/ASEM/ Academy of Economic Studies of Moldova

DSpace CRIS Repository at ASEM **https://cris.ase.md**

IREK ASEM Facultatea Contabilitate

Cyber fraud as a new type of banking risk

Kasevich, Olga

ASEM

https://cris.ase.md/handle/123456789/5095

978-9975-155-87-8 (PDF)

Downloaded from DSpace CRIS Repository at ASEM, DSpace CRIS at ASEM serve as Institution's institutional repo

DOI 10.5281/zenodo.6758975
CZU [336.46:004.056.53]:336.71(476)

CYBER FRAUD AS A NEW TYPE OF BANKING RISK

КИБЕРМОШЕННИЧЕСТВО КАК НОВЫЙ ВИД БАНКОВСКОГО РИСКА

Olga KASEVICH
olyakasevich8@gmail.com
Science coordinator: **Irina STROGANOVA**
stroganova.ira@list.ru
Polotsk State University, Belarus

Abstract. *Importance: With the development of technology and the proliferation of communication networks, the importance of security has grown. In this regard, there is a need to modernize the banking risk management system and to develop measures to improve the cybersecurity of financial institutions in the context of digital transformation.*
Research methods: system approach, deduction, analysis and synthesis, unity of historical and logical approaches, inference by analogy.
Results of the study: the definition of the concept of «banking risk» was proposed; the sources of cyber risks in the credit and financial sphere of the Republic of Belarus were considered, as well as the proposal to form a single center of response to cyber risks was developed.

Keywords: *cyber fraud, banking risks, risk management, skimming, shimming, phishing, vishing*
JEL: G320

Введение

Условием стабильного функционирования денежно-кредитной системы является устойчивая работа банковской системы. В современных условиях увеличивается количество факторов риска, приводящих к неопределенности результатов деятельности банков. Среди самых значимых можно выделить: последствия пандемии Covid-19, высокую волатильность курсов иностранных валют, цен на нефть, энергоресурсы, а также политическую нестабильность на мировом уровне.

Развитие информационного общества предполагает внедрение информационных технологий во все сферы жизни, но это означает и появление новых угроз безопасности – от утечек информации до кибертерроризма. На ранних стадиях развития сетей связи вопросы безопасности не были главными из-за небольшого количества пользователей и наличия в основном локальных сетей, в которых подразумевается доверие всех пользователей друг другу. С развитием технологий и разрастанием сетей связи выросло и значение обеспечения безопасности. В связи с этим возникает потребность в модернизации системы управления банковскими рисками и разработке мероприятий по повышению кибербезопасности кредитно-финансовых организаций в условиях цифровой трансформации

Основная часть

В настоящее время одним из важнейших направлений является управление рисками в банковской системе как область стандартизации и средство повышения эффективности деятельности банка.

В рамках исследования сущности понятия «банковский риск» рассмотрены подходы различных авторов к данному определению. Автор выделяет три основных подхода: «угроза потери в результате финансовых операций», «вероятность потерь и ухудшение ликвидности, связанные с внутренними и внешними факторами», а также «вероятность возникновения потерь в виде утраты активов».

Проведенный анализ различных точек зрения, изложенных в специальной экономической литературе, нормативных правовых документах позволил обосновать экономическое содержание понятия «банковский риск» и предложить иную трактовку вышеуказанного понятия. Под банковским риском, по мнению автора, следует понимать присущую банковской деятельности возможность понесения банком потерь и ухудшения ликвидности вследствие наступления неблагоприятных событий, связанных с внутренними и внешними факторами деятельности банка.

В условиях широты сферы банковской деятельности и многообразия банковских продуктов и услуг важно осуществить их классификацию. В зависимости от определенных критериев различные авторы представляют ее следующим образом, приведенном в Таблице 1

Таблица 1 – Классификация банковских рисков

КРИТЕРИИКЛАССИФИКАЦИИ	**ВИДЫ БАНКОВСКИХ РИСКОВ**
Уровень риска	Риски на макроуровне отношений Риски на микроуровне отношений
Характер банковского продукта, услуг и операций	Риск по забалансовым операциям Кредитный риск Валютный риск Операционный риск и др.
Степень обеспечения устойчивого развития банка	Риск несбалансированной ликвидности Процентный риск Риск потери доходности Риск потери конкурентоспособности Риск капитальной базы Риск-менеджмент
Факторы, образующие риск	Внешние Внутренние
Величина риска	Низкие риски Умеренные риски Полные риски
Характер учёта операций	Риск по балансовым операция Риск по внебалансовым операциям

Источник: собственная разработка на основе изучения специальной литературы [1-2].

На основе данных Таблицы 1 отметим, что наиболее значимым риском, оказывающим негативное влияние на устойчивость банковского сектора, являются кредитный и процентный риск. Однако технологии шагают вперед и все ранее приведенные классификации уже устарели и в связи с цифровой трансформацией банков выделяют новый вид риска – риск кибермошенничества.

В 2019 году зафиксировано большое количество фактов кибератак. В рамках деятельности центра мониторинга и реагирования на компьютерные угрозы в кредитно-финансовой сфере (далее – FinCERTby) получено и проанализировано более 9000 отдельных сообщений об инцидентах, направлено более 270 информационных рассылок.

По официальным данным большая часть сообщений, направленных в FinCERTby, относится к мошенничеству, совершенному при помощи метода социальной инженерии «Вишинг». В течение месяца зафиксировано более 4500 обращений от пострадавших граждан. Злоумышленники, помимо звонков по телефону, активно использовали Viber и Skype. Активно использовалось программное обеспечение, позволяющее подменять официальные номера банков. Наряду с дистанционным хищением денег из банковской системы свою популярность не потеряли, и так называемые, физические атаки, которые подверглись некоторым модификациям, что обусловлено непрерывным развитием информационных технологий. К атакам такого рода можно отнести:

1) Скимминг – установка специальных технических средств, причем не обязательно в картоприемник, для хищения данных, записанных на магнитную ленту платежной карты. PIN-код, как правило, похищается с помощью отдельного технического устройства – видеокамеры или фальшивой накладки на PIN-пад;

2) Шимминг – установка в картоприемник специальных технических средств, предназначенных для хищения данных с EMV-чипа карты. Таким образом, похищается следующая информация: история платежей, информация, содержащаяся на Track 2 карты, срок действия;

3) Black Box – установка либо подключение технического устройства, взаимодействующего с компонентами банкомата (чаще всего с диспенсером) и отдающего последнему команду для выдачи денежных средств;

4) Подмена процессинга – в этом случае банкомат отключается от процессинга кредитной организации и подключается к устройству, имитирующему его. Передовые устройства могут эмулировать нормальное состояние банкомата (обслуживание клиентов) для мониторинга программного обеспечения;

5) Transaction Reversal Fraud (TRF) – получение наличных денежных средств с одновременным воздействием на работу банкомата и процессингового центра, в результате чего отсутствует корректное завершение операции по выдаче наличных средств и не меняется баланс по карте (манипулирование карточным счетом

Схожее устройство банкоматов позволяет злоумышленникам использовать одно и то же вредоносное программное обеспечение в различных кампаниях по всему миру. Так, GreenDispenser, который использовали при атаках на банкоматы в Мексике, через некоторое время был обнаружен в странах Восточной Европы. Полная статистика заражений по всему миру на начало марта 2022 г. представлена в Таблице 2:

Таблица 2 – статистика заражений по всему миру на начало марта 2022

СТРАНА	**ПРОЦЕНТ ЗАРАЖЕНИЙ, %**	**СТРАНА**	**ПРОЦЕНТ ЗАРАЖЕНИЙ, %**
Афганистан	10,04	Того	8,26
Китай	9,2	Мьянма	8,13
Бурунди	9,08	Эфиопия	8,13
Бенин	9,03	Республика Конго	8,04
Центральная Африканская Республика	8,88	Кот-д'Иваур	7,96
Демократическая Республика Конго	8,48	Гвинея	7,94

Алжир	8,43	Мавритания	7,84
Руанда	8,4	Буркина-Фасо	7,81
Камерун	8,4	Мали	7,8
Гвинея-Бисау	8,28	Южный Судан	7,79

Источник: собственная разработка на основе изучение специальной литературы [3].

На данный момент кредитно-финансовая сфера одна из самых привлекательных зон интересов киберпреступников, о чем свидетельствует значительный рост числа киберпреступлений и целевых атак на банки. Для уверенного и безопасного функционирования банков должно использоваться качественное и надежное программное обеспечение. В Республике Беларусь существует три ведущие IT-компании, которые являются разработчиками банковского программного обеспечения [4-6]:

1. Системные технологии;
2. Центр банковских технологий (далее - ЦБТ);
3. SoftClub.

SoftClub – международный поставщик решений для автоматизации банковских процессов и решения сложных интеграционных задач. Данная компания каждый день разрабатывает продукты в сложнейших сферах, в которых надежность и безопасность стоит на первом месте. SoftClub был создан на базе Научно-исследовательского института систем автоматизации. Эта компания стояла у истоков разработки программного обеспечения всех банков Республики Беларусь и стоит отметить, что SoftClub до сих пор остается лидером разработчиком в этой сфере. Изначально SoftClub должен был стать единым центром по защите банков от киберпреступлений, который способен быстро и оперативно проводить анализ и реагировать на случаи кибермошенничества. Но с появлением банков с российским капиталом вся единая система отошла на второй план, поскольку у этих банков используется частично программное обеспечение SoftClub, а частично свои разработки. В Таблице 3 отображен перечень некоторых продуктов компании SoftClub.

Таблица 3 – основные продукты SoftClub

№	Название	Краткое описание
1	2	3
2.	SC-АНАЛИТИКА	Быстрая аналитика всех данных для постоянного контроля финансового положения банка
3.	SC-BUSINESS.PRO	Комплексная система дистанционного банковского обслуживания для юридический лиц и индивидуальных предпринимателей.
4.	SC-АРХИВ	Автоматизация процессов направления и управления архивами электронных документов, обеспечивая их надежное и долгосрочное хранение
5.	SC-SRM	Система для управления закупками, позволяющая автоматизировать и систематизировать все закупочные процессы компании любых размеров
6.	CASH FUSION	Позволит сотрудникам вашего банка обеспечивать максимальный уровень обслуживания клиентов
7.	SC-BANK NT	Обеспечивает автоматизацию операций, учета, управления, аналитику универсального многофилиального банка

Источник: собственная разработка на основе изучения специальной литературы [6].

Исходя из таблицы стоит отметить, что среди продуктов данной компании имеются «Система для управления закупками», «Автоматизация процессов направления и управления архивами электронных документов» и все эти данные о клиентах подвержены большому риску, поэтому компания также предлагает услугу по защите и информации. Но далеко не

каждый банк может позволить себе содержать целое структурное подразделение IT-специалистов по разработке системы защиты банка от кибермошенничества, т.к. для этого требуются различные лаборатории, тестирование и много других этапов, которые предполагают вложение большого количества денежных средств.

В Республике Беларусь на текущий момент существует лишь небольшое количество банков, которые обладают мощными ресурсами для организации данной системы. Соответственно возникает проблема для средних банков, которые не обладают достаточными ресурсами.

Согласно пунктам 5.2 и 6.2 Постановления от 2 марта 2016 года №108 [7], для необходимого уровня безопасности в области электронного взаимодействия необходимо изучить возможность создания единого центра реагирования на инциденты, связанные с нарушением информационной безопасности в финансовой сфере. На данный момент в Республике Беларусь отсутствует единый центр реагирования на кибератаки, в связи с чем считаем целесообразным:

1. Создание единой системы, которая обеспечит противодействие кибермошенничеству на уровне центрального банка. Функционирование данной системы будет базироваться на принципе своевременного предоставления статистики от банков в установленном порядке с определенной периодичностью.

2. В качестве разработчика автором рекомендуется ЦБТ, так как он является обладателем специального разрешения (лицензии) №01019/14, выданного Оперативно-аналитическим центром при Президенте Республики Беларусь на право осуществления деятельности по технической и (или) криптографической защите информации.

Выводы

За период своей деятельности ОАО «Центр банковских технологий» стало одним из основных разработчиков программных решений для Национального банка Республики Беларусь, которые находятся у предприятия на сопровождении в целях обеспечения требуемого уровня автоматизации бизнес-процессов. Благодаря высокой квалификации своих сотрудников, ОАО «Центр банковских технологий» привлекается Национальным банком к реализации инновационных проектов государственного масштаба.

Стоит отметить, что киберпреступность в банковской сфере является серьезной проблемой для всех стран мира. В связи с этим все экономическое сообщество должно объединить свои усилия для разработки более совершенных систем защиты от кибератак, что позволит снизить потери от действий злоумышленников.

Библиографические ссылки

1. ВЕРЕНИЧ, Н.К. Анализ деятельности банков и управления рисками (в схемах, таблицах, формулах): учеб.-метод. пособие. / Н.К.Веренич, Н.Г.Петрукович, А.И.Синкевич. 2-е изд., перераб. и доп. – Минск : Мисанта, 2015. – 142 с.
2. СЕМЕНОВА, К.А. Банковские риски: сущность и классификация / /К.А. Семенова, Л.Т. Кутукова // Молодой ученый [Электронный ресурс]. – 2019. – № 38 (276). – С. 125-127. – Режим доступа: https://moluch.ru/archive/276/62543/ Дата доступа: 14.03.2021.
3. Интерактивная карта киберугроз // Лаборатория Касперского [Электронный ресурс]. – Режим доступа: https://cybermap.kaspersky.com/ru. – Дата доступа: 11.03.2022.

4. Эффективные IT-решения для автоматизации бизнеса [Электронный ресурс] // Официальный сайт компании Системные технологии – Режим доступа: https://www.st.by Дата доступа: 09.05.2021.

5. Современные и эффективные IT-решения для банковской и финансовой сферы [Электронный ресурс] // Официальный сайт компании Центр банковских технологий Режим доступа: https://cbt.by Дата доступа: 09.05.2021.

6. Готовые решения для бизнес-процессов банка [Электронный ресурс] // Официальный сайт компании SoftClub – Режим доступа: https://softclub.com Дата доступа: 09.05.2021.

7. Об одобрении Стратегии развития цифрового банкинга в Республике Беларусь на 2016-2020 годы, Постановление правления Национального Банка Республики Беларусь, 02.03.2016, № 108 // Сайт Национального банк Республики Беларусь [Электронный ресурс]. – Режим доступа: https://www.nbrb.by/legislation/documents/digitalbankingstrategy2016.pdf Дата доступа: 09.05.2021.