УДК 336.71

КИБЕРМОШЕННИЧЕСТВО КАК НОВЫЙ ВИД БАНКОВСКОГО РИСКА

О. А. Касевич

студент, Полоцкий государственный университет, г. Новополоцк, Республика Беларусь, e-mail: olyakasevich8@gmail.com

Научный руководитель **И. А. Строганова**

магистр экономических наук, старший преподаватель, кафедра учёта, финансов, логистики и менеджмента, Полоцкий государственный университет, г. Новополоцк, Республика Беларусь, e-mail: i.stroganova@psu.by

Условием стабильного функционирования денежно-кредитной системы является устойчивая работа банковской системы. В настоящее время увеличивается количество факторов риска, приводящих к неопределенности результатов деятельности банков. Вместе с развитием информационных технологий увеличивается уровень кибератак. В связи с этим, требуется создание единого центра реагирования на инциденты, связанные с нарушением информационной безопасности в финансово-банковской сфере.

Ключевые слова: кибермошенничество; вишинг; фишинг; вредоносное программное обеспечение

CYBER FRAUD AS A NEW TYPE OF BANKI NG RISK

O. A. Kasevich

Student, Polotsk State University, Novopolotsk, Republic of Belarus,, e-mail: olyakasevich8@gmail.com

Supervisor: **I. A. Stroganova**

Master of Economic Sciences, Senior Lecturer, Department of Accounting, Finance, Logistics and Management, Polotsk State University, Novopolotsk, Republic of Belarus, e-mail: i.stroganova@psu.by

The stable operation of the banking system is a prerequisite for the stable functioning of the monetary system. Currently, the number of risk factors that lead to uncertainty in the performance of banks is increasing. Along with the development of

information technologies, the level of cyber-attacks increases. In this regard, it is necessary to create a single center for responding to incidents related to information security violations in the financial and banking sector.

Keywords: cyber fraud; vishing; phishing; malicious software.

Введение. Ввиду широты сферы банковской деятельности и многообразия банковских продуктов и услуг представляется необходимым актуализировать классификацию банковских рисков. Различные авторы, представители российской экономической школы такие как российский учёный Лаврушин О. И., Тавасиев А. М., Белоглазова Г. Н., а также белорусские авторы – Тарасов В. И., Кравцова Г. И., Рабыко И. Н. предлагают свои классификации в зависимости от определенных критериев. Следует заметить, что цифровая трансформация банкинга переносит акцент на информационные технологии. Вместе с развитием информационных технологий увеличивается уровень кибератак в финансово-банковской сфере.

Основная часть. В 2019 году зафиксировано большое количество фактов кибермошенничества. 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. Большая часть сообщений, направленных в FinCERTby, относится к мошенничеству, совершенному при помощи метода социальной инженерии «Вишинг», пик которого пришелся на ноябрь 2019 г. В течение месяца зафиксировано более 4500 обращений от пострадавших граждан [2]. Злоумышленники, помимо звонков по телефону, активно использовали в качестве связи с клиентами такие мессенджеры, как Viber и Skype. Активно использовалось программное обеспечение, позволяющее подменять официальные номера банков, размещенные на сайтах.

По данным Национального банка Республики Беларусь в таблице 1 представлена статистика заражения компьютеров пользователей (физических и юридических лиц Республики Беларусь).

По данным таблицы 1 следует отметить, что в первом полугодии 2019 г. основным способом заражения компьютеров пользователей вредоносным программным обеспечением (далее – ВПО) были массовые рассылки электронных писем. Во втором же полугодии 2019 г. тенденция изменилась: возросло количество случаев, связанных с социальной инженерией и несанкционированными денежными переводами. Так, в IV квартале 2019 г. FinCERTby наблюдал снижение направляемых сообщений, связанных с ВПО, примерно в 5 раз, а количество зафиксированных случаев, связанных с социальной инженерией, выросло более чем в 6 раз [2].

Все поступающие в FinCERTby инциденты от банков и НКФО классифицируются согласно регламенту передачи данных следующим образом:

MLW – рассылка ВПО посредством электронной почты, фишинговых ссылок;

SCN – попытки сканирования портов для взлома сети;

DOS – DDoS-атаки;

EXP – попытки эксплуатации уязвимостей веб-приложений;

URL – выявление поддельных сайтов (аккаунтов) банков;

SQL – попытки использования SQL-инъекций;

SOI – попытки совершения несанкционированного перевода денежных средств в результате обмана или злоупотребления доверием;

BRT – попытки взлома учетных записей посредством автоматизированного подбора комбинаций логинов и паролей.

Таблица 1 – **Статистика заражения ВПО**

№	Количество сообщений об инцидентах	Способ заражения
I квартал	998	1. Массовые рассылки электронных писем с ВПО
II квартал	836	1. Массовые рассылки электронных писем с ВПО 2. Рассылки писем с использованием вредоносных ссылок 3. Использование поддельных сайтов, аккаунтов и «лже-консультантов» в социальных сетях, якобы принадлежащих банкам Республики Беларусь
III квартал	1313	1. Мошенничество посредством социальной инженерии 2. Несанкционированные денежные переводы 3. Массовые рассылки электронных писем с ВПО
IV квартал	5623	1. Мошенничество посредством социальной инженерии 2. Массовые рассылки электронных писем с ВПО

Примечание – Источник: составлено автором на основе [2].

Стоит отметить, что мошенничество носит «сезонный» характер и может быть связано с тенденциями в ближайших странах, в основном в Российской Федерации, в частности из-за отсутствия языкового барьера, схожести процессов и др.

В 2019 году можно выделить 2 наиболее часто встречаемых типа мошенничества на объекты кредитно-финансовой сферы Республики Беларусь:

1. Рассылка ВПО посредством электронной почты, фишинговых ссылок для вымогательства и хищения денежных средств;

2. Несанкционированные переводы денежных средств, осуществляемые с помощью методов социальной инженерии.

В Республике Беларусь существует три ведущие IT-компании, которые являются разработчиками банковского программного обеспечения [1, 4, 5]:

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 компа-

ния 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.

Среди продуктов данной компании существуют «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.

Далеко не каждый банк может позволить себе содержать целое структурное подразделение IT-специалистов по разработке системы защиты банка от кибермошенничества. Ведь для этого нужны лаборатории, тестирование и много других этапов, которые требуют большое количество денежных средств. В Республике Беларусь на данный момент существует совсем небольшое количество банков, которые обладают мощными ресурсами для организации всей этой системы. А что делать средним банкам, которые не имеют таких возможностей?

Согласно п. 5.2 и п. 6.2 Постановления от 2 марта 2016 года № 108 [3], 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.

За период своей деятельности ОАО «Центр банковских технологий» стало одним из основных разработчиков программных решений для Национального банка Республики Беларусь (более 50 автоматизированных систем и программных комплексов), 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.

Заключение. Исходя из проведённых данных по заражению ВПО и анализе ведущих IT-компаний по разработке банковского программного обеспечения, предлагается создание единого центра реагирования на инциденты, связанные с нарушением информационной безопасности в финансово-банковской сфере. В качестве единого центра реагирования рекомендуется Центр банковским технологий, который благодаря высокой квалифицированности своих сотрудников и наличию специального разрешения, выданного Оперативно-аналитическим центром при Президенте Республики Беларусь, будет обеспечивать безопасное функционирование банков и финансовых учреждений.

Библиографические ссылки

1. Готовые решения для бизнес-процессов банка : сайт компании SoftClub. URL: https://softclub.com (дата обращения: 09.05.2021).

2. Национальный банк, Финансовая стабильность Республики Беларусь : Сайт Национального банка Республики Беларусь, 2019. URL: https://www.nbrb.by/publications/finstabrep/finstab2019.pdf (дата обращения: 09.05.2021).

3. 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 : сайт. URL: https://www.nbrb.by/legislati-on/documents/digital-bankingstrategy_2016.pdf (дата обращения: 09.05.2021).

4. Современные и эффективные IT-решения для банковской и финансовой сферы : сайт компании Центр банковских технологий. URL: https://cbt.by (дата обращения: 09.05.2021).

5. Эффективные IT-решения для автоматизации бизнеса : сайт компании Системные технологии. URL: https://www.st.by (дата доступа: 09.05.2021).

УДК 336.648

ФИНАНСИРОВАНИЕ КОММЕРЧЕСКИМИ БАНКАМИ ИННОВАЦИОННОЙ (ВЕНЧУРНОЙ) ДЕЯТЕЛЬНОСТИ

В. Л. Клюня[1)], Е. А. Ерш[2)]

[1)] *доктор экономических наук, профессор, Полоцкий государственный университет, г. Новополоцк, Республика Беларусь, e-mail: alexeyk75@mail.ru*

[2)] *аспирант, Белорусский государственный университет, г. Минск, Республика Беларусь, e-mail: 1143858@gmail.com*

В статье рассмотрены вопросы участия банковского капитала в венчурном финансировании инновационных проектов. Обосновывается тезис о необходи-