DOI 10.37882/2223–2974.2022.10.20

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОММЕРЧЕСКИХ БАНКОВ В СОВРЕМЕННЫХ УСЛОВИЯХ

PROBLEMS OF INFORMATION SECURITY OF COMMERCIAL BANKS IN MODERN CONDITIONS

V. Krasnopolsky

Summary. The article discusses various forms and methods of fraud in the field of information and telecommunication technologies used in relation to commercial banks and their clients, as well as ways to protect bank clients from illegal encroachments aimed at stealing personal data.

Keywords: digitalization, social engineering, cyber fraud, personal data theft, self-transfers, skimming, fraud monitoring.

Краснопольский Владимир Вячеславович
Магистрант
Институт мировой экономики и бизнеса
Российского университета дружбы народов
г. Москва
A9629230000@icloud.com

Аннотация. В статье рассматриваются различные формы и методы мошенничества в сфере информационно-телекоммуникационной технологий, используемых в отношении коммерческих банков и их клиентов, а также способы защиты клиентов банков от противоправных посягательств направленных на хищение персональных данных.

Ключевые слова: цифровизация, социальная инженерия, кибермошенничество, «кража личности», «самопереводы», скиминг, фрод-мониторинг.

Современная глобальная **цифровизация** (от английского digital — цифровой) охватывает большинство сфер человеческой жизни. Некоторые мировые эксперты справедливо называют текущий этап развития человечества «четвертой промышленной революцией». Особенно отчетливо цифровизация стала заметна в сфере финансовых услуг. А еще большую актуальность цифровизация приобрела в период пандемийных катаклизмов, когда во всем мире человек вынужден был изолироваться и единственным способом сохранить связь с внешним миром являлись глобальные сети, основанные на цифровых каналах связи. И чем цифровая связь была совершеннее, тем меньше человек чувствовал неудобства от своей изоляции. Равно как и коммерческие организации, отвечая на все новые вызовы современности, находясь в условиях постоянно растущей конкуренции, вынуждены были обеспечить соответствующую скорость передачи и обработки данных. Те компании, которые научились обеспечивать соответствующий уровень цифровизации, смогли не только сохранить финансовую устойчивость, но кратно повысить свою доходность.

Особенно отчетливо цифровизация стала заметна в сфере финансовых услуг. Сегодня целый ряд крупнейших российских банков заявляет о своих амбициях в технологическом лидерстве не только как финансовые институты, но и как полноценные экосистемы сервисов вокруг потребностей человека. Новые сервисы позволяют людям получать быстрый и полноценный доступ к различным услугам на экранах своих компьютеров и смартфонов в любое время суток и в любой точке планеты. Конкурентами таких компаний становятся уже не банки, а крупные технологические гиганты, такие как Google, Facebook, Amazon.

Очевидно, что такая огромная цифровизация в отрасли, которая охватывает сотни миллионов человек и непосредственно хранит, и обрабатывает колоссальные финансовые активы своих клиентов, не могла остаться незамеченной со стороны криминального мира. По данным Генеральной прокуратуры Российской Федерации, за последние семь лет число регистрируемых в России киберпреступлений выросло почти в 30 раз — если в 2013 г. подобных преступлений было 11 тысяч, то в 2019 г. уже 294 тысячи[1]. Половина таких преступлений совершается с использованием сети Интернет, а более трети — с использованием средств мобильной связи. Действительно, зачем рисковать и нападать на отделения банка или на клиентов, когда можно воспользоваться всеми удобствами цифрового мира, таких как анонимность, скорость операций, а главное доверчивость.

Эволюция методов мошенничества в информационно-телекоммуникационной сфере напрямую отражает изменения в предпочтениях клиентов в выборе банковских продуктов. Если до 2014 г. основным ка-

[1] Сайт Генеральной Прокуратуры Российской федерации // инфографика.
URL: https://epp.genproc.gov.ru/web/gprf/mass-media/infographics

Таблица 1. История распределения схем мошенничества.

Вид мошенничества	2014	2021
Скримминг	75%	1,3%
Вирусы	8%	1,6%
Другое	3%	3,8%
Социальная инженерии	14%	93,3%

Источник: сайт Генеральной Прокуратуры Российской федерации // инфографика.
URL: https://epp.genproc.gov.ru/web/gprf/mass-media/infographics

Таблица 2. Доля телефонного мошенничества в социальной инженерии

Год	2017	2018	2021
Звонков	23%	48%	93%
СМС	62%	40%	5%
E-mail, Интернет сообщений	15%	12%	2%
Всего случаев	161 630	399 361	2 496 808

Источник: сайт Генеральной Прокуратуры Российской федерации // инфографика.
URL: https://epp.genproc.gov.ru/web/gprf/mass-media/infographics

налом доступа к личным средствам были банкоматы, то к 2021 г. мы наблюдаем совершенно иную картину. Сегодня люди гораздо реже обналичивают деньги для оплаты товаров и услуг, практически повсеместно доступна оплата картой или, в крайнем случае, переводом.

Аналогично изменились и сценарии мошенничества: одним из самых популярных видов мошенничества является — **скимминг** (от английского skimming — снятие) — это мошеннические действия, направленные на получение данных банковской карты с помощью специального считывающего устройства (скиммера), сегодня занимает весьма скромную долю в общем объеме мошенничества, а значительная доля мошенничества в последние годы реализуется с использованием методов **социальной инженерии** (от английского Social — социальное, engineering — инженерия) или «атака на человека» -это совокупность психологических и социологических приёмов, методов и технологий, которые позволяют получить конфиденциальную информацию. Кибермошенников, которые используют эти приёмы на практике, называют **социальными** инженерами.

В свою очередь, доля и методы социальной инженерии тоже растут и эволюционируют. Если в 2017 г. доля социальной инженерии составляла 75% от всего объема **кибермошенничества** (от английского Cyberspace — киберпространство, Fraud — мошенничество) — один из видов киберпреступлений, целью которого является причинение материального, или иного ущерба, путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.), то в 2019–2021 гг. она уже составляла уже 79%, 89% и более 90% соответственно.

Условно мы можем выделить три этапа эволюции мошенничества в сфере социальной инженерии:

1. До 2017 г., когда основным способом воздействия на клиентов были массово рассылаемые SMS-сообщенияс текстом «Ваша карта заблокирована, перезвоните в банк» и номер телефона якобы «банка». При звонке на этот номер клиент после психологической обработки от так называемой «службы безопасности» оставался без денег.
2. С 2017 г. до 2019 г. когда SMS-сообщения постепенно стали уступать место телефонным звонкам от так называемой «службы безопасности».
3. С начала 2019 г. и до настоящего времени — это массовые телефонные звонки через возможности IP-телефонии из профессиональных call — центров, с использованием подмены номеров официальных банковских учреждений.

На текущий момент злоумышленники активно скупают краденные персональные данные клиентов банков на площадках «теневого» Интернета, их скрипты разговоров имитируют профессиональные call — центры. Как правило, такие звонки поступают с подменных телефонных номеров звонящих злоумышленников на городские номера 495/499 и осуществляются с территорий сопредельных государств, где мошенники

Таблица 3. Распределение мошенничетва по типам 2017–2021 гг.

Год	2017	2021
Кража личности	40%	13%
Самопереводы	60%	27%

Источник: сайт Генеральной Прокуратуры Российской федерации // инфографика. URL: https://epp.genproc.gov.ru/web/gprf/mass-media/infographics

Таблица 4. Процесс «Самоперевода»

Описание	Мошенник совершает звонок клиенту и под различными предлогами (объявления, компенсации и т.д.) убеждает клиента совершить перевод по своим реквизитам	Клиент самостоятельно переводит средства
Этап	1	2

Таблица 5. Пример реализации схемы «Самоперевода»

Участник диалога	Содержание сообщения
Клиент	Здравствуйте. Скажите пожалуйста, сегодня произошла какая-то очень странная история со мной. Вы не могли бы проверить мою карту? Мне позвонили буквально минут тридцать — сорок назад, представились поддержкой банка и сказали, что моя карта и личный кабинет взломаны
Оператор ЕРКЦ	Какие-то данные вы сообщали?
Клиент	Я вообще ничего не сообщала, только вернула свои средства на счет
Оператор ЕРКЦ	Вы сегодня проводили перевод на четыреста девяносто пять тысяч в «Банк Онлайн»? Это ваши платежи?
Клиент	Да, это мои платежи. Меня каким-то образом заставили сделать эти списания
Оператор ЕРКЦ	То есть этот платеж, вы делали самостоятельно, правильно я вас понимаю?
Клиент	Да, я делала самостоятельно, они меня заставили перевести на какую-то страховую ячейку, чтобы не украли мои деньги, потому что кто-то взломал мой личный кабинет. Скажите, пожалуйста, вы можете отменить эти транзакции?

скрываются от правоохранительных органов Российской Федерации. В последнее время активизировались звонки мошенников из

call — центров, расположенных на территории Украины. Преступные устремления мошенников не ограничиваются какими-то конкретными финансовыми институтами, а нацелены на всю банковскую систему и все крупные цифровые банки России!

Очевидно, что социальная инженерия через телефонный звонок — не единственная угроза, существует огромное количество схем и сценариев. Тем не менее, в общем объеме она занимает доминирующее положение, оставив высокотехнологические инструменты, например, таких как: хищение через удаленное управление персональным компьютером клиента или вирусные заражения мобильных телефонов и т.д., позади. Это объясняется простой реализацией схемы социальной инженерии, их безопасностью, высокой эффективностью и низкими затратами.

Однако необходимо отметить, что коммерческие банки научились довольно эффективно выявлять высокотехнологичные схемы мошенничества, поэтому мошенники стали использовать более сложные схемы и достаточно затратные для безопасности банков. Идеальным вариантом для мошенника является маскировка своих операций под операции самого клиента, так называемая, «**кража личности**» (с английского Personal — личный, Data — данные, Theft — кража) или другой вариант, убедить клиента коммерческого банка самостоятельно совершить операцию в интересах мошенника, так называемый, «**самоперевод**» (с английского Self — себя, Transfer — передача). Оба указанных варианта довольно просто реализовать с помощью социальной инженерии.

Итак, выделяют два основных типа кибермошенничества, уже упомянутых выше:

1. «Самопереводы» — клиенты самостоятельно проводят операции под руководством мошенников.

Таблица 6. Процесс «Кража личности»

Описание	Клиент получает звонок от мошенника («служба безопасности банка», по объявлению в Интрнете и т.д.)	Под различными предлогами мошенник убеждает клиента сообщить номер карты, пароль из SMS-сообщения для регистрации мобильного мобильного приложения	Мошенники проводя регистрацию мобильного приложения к профилю клиента на своем мобильном телефоне и проводят за клиента операции
Этап	1	2	3

Таблица 7. Пример реализации схемы «Кража личности»

Участник диалога	**Содержание сообщения**
Клиент	У меня, наверное, сейчас деньги с карты перевели. Что мне нужно сделать? Только что мне звонили по поводу объявления. Я объявление подавал, они хотели перевести на номер карты сумму
Оператор ЕРКЦ	Номер карты вы сказали?
Клиент	Да, номер карты
Оператор ЕРКЦ	А код от «Банк Онлайн» сообщили?
Клиент	Не знаю, пришла смс-ка с кодом, чтобы провести операцию, нужно было произнести код
Оператор ЕРКЦ	Этого делать ни в коем случае нельзя! Код пришел для регистрации «Банк Онлайн»? Для чего код поступил?
Клиент	Да, по-моему, да
Оператор ЕРКЦ	Кроме номера карты дебетовой маэстро, что-то еще сообщали?
Клиент	Нет, ну номер карты и вот этот код
Оператор ЕРКЦ	С вашей дебетовой карты был проведен перевод другому лицу «Банк Онлайн»

2. «Кража личности» злоумышленники компрометируют идентификаторы клиента, необходимые для проведения операций (номера карт и CVV, логин и пороли, номер телефона в SMS-банке, паспорт) и совершают операцию от имени клиента.

С 2010 года системы защиты клиентов коммерческих банков начали кардинально трансформироваться. За это время банки прошли все этапы становления службы, так называемого **Фрод** (от англ. Fraud — «мошенничество») — вид мошенничества в области информационных технологий, в частности, несанкционированные действия и неправомочное пользование ресурсами и услугами в сетях связи — **мониторинга** (от англ. Monitoring — мониторинг). Начиная с реализации защиты самих продуктов коммерческих банков и заканчивая суперсовременным комплексом риск-скоринга операций, центрами верификации операций, наличием экспертных команд.

Сегодня основным инструментом борьбы с кибермошенничеством в коммерческих банках является си-

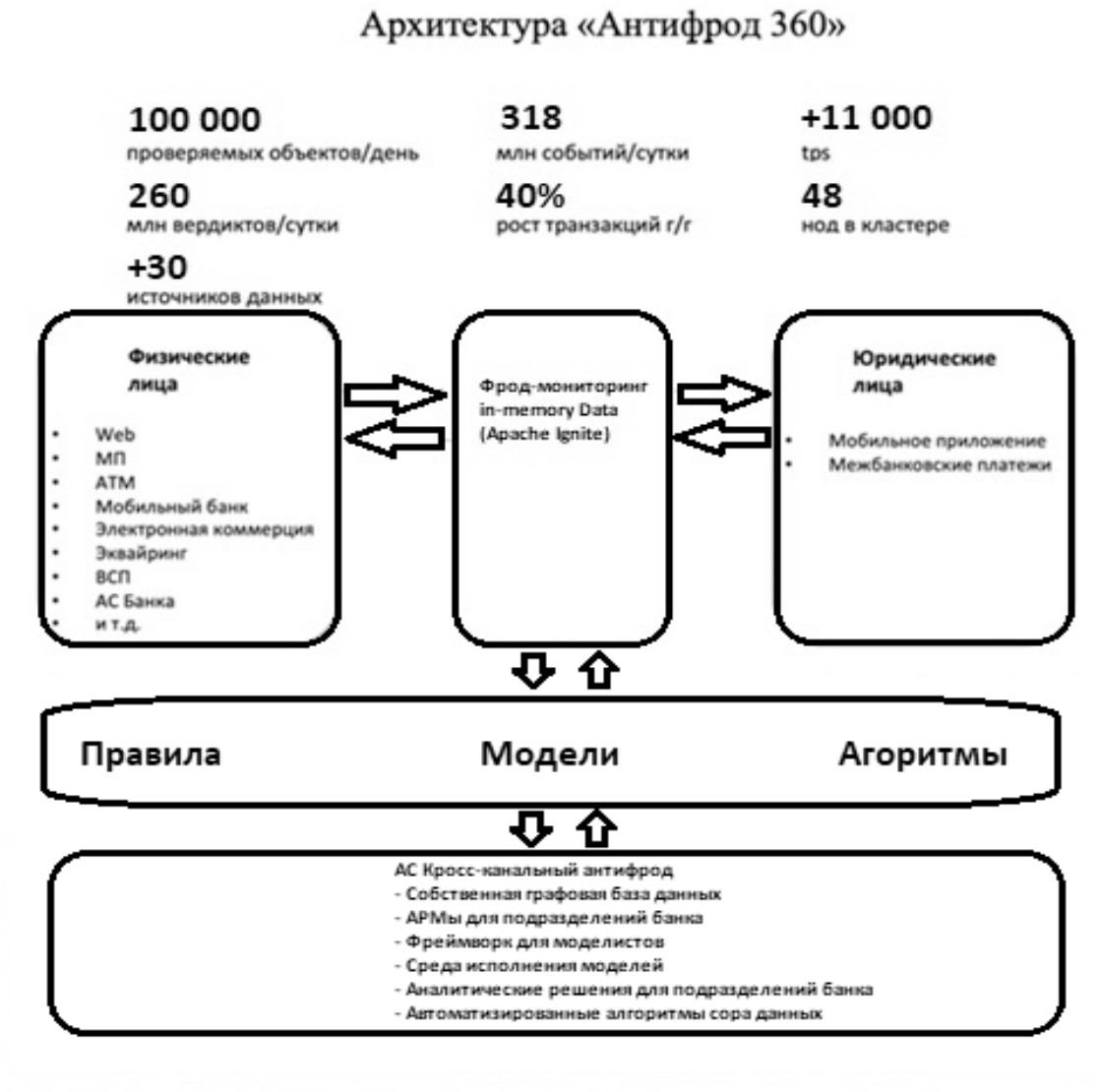

Рис. 1. Архитектура «Антифрод 360»

стема транзакционного фрод-мониторинга для физических и юридических лиц, позволяющая проверять большой объем операций в режиме реального времени, а также проводить расследования и строить сложную аналитику. Пример архитектуры системы фрод-мониторинга приведен на рис. 1: Архитектура «Антифрод 360».

Организация такого программно-аппаратного комплекса информационной безопасности в коммерческих банках и есть один из эффективных способов защиты банков от киберпреступлений и защиты персональных данных их клиентов в современных условиях.

Однако система информационной безопасности коммерческих банков несовершенна, и разработка новых методов защиты до сих пор остаётся актуальной, тем более в век развивающихся технологий и ростом влияния так называемого «искусственного интеллекта».

ЛИТЕРАТУРЫ

1. Бабукин Г.М. Использование информационных технологий в обеспечении безопасности банка. Вектор экономики. 2021.
2. Брагина И.О. информационная безопасность банков: причины возникновения угроз и методы их предотвращения. В сборнике: Роль учёта, контроля и управления в системе обеспечения устойчивого развития государственного и коммерческого секторов экономики. Симферополь, 2021. С.

3. Левшин М.А. Информационные технологии в российских банках и безопасность данных. Вектор экономики. 2020. № 12 (54). С. 65.
4. Салкуцан А.А., Ниязов Р.Т. Анализ современных уязвимостей информационной безопасности финансовых приложений российских банков. Экономический журнал. 2020. № 2 (58). С. 61–74.
5. Саяпина Н.Н., Кусакин Л.А. Информационная безопасность банка как необходимое условие его функционирования. В сборнике: Экономика сферы сервиса: проблемы и перспективы. Материалы V Всероссийской научно-практической конференции. Минобрнауки России, ОмГТУ; под общ. Ред. А.С. Полынского. 2019. С. 84–87.
6. Сайт Генеральной Прокуратуры Российской федерации // инфографика. URL: https://epp.genproc.gov.ru/web/gprf/mass-media/infographics

Журнал «Современная наука: актуальные проблемы теории и практики»

Российский Университет Дружбы Народов