УДК 340

Барашева Елена Викторовна
кандидат экономических наук, доцент,
доцент кафедры государственно-правовых дисциплин,
Российский государственный университет правосудия
barahevaev@bk.ru
Степаненко Диана Аркадьевна
доктор юридических наук, профессор,
профессор кафедры криминалистики,
судебных экспертиз и юридической психологии,
Байкальский государственный университет
mail@esbrsuj.ru
Eleva V. Barasheva
PhD in Economics, Associate Professor,
Associate Professor, Department of State Law Disciplines,
Russian State University of Justice
barahevaev@bk.ru
Diana A. Stepanenko
Doctor of Law, Professor,
Professor of Criminology, Forensic Examinations and Legal psychology,
Baikal State University
diana-stepanenko@mail.ru

Историко-правовые аспекты киберпреступности в банковской сфере

Historical and legal aspects of cybercrime in the banking sector

Аннотация. *Информационные технологии развиваются с огромной скоростью, позволяя человечеству сделать прорыв во многих научных сферах. В настоящее время можно с уверенностью отметить все более растущую значимость информационных технологий. В статье рассматриваются историко-правовые аспекты киберпреступности в банковской сфере, определены этапы развития данных преступлений и их особенности, определены факторы, стимулирующие развитие данных преступлений и их подавление.*

Ключевые слова: *преступление, технологии, информация, государство, экономика.*

Annotation. *Information technology is developing at a tremendous speed, allowing humanity to make a breakthrough in many scientific fields. Currently, it is safe to note the increasingly growing importance of information technology.The article examines the historical and legal aspects of cybercrime in the banking sector, identifies the stages of development of these crimes and their features, identifies the factors that stimulate the development of these crimes and their suppression.*

Keywords: *crime, technology, information, state, economy**.***

Информационные технологии развиваются с огромной скоростью, позволяя человечеству сделать прорыв во многих научных сферах. В настоящее время можно с уверенностью отметить все более растущую значимость информационных технологий, что подтверждается принятием на государственном уровне Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы[1].

Как любое явление, информационные технологии имеют как позитивные, так и негативные стороны. Однако их польза и удобство столь велики, что общество уже не сможет отказаться от информационных технологий, поэтому мы должны учитывать, прогнозировать и предупреждать все негативные последствия их использования.

Вместе с развитием информационных технологий появилось новое явление известное как «киберпреступность». Киберпреступления – это преступная деятельность, целью которой является незаконное использование компьютера и сети Интернет.

Банковская сфера всегда была одним из наиболее желанных для киберпреступников (хакеров) пространством для совершения преступлений, в основном, посредством проведения хакерских атак. Так, начиная с 2016 года, в Российской Федерации наблюдалось увеличение количества хакерских атак на кредитно-финансовые организации. Наиболее популярным инструментом осуществления хакерских атак было использование Metasploit Framework, Cobalt Strike, Empire, разработанных с использованием техник, которые затрудняли их обнаружение в системе. Главное преимущество перечисленных инструментов состоит в том, что они представляют собой простой в использовании механизм удаленного управления «зараженными» компьютерами, что не требует от злоумышленника особых технических знаний.

На X-ом Уральском форуме «Информационная безопасность финансовой сферы» заместитель председателя Центрального Банка Российской Федерации Дмитрий Скобелкин отметил, что в 2017 году общие потери кредитных организаций России от хакерских атак с использованием Cobalt Strike превысили 1 млрд рублей[2].

Действительно, Cobalt Strike в 2016-2017 гг. был наиболее популярным в использовании инструментом. Так, злоумышленники, в основном, осуществляли атаки на банкоматы и банковские карты, используя следующую типовую схему:

1. Посредством массовой рассылки вредоносных электронных писем на адреса кредитных (финансовых) организаций запускается вредоносное вложение на компьютере получателя, после чего хакер получает доступ к зараженному компьютеру.

2. Хакер устанавливает доступ к контроллеру домена сети для получения паролей администраторов, после чего проводит поиск интересующих серверов - наибольший интерес в данном случае для злоумышленника представляет такой

сервер или компьютер, с которого предоставляется доступ в подсеть, где находятся банкоматы или сегмент процессинга банковских карт.

3. После получения полного доступа к банкоматам, к преступной деятельности привлекаются соучастники, главной задачей которой является обеспечение их присутствия около банкоматов для непосредственного вывода средств в установленное хакреами время.

4. Финалом всего процесса служит удаление программного обеспечения с банкоматов.

В 2016-2017 гг. в качестве основных методов борьбы с подобными атаками использовались, прежде всего, организационные методы, представляющие собой повышение квалификации в области информационной безопасности сотрудников, как правоохранительных органов, так и непосредственно сотрудников финансовых (кредитных) организаций. Наиболее востребованными техническими методами выступали:

1. Создание и систематическое обновление антивирусных баз, с помощью которых блокировались вредоносные письма, тем самым останавливая преступную схему на начальном этапе.

2. Систематическое обновление сигнатур для систем IDS/IPS для устранения вредоносного (подозрительного) трафика.

В случаях, когда атаку предупредить не удалось, главной задачей, стоящей перед компетентными сотрудниками, являлось закрытие доступа к сети Интернет всех элементов Beacon, что создаст препятствие для коммуникации злоумышленника с сервером.

Стоит отметить, что в 2016-2017 гг. основные методы борьбы с киберпреступлениями сводились к детектированию сигналов внешних сетевых соединений по адресам командных центров и поиску подозрительных сетевых соединений с последующей очисткой узлов от компонентов вредоносных программ.

Конец же 2019 – 2020 года ознаменовался ростом кибрепреступности во всех сферах, в том числе, в банковской, что определено пандемией COVID-19. Так, большая часть организаций (включая кредитно-финансовые) перешла на работу в дистанционном режиме, что, в основном, было продиктовано стремлением бесперебойно обеспечивать основные потребности граждан. Однако такой переход перестроил и фокус внимания злоумышленников.

Киберпеступность 2019-2021 гг. имеет яркое отличие от киберпеступности 2016-2017 гг. Так, если финансовые организации были отчасти готовы к борьбе и прогнозированию кибер-атак, что во многом продиктовано многолетним опытом работы в этой области, то в 2019-2021 гг. с кибер-атаками столкнулись именно клиенты финансовых организаций – как физические, так и юридические лица. Стоить отметить, что преступные схемы с использованием Metasploit Framework, Cobalt Strike, Empire, которые привлекали к себе особое внимание в 2016-2017 гг., стали не такими востребованными, а в последствие и вовсе перестали существовать.

В 2019-2021 гг. злоумышленники, в основном, использовали методы социальной инженерии в отношении клиентов финансовых организаций, а именно телефонное мошенничество.

Как таковое, телефонное мошенничество существует уже довольно длительное время, поэтому во времена пандемии перед злоумышленниками стояла важная задача – преодолеть порог недоверия клиентов финансовых организаций. Как следствие на черном рынке стремительно увеличился спрос на персональные данные клиентов.

Современные киберпреступления в банковской сфере в настоящее время, в основном, реализуются с использованием следующей схемы - злоумышленник, получив полную (достаточную) для преодоления барьера недоверия информацию, звонит конкретному клиенту финансовой организации, представляясь при этом сотрудником определенного банка, и под разными предлогами, используя психологические манипуляции (уловки), выясняет у потенциальной жертвы все необходимые данные: номер карты, CVC-код, срок действия карты и т.д.

Однако нельзя с полной гарантией говорить, что это - единственная схема, которую используют злоумышленники. В настоящее время происходит непрерывный процесс совершенствования схем совершения киберпреступлений (в основном краж), поэтому, для разрешения данной проблемы, которую можно без преувеличения назвать глобальной, важно объединить, в первую очередь, государства. Эффективно объединив международные системы безопасности посредством тесного сотрудничества правоохранительных органов (спецслужб) государств, можно добиться построения относительно крепкого фундамента для противодействия киберпреступности.

Во-вторых, важнейшим способом решения проблемы киберпреступности в экономической сфере является необходимость взаимодействия государства и частного сектора экономики. В данном случае, способом решения проблемы может выступать разработка стратегии и программного обеспечения в отношении кибербезопасности на уровне национальной экономики, а также - системное улучшение национального законодательства.

В силу отсутствия у клиентов финансовых организаций (преимущественно, физических лиц) необходимого опыта для противодействия кибер-аткам, основная задача в борьбе по предупреждению киберпреступности, особенно, в годы, набирающей популярность цифровизации, лежит на правоохранительных органах и структурных подразделениях финансовых организаций, осуществляющих информационную безопасность.

Центральным банком Российской Федерации в 2019 году было разработано положение[1], которое устанавливает обязательное требование к

[1] Положение Банка России от 17 апреля 2019 г. N 683-П "Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента"

кредитным организациям. Так, кредитные организации обязаны обеспечить защиту информационной инфраструктуры, используемой для обработки, передачи и хранения защищаемой информации в целях осуществления банковских операций.

Финансовые организации для осуществления финансовых операций в сети Интернет обязаны использовать только то программное обеспечение, которое сертифицировано в системе сертификации Федеральной службы по техническому и экспертному контролю на соответствие требованиям безопасности информации. Стоит так же отметить, что кредитные финансовые организации должны проводить ежегодные плановые тестирования на возможность проникновения к базам данных и анализировать все уязвимые места объектов информационной инфраструктуры.

Однако, на наш взгляд, наряду с техническими методами прогнозирования и борьбы с кибератаками, нужно использовать социально-психологические методы. Так, необходимо обеспечить стабильное и доступное для каждого лица информирование о способах защиты от киберпреступлений. Так, регулярное транслирование в сети Интернет и в средствах массовой информации красочных, коротких и доступных к пониманию видео-роликов позволило бы в разы сократить количество кибер-атак в отношении клиентов финансовых организаций.

Информационные технологии совершенствуются ежедневно, как следствие, меняются виды и способы совершения преступлений в сети Интернет, поэтому крайне важно создать специальную нормативно-правовую, техническую и образовательную базу, которая бы позволила оперативно реагировать на появление новых схем киберпреступлений.

Литература

1. Указ Президента Российской Федерации от 09.05.2017 г. № 203 О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы http://pravo.gov.ru;

2. X Уральский форум — Дмитрий Скобелкин (Банк России): Ключевой доклад https://youtu.be/yvFiwpu8yvM;

3. Положение Банка России от 17 апреля 2019 г. # 683-П "Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента";

4. Маныч, Е. Г. Кража финансовых данных или данных банковских карт - один из видов киберпреступления / Е. Г. Маныч // Цифровые технологии в борьбе с преступностью: проблемы, состояние, тенденции : Сборник материалов I Всероссийской научно-практической конференции, Москва, 27 января 2021 года. – Москва: Федеральное государственное казенное образовательное учреждение высшего образования "Университет прокуратуры Российской Федерации", 2021. – С. 156-158. – EDN QAGKSC.

Literature

1. Decree of the President of the Russian Federation No. 203 of 09.05.2017 On the Strategy for the Development of the Information Society in the Russian Federation for 2017-2030 http://pravo.gov.ru;

2. X Ural Forum — Dmitry Skobelkin (Bank of Russia): Key Report https://youtu.be/yvFiwpu8yvM;

3. Regulation of the Bank of Russia dated April 17, 2019 # 683-P "On the establishment of mandatory requirements for credit institutions to ensure the protection of information during banking activities in order to counteract the implementation of money transfers without the consent of the client";

4. Manych, E. G. Theft of financial data or bank card data is one of the types of cybercrime / E. G. Manych // Digital technologies in the fight against crime: problems, state, trends : Collection of materials of the I All-Russian Scientific and Practical Conference, Moscow, January 27, 2021. – Moscow: Federal State State Educational Institution of Higher Education "University of the Prosecutor's Office of the Russian Federation