УДК 343.9

Степаненко Диана Аркадьевна
доктор юридических наук, профессор, профессор
кафедры криминалистики, судебных экспертиз и
юридической психологии, Институт юстиции
Байкальского государственного университета, г. Иркутск
diana-stepanenko@mail.ru
Diana A. Stepanenko
Doctor of Law, Professor, Professor of the Department of Criminalistics,
Forensic Examinations and Legal Psychology
of the Institute of Justice of Baikal State University, Irkutsk
diana-stepanenko@mail.ru

Криминологические аспекты выявления и предупреждения кибератак в банковской сфере

Criminological aspects of detecting and preventing cyber attacks in the banking sector

Аннотация. *Научная статья посвящена проблеме возникновения кибератак в банковской сфере, их своевременного выявления и предупреждения. Данная проблема достаточно актуальна, поскольку в условиях цифровизации общества хакеры разрабатывают различные способы хищения денежных средств в значительных объемах. Также, в результате исследования были представлены возможные инструменты, позволяющие минимизировать ущерб, причиненный кибератаками, путем быстрого реагирования на их возникновение.*

Ключевые слова: *кибератака, преступление, хищение, хакерство, банковская деятельность, банковская операция, денежные средства.*

Annotation. *The scientific article is devoted to the problem of the emergence of cyberattacks in the banking sector, their timely detection and prevention. This problem is quite relevant, because in the conditions of digitalization of society, hackers are developing various ways to steal money in significant amounts. Also, as a result of the study, possible tools were presented to minimize the damage caused by cyberattacks by quickly responding to their occurrence.*

Keywords: *cyberattack, crime, theft, hacking, banking, banking operation, cash.*

На сегодняшний день, современное общество отличается высоким уровнем мобильности, доступности информации, качеством и удобством совершения тех или иных действий путем использования инновационных

технологий, а также через Интернет-пространство. Так, действия в области банковской деятельности не стало исключением. Практически все организации, в том числе и банковские, осуществляют свою деятельность через компьютерные технологии, ведь они значительно снижают трудовую нагрузку сотрудникам таких организаций, повышают уровень оперативности совершения операций, а также в разы увеличивают количество выполненных действий. Однако, использование таких технологий не способно обеспечить качество сохранности и защиты данных, содержащихся на компьютерных носителях.

Итак, необходимо разобраться в понятии «банковская деятельность». На первый взгляд, кажется очевидным, что банковская деятельность представляет собой деятельность банков, однако, все не так просто. Для того, чтобы деятельность считалась банковской, она обязана соответствовать некоторым требованиям, а именно:

1. Специальная правоспособность организаций. Такая правоспособность выражается в лицензировании деятельности, то есть наличии специального разрешения на осуществление того или иного вида деятельности, в данном случае, банковской. Так, Банк России кроме защиты и обеспечения устойчивости рубля, наделяет специальной правоспособностью кредитные организации, исходя из положений, закрепленных в ст. 4 Федерального закона от 10.07.2002 № 86-ФЗ (ред. от 30.12.2021) «О Центральном банке Российской Федерации (Банке России)» (далее – ФЗ «О Банке России») [1].

2. Осуществление специальным субъектом. Основываясь на вышеперечисленном требовании, следует сделать вывод о том, что не каждый способен совершать банковские операции и сделки. Кроме этого, организации, осуществляющие банковскую деятельность, тесно взаимосвязаны между собой и составляют банковскую систему России. Так, к элементам банковской системы Российской Федерации, согласно ч. 1 ст. 2 Федерального закона от 02.12.1990 № 395-1 (ред. от 14.07.2022) «О банках и банковской деятельности» (далее – ФЗ «О банках и банковской деятельности»), относятся Банк России, кредитные организации, а также - представительства иностранных банков [2].

3. Особое правовое регулирование. Данное требование акцентирует внимание на том, что банковская деятельность четко регламентируется нормами права. Так, согласно ч. 2 ст. 2 ФЗ «О банках и банковской деятельности», правовое регулирование банковской деятельности осуществляется Конституцией Российской Федерации, настоящим Федеральным законом, Федеральный законом «О Центральном банке Российской Федерации (Банке России)», другими федеральными законами, нормативными актами Банка России [2]. К тому же, существующая норма

свидетельствует о том, что банковская деятельность регулируется исключительно на федеральном уровне.

Таким образом, под банковской деятельностью необходимо понимать осуществление банковских операций исключительно кредитными организациями и Банком России [3].

Так, учитывая значимость банковской деятельности, а также слабость защиты банковских данных, начиная с 2016 года, в Российской Федерации наблюдалось увеличение количества хакерских атак на кредитно-финансовые организации [4]. Не удивительно, что большинство кибератак направлены именно на данную сферу, ведь одним из частых мотивов преступников является незаконное обогащение. Кибератаки, в свою очередь, это незаконные действия, выраженные в проникновении в информационную систему для получения, искажения или использования конкретных данных в корыстных целях.

Для создания возможных методов эффективной борьбы с данными преступлениями, необходимо начать с конкретных проблем, препятствующих их выявлению:

1. Несовершенство отечественного законодательства. Так, в действующем уголовном законодательстве отсутствует четкое определение киберпреступления. Кроме этого, наряду с такими преступлениями, как не установлена уголовная ответственность за фишинг. Фишинг – это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей (логинам и паролям) [5]. И для решения данной проблемы необходимо детально регламентировать такой вид преступной деятельности, который с каждым годом только набирает свои обороты.

2. Низкий уровень технического оснащения государственных структур. [6, с. 38]. Не трудно предположить, что данная проблема напрямую связана с огромными материальными затратами государства на оснащение государственных структур новейшими технологиями, однако одного наличия таких средств недостаточно. Для эффективного применения таких технологий необходимо обладать высоким уровнем компьютерной грамотности и осведомленности о современных кибератаках. К сожалению, такими качествам обладают далеко не все соответствующие государственные служащих.

3. Субъективные факторы со стороны клиентов банков. Большинство граждан, как и государственные служащие тоже отличаются некой неграмотностью и неосведомленностью о возможных киберугрозах. Кроме этого, многие легкомысленно относятся к выбору логинов и паролей для своих учетных записей в личных кабинетах клиентов банков, а также быстро ведутся на многие мошеннические уловки, а именно, звонки, спам-

сообщения, выдавая свои личные данные посторонним, ставя свое имущество под угрозу.

Подводя итог вышесказанному, следует отметить, что для повышения эффективности выявление кибератак в банковской сфере необходимо регламентировать понятие «киберпреступность», а также классифицировать виды таких преступлений. Далее, необходимо повышать качество подготовки и обучения сотрудников правоохранительных и иных органов, а также, проводить все возможные мероприятия по повышению уровня знаний среди граждан-клиентов о киберпреступлениях и защите своих денежных средств.

Так, исходя из вышеперечисленных проблем выявления кибератак в банковской деятельности, можно определить ряд мер по предотвращению данных противоправных действий:

1. Совершенствование деятельности правоохранительных органов путем взаимодействия с иными ведомствами и организациями. Так, государственные органы для эффективной борьбы с кибератаками в банковской деятельности обязаны сотрудничать как с самими кредитными организациями, так и со специализированными организациями в области IT-технологий.

2. Постоянное обновление систем защиты и безопасности кредитных организаций. Ведь взлом различным информационных систем требует времени и, возможно, постоянного подбора кодов и шифров, а постоянное обновление системы не позволит хакерам добиться желаемого. Кроме этого, для минимизации совершения каких-либо ошибок, сотрудники всех кредитных организаций обязаны производить банковские операции в соответствии с конкретными правилами.

3. Проверка сотрудников банковских организаций, во избежание распространения конфиденциальной информации [7]. Данная мера способна избежать преступлений среди сотрудников кредитных организаций, поскольку они обладают всех необходимой информацией о системном обеспечении соответствующей организации.

Следует отметить, что кибератаки в банковской деятельности, помимо посягательства на счета населения, негативно влияют на финансовую стабильность государства в целом. Так, по оценкам Международного валютного фонда, потери кредитных организаций от кибератак, в среднем, могут составлять несколько сот миллиардов долларов в год, что уменьшает прибыль банков и потенциально угрожает финансовой стабильности.

Таким образом, можно сделать вывод о том, что кибератаки являются достаточно острой проблемой современного общества. Помимо нарушения прав и законных интересов граждан, киберпреступления также негативно сказываются на деятельности кредитных организаций и государства, в целом, путем увеличения затрат на предотвращение и ликвидацию последствий противоправных действий злоумышленников.

Литература:

1. О Центральном банке Российской Федерации (Банке России): Федеральный закон от 10.07.2002 N 86-ФЗ (ред. от 30.12.2021) (с изм. и доп., вступ. в силу с 29.05.2022) // СЗ РФ. — 15.07.2002. — № 28. — Ст. 2790.

2. О банках и банковской деятельности: Федеральный закон от 02.12.1990 № 395-1 (ред. от 14.07.2022) // СЗ РФ. — 05.02.1996. — № 6. — Ст. 492.

3. Барашева Е. В., Степаненко Д. А. Историко-правовые аспекты киберпреступности в банковской сфере / Е. В. Барашева, Д. А. Степаненко // Гуманитарные, социально-экономические и общественные науки. — Иркутск, 2022. — № 6. — С. 1-6.

4. Жмуров Д.В. Кибержертва: особенности классификации/ Жмуров Д.В. Всероссийский криминологический журнал. — Иркутск, 2022. — № 4.

5. Репецкая А.Л., Петрякова Л.А. Виктимологическая характеристика мошенничеств в банковской сфере (по материалам Сибирского федерального округа) / Репецкая А.Л., Петрякова Л.А./ Всероссийский криминологический журнал. — Иркутск, 2022. — № 4.

6. Сарычев А. В., Архипцев И. Н. Современное состояние раскрытия и расследования преступлений, совершаемых с использованием информационных технологий / А. В. Сарычев, И. Н. Архипцев // Проблемы правоохранительной деятельности. — Белгород, 2020. — С. 36-40.

7. Хисамова З.И., Бегишев И.Р. Цифровая преступность в условиях пандемии: основные тренды/ 8. Хисамова З.И., Бегишев И.Р /Всероссийский криминологический журнал. — Иркутск, 2022. — № 2.

Bibliography:

1. About the Central Bank of the Russian Federation (Bank of Russia): Federal Law No. 86-FZ of 10.07.2002 (as amended on 30.12.2021) (with amendments and additions, intro. in force from 29.05.2022) // SZ RF. — 15.07.2002. — No. 28. — Article 2790.

2. On banks and banking activities: Federal Law No. 395-1 of 02.12.1990 (ed. of 14.07.2022) // SZ RF. — 05.02.1996. — No. 6. — Article 492.3.

3. Barasheva E. V., Stepanenko D. A. Historical and legal aspects of cybercrime in the banking sector / E. V. Barasheva, D. A. Stepanenko // Humanities, socio-economic and social sciences. — Irkutsk, 2022. — No. 6. — pp. 1-6.

4. Zhmurov D.V. Cyberhertva: features of classification / Zhmurov D.V. All-Russian Journal of Criminology. — Irkutsk, 2022. — No. 4.

5. Repetskaya A.L., Petryakova L.A. Victimological characteristics of fraud in the banking sector (based on the materials of the Siberian Federal District) / Repetskaya A.L., Petryakova L.A./ All-Russian Journal of Criminology. — Irkutsk, 2022. — No. 4.

6. Sarychev A.V., Arkhiptsev I. N. The current state of disclosure and investigation of crimes committed using information technologies / A.V. Sarychev, I. N. Arkhiptsev // Problems of law enforcement. — Belgorod, 2020. — pp. 36-40.

7. Hisamova Z.I., Begishev I.R. Digital crime in a pandemic: the main trends/ 8. Hisamova Z.I., Begishev I.R. /All-Russian Journal of Criminology. — Irkutsk, 2022. — No. 2.