МАУК «Центральная библиотека
Очёрского городского округа»
Отдел электронных ресурсов и информационных технологий

Безопасный Интернет

Дайджест актуальных статей
из СПС «КонсультантПлюс»

Очер 2022

СОДЕРЖАНИЕ

Антропова, Т. Ю. По секрету - всему интернету, или как не попасться web-паукам / Т. Ю. Антропова // Руководитель автономного учреждения. – 2021. – № 9. – С. 67–78.

ПО СЕКРЕТУ - ВСЕМУ ИНТЕРНЕТУ, ИЛИ КАК НЕ ПОПАСТЬСЯ WEB-ПАУКАМ

В Интернете трудно сохранить приватность. Каждый шаг в Сети оставляет след. В эпоху компьютерных технологий любой человек может связаться с любым человеком или собрать на него неплохое досье. Хорошо, если это делается с мирными намерениями. А если действует злоумышленник, цель которого - отъем денег?

Есть ли способы защиты? Есть. И мы их обсудим.

Да, компьютер может быть заражен вирусом. И плохо то, что иногда сам пользователь как бы предлагает хакерам взломать его устройство, сам приглашает супостатов в свое интернет-пространство, разве что красную дорожку не стелет.

Способов виртуального мошенничества достаточно много, и каждый день список пополняется. Большинство этих способов основано на трех человеческих слабостях: жадность, любопытство и сверхдоверчивость. Враждебные действия могут быть направлены **против "железа"** или **против его хозяина**. В первом случае недоброжелатель заражает компьютер вирусом, во втором - выуживает нужную ему информацию при помощи методов социальной инженерии.

Когда безопасность в опасности

Мы понимаем, что охранять свою виртуальную территорию надо. Но знаем, что абсолютно защищенных доступов не бывает, как и не бывает невскрываемых дверей.

И тут возникает вопрос: если хакеры взломали даже такой суперресурс, как сервер NASA, стоит ли простому пользователю пытаться обеспечить себе интернет-приватность? Не проще ли пойти по пути садовода, по завершении сезона оставляющего дом открытым и вешающего табличку "Здесь брать нечего"?

Не проще. Потому что, в отличие от садовода, который все ценное имущество либо вывез в город, либо спрятал в надежном месте, нашему пользователю есть что терять. Практически каждый гражданин имеет банковскую карту, а бесконтактные платежи становятся все популярнее, и соблазн получить доступ к чужим онлайн-счетам у нечистых на руку субъектов все больше. Карты нет? А может, есть опасный секрет? Его тоже можно дистанционно обнаружить - вот вам и повод для вымогания денег. Да мало ли причин для сбора чужой информации.

Однако любой взлом - это время, нервы и деньги. Преступники стремятся использовать свои ресурсы рационально. Многие из них понимают: за сутки возни с защищенным компьютером можно вскрыть три-

четыре незащищенных. Помните эпизод из фильма "Джентльмены удачи" с перетаскиванием батарей в детском саду? Работали бы Хмырь, Косой и Василий Алибабаевич с таким энтузиазмом, зная, какая именно сумма лежит в тумбочке? Ситуация с защитой аналогична: хозяин компьютера должен **усложнить работу непрошеному гостю до такой степени, чтобы он не захотел заниматься этой работой**.

Зачем же лезть в чужой компьютер?

Поколение хакеров - умненьких шалунов, внедряющих вредителей в чужие интернет-системы забавы ради, постепенно уходит в историю. Это те юмористы, которые в 2014 году на дорожном табло в Сан-Франциско, предупреждающем о пробках и ремонтных работах, разместили светящуюся надпись "Годзилла атакует! Поворачивай!"; годом раньше - в аккаунте Burger King заменили его логотип на символ главного конкурента, компании McDonald's...

Современные взломщики более меркантильны, но их методы не менее креативны.

Как отнимают деньги?

Представим, что хакер уже проник в чужой компьютер и начинает там свою деятельность. Каковы могут быть его коварные планы?

Уводят средства с онлайн-счета

Компьютер - это лишь машина. Умная, быстрая, незаменимая, но всего лишь машина. Он не может самостоятельно отличить хозяина от чужака. Если нет установленного запрета, все равно, кто нажимает на кнопки, кто открывает файлы и кто на какие сайты заходит. "Железо" выполняет команды человека. Того человека, в чьих руках "бразды правления".

Цель хакера - завладеть управлением. И тогда ваши возможности - это его возможности. Захочет - посетит онлайн-банк и переведет куда надо ваши сбережения. Пожелает - приобретет себе что-то нужное и расплатится от вашего имени. Возможности поистине безграничны, хватило бы средств на их реализацию. Ваших средств. Впустили на свою территорию чужака - расплачивайтесь. В буквальном смысле этого слова.

"Купите ваши же секреты!"

Остап Бендер смог получить миллион от Корейко, используя добытую информацию против него. Компромат аферист собирал тщательно и с большим трудом. В век Интернета все было бы проще.

Безупречных людей нет. Кто-то что-то кому-то сообщил в личной беседе, кто-то что-то сделал, не подозревая, что камера включена дистанционно, кто-то сохранил приватное видео. Вот и материал для шантажа.

За примером ходить далеко не надо - возьмем хотя бы звездные

скандалы. Памела Андерсен в первый раз судилась со взломщиками в начале 1990-х - они выложили в открытый доступ ее домашнее видео с мужем, Томми Ли, не предназначенное для посторонних глаз. Через 10 лет история повторилась. Видеодива отсудила у наглецов, посмевших вторгнуться в ее частную жизнь, более 90 млн долл. Но компромат-то в Сети остался. Аналогичная история произошла в 2006 году с Ким Кардашьян.

Свои "скелеты в компьютере" есть у многих. Задача взломщика - найти эти "скелеты" и продать подороже.

Существует и другой вид вымогательства, опасный даже для людей с безупречной репутацией. Представьте темный экран монитора, внезапно "сдохшую" компьютерную мышь и системный блок, работающий бессистемно. Это постарался вирус-разрушитель, внедренный из присланного файла или подхваченный с какого-то сайта.

И вот, когда уже у пользователя опустились руки, когда он понял, что важные записи утеряны навсегда, а любимый ноутбук годен лишь в качестве подставки под горшок с фиалкой, на экране появляется надпись: переведите по указанному счету энную сумму, и будет вам счастье - все оживет и заработает. Ничего личного, это бизнес.

Может быть, все действительно начнет работать после совершения транзакции (хотя такое очень редко случается). Но деньги-то уйдут. И уйдут безвозвратно, поскольку подобные преступления раскрывать трудно.

Делаем вывод: чтобы вымогатели и грабители не считали работу с вами подарком судьбы, **не распаковываем сомнительные файлы, не ходим по сомнительным ссылкам**. А если очень хочется это сделать, активно "обеззараживаем" все антивирусной программой.

Зачем выуживают информацию?

Про деньги все понятно. Их надо охранять. Но зачем нужна информация - простые подробности жизни, которые и скрывать-то нет смысла?

На первый взгляд, в обычной информации нет ничего особенного. Какая разница, знает ли посторонний кличку вашего питомца, дату рождения ребенка или девичью фамилию матери? Разберемся.

"Информация - власть!" - говаривал доктор Хаус из известного сериала. Представьте ситуацию, когда вдруг на телефон заботливой мамы или любящего папы поступает звонок от "следователя по особо важным делам", который, обращаясь к собеседнику по имени-отчеству, сообщает, что чадо такого-то возраста по такому-то имени совершило преступление, что ребенка срочно нужно спасать, что спасение дорогое, но оно того стоит! И вот уже родитель в панике продает соседу фамильные драгоценности, чтобы как можно быстрее передать сумму нужному человеку "из компетентных органов". А после передачи и заверений "Теперь все будет хорошо, но вы впредь за ребеночком приглядывайте", после исчезновения "благодетеля" с деньгами заспанный отпрыск вдруг выплывает из своей комнаты с

удивленным видом: "Да, я сегодня поздно явился и тихонько лег в постель, дабы вас, уже спящих, не тревожить".

Тут родители - они же наивные пользователи, не принявшие меры интернет-безопасности, - понимают, что звонил им злоумышленник, и недоумевают, где же он взял нужные сведения. Потерпевшие не подозревают, что сами преподнесли все "на блюдечке", выложив в Интернет информацию и не позаботившись о ее защите. В соцсетях есть имена, фамилии, полнейшие отчеты о передвижениях, сведения о недвижимости и движимости и т.д. В переписке и комментариях - факты из личной жизни, какие-то интересные подробности.

Описанный случай показательный, но не единственный пример использования краденой информации в корыстных целях. Зачастую последствия взлома могут быть серьезнее, чем передача неизвестному половины вашего месячного оклада.

К сведению. Одна популярная телепрограмма, основанная на демонстрации чудесных возможностей людей с якобы паранормальными способностями, долгие годы делает себе рейтинг путем тщательной подготовки каждого "испытания". Команда профессионалов выуживает информацию о каждом человеке, обратившемся к "чудо-людям" за помощью. Основным источником сведений, разумеется, выступает Всемирная паутина. А потом та же команда удивляет телезрителей подробностями "видений" участников шоу.

Обратившиеся за помощью даже не подозревают, сколько информации о них можно найти в Сети, и искренне восторгаются: "Этого никто о нас не знает!".

Как защитить свой компьютер?

Страшные рассказы об интернет-вымогателях и интернет-взломщиках могут дать повод думать, что современному пользователю надо денно и нощно проявлять бдительность. Но это не так.

Правила компьютерной безопасности для обычного человека существуют. И они не сложнее, чем нормы этикета или требования гигиены.

Антивирус: всегда обновлен и всегда в деле

Антивирусная защита должна быть на каждом компьютере - это не обсуждается. Вторая аксиома - на вирусы следует проверять не только то, что нужно открывать или распаковывать (флешки, диски, файлы и т.д.), но и (периодически) все содержимое компьютера. Третье железное правило - ваш антивирус должен обновляться. Создатели вредоносных программ регулярно "радуют" пользователей своими новыми достижениями. Разработчики интернет-защиты тоже не отстают: регулярно изобретают способы противодействия, "вшивают" их в очередную версию существующей программы и предлагают клиентам.

Как и когда обновлять программу? Обычно компьютер сам напоминает "Пора!" и выдает алгоритм действий.

Правило обновления действует и для обычных программ, новые версии которых более устойчивы к интернет-атакам. А само программное обеспечение безопаснее скачивать с проверенных сайтов.

Пароли: не надо бояться сложностей

Лет десять назад, в эпоху расцвета компьютерных клубов, чуть ли не треть заведений называлась QWERTY. Знакомое сочетание, не так ли? Правильно, это первые шесть букв клавиатуры в английской раскладке - один из самых популярных паролей.

Правда, существует группа еще более ленивых пользователей, которые предпочитают, например, нажимать несколько раз подряд одну и ту же цифру или букву для входа в систему.

Те, кто похитрее, используют в качестве кода доступа кличку питомца, девичью фамилию (свою или мамы), значимую дату, не подозревая, что и эта информация есть во Всемирной паутине (соцсети, переписки, форумы, сайты).

Еще более ушлые набирают на английской раскладке какую-либо фразу без пробелов, например vjqgfhjkm, хотя у взломщиков есть специальные программы, которые быстро вычислят "мойпароль", зашифрованный столь примитивно.

При подборе пароля надо применять **следующие правила:**

- сочетание не только букв, но и цифр, а также символов обязательно;
- сочетание бессистемно - это случайный набор;
- буквы не только прописные, но и строчные;
- длина кода - минимум шесть знаков.

Если фантазии для создания пароля не хватает, воспользуйтесь услугами генератора, благо в Интернете их предостаточно (Password, Avast Passwords, Norton Password Manager и т.д.).

Еще одно правило парольной безопасности: **коды нужно периодически менять.**

Да, сложный пароль труден не только для взломщика, но и для того, кто им пользуется, - попробуй запомнить последовательность всех этих знаков хотя бы для одного секретного сочетания! Тут, как ни крути, не обойдешься без записи. Но какому носителю можно доверить столь важную информацию? Компьютер взломают, в блокнот подсмотрят.

Попробуйте сделать так.

1. Сгенерируйте, например, шестизначное сочетание, запишите его или запомните.

2. В дальнейшем используйте это сочетание при создании паролей, вставляя его в любое место наряду с другими символами.

3. Заведите тетрадь или создайте файл для хранения паролей и записывайте туда всю информацию в зашифрованном виде, заменяя

шестизначное сочетание звездочкой или другим значком, понятным только вам. Вы будете знать, что именно скрывается за такой цифрой, буквой, символом, а посторонний - нет.

А если информация, хранящаяся в вашем компьютере или на другом устройстве, очень ценная, используйте еще и биометрическую аутентификацию - например, вход по отпечатку пальца, скану радужной оболочки глаза.

Слово не воробей, но Сетью ловится

Интровертам проще - информацию из них приходится выуживать. Экстраверты готовы рассказать все о себе первому встречному. Поэтому экстраверты чаще страдают от интернет-мошенников. Однако любой сможет хранить секреты, если осознает последствия, которые могут наступить при их разглашении.

Защита в этом направлении одна - **не болтать**. Помните: все, что вы выложите во всеобщий доступ, может быть использовано против вас. Например, многие перед путешествием любят публиковать на страничке в соцсети фото билетов. Почему это плохая идея? Да хотя бы потому, что злоумышленник поймет, когда вас не будет дома. В посадочных документах имеются и другие важные сведения. Кто-то может позвонить перевозчику от вашего имени и, указав необходимые данные, отменить поездку и попросить вернуть деньги. А уж шестизначный код бронирования - временный пароль, известный также как PNR (запись имени пассажира), вообще подарок для злоумышленников. Человек, знающий этот код и фамилию владельца билета, может получить доступ к его багажу или улететь его рейсом.

С билетами на концерт - та же история. В 2016 году некий москвич пожаловался в Instagram, что не смог попасть на концерт любимой группы Black Sabbath, поскольку некто скопировал штрих-код с фото билета, выложенного в профиле, и проник на площадку раньше.

Но если информация не идет к вымогателю, **вымогатель идет к информации**: создает очень привлекательные сайты, делает предложения, от которых трудно отказаться. Кто-то поведется на сообщение о распродаже конфиската, при которой брендовая одежда уходит к счастливчикам за смешные деньги. Кого-то соблазнит приглашение на суперработу, например три часа в день собирать шариковые ручки за оклад директора мини-завода. Цель посулов одна - заставить потенциальную жертву зарегистрироваться, указав персональные данные (а иногда требуется еще и подтвердить серьезность намерений вступительным взносом). Обычно после регистрации связь с сайтовладельцами прекращается.

Стоит ли принимать подобные предложения, человек разумный решает самостоятельно. Для начала можно задуматься: а почему на такую привлекательную распродажу торговец не зовет своих знакомых, почему на суперработу не устраивает родственников? Если и после этого соблазн остается, посмотрите отзывы о предложении в Интернете. Но ищите не по

названию компании или магазина (изменить его недолго), а по тексту сообщения - как правило, с вариациями на эту тему отправители не заморачиваются.

Компьютер, щетка и расческа должны быть личными

Жил-был ответственный пользователь. На сомнительные сайты не ходил. Файлы от незнакомцев не открывал. Уходя из своего офиса, оставлял охранника.

Все эти меры предосторожности оказались напрасными: устройство взломали, вирус внедрили. А все потому, что скучающий охранник развлекался на хозяйском компьютере - и на разные сайты заглядывал, и сомнительные вложенные файлы открывал.

Мораль этой правдоподобной истории проста: безопасность компьютера зависит от всех его пользователей. Такими пользователями могут быть и сослуживцы, и домочадцы, и просто знакомые.

Не хотите "случайных связей" - **поставьте пароль на вход.**

Скачок трафика - это опасно

Вирусы-шпионы незаметны, но производительны. Наряду с постоянным сканированием компьютера на предмет заражения нужно следить за своей интернет-активностью. Например, если трафик за день вырос до 1 Гб, а вы только пару раз открывали почту, что-то тут нечисто. Кто-то пользуется Интернетом от вашего имени - шлет спам, отправляет собранную информацию, а может, добывает криптовалюту за счет ресурсов вашего процессора.

Расходование трафика можно отследить, найдя в разделе "Параметры" подраздел "Сеть и Интернет". Там же можно этот трафик ограничить.

Поверим, не проверим?

Письма по-прежнему являются одним из самых действенных способов проникновения в чужой компьютер или получения заветной суммы. Письма могут маскироваться под следующую корреспонденцию.

1. **Весточка от друга.** Это письмо действительно отправлено с почтового ящика вашего знакомого, но не им, а хакером, взломавшим ящик. Чтобы распознать мошенника, обратите внимание на безличные предложения (скорее всего, рассылка веерная, злоумышленнику некогда разбираться с приветствиями) и изменение привычной лексики (чрезмерную фамильярность или официоз), просьбы перейти на сайт или как можно быстрее посмотреть присланные файлы ("а то обижусь"), мольбы о материальной помощи. Проигнорируйте такое письмо. А если боитесь обидеть отправителя, свяжитесь с ним по телефону или найдите другой способ уточнить информацию.

2. **Официальное послание.** Иногда мошенники поступают примитивно - выбирают любой адрес и отправляют провокационное сообщение типа

"Списание с вашего счета 5 тыс. руб. одобрено банком", "Из-за грубых нарушений ваш аккаунт заблокирован", "А у вас молоко убежало". Далее обязательно следует ссылка, по которой надо пройти, чтобы во всем разобраться. Испуганный адресат переходит на нужную страницу, недоумевает: "Позвольте, какое молоко? У меня на плите нет молока!" А вредоносный вирус уже топчется в его компьютере.

Поэтому не торопитесь, вначале проанализируйте ситуацию.

Более старательные преступники маскируют письма под известные бренды: "Госуслуги", "Сбербанк", "Авито" и т.д. В этом случае обязательно смотрите на адрес отправителя. Буквы и цифры после "собаки" (@) должны совпадать с доменом официального сайта. Например, послание, пришедшее с Avito, будет заканчиваться так: @avito.ru. Если в конце стоят awito.ru, ovito.ru или avita.ru - сообщение отправлял злоумышленник. Корпоративная символика и другой официоз оформления вводить в заблуждение не должны.

3. **Ошиблись адресом.** Много ли мужчин устоит, получив, например, такое сообщение "от Анжелы": "Привет. Классно вчера посидели в баньке. Высылаю фотки. Но только для тебя"? Желание посмотреть, что же такого было в этой баньке, частенько пересиливает понимание, что отправитель ошибся адресом и что читать чужие письма, смотреть чужие фотографии - плохо. Заинтригованный получатель идет по ссылке или распаковывает файл. Возможно, он видит то, что хочет. Но в это время вирус идет к нему в компьютер и делает то, что может.

Совет: если любопытство пересиливает разумные доводы, проверьте ссылку на вирусы хотя бы на сайте vms.drweb.ru/online или просканируйте присланный файл антивирусной программой.

4. **Просьба о помощи.** Один из самых гнусных онлайн-обманов касается благотворительности. Прошли времена массового получения писем от умирающих миллионеров, которые наслышаны о филантропических качествах адресата и готовы перевести на его счет все свои деньги. Но когда на почту приходит просьба помочь в сборе средств на операцию для ребенка или приюту для животных, проверьте честность отправителя.

Например, автор этой статьи получил сообщение с мольбой о материальной помощи прооперированной собаке, которую готовы выбросить на улицу, поскольку не оплачен стационар. В письме были фотографии документов и, конечно, снимок несчастного животного. Простое обращение в клинику, где работают "бессердечные ветеринары", показало, что сообщение не что иное, как вымогательство: никакой похожей собаки в клинике не было, там не было даже стационара. "Вы не первая, кто к нам обращается, про эту собаку постоянно спрашивают", - устало сообщил врач по телефону.

Будьте бдительны! Благотворительность почетна, но ваши деньги должны действительно приносить пользу, а не обогащать мошенников. Сомневаетесь - введите в поисковик наиболее характерную фразу из письма или указанный телефон. Как правило, аналогичные письма не первый день

гуляют по Интернету. Либо найдите контакты названного в письме заведения и проверьте все сведения лично.

Второй почтовый ящик - не роскошь

При регистрации на сайтах, при интернет-покупках и других действиях в Сети зачастую требуется вписать адрес электронной почты. Бывает, что база данных с этих сайтов попадает в руки мошенников. В лучшем случае адресата заваливают спамом, в худшем - при помощи полученных данных воруют деньги.

Поэтому желательно иметь два почтовых ящика. Один для важной переписки, а другой - для своей интернет-деятельности.

Чужой компьютер - свои правила

Отдельно рассмотрим ситуацию, когда приходится работать на стороннем компьютере. В этом случае желательно оповестить об этом машину, нажав соответствующую кнопку при входе. Тогда все "пароли, адреса, явки" не будут сохраняться автоматически, как это бывает на домашнем устройстве.

Дополнительными мерами безопасности станут очистка истории просмотров (кнопка находится справа, вверху страницы браузера) и удаление личных файлов, в том числе из "корзины" и из папки "Загрузки".

И не совершайте самую распространенную ошибку - по завершении работы обязательно выйдите из своей почты.

* * *

Компьютер надо защищать в любом случае - хорошая защита отобьет у хакеров желание тратить на вас нервы и время. Кроме того, следует заботиться об интернет-безопасности, выполняя не очень сложные, но важные правила:

1) доверять, но проверять;
2) не ходить, куда не надо;
3) пользоваться антивирусом;
4) применять сложные пароли и регулярно менять их;
5) систематически обновлять программное обеспечение.

"

Подписано в печать
24.08.2021

Аксенов, В. А. Современное состояние и мировые тенденции совершения мошенничества с использованием информационно-телекоммуникационных технологий в период пандемии COVID-19 / В. А. Аксенов // Безопасность бизнеса. – 2021. - № 5. – С. 45–49.

СОВРЕМЕННОЕ СОСТОЯНИЕ И МИРОВЫЕ ТЕНДЕНЦИИ СОВЕРШЕНИЯ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ПЕРИОД ПАНДЕМИИ COVID-19

Изменения, происходящие в различных сферах общественной жизни как в мире, так и в Российской Федерации, в том числе связанные с внешнеполитическими разногласиями между странами, привели к уменьшению социальной стабильности и увеличению уровня криминализации общества.

В конце 2019 г. в мире произошла глобальная социально-эпидемиологическая катастрофа, которая в процессе своего развития приобрела форму пандемии под условным наименованием COVID-19, унесшей множество жизней. Нынешний кризис является беспрецедентным в мировой истории. Пандемия проиллюстрировала отсутствие вариантов оперативного воздействия на такого рода кризисы на территории всего мира. Одной из первых мер реагирования государств на возрастание количества заболеваемости явилось внедрение практики принудительной самоизоляции граждан. Отметив положительный эффект от внедрения данной методики, необходимо отразить и отрицательную сторону - увеличение общего количества кибермошенничеств.

COVID-19 продемонстрировал, что преступность в сфере информационно-телекоммуникационных технологий, по сути, не меняется, за исключением того, что преступники изменяют методики в ее использовании. Они адаптируют специфику своих подходов к обществу как средство повышения скорости их успеха. Традиционные киберпреступления, такие как фишинг и интернет-мошенничество, оперативно использовали общественные уязвимости, так как большинство людей, в том числе представители сферы бизнеса, искали источники информации с целью получения ответа на интересующие их вопросы. Ссылка на COVID-19 - одна из последних наиболее популярных методик социальной инженерии, используемых киберпреступниками.

Отличие периода пандемии COVID-19 заключается в том, что из-за введенных физических ограничений, связанных с последующим увеличением работы с использованием технологий удаленного доступа в домашних условиях, многие люди и компании, которые до кризиса не использовали в достаточной мере возможности информационно-телекоммуникационных технологий и не обладали базовыми знаниями в сфере информационной

безопасности, стали прибыльной целью для мошенников.

Весомый вклад в получение аналитической информации о данной категории мошенничеств, связанных со злоупотреблением информацией о пандемии COVID-19, на территории стран - участниц Европейского союза внес Европол. В целях подготовки к крупным трансграничным кибератакам 11 декабря 2018 г. Советом Европейского союза принят Протокол "О чрезвычайных ситуациях правоохранительных органов Европейского союза", отводящий главенствующую роль Европейскому центру по борьбе с киберпреступностью (EC3) Европола, являющемуся частью плана Европейского союза по скоординированному реагированию на крупномасштабные трансграничные инциденты и кризисы в области кибербезопасности.

Отчет с наименованием IOCTA, опубликованный Европейским центром по борьбе с киберпреступностью (EC3) Европола, отражает, что пандемия COVID-19 показала, насколько активно преступники стали извлекать выгоду из общества в наиболее уязвимых местах. Преступники адаптировали существующие схемы мошенничеств под пандемию, злоупотребляя неопределенностью ситуации и потребностями общества в достоверной информации. По всем направлениям - от социальной инженерии до DDoS-атак и распространения программ-вымогателей - преступники активно злоупотребляли кризисом, пока остальные члены общества пытались сдержать ситуацию

В опубликованном отчете Международной организации уголовной полиции (Интерпол) выделены следующие разновидности кибермошенничеств, связанных с пандемией COVID-19 :

1) интернет-мошенничество и фишинг. Киберпреступники создают поддельные сайты, связанные с COVID-19, чтобы побудить жертв открыть вредоносные вложения или фишинговые ссылки, приводящие к незаконному доступу в личные кабинеты;

2) вредоносные домены. За время пандемии увеличилось количество доменов, зарегистрированных по ключевым словам "COVID" или "Корона", в целях привлечения внимания лиц, которые осуществляют поиск информации о COVID-19. По состоянию на конец марта 2020 г. специалисты Palo Alto Networks выявили 116 357 фактов регистрации новых доменных имен, связанных с коронавирусом. Из них 2 022 вредоносных и 40 261 - с высокой степенью риска;

3) деструктивное вредоносное программное обеспечение. Киберпреступники используют деструктивное вредоносное программное обеспечение, такое как программы-вымогатели, против объектов критической инфраструктуры и ответственных учреждений - больниц и медицинских центров, которые переполнены из-за кризиса в сфере здравоохранения.

Пандемия COVID-19 не имеет границ, вследствие чего Российская Федерация также столкнулась с проблемами использования данной

информации в методиках социальной инженерии при совершении мошенничеств. Специалисты в сфере кибербезопасности Group IB сообщают, что суть мошенничеств с годами не меняется, а вот их формат и схемы - телефонный звонок от имени социальных работников, продажа электронных QR-кодов или рассылка информации о нарушениях карантина - меняются постоянно. Зачастую информационные поводы, используемые мошенниками, опережают повестку средств массовой информации.

В целях выявления состояния и динамики кибермошенничеств в период пандемии COVID-19 проведем сравнительный анализ статистических данных за период с 2018 по 2020 год на территории Российской Федерации, Австралии и Соединенных Штатов Америки.

В России под признаки мошенничества, совершенного с использованием информационно-телекоммуникационных технологий, подпадают три состава преступления из Уголовного кодекса РФ: ст. 159 "Мошенничество", ст. 159.3 "Мошенничество с использованием электронных средств платежа" и ст. 159.6 "Мошенничество в сфере компьютерной информации". Так, в 2020 г. состояние преступности данной категории имело следующие числовые значения: ст. 159 УК РФ - 210 493, динамика роста по отношению к 2019 г. на 75,5%, к 2018 г. - на 132,2%, ст. 159.3 УК РФ - 25 820, динамика роста по отношению к 2019 г. на 60,2%, к 2018 г. - на 508,7%, ст. 159.6 УК РФ - 970, динамика роста по отношению к 2019 г. на 10,8%, однако по отношению к 2018 г. наблюдается отрицательная динамика на 21,5%. По мнению автора, отсутствие планомерного роста динамики по ст. 159.6 УК РФ связано с использованием в правоприменительной деятельности правоохранительных органов рекомендаций, изложенных в Постановлении Пленума Верховного Суда РФ от 30 ноября 2017 г. N 48 "О судебной практике по делам о мошенничестве, присвоении и растрате", которые оказали значительное влияние на квалификацию преступлений данной категории. Также необходимо выделить высокий уровень латентности мошенничеств, совершенных в сфере компьютерной информации.

Состояние мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий на территории РФ

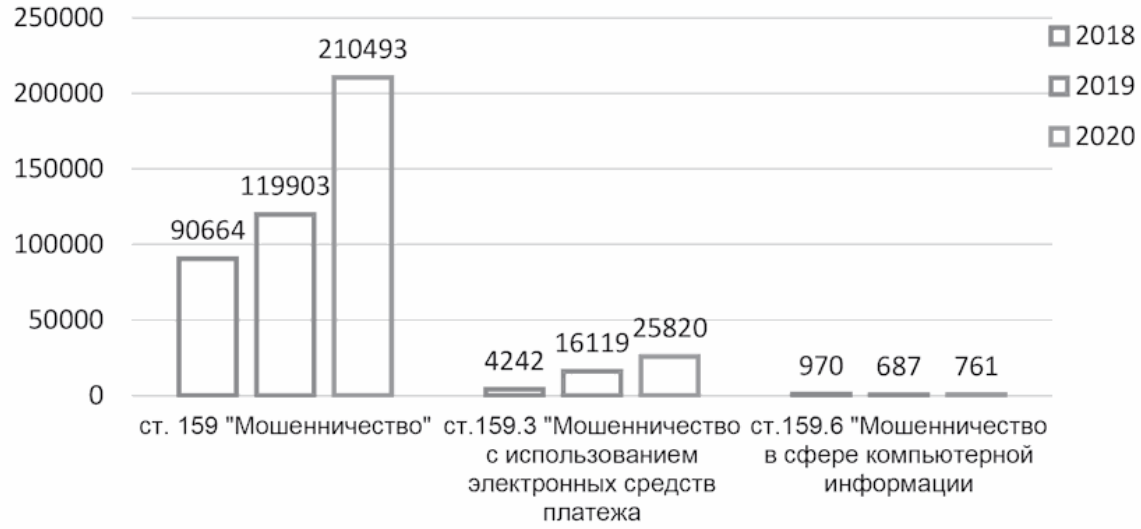

Диаграмма N 1

Согласно опубликованному отчету Австралийской комиссии по конкуренции и защите прав потребителей, в 2020 г. на территории данного государства зарегистрировано 216 086 обращений по факту совершения кибермошенничества. Ущерб от мошенничеств данной категории за 2020 г. составил 175 695 558 австралийских долларов. В 2019 г. общее количество обращений составило 167 801, ущерб от противоправной деятельности - 142 898 217 австралийских долларов. Таким образом, динамика роста преступности составила 28,8%. В 2018 г. зарегистрировано 177 517 мошенничеств данной категории, ущерб составил 107 001 471 австралийский доллар, динамика роста по отношению к 2020 г. составила 21,7%.

Состояние мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий на территории Австралии

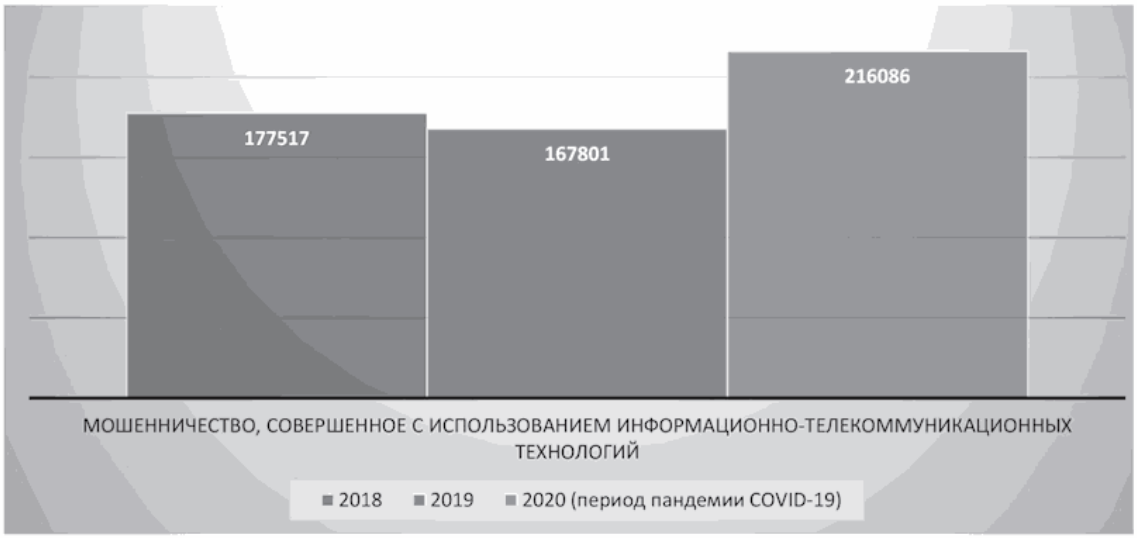

Диаграмма N 2

Центром жалоб на интернет-преступления, являющимся подразделением Федерального бюро расследований, опубликованы статистические данные с результатами обращения за 2020 г. и суммой причиненного ущерба. В опубликованном отчете данным подразделением отдельно отражена информация об активном использовании мошенниками предлогов, связанных с пандемией COVID-19. Так, в 2020 г. на территории США зарегистрировано 791 790 обращений жертв мошенничеств данной категории, ущерб составил 4,2 миллиарда долларов США. В 2019 г. на территории данной страны было совершено 467 361 мошенничество, сумма ущерба - 3,5 миллиарда долларов США. Таким образом, динамика роста преступлений данной категории составила 69,4%, а причиненного ущерба - 20%. В 2018 г. зарегистрировано 351 937 обращений по факту совершения кибермошенничеств (динамика роста по отношению к 2020 г. на 125%), общая сумма причиненного имущественного ущерба - 2,7 миллиарда долларов США (динамика роста по отношению к 2020 г. на 55,5%)

Состояние мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий на территории США

Диаграмма N 3

Изучив статистические данные кибермошенничества, мы пришли к выводу об общемировой тенденции роста преступлений данной категории, где одним из главных условий преступности является распространение пандемии COVID-19.

Таким образом, человечество, столкнувшись с глобальной проблемой современности - пандемией COVID-19, продемонстрировало высокий уровень виктимности по отношению к мошенничествам, совершенным с использованием информационно-телекоммуникационных технологий. Несмотря на имеющиеся положительные результаты борьбы с преступлениями данной категории на общемировом уровне, принимаемые меры по предупреждению мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий, и противодействию им являются недостаточными. Учитывая их транснациональный характер и дальнейшее существование пандемии COVID-19, правоохранительным органам различных стран мира необходимо усилить взаимодействие в целях своевременного устранения причин и условий, способствующих совершению данных преступлений.

Подписано в печать
17.09.2021

Долгополов, П. С. Телефонное мошенничество / П. С. Долгополов // СПС КонсультантПлюс. –2022.

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

Телефонная связь, ее возможности и особенности зачастую используются злоумышленниками для незаконного обогащения. Телефонное мошенничество - это очень распространенный в настоящее время вид мошеннических действий, направленный на обогащение путем обмана телефонного собеседника без визуального контакта с ним. Как правило, мошенники представляются своим жертвам родственниками или обманным путем действуют от имени банка.

Квалификация телефонного мошенничества

Действия телефонных мошенников квалифицируются по ст. 159 УК РФ как мошенничество, т.е. умышленные действия, направленные на хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

При этом под хищением понимаются совершенные с корыстной целью противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившие ущерб собственнику или иному владельцу этого имущества (примечание 1 к ст. 158 УК РФ).

Обман как способ совершения хищения или приобретения права на чужое имущество может состоять в сознательном сообщении (представлении) заведомо ложных, не соответствующих действительности сведений, либо в умолчании об истинных фактах, либо в умышленных действиях (например, в предоставлении фальсифицированного товара или иного предмета сделки, использовании различных обманных приемов при расчетах за товары или услуги или при игре в азартные игры, в имитации кассовых расчетов и т.д.), направленных на введение владельца имущества или иного лица в заблуждение. Злоупотребление доверием при мошенничестве заключается в использовании с корыстной целью доверительных отношений с владельцем имущества или иным лицом, уполномоченным принимать решения о передаче этого имущества третьим лицам. Доверие может быть обусловлено различными обстоятельствами, например служебным положением лица либо его личными отношениями с потерпевшим (п. п. 2, 3 Постановления Пленума Верховного Суда РФ от 30.11.2017 N 48 "О судебной практике по делам о мошенничестве, присвоении и растрате", далее - Постановление Пленума N 48).

Мошенничество признается оконченным с момента, когда имущество поступило в незаконное владение виновного или других лиц и они получили реальную возможность пользоваться или распорядиться им по своему

усмотрению.

Если предметом преступления являются безналичные денежные средства, в том числе электронные денежные средства, то по смыслу п. 1 примечаний к ст. 158 УК РФ и ст. 128 ГК РФ содеянное должно рассматриваться как хищение чужого имущества. Такое преступление следует считать оконченным с момента изъятия денежных средств с банковского счета их владельца или электронных денежных средств, в результате которого владельцу этих денежных средств причинен ущерб (п. 5 Постановления Пленума N 48).

Ответственность за телефонное мошенничество

Телефонное мошенничество в зависимости от размера похищенного и других обстоятельств деяния (например, имеются или отсутствуют признаки преступления) может повлечь административную или уголовную ответственность.

На основании ч. 1 ст. 7.27 КоАП РФ мелкое хищение чужого имущества, стоимость которого не превышает одну тысячу рублей, путем кражи, мошенничества, присвоения или растраты при отсутствии признаков преступления влечет наложение административного штрафа в размере до пятикратной стоимости похищенного имущества, но не менее одной тысячи рублей, либо административный арест на срок до пятнадцати суток, либо обязательные работы на срок до пятидесяти часов.

Согласно ч. 2 указанной статьи мелкое хищение чужого имущества стоимостью более одной тысячи рублей, но не более двух тысяч пятисот рублей путем кражи, мошенничества, присвоения или растраты при отсутствии признаков преступления влечет наложение административного штрафа в размере до пятикратной стоимости похищенного имущества, но не менее трех тысяч рублей, либо административный арест на срок от десяти до пятнадцати суток, либо обязательные работы на срок до ста двадцати часов.

Кроме того, на основании ст. 7.27.1 КоАП РФ причинение имущественного ущерба собственнику или иному владельцу имущества путем обмана или злоупотребления доверием при отсутствии признаков уголовно наказуемого деяния влечет наложение административного штрафа в размере до пятикратной стоимости причиненного ущерба, но не менее пяти тысяч рублей.

Статья 159 УК РФ предусматривает различные виды уголовной ответственности за мошенничество в зависимости от конкретных обстоятельств.

Согласно ч. 1 указанной статьи мошенничество наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом

на срок до четырех месяцев, либо лишением свободы на срок до двух лет.

Квалифицирующими признаками телефонного мошенничества, к примеру, являются следующие:

- совершение группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину;

- совершение лицом с использованием своего служебного положения, а равно в крупном размере и др.

Эти и другие признаки, указанные в ч. ч. 2 - 7 ст. 159 УК РФ, влекут более суровую ответственность вплоть до лишения свободы сроком до десяти лет.

Если действия лица при мошенничестве, присвоении или растрате хотя формально и содержали признаки указанного преступления, но в силу малозначительности не представляли общественной опасности, то суд прекращает уголовное дело на основании ч. 2 ст. 14 УК РФ (п. 33 Постановления Пленума N 48).

Действия, которые необходимо предпринять, став жертвой телефонного мошенничества

Если гражданин предполагает, что стал жертвой телефонного мошенничества, ему необходимо обращаться в органы внутренних дел с соответствующим заявлением. В заявлении следует максимально подробно рассказать о всех обстоятельствах события. Кроме этого, следует сообщить о факте телефонного мошенничества в абонентскую службу мобильного оператора, который обслуживает номер преступника. Если гражданин, к примеру, совершил перевод денежной суммы по мобильной сети, то принятие оператором экстренных мер может позволить заблокировать перевод и вернуть деньги.

Для того чтобы не стать такой жертвой, необходимо следовать определенным правилам. Например:

- если получен звонок с просьбой о срочной денежной помощи для известного гражданину лица (знакомого, родственника и т.п.), следует не принимать решение сразу, идя на поводу у позвонившего, а проверить полученную от него информацию, перезвонив вышеуказанным лицам, или связаться с ними иными способами;

- нельзя сообщать по телефону личные сведения или данные банковских карт, которые могут быть использованы злоумышленниками для неправомерных действий;

- нельзя перезванивать на номер, если он незнаком, и т.п.

Расследование телефонного мошенничества

При расследовании данного вида правонарушений важно определить время и место его совершения.

На основании ч. 1 ст. 152 УПК РФ по общему правилу предварительное расследование производится по месту совершения деяния, содержащего

признаки преступления.

Поскольку обман жертвы осуществляется злоумышленником в процессе телефонного общения между ними, то местом совершения правонарушения признается то место, в котором последний находится во время звонка (ч. 1 ст. 152 УПК РФ).

Однако местом окончания мошенничества является то место, из которого жертва телефонного мошенничества перечислила денежные средства, т.к. ущерб для нее наступил именно в этом месте (ч. 2 ст. 152 УПК РФ).

Если преступления совершены в разных местах, то по решению вышестоящего руководителя следственного органа уголовное дело расследуется по месту совершения большинства преступлений или наиболее тяжкого из них (ч. 3 ст. 152 УПК РФ).

Кроме того, предварительное расследование может производиться по месту нахождения обвиняемого или большинства свидетелей в целях обеспечения его полноты, объективности и соблюдения процессуальных сроков (ч. 4 ст. 152 УПК РФ). Таким образом, место, в котором будет возбуждено и расследовано уголовное дело по факту телефонного мошенничества, зависит от конкретных обстоятельств дела.

Тресков, В. И. Фишинг - новый вид "рыбалки" для мошенников в интернете / В. И. Тресков // Осторожно: мошенничество! Как защитить себя и своих близких . – Москва : Редакция "Российской газеты". – 2018. – Выуск 8. – 144 с.

ФИШИНГ - НОВЫЙ ВИД "РЫБАЛКИ" ДЛЯ МОШЕННИКОВ В ИНТЕРНЕТЕ

Как мы уже неоднократно говорили, фантазия мошенников по ограблению честных граждан не знает предела и совершенствуется синхронно с техническим прогрессом, не отставая от него ни на шаг, а иногда его опережая.

Фи́шинг (англ. **phishing** - рыбная ловля, выуживание) - вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей - логинам и паролям.

Это достигается путем проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков, сервисов или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего. Оказавшись на таком сайте, пользователь может сообщить мошенникам ценную информацию, позволяющую получить доступ к аккаунтам и банковским счетам.

Таким образом, фишинг - одна из разновидностей социальной инженерии, основанная на незнании пользователями основ сетевой безопасности.

В частности, многие не знают простого факта: сервисы не рассылают писем с просьбами сообщить свои учетные данные, пароль и проч.

По данным МВД России, так называемый фишинг - это наиболее распространенный способ совершения преступлений, направленный на получение платежной информации и хищение денежных средств в Интернете. Основная цель злоумышленников - получить данные кредитной карты, пароль в мобильный банк для последующего незаконного списания средств с банковских счетов. При этом фишинговые сайты внешне сделаны так, чтобы пользователи принимали их за существующие популярные ресурсы. Обманным путем такие порталы могут выудить у неопытного юзера персональные данные или платежную информацию.

Также все большую популярность обмана доверчивых граждан набирает голосовой фишинг, когда клиенту банка звонят от имени финансовой организации и под разными предлогами стараются узнать платежную информацию. Мошенники находят способы для блокировки облачных хранилищ с личными данными, устройств **Apple** в целях последующего шантажа.

Сложность раскрываемости таких преступлений обусловлена тем, что жертва электронной кражи узнает о потере денег не сразу. Чем больше проходит времени с момента незаконного списания средств до обращения в правоохранительные органы, тем меньше шансов поймать нарушителей закона. Подобные преступления - дело рук организованных преступных сообществ, в которых действия строго поделены между членами банды. Еще одна сложность в раскрываемости такого вида преступлений состоит в том, что сайт-двойник существует максимум сутки.

Фишинг-мошенничества очень распространены, а недавно начали набирать популярность в сообществе держателей криптовалют.

Криптовалюта - это цифровая (виртуальная) валюта, которая используется участниками оборота в целях проведения интернет-расчетов, защищенная от подделки путем шифрования данных, не подлежащих дублированию.

Первой и самой известной из множества криптовалют является биткоин.

Фишинг-атаки на криптовалюту могут быть такими.

Первый вариант: мошенники от имени различных сайтов и бирж, связанных с криптовалютой, рассылают потенциальным жертвам письма (это может быть оповещение о безопасности, в котором вам предлагается изменить пароль на новый, опрос, каким-либо образом связанный с миром криптовалют), содержащие ссылки, при переходе по которым доверчивые пользователи вводят данные учетных записей своих кошельков.

Второй вариант: злоумышленники находят на различных биржах набирающие популярность сообщества, создают якобы его официальную страницу в **Facebook**, а затем делают ее оформление максимально похожим на оригинал на этом форуме. Адрес фальшивой страницы обычно похож на основной (может быть изменена одна буква или знак). На странице созданной группы владельцы создают пост с указанием имен участников и прикреплением их фотографии, указывая ссылки на этих пользователей. Кроме этого, прилагается ссылка с сайтом, похожим на исходный, при заходе на который якобы можно забрать выигрыш. Обрадовавшиеся "победители" переходят на сайт, вводят свои данные и...

Третий вариант: мошенники предлагают перевести биткоины или их часть на отдельный кошелек с дальнейшей возможностью якобы получить процент от этой суммы.

Четвертый вариант: в мессенджерах (**Telegram, Viber, WhatsApp** и т.д.) злоумышленники создают отдельные группы или чаты с владельцами криптокошельков, в которых происходит общение, обсуждение различной информации, связанной с деятельностью криптолюбителей. В один момент создатели этой самой группы скидывают фальшивые страницы криптовалютных бирж, в которых доверчивые пользователи оставляют свои данные.

Киберриски в новой реальности [Интервью с И. Чичканом] // Современные страховые технологии. – 2021. – № 1. – С. 52 –55.

КИБЕРРИСКИ В НОВОЙ РЕАЛЬНОСТИ

В прошлом году в связи с пандемией коронавируса произошел массовый переход многих компаний на удаленный режим работы. О том, какие риски в связи с этим возникли и как на них отреагировал рынок киберстрахования, рассказал Игорь Чичкан, руководитель отдела страхования финансовых рисков AIG в России.

- Современные страховые технологии: Возникли ли в связи с пандемией новые риски и требования к обеспечению кибербезопасности в работе предприятий?

- Игорь Чичкан: В целом риски остались прежними, но вероятность их реализации значительно возросла. В основном они связаны с методом доступа и подключения к незащищенным сетям.

Работа через удаленный доступ, через настройки APN (Access Point Name) заставила многие компании обратить особое внимание на каналы, рабочие инструменты и системы безопасности. До пандемии в удаленном режиме работали 3 - 5% сотрудников, теперь в некоторых компаниях - до 95%.

Дистанционные каналы априори менее защищены. Злоумышленники с большей вероятностью и значительно проще могут получить доступ к домашним компьютерам сотрудников, а значит, и к корпоративным информационным системам. Дома или в публичных точках доступа wi-fi иногда вообще не защищен, а это делает уязвимыми все подключенные устройства.

Если на домашнем или рабочем компьютере сотрудников стоит личная почта, любое письмо с вредоносным кодом способно подвергнуть риску корпоративную систему. Вероятность подобного сценария увеличилась в условиях дистанционной работы, как и количество атак, попыток доступа через e-mail и зараженные рассылки.

Другой тренд прошлого года - создание сайтов-клонов, особенно в социальной сфере: выплата пособий, выплаты на детей, госпрограммы поддержки туристической отрасли и т.д.

Кибератака может затронуть огромное количество предприятий одновременно в разных странах мира, разных масштабов - от небольших компаний в торговле и сфере услуг до промышленных гигантов. В таком случае к нам в агрегации попадают все индустрии, страны и категории компаний, и риск такой агрегации велик.

- ССТ: Как в связи с этим изменился подход страховщиков и страхователей к страхованию киберрисков?

- И.Ч.: Программы страхования киберрисков становятся менее доступными, поскольку риски растут. Готовность предприятий к самостоятельному противостоянию рискам снижается. Складывается ситуация, когда компании все больше интересует страхование киберрисков, но из-за зашкаливающего количества убытков и их масштабов оно становится не только дороже - в значительной степени снижаются и риск-аппетиты страховщиков. В силу целого ряда причин некоторым компаниям мы уже не можем предложить страхование киберрисков.

В 2020 году выросла активность кибервымогательства. Классический пример - когда компьютер заражен вредоносной программой и вас просят перевести определенную сумму в долларах или биткоинах за ключ разблокировки. В Норвегии злоумышленники таким образом блокировали деятельность алюминиевого завода, а производитель электроники GARWIN заплатил около 10 млн долл. выкупа за разблокировку своих систем. В России пока ни один наш клиент не заявил о подобных убытках.

Тем не менее в связи с волной киберрисков AIG, как и многие страховщики, глобально корректирует свою стратегию. У нас существенно снижаются емкости, с которыми мы работаем, и бизнес-аппетиты. Мы крайне осторожно подходим к страхованию любых убытков, связанных с кибервымогательством.

Рынок стал намного строже подходить к андеррайтингу. Мы просим клиента заполнить специальную анкету и указать используемые методы защиты и предупреждения киберугроз, внимательно изучаем их. Исходя из данных анкеты, мы понимаем, готовы ли страховать предприятие и, если да, будем полностью покрывать этот риск или частично. Предлагаем сострахование: 50% риска клиент берет на себя, а 50% передает страховщику. Бывают случаи, когда мы вынуждены отказывать в заключении договора страхования.

Примечание. В мае 2018 года Европа перешла на обновленные правила обработки персональных данных, установленные Общим регламентом по защите данных – GDPR.

Он имеет прямое действие во всех 28 странах ЕС и заменил рамочную Директиву о защите персональных данных 95/46/ЕС от 24 октября 1995 года.

Важным нюансом GDPR является экстерриториальный принцип действия новых европейских правил обработки персональных данных, поэтому российским компаниям следует внимательно отнестись к ним, если услуги ориентированы на европейский или международный рынок.

- ССТ: От каких последствий кибератак предприятия страхуются прежде всего?

- И.Ч.: Мы видим повышенный интерес к страхованию киберрисков со стороны финансовых институтов. Сейчас наши основные клиенты - это компании, у которых есть контракты с иностранными заказчиками. Большую

долю в нашем портфеле занимают ИТ-компании - они лучше остальных понимают степень риска и пытаются подкрепить свою защиту нашим полисом.

- ССТ: В финансовой сфере стало больше инцидентов с хищением баз данных. Ожидаете ли вы, что появятся крупные иски за утечку персональной информации клиентов?

- И.Ч.: Пока нет изменений в законодательстве или процедурах, которые позволили бы более активно подавать такие требования, развития судебной практики ожидать не стоит. Но нужно разделять страхование киберрисков и мошенничество в Интернете, которым занимаются физические лица. Безусловно, утечки данных из-за мошенников несут существенные репутационные и иногда финансовые риски для банков. Но физическим лицам предъявить претензии банку проблематично. Скорее, это вопрос к Росфинмониторингу, к регулятору, которые должны штрафовать финансовые организации.

В Европе с 2018 года действует стандарт General Data Protection Regulation. В Великобритании и континентальной Европе сам факт утраты данных является основанием для штрафов, которые могут достигать 5% годовой выручки финансовой организации. Физическое лицо может подавать требования компании - оператору данных, основываясь на самом факте утраты, который уже считается основанием для возмещения ущерба. Но больше всего финансовые организации опасаются регуляторов, чьи требования гораздо серьезнее.

Примечание. Виктор Верещагин, президент Русского общества управления рисками (РусРиск), кандидат исторических наук

Проблема кибербезопасности приобрела глобальный характер. Во всех опросах риск-менеджеров, которые проводились последние несколько лет в Европе и мире, киберриски попадают в первую тройку самых актуальных, их значимость постоянно растет. В полной мере это относится и к России.

Прежде всего, предприятия опасаются утечки коммерческих и персональных данных, а также вредоносного вмешательства в закрытые системы управления данными. Но разные сегменты бизнеса воспринимают и реагируют на киберугрозы по-разному. Более подготовлены к угрозам финансовый сектор и, прежде всего, банки. В реальном секторе экономики многие предприятия и компании не готовы в полной мере противостоять растущим киберугрозам из-за незнания и непонимания, как это нужно делать.

Несмотря на то что о проблеме много пишут, ею активно занимаются ИТ и специализированные компании в области информационной безопасности, киберагрессоры действуют изощренно и часто оказываются на шаг впереди. Разработчики средств защиты зачастую предлагают новые инструменты по факту реализации угрозы, чтобы залатать пробоину.

Понимая серьезность угрозы, мы создаем в РусРиске рабочую группу по

киберрискам с участием крупных ИТ-компаний, консалтеров и экспертов реального сектора. Мы планируем выработать серьезные комплексные меры, включая корректировку законодательной и нормативной базы, управленческие решения, возможно - страхование киберрисков. Мы также намерены пригласить к сотрудничеству коллег из ВСС, чтобы привлечь к работе и страховщиков.

- ССТ: Страховать или не страховать киберриски - решение топ-менеджеров. Могут ли к ним быть предъявлены претензии со стороны акционеров, если предприятие понесет убытки из-за отсутствия договора страхования?

- И.Ч.: Претензии, безусловно, могут возникнуть из-за отсутствия полиса. При наличии договора страхования убытки можно минимизировать, а если его нет - директора могут столкнуться с требованиями акционеров о недостаточном обеспечении страховой защиты предприятия.

Таких прецедентов в России не было, а в США после киберинцидента, когда компания понесла значительные убытки, акционеры предъявили требования к совету директоров. Они были связаны с тем, что совет директоров не приобрел защиту от киберрисков, решив сэкономить бюджет. Убытки во много раз превысили потенциальную страховую премию.

- ССТ: Возможна ли в России ситуация, когда каждое предприятие будет иметь полис страхования киберрисков?

- И.Ч.: Каждое - вряд ли, особенно когда не все предприятия покупают даже обязательные виды страхования.

Большинство руководителей предприятий в России не воспринимают страхование как инвестиции в безопасность. Расходы на антивирусные программы, ИТ-безопасность и специалистов тоже достаточно велики, но они материальны. Страхование воспринимают как гипотетическую договоренность, ее сложно потрогать. Так что сложно представить, какие должны быть предпосылки, чтобы большинство компаний страховали киберриски. Возможно, помогут определенные льготы, возможность отнесения на затраты расходов на страхование киберрисков.

Должны измениться отношение к страхованию в обществе в целом, культура риск-менеджмента. Надеюсь, что через некоторое время это произойдет.

Подписано в печать
10.03.2021

Кецко, К. В. Преступность в сфере электронной коммерции / К. В. Кецко // Российский следователь. – 2021. – № 9. – С. 58–63.

ПРЕСТУПНОСТЬ В СФЕРЕ ЭЛЕКТРОННОЙ КОММЕРЦИИ

Электронная коммерция стремительно развивается в современном мире, занимая огромные ниши в различных экономических сферах общества. Количество операций, участников, обороты денежных средств, которые происходят в электронном мире, растут с молниеносной скоростью. Преимущества электронной коммерции, с учетом набирающей обороты пандемии вирусных заболеваний в современном мире, делают данный вид экономических отношений наиболее перспективным и востребованным. Каждый вид коммерческой сделки, в которой участники готовят или совершают свои деловые операции в электронном виде, может рассматриваться как электронная коммерция.

Ежегодно одним из основных направлений развития Российской Федерации (далее также - РФ) является системное развитие информатизации во всех экономических и иных сферах жизни общества, что в свою очередь дает мощный толчок развитию электронной коммерции.

При этом даже в Послании Президента Российской Федерации Федеральному Собранию Российской Федерации 2021 г., в условиях, когда все усилия направлены на развитие здравоохранения и создание эффективной социальной поддержки населения, прослеживается необходимость так называемой информатизации экономических процессов во всех сферах.

Так, например, в Послании говорится: "...Уже через три года абсолютное большинство государственных и муниципальных услуг должно предоставляться гражданам России дистанционно в режиме 24 часа в сутки семь дней в неделю, то есть на постоянной основе Этот год объявлен в нашей стране годом науки и технологий. Мы понимаем, что наука в современном мире имеет абсолютно ключевое значение. До 2024 г. на гражданские, в том числе фундаментальные, исследования Россия только из федерального бюджета направит 1 триллион 630 миллиардов рублей. Но это не все... Эпидемия повсеместно и многократно ускорила внедрение телемедицины, искусственного интеллекта.

Кроме того, продуктивно и масштабно Министерством цифрового развития, связи и массовых коммуникаций РФ воплощается в жизнь национальный проект "Цифровая экономика" на период с 2019 по 2024 г.

Определяющим моментом в сфере электронной коммерции является правовое регулирование в данной отрасли. В 1996 г. комиссией ООН по праву международной торговли принят "Типовой закон об электронной торговле", который является базовым нормативно-правовым актом в данной сфере.

В настоящий период в России специализированного нормативно-правового акта, регулирующего электронные экономические отношения, нет, что является одной из основных причин возникновения различных махинаций и обмана в данной сфере. При этом предпосылки правового регулирования возникали в нашей стране уже давно, законопроект "Об электронной торговле" выносился на рассмотрение еще в 2000-х гг., однако не был принят и снят с рассмотрения. Одной из основных причин, по мнению комитета Государственной Думы по информационной политике, являлось копирование законопроекта из США, а также разнообразие иных действующих нормативно-правовых актов, в той или иной степени охватывающих и регулирующих отношения, возникающие в сфере электронной коммерции.

Действительно, в РФ существует множество нормативно-правовых актов, так или иначе затрагивающих отношения в сфере электронной коммерции: Федеральные законы "Об основах государственного регулирования торговой деятельности в Российской Федерации"; "Об информации, информатизации и защите информации", "Об электронной цифровой подписи", "О бухгалтерском учете", Гражданский кодекс Российской Федерации, Арбитражный процессуальный кодекс Российской Федерации, Кодекс Российской Федерации об административных правонарушениях и иные.

Но, конечно же, отношения в сфере электронной коммерции являются очень специфическими и требуют отдельного и пошагового регулирования. В Европе, США и иных развитых и развивающихся странах данная отрасль регулируется специализированным законодательством. Так, например, в Китае, где обороты электронной коммерции набирают мощнейшие обороты, в 2018 г. принят закон "Об электронной коммерции".

В России основополагающим документом, регулирующим отношения в сфере электронной коммерции, является Постановление Правительства Российской Федерации от 31 декабря 2020 г. N 2463 "Об утверждении Правил продажи товаров по договору розничной купли-продажи, перечня товаров длительного пользования, на которые не распространяется требование потребителя о безвозмездном предоставлении ему товара, обладающего этими же основными потребительскими свойствами, на период ремонта или замены такого товара и перечня непродовольственных товаров надлежащего качества, не подлежащих обмену, а также о внесении изменений в некоторые акты Правительства Российской Федерации", хотя регулирование отношений субъектов, возникающих при реализации различных электронных процессов при оформлении и совершении сделок купли-продажи и поставки товаров, выполнении работ и оказании услуг и иных с ними связанных юридических действий с использованием информационно-коммуникационных технологий, образующих сферу электронной коммерции, требует отдельного контроля.

Современное общество стало свидетелем революции в области связи и транспорта, развития глобальных рынков, распада централизованно планируемой экономики и ее замены рыночной. Это привело к массовому расширению законной глобальной торговли товарами и услугами и исходя из принципа "преступность следует за возможностями" также способствовало перестроению, трансформации всей преступной деятельности под реалии развития нового типа современной цивилизации - "цифровой цивилизации".

Преступления в сфере электронной коммерции в большинстве случаев совершаются в сфере экономической деятельности как в открытом секторе экономики, так и в теневой его части. Огромная часть экономических преступлений в данной сфере, с учетом слабого гражданско-правового регулирования электронной коммерции, малоэффективных способов защиты электронных транзакций, малограмотности большинства участников данных сделок, остаются нераскрытыми, что несет существенный материальный ущерб и в определенной степени дестабилизирует развитие экономики страны в различных отраслях.

Согласно данным ГИАЦ МВД России за 2020 г. на территории РФ совершено 57 823 преступления в сфере экономической деятельности, в аналогичном периоде 2019 г. - 56 214, в 2018 г. - 53 366, в 2017 г. - 45 152. Преступлений экономической направленности за 2020 г. - 105 480, в аналогичном периоде 2019 г. - 104 927, 2018 г. - 109 463, 2016 г. - 105 087. Преступлений, совершенных с использованием информационно-телекоммуникационных технологий и в сфере компьютерной информации за 2020 г. - 510 396 (темп прироста составил 173%), за аналогичный период 2019 г. - 294 409 (темп прироста составил 168%), за 2018 г. - 174 674 (темп прироста составил 192%), за 2017 г. - 90 587 преступлений (диаграмма 1).

Динамика различных видов преступлений в России

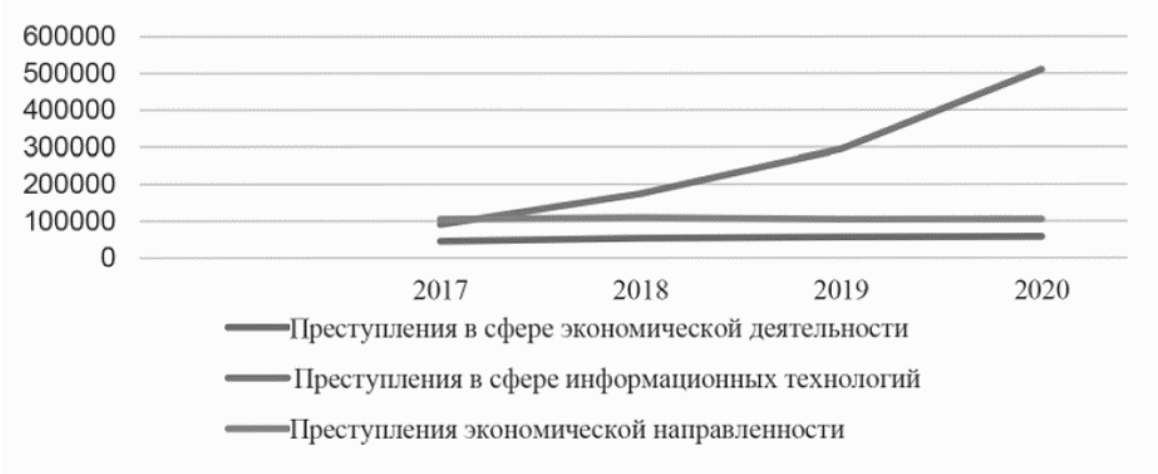

Диаграмма N 1

Электронная коммерция, несомненно, дает огромные возможности и преимущества своим субъектам, по сравнению с традиционными видами

экономических отношений, однако развитие и активное внедрение электронной коммерции порождает и определенные негативные последствия.

Плюсы электронной коммерции очевидны, в "цифровом" обществе люди хотят использовать все возможности и технологии прогресса на максимальном уровне. В свою очередь, преступность подстраивается под развитие общества, и наверняка большая часть населения, ведущая свой бизнес с использованием сети Интернет и информационно-телекоммуникационных технологий, уже сталкивалась с так называемой киберпреступностью.

Считается, что киберпреступность может полностью прервать торговую деятельность фирмы, и публичные компании теряют миллиарды фунтов стерлингов ежегодно в результате киберпреступности, они теряют активы, бизнес и репутацию.

Во многих зарубежных странах принимаются стратегии, положения и иные документы по кибербезопасности государств. В 2014 г. в России тоже была попытка принять свою стратегию кибербезопасности, которая провалилась, не была поддержана руководством спецслужб страны и вызвала больше вопросов. В настоящее время руководство страны опять задумывается о принятии основополагающего нормативно-правового акта для обеспечения кибербезопасности. Так, в ходе выступления на заседании ежегодной коллегии ФСБ в 2021 г. президент высказался: "России нужна выверенная стратегия по борьбе с киберпреступностью, основанная на прогнозировании ситуации, на учете потенциальных рисков для общества и государства".

Основными проблемами борьбы с киберпреступностью являются:

1) проблема получения так называемых "цифровых доказательств" из различных регионов по всему миру. Киберпреступность в большинстве случаев носит межгосударственный характер, следовательно, при необходимости получения определенных документов и сведений, проведения проверочных и процессуальных действий возникает проблема в различном законодательстве по одной и той же отрасли права, а иногда и проблема политических отношений между странами;

2) слабый уровень образованности и осведомленности населения большинства стран субъектов электронной коммерции. Одной из основополагающих составляющих борьбы с киберпреступностью является предупреждение или профилактика, которые, несомненно, связаны с определенным уровнем осведомленности населения о рисках и необходимом поведении при участии в электронной коммерции;

3) огромная ответственность большинства участников электронной коммерции, а именно юридических лиц, которые в силу обстоятельств становятся хранителями большого количества персональных данных, не обеспечивая надежный уровень защиты, ввиду корыстной заинтересованности в получении как можно большей прибыли. Сотрудники в данных организациях являются ключом к компьютерной и информационной

безопасности. Поэтому "первой линией" борьбы с преступностью в сфере электронной коммерции должна быть самооборона: для обеспечения эффективной защиты от угроз в электронной среде потребуются стратегии управления рисками со стороны частного сектора и частных лиц, хотя и при поддержке и содействии государства и правоохранительных органов;

4) огромное количество разнообразных устройств с различным уровнем защищенности, предоставляющих доступ в Интернет, а следовательно, и дающих возможность стать участником электронной коммерции;

5) несвоевременное и медленное реагирование со стороны государств и международных объединений при разработке и принятии правового регулирования как местного, так и международного уровня, с другой стороны - большое разнообразие и стремительное развитие киберпреступлений;

6) отсутствие в большинстве государств специалистов в области противодействия киберпреступности, специализированных отделов.

Конечно же, это не исчерпывающий перечень проблем в данной сфере, так как киберпреступления очень специфичны и по-разному могут трактоваться на территории различных государств.

Данное направление преступности представляет реальную угрозу экономическим отношениям в сфере электронной коммерции, так как, когда кто-то из субъектов электронной коммерции осознает, что у него имеется определенный риск потерять свои денежные средства, товар и иное, конечно, он задумается, а надо ли вступать в такие незащищенные экономические отношения, какие варианты еще существуют для проведения необходимой безопасной сделки. Крупные фирмы, задействованные в данной сфере, в попытках защитить свою репутацию и не потерять клиентов теряют свои денежные средства.

С момента зарождения электронной коммерции ставится вопрос о том, какого уровня правового регулирования она требует.

Основные субъекты электронной коммерции должны быть уверены в достаточной безопасности практически каждой сделки, при этом огромные преимущества данного вида коммерции - анонимность сети Интернет, скорость передачи данных, количество участников, быстрота оформления любых сделок, размах и отдаленность участников и иные - с одной стороны, организуют экономический подъем, с другой - вызывают опасения участников и определенные очевидные риски, такие как доступность внешнего проникновения, спам-атаки, возможный отказ в обслуживании, создание сайтов-дубликатов и иное. В большинстве случаев отсутствие личного визуального контакта между субъектами электронной коммерции, при наличии определенных уровней или рубежей защиты, создает определенные риски.

Так называемое онлайн-мошенничество становится нормой в современном обществе. Наверное, большинство жителей страны сталкивалось с мошенниками в данной сфере. При этом данный вид

преступлений в РФ набирает катастрофические обороты.

Согласно данным ГИАЦ МВД России, за 2020 г. на территории РФ совершено 25 820 мошенничеств с использованием электронных средств платежа, в аналогичном периоде 2019 г. - 18 133, в 2018 г. - 4 917, в 2017 г. - 228, в 2016 г. - 266. Мошенничеств в сфере компьютерной информации за 2020 г. - 761 преступление, в аналогичном периоде 2019 г. - 687, в 2018 г. - 970, в 2017 г. - 2 195, в 2016 г. - 4 329. Преступлений по ст. 273 УПК РФ "Создание, использование и распространение вредоносных компьютерных программ" за 2020 г. - 371, за 2019 г. - 455, за 2018 г. - 733, за 2017 г. - 802, за 2016 г. - 751 (диаграмма N 2).

Динамика различных видов преступлений
в сфере информационных технологий

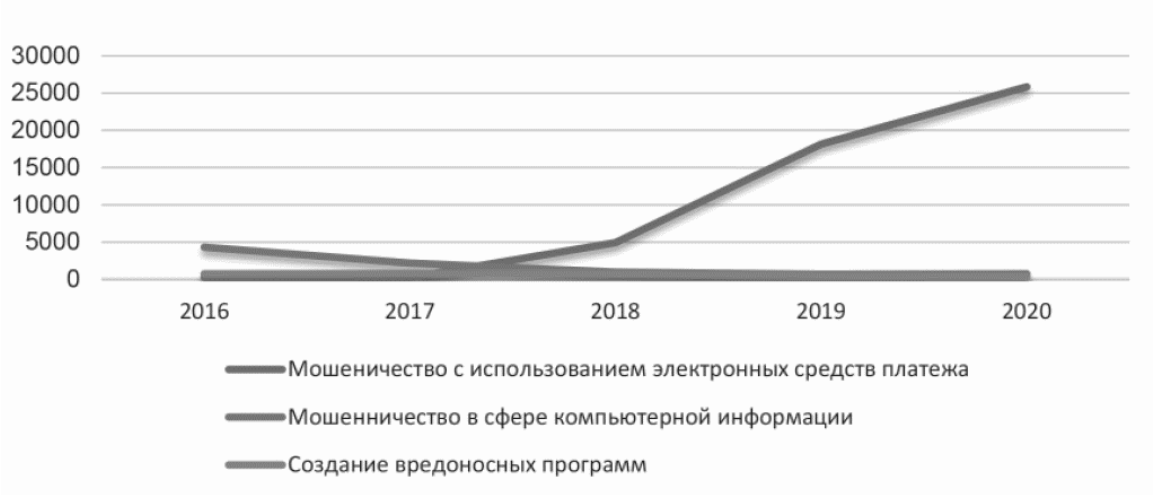

Диаграмма N 2

Самым распространенным видом мошенничества является так называемая кража персональных данных и дальнейшее использование данных с целью хищения денежных средств либо имущества. Мошенники пытаются завладеть данными о личности человека и в дальнейшем используют эти данные для совершения незаконных сделок и различных операций. При этом такими данными могут быть различные адреса электронной почты, номера сотовых телефонов, данные банковских карт, регистрационные данные с различных личных онлайн-кабинетов и страниц. Виды дальнейших незаконных операций и сделок разнообразны, при этом ущерб могут в дальнейшем нести не только сами клиенты, но и, например, кредитные, страховые организации, переживающие за свою репутацию. Кроме того, мошенники могут пользоваться данными и онлайн-организаций, фирм, осуществляющих свою деятельность с использованием сети Интернет. Яркими примерами, причиняющими огромный ущерб гражданам, является создание сайтов клонов крупных онлайн-компаний. То есть гражданин, заходя на такой сайт и произведя определенные действия для идентификации

компании, не понимает, что фактически находится в поле зрения мошенников, готовых совершить незаконную операцию от имени реальной компании. Такое мошенничество может иметь огромные масштабы и дестабилизировать экономические отношения в данной сфере.

Из вышеуказанных схем могут вытекать следующие виды кибермошенничества, приносящие огромные убытки компаниям. Так, мошенники, используя украденные персональные данные, осуществляют онлайн-заказ, который по истечении определенного допустимого времени отменяют, сообщая в компанию, что их персональные данные украдены и заказ ими не производился. То есть в данном случае компания может понести ущерб в двойном размере, потеряв товар и сделав возврат.

Следующим набирающим обороты видом мошенничества является "кража" или несанкционированный взлом учетных записей и аккаунтов в различных социальных сетях, интернет-магазинах, онлайн-компаниях. Такой украденный аккаунт может использоваться неоднократно для совершения незаконных сделок до того момента, пока не выяснится истинный владелец аккаунта.

Все указанные виды преступлений совершаются с использованием сети Интернет, в каких-то случаях с использованием банковских карт, в иных - с использованием электронных средств платежа.

Согласно данным ГИАЦ МВД России за январь - май 2021 г. зарегистрировано преступлений, совершенных с использованием сети Интернет, - 151 593 (рост + 48,4%), в том числе большинство преступлений на территории Центрального федерального округа (далее ЦФО) - 35 353, Приволжского федерального округа (далее - ПФО) - 34 760; преступлений, совершенных с использованием или применением расчетных (пластиковых карт) - 75 387 (рост 18,4%), в том числе большинство преступлений на территории ЦФО - 19 262, ПФО - 14 589; зарегистрировано мошенничеств - 93 423 (рост + 31,3%), в том числе большинство преступлений на территории ЦФО - 26 596, ПФО - 18 106; зарегистрировано преступлений по ст. 159.3 УК РФ "Мошенничество с использованием электронных средств платежа" - 4 510 (рост 58,3%), в том числе большинство преступлений на территории ПФО - 937, ЦФО - 704. Аналогичные тенденции наблюдаются в ходе анализа статистики преступлений за 2019 г. и 2020 г. (Диаграмма N 3).

Динамика отдельных видов преступлений в России

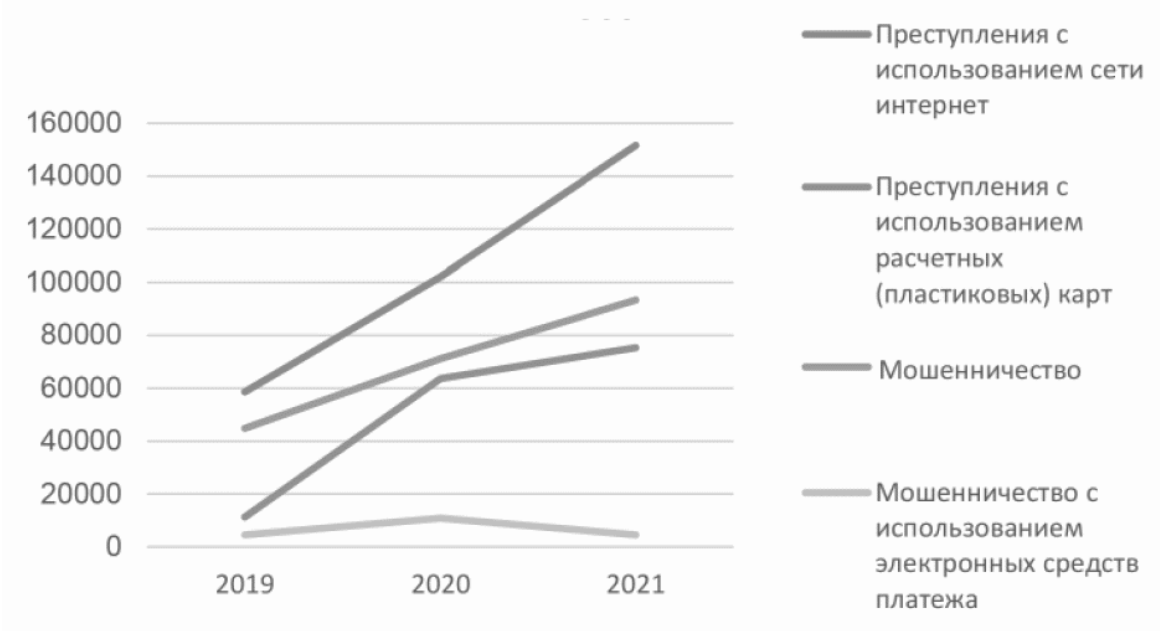

Диаграмма N 3

В предупреждении, выявлении и раскрытии преступлений в сфере информационных технологий основополагающая роль отводится сотрудникам органов внутренних дел (далее - ОВД).

Так, согласно данным ГИАЦ МВД России, за январь - май 2021 г. выявлено преступлений в сфере информационных технологий 226 962 (рост + 25,7%), из них сотрудниками ОВД - 223 029, ФСБ - 1 384, прокуратуры - 1 267. За аналогичный период 2020 г. выявлено преступлений в сфере информационных технологий 180 498 (рост + 85,1%), из них сотрудниками ОВД - 177 915, ФСБ - 1 041, прокуратуры - 519. За аналогичный период 2019 г. выявлено преступлений в сфере информационных технологий 97 524 (рост + 52,5%), из них сотрудниками ОВД - 95 735, ФСБ - 768, прокуратуры - 261.

Анализируя статистические данные, можно сказать, что сотрудники ОВД являются основными субъектами борьбы с так называемыми киберпреступлениями. Соответственно развитие и совершенствование методики, тактики, способов и иных средств именно через правоохранительные органы, в лице специализированных сотрудников ОВД, является основополагающим фактором в предупреждении киберпреступности.

Подписано в печать
25.08.2021

Обязан ли банк вернуть деньги при списании их с банковской карты или через интернет-банк без согласия клиента? // Азбука права: электронный журнал. – 2022.

ОБЯЗАН ЛИ БАНК ВЕРНУТЬ ДЕНЬГИ ПРИ СПИСАНИИ ИХ С БАНКОВСКОЙ КАРТЫ ИЛИ ЧЕРЕЗ ИНТЕРНЕТ-БАНК БЕЗ СОГЛАСИЯ КЛИЕНТА?

> Банк обязан вернуть деньги, списанные с карты клиента без его согласия, если он не проинформировал клиента о списании. Если клиент был проинформирован и вовремя представил уведомление о несогласии, банк обязан возместить суммы, списанные после представления такого уведомления, а в отдельных случаях - списанные до его представления.

1. Обязанности банка и клиента

Банковские карты и интернет-банк относятся к электронным средствам платежа (ЭСП).

Законодательством для банка и клиента установлен ряд обязанностей, от соблюдения или несоблюдения которых зависит, будут ли клиенту возвращены суммы, похищенные с его счета, или нет (п. 19 ст. 3, ст. 9 Закона от 27.06.2011 N 161-ФЗ).

Основная обязанность банка - информировать клиента о каждой операции, совершенной с использованием ЭСП, путем направления клиенту уведомления (далее - уведомление об операциях) в порядке, установленном договором с клиентом (ч. 4 ст. 9 Закона N 161-ФЗ).

При выявлении банком операций, соответствующих признакам перевода денежных средств без согласия клиента, банк должен приостановить использование клиентом банковской карты и предоставить ему соответствующую информацию. Указанные признаки устанавливаются Банком России и размещаются на его официальном сайте (ч. 5.1, 5.2 ст. 8, ч. 9.1 ст. 9 Закона N 161-ФЗ; Признаки, утв. Приказом Банка России от 27.09.2018 N ОД-2525).

При этом банк обязан в день приостановления использования клиентом банковской карты предоставить ему соответствующую информацию (уведомление) с указанием причины приостановления. Такие уведомления направляются в порядке, установленном договором (ч. 9.2 ст. 9 Закона N 161-ФЗ).

Способы направления уведомлений об операциях, используемые банками, различны - это могут быть и СМС-уведомления, и рассылка по электронной почте, и информирование в интернет-банке. При этом хотя бы один из способов информирования должен быть бесплатным для клиента.

Основная обязанность клиента - уведомить банк в случае утраты ЭСП и (или) его использования без согласия клиента. При этом клиент обязан направить в банк указанное уведомление (далее - уведомление о несогласии) незамедлительно после обнаружения факта утраты ЭСП и (или) его использования без согласия клиента, но не позднее дня, следующего за днем получения от банка уведомления об операциях (ч. 11 ст. 9 Закона N 161-ФЗ).

Способ информирования устанавливается договором. На практике чаще всего используется звонок в контакт-центр банка с последующим представлением уведомления о несогласии в письменной форме.

День получения от банка уведомления об операциях - это не день, когда вы фактически его прочитали, а день, определенный в качестве такового договором. В договоре обычно указывают, что вы считаетесь получившим уведомление в день его направления банком установленным договором способом, например по указанному вами номеру мобильного телефона. Если вы вовремя не прочитали уведомление, это ваша вина.

2. Операции, суммы которых банк обязан возместить клиенту

Банк обязан возместить вам суммы несанкционированных операций, совершенных с ЭСП, в следующих случаях (ч. 12, 13, 15 ст. 9 Закона N 161-ФЗ):

1) если банк не направлял вам уведомления о совершенных операциях, он обязан возместить вам суммы операций, которые были совершены без вашего согласия (далее также - несанкционированные операции) и о которых вы не были банком проинформированы. Соответственно, в данном случае срок, установленный для направления вами уведомления о несогласии, не применяется;

2) если банк надлежащим образом направлял вам уведомления о совершенных операциях и вы вовремя представили в банк уведомление о несогласии, банк обязан возместить вам суммы несанкционированных операций, совершенных после представления вами уведомления о несогласии;

3) если банк надлежащим образом направлял вам уведомления о совершенных операциях и вы вовремя представили в банк уведомление о несогласии, банк обязан возместить вам суммы несанкционированных операций, совершенных до момента представления вами указанного уведомления о несогласии, но только в том случае, если не сможет доказать,

что вы сами нарушили порядок использования ЭСП, из-за чего и произошли несанкционированные операции.

3. Операции, суммы которых банк не обязан возмещать клиенту

Банк не обязан возмещать вам суммы несанкционированных операций в следующих случаях (ч. 14, 15 ст. 9 Закона N 161-ФЗ):

1) если банк надлежащим образом направлял вам уведомления о совершенных операциях, но вы не представили в банк уведомление о несогласии в установленный срок;

2) если банк надлежащим образом направлял вам уведомления о совершенных операциях и вы вовремя представили в банк уведомление о несогласии, но при этом банк смог доказать, что причиной возникновения несанкционированных операций, совершенных до момента представления вами в банк уведомления о несогласии, стало нарушение вами порядка использования ЭСП. Таким нарушением может быть, в частности:

- сообщение вами третьим лицам реквизитов вашей банковской карты, ПИН-кода, логина, пароля и (или) средств подтверждения операций в интернет-банке, а также небрежное хранение карты и информации о ПИН-коде (логине и т.п.), в результате чего к ним получили доступ третьи лица;

- оплата покупки в интернет-магазине с компьютера, зараженного вирусом, передающим мошенникам реквизиты банковских карт.

Пропуск установленного срока уведомления о несогласии не означает невозможность оспорить операцию, с которой вы не согласны, поскольку мошеннические операции могут совершаться при отсутствии вашей вины (например, если реквизиты карты стали известны мошенникам в результате установки ими скимминговых устройств на банкомат). Поэтому обращайтесь в банк с претензией всегда, если вы обнаружили операцию, с которой не согласны.

> **Обратите внимание!** С 01.01.2021 по общему правилу клиент банка вправе заявить свои требования к нему в судебном порядке только после обращения к финансовому уполномоченному, что, в свою очередь, возможно после направления соответствующего заявления в банк (ч. 1, 2 ст. 15, ч. 1 ст. 16, ч. 2 ст. 25, п. 5 ч. 1 ст. 28, ч. 2 ст. 29, ч. 3 ст. 32 Закона от 04.06.2018 N 123-ФЗ).

Как не стать жертвой мошенников : памятка от соцстраха // Главная книга. – 2019. – № 18. – с. 75.

КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ: ПАМЯТКА ОТ СОЦСТРАХА

ФСС сообщил, что в последнее время участились случаи мошенничества с использованием Интернета и телефона. Злоумышленники обещают некие социальные выплаты и пытаются получить доступ к банковским счетам и персональным данным граждан. В связи с этим важно помнить, что официальное название соцстраха - Фонд социального страхования РФ (ФСС РФ). В то время как мошенники иногда используют название "Федеральная служба социального страхования". Такого ведомства нет.

Официальные сайты ФСС имеют следующую структуру:

- http://fss.ru - центральный аппарат Фонда;

- https://r03.fss.ru - региональные отделения Фонда. Цифра перед fss.ru - это код региона отделения (например, r03 - Республика Бурятия, r50 - Московская область и т.д.).

Сайты с иной структурой адреса не являются официальными веб-страницами соцстраха и могут содержать недостоверную информацию.

Все электронные адреса сотрудников ФСС выглядят так: имя сотрудника + @ + fss.ru (например, m.morozov@fss.ru). Если вам на почту пришло письмо "от ФСС", но с адреса иной структуры, это однозначно мошенники.

Фонд не пользуется телефонными номерами типа 8 (800) XXX-XX-XX. Сотрудники ФСС никогда не попросят в телефонном разговоре продиктовать срок действия вашей банковской карты, контрольный код и/или СМС-код подтверждения.

Если вам поступило сообщение (по СМС или по электронной почте) якобы от ФСС с текстом вроде "Узнайте свой размер компенсации от государства", не перезванивайте по указанным номерам и тем более не сообщайте свои личные данные (реквизиты паспорта, банковской карты и пр.).

Подписано в печать

06.09.2019

ББК 67.408.1

Безопасный Интернет : дайджест актуальных статей из СПС «КонсультантПлюс» / Центральная библиотека Очёрского городского округа, отдел электронных ресурсов и информационных технологий ; составитель Е. О. Шадская. – Очёр, 2022 г. – 40 с.

Пособие объединяет актуальные статьи по теме обеспечения интернет-безопасности, описания и предотвращения преступлений, совершаемых с использованием информационно-коммуникационных технологий за 2019-2022 годы. Использованы материалы справочно-правовой системы «КонсультантПлюс» (ООО «ТелекомПлюс»). Для широкого круга читателей.