уголовно наказуем

Уголовным кодексом Российской Федерации предусмотрена ответственность за совершение преступлений террористического характера:

– ст. 205 УК РФ - Террористический акт – пожизненное лишение свободы;

– ст. 205.1 УК РФ - Содействие террористической деятельности – лишение свободы на срок до пятнадцати лет со штрафом в размере до одного миллиона рублей либо в размере заработной платы или иного дохода осужденного за период до пяти лет либо без такового и с ограничением свободы на срок до двух лет либо без такового;

– ст. 205.2 УК РФ - Публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма – лишение свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет;

– ст. 206 УК РФ - Захват заложника – пожизненное лишение свободы;

– ст. 207 УК РФ - Заведомо ложное сообщение об акте терроризма – лишение свободы на срок до трех лет;

ТЕРРОРИСТИЧЕСКАЯ ДЕЯТЕЛЬНОСТЬ:

- организация, планирование, подготовка, финансирование и реализация террористического акта;

- подстрекательство к террористическому акту;

- организация незаконного вооруженного формирования, преступного сообщества, организованной группы для реализации террористического акта;

- вербовку, вооружение, обучение и использование террористов;

- информационное или иное пособничество в планировании, подготовке или реализации террористического акта;

- пропаганду идей терроризма, распространение материалов или информации, призывающих к осуществлению террористической деятельности.

ТЕРРОРИСТИЧЕСКИЙ АКТ

совершение взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях дестабилизации деятельности органов власти или международных организаций либо воздействия на принятие ими решений, а также угроза совершения указанных действий в тех же целях

– ст. 239 УК РФ - Организация объединения, посягающего на личность и права граждан – лишение свободы на срок до двух лет.

Чтобы не стать жертвой проявления терроризма, будьте бдительны и **ПОМНИТЕ**! Террористические группы могут установить взрывные устройства на объекте в самых неожиданных местах (в подвалах строящегося здания, в общественном транспорте; в местах массового скопления людей, в припаркованных машинах, на рабочих местах т.д.).

Если произошел взрыв:

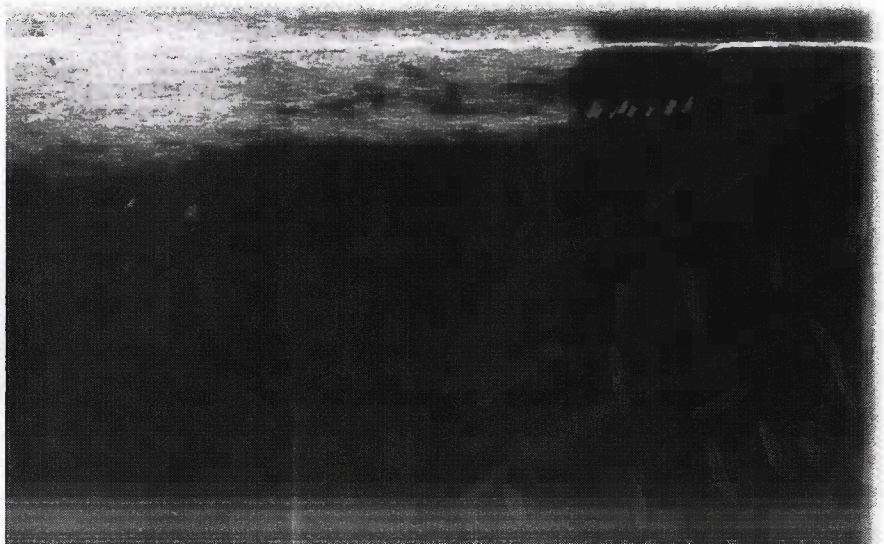
1. Постарайтесь успокоиться и уточнить обстановку.

2. Продвигаться следует осторожно, не трогать поврежденные конструкции, оголившиеся провода.

3. В разрушенном или поврежденном помещении из-за опасности взрыва скопившихся газов нельзя пользоваться открытым пламенем (спички, свечи, факел и т.д.).

4. При задымлении защитите органы дыхания смоченным носовым платком (лоскутом ткани, полотенцем)

5. При наличии пострадавших, примите меры по оказанию первой медицинской помощи и выходу из района



Если Вы стали жертвой терроризма:

Правильные, грамотные действия каждого гражданина могут предупредить террористический акт, значительно снизить его последствия, сохранить Вашу жизнь и жизнь других!

Вас завалило обломками стен:

1. Успокойтесь, старайтесь дышать глубоко, ровно, не торопитесь.

2. Голосом и стуком привлекайте внимание людей к себе.

3. Если вы находитесь глубоко от поверхности земли, перемещайте влево-вправо любой металлический предмет (кольцо, ключи и т. д.) для обнаружения вас металлоискателем.

4. Если пространство около Вас относительно свободно, не зажигайте спички, свечи – берегите кислород.

5. Продвигайтесь осторожно, стараясь не вызвать нового обвала. Ориентируйтесь по движению воздуха, поступающего снаружи.

6. По возможности укрепите отвисающие балки или потолок с помощью других предметов и дожидайтесь помощи.

Заметив подозрительный предмет:

Не подходите близко к нему, не трогайте руками, сообщите в отдел полиции, ответственным лицам в зданиях массового скопления граждан и не пытайтесь открывать до прибытия представителей МВД и ФСБ России.

ПАМЯТКА

Обязанность поведения государственного служащего в целях противодействия коррупционным проявлениям

Статьей 9 Федерального закона от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции» установлено, что для государственных служащих является неприемлемым поведение, которое может восприниматься окружающими как обещание дачи взятки или предложение дачи взятки либо как согласие принять взятку или как просьба о даче взятки, поскольку оно заставляет усомниться в объективности и добросовестности государственного служащего, наносит ущерб репутации системы государственного управления в целом.

Для предупреждения подобных негативных последствий государственным служащим следует уделять внимание манере своего общения с коллегами, представителями организаций, иными гражданами и, в частности:

1) Воздерживаться от поведения, которое может восприниматься окружающими как обещание или предложение дачи взятки либо как согласие принять взятку или как просьба о даче взятки, например, от таких выражений как: "вопрос решить трудно, но можно"; "спасибо на хлеб не намажешь"; "договоримся"; "нужны более веские аргументы"; "нужно обсудить параметры"; "ну, что делать будем?" и т.п.

2) Воздерживаться от обсуждения определенных тем, например, таких как:

- низкий уровень заработной платы государственного служащего и нехватка денежных средств на реализацию тех или иных нужд;

- желание приобрести то или иное имущество, получить ту или иную услугу, отправиться в туристическую поездку;

- отсутствие работы у родственников государственного служащего;

- необходимость поступления детей государственного служащего в образовательные учреждения и т.п.

3)<u>Воздерживаться от определенных предложений</u>, особенно если они адресованы представителям организаций и гражданам, чья выгода зависит от решений и действий государственного служащего, даже если они продиктованы благими намерениями и никак не связаны с личной выгодой государственного служащего, например, от таких предложений как:

- предоставить государственному гражданскому служащему и (или) его родственникам скидку;

- воспользоваться услугами конкретной компании и (или) экспертов для устранения выявленных нарушений, выполнения работ в рамках государственного контракта, подготовки необходимых документов;

- внести деньги в конкретный благотворительный фонд;

- поддержать конкретную спортивную команду и т.д.;

4)<u>Не совершать определенных действий</u>, например, таких как:

- регулярное получение подарков, даже стоимостью менее 3 000 рублей;

- посещение ресторанов совместно с представителями организации, которая извлекла, извлекает или может извлечь выгоду из решений или действий (бездействия) государственного служащего.

Прокуратура Коченевского района Новосибирской области

Председатель редакционного совета Н.Н.Баландюк

Тираж 50 экз.