

Индекс чистой прибыли банка Ip_i рассчитывается следующим образом (2):

$$Ip_i = \frac{Profit_i}{Profit_{max}} \quad (2)$$

где $Profit_i$ – чистая прибыль i -го банка; $Profit_{max}$ – показатель максимальной чистой прибыли i -ых банков ($i = 1..k$, k – количество банков для сравнения).

Индекс цифрового продвижения i -го банка Id_i рассчитывается по формуле (3):

$$Id_i = \sqrt{\frac{IY_i^2 + IGY_i^2 + IVk_i^2 + IF_i^2}{4}} \quad (3)$$

где IY_i – частный индекс активности в Youtube, IGY_i – частный индекс видимости сайта в Google и Yandex; IVk_i – частный индекс общего количества подписчиков сообщества в ВКонтакте; IF_i – частный индекс общего количества подписчиков сообщества в Facebook i -го банка.

Частные индексы IY_i , IGY_i , IVk_i , IF_i рассчитываются аналогично индексу чистой прибыли (2) и зависят от показателей: активность банка в Youtube (Y); видимость сайта банка в Google и Yandex (G&Y); общее количество подписчиков сообщества банка в ВКонтакте (Vk); общее количество подписчиков сообщества банка в Facebook (F), соответственно.

Анализ полученных результатов (таблица) показал, что в ТОП-5 по цифровому продвижению банков в сети Интернет по цифровым каналам Youtube Google, Yandex, ВКонтакте и Facebook по показателю чистой прибыли и общему индексу конкурентоспособности входят коммерческие банки: ОАО «АСБ Беларусбанк», ОАО «Приорбанк», ОАО «БПС-Сбербанк», ЗАО «Альфа-Банк», ЗАО «МТБанк».

Применение инструментов регрессионного анализа позволило построить экономико-математические модели для оценки комплексного влияния каналов цифрового продвижения банка на показатель чистой прибыли (4) и общий показатель (индекс) его конкурентоспособности (5).

$$Ip = 0,78 * Id; R^2 = 0,70; F(18,80) > \text{Значимость } F(0,0003) \quad (4)$$

$$Ic = 0,93 * Id; R^2 = 0,92; F(117,73) > \text{Значимость } F(7,89E-10) \quad (5)$$

Список использованных источников

1. Глобальные исследования банковского рынка в Республике Беларусь. [Электронный ресурс]. – Режим доступа: URL <https://www.artox-media.by/wiki/artox-media-predstavila-globalnoe-digital-issledovanie-bankovskogo-rynka-belarusi/>. – Дата доступа: 10.02.2019.
2. Рейтинги банков Беларуси по параметру Чистая прибыль [Электронный ресурс]. – Режим доступа: URL: https://viberi.by/ratings/net_profit. – Дата доступа: 10.02.2019.
3. Рейтинг Видимости сайтов в поисковых системах: Яндекс и Google. [Электронный ресурс]. – Режим доступа: URL: <https://www.artox-media.by/researches/seo/> – Дата доступа: 10.02.2019.
4. Забродская, К.А. Модели и методическое обеспечение оценки уровня развития инфокоммуникационных услуг в Республике Беларусь: дис...к-та экон. наук: 08.00.13 / К.А. Забродская. – Минск, 2015. – 180 с.

ОРГАНИЗАЦИЯ ЭФФЕКТИВНОЙ СИСТЕМЫ КИБЕРБЕЗОПАСНОСТИ В БАНКОВСКОМ СЕКТОРЕ РЕСПУБЛИКИ БЕЛАРУСЬ

Григорьева Я. И., Тарасов В. И., *Белорусский государственный университет, г. Минск, Беларусь*

Современные цифровые технологии, постоянно растущие ожидания со стороны клиентов и высокая конкуренция дали толчок к трансформации некогда традиционных процессов. Синергия данных факторов предопределила интеграцию передовых технологических решений в финансовые системы по всему миру.

Сегодня все чаще международные эксперты говорят о новых точках роста с внедрением технологий будущего, но, вместе с тем, обращают внимание на новый тип угроз, который таит в себе современное информационно-цифровое пространство. Высокие темпы имплементации ранее не используемых каналов и устройств передачи и хранения данных несут в себе и реальные риски для кибербезопасности.

С активным внедрением финансовых технологий или финтех (financial technology) особую актуальность стали представлять киберугрозы и обеспечение кибербезопасности. Кибернападения на финансовую систему становятся все более частыми и изощренными. Ландшафт киберугроз расширяется изо дня в день и постоянно меняется. Методы и технологии, используемые киберпреступниками для несанкционированного доступа к конфиденциальной информации, совершенствуются и постоянно трансформируются.

По последним оценкам, прямые издержки от нарушений кибербезопасности могут вырасти с 1,7 млрд долл. США в 2015 году до более чем 6,8 млрд долл. США к 2020 году [1, с. 5]. Помимо очевидного финансового ущерба от последствий киберпреступности, растут и финансовые затраты на меры по ее предотвращению. В 2017 году исследование 254 компаний в семи странах мира показало, что в годовом исчислении затраты этих компаний на реагирование и предотвращение кибератак увеличатся на 27,4 % [2, с. 15].

Значительные финансовые потери, репутационный ущерб и потеря доверия со стороны клиентов – вот то немного, с чем может столкнуться отдельная финансовая организация. А в случае последовательного заражения глобальные проблемы могут угрожать стабильности финансовой системы целой страны.

Для Республики Беларусь характерно доминирование банковского сектора, что обуславливает прямую зависимость между уровнем финансовой устойчивости в банковских организациях и стабильного функционирования всей финансовой системы страны.

Когда серьезность атаки возрастает, вполне вероятно, что только устойчивая и гибкая модель кибербезопасности может подготовить финансовые организации к выживанию в условиях неизбежных киберрисков.

Согласно глобальному индексу кибербезопасности (Global Cybersecurity Index, далее – GCI), отражающему степень готовности стран к кибератакам, среди рассматриваемых 60-стран мира по итогам 2018 года Беларусь заняла лишь восьмое место (рис. 1), при этом, возглавила данный рейтинг Япония как самая безопасная страна с точки зрения киберугроз.

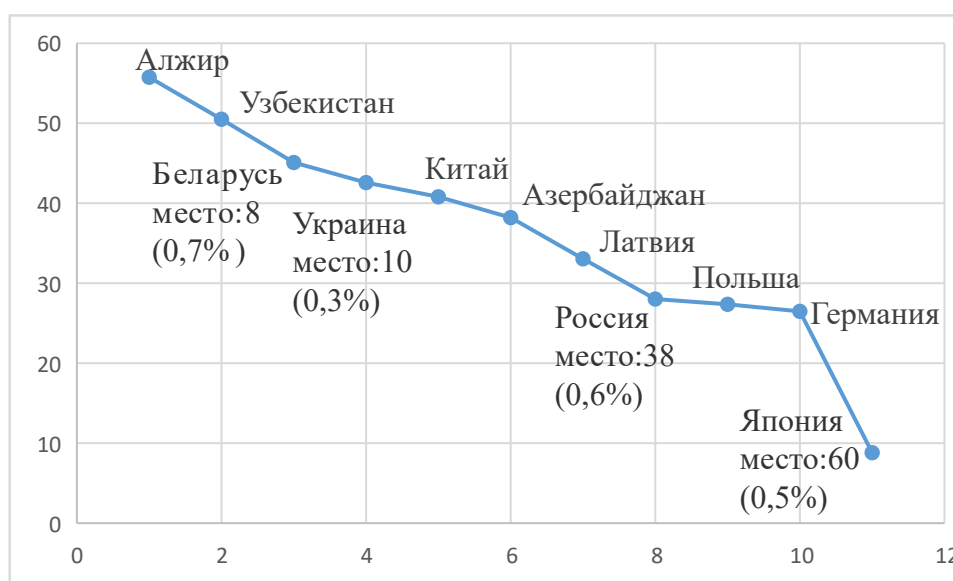


Рисунок 1 – Рейтинг стран по индексу GCI (в т. ч. финансовые атаки вредоносных программ (% пользователей))

Источник: собственная разработка на основе [3].

Для формирования эффективной системы кибербезопасности следует достоверно располагать информацией об источниках происхождения и основных каналах распространения киберугроз. Однако, киберриск – это относительно новая угроза для финансового сектора. Ввиду этого, данные о киберинцидентах скудны, а их количественного анализа недостаточно по причине отсутствия в финансовом секторе стран мира единых стандартов оценки киберриска.

На фоне растущего влияния внедряемых финансовых технологий, а также участвовавших технологических инцидентов Базельский комитет по банковскому надзору (Basel Committee on Banking Supervision, далее – БКБН) учредил целевую экспертную группу для изучения этого явления и последствий от активного внедрения финтех в банковских организациях. Результатом совместной работы стал опубликованный в декабре 2018 г. БКБН доклад «Cyber-resilience: range of practices» с описанием и сравнением ряда наблюдаемых практик киберустойчивости банков. При этом в докладе подчеркивается, что в целом в большинстве стран все еще отсутствуют общие нормативные требования к архитектуре и стандартам в области управления киберрисками [4, п.п. 3.4, с. 14].

Стратегия развития финансового рынка Республики Беларусь до 2020 года предусматривает цифровизацию банковского и иных секторов финансового рынка [5, с. 3]. При этом, для страны особую значимость на современном этапе развития представляет не только стремление к созданию полноценно функционирующей цифровой экономики, но и параллельная разработка и поэтапное внедрение эффективного механизма безопасного функционирования данной экономики будущего. А для лучшей адаптации к изменениям необходимо в первую очередь научиться своевременно оценивать потенциальные риски, а также умело управлять растущей изменчивостью, неоднозначностью и сложностью современного цифрового пространства.

Национальным банком Республики Беларусь (далее – НБРБ) в 2018 г. был предпринят ряд мер в целях повышения устойчивости банковского сектора. В частности, в рамках совершенствования надзорных требований и процедур перечень основных видов операционного риска был дополнен киберриском, дано его определение, указаны источники его возникновения [6, с. 18].

В рамках реализации мер по защите информации и кибербезопасности в Республике Беларусь в августе 2018 г. в структуре НБРБ был создан Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERTby) [7, с. 15]. В свою очередь, представители банковских учреждений выразили готовность сотрудничать и поддерживать функционирование FinCERT в нашей стране, пожелав автоматизировать процесс обмена данными об угрозах, что позволит скоординировать обмен информацией Центра, правоохранительных органов и банков, осуществлять в реальном времени анализ данных о фактах компьютерных атак в финансовых организациях и подготовку аналитических материалов, устанавливать рекомендации (стандарты) в области обеспечения защиты информации при осуществлении банковской деятельности [8, с. 62].

В период с 15 октября 2018 г. (т. е. с момента начала информационного обмена между банками, небанковскими кредитно-финансовыми организациями (далее – НКФО) и Центром мониторинга) по 22 января 2019 г. от 21 банка и НКФО получено и проанализировано 501 отдельное сообщение об инцидентах. Из них почти 70% классифицировано как рассылка вредоносного ПО и фишинговых ссылок, 17 % – как попытки эксплуатации уязвимостей веб-приложений, 8 % – как попытки совершения несанкционированного перевода денежных средств [9, с. 11].

В рамках проводимой работы по цифровой трансформации финансовой сферы в планах Национального банка Республики Беларусь на 2019 год предусмотрено также дальнейшее развитие цифровых банковских технологий по оказанию финансовых услуг и создание дополнительных стимулов по более активному использованию электронных платежных инструментов и средств платежа. Данная работа будет сопровождаться реализацией системных мер по противодействию киберугрозам и ограничению рисков [10, с. 6].

Поэтапные меры по организации эффективной системы управления киберриском в банковской системе Республики Беларусь с целью обеспечения кибербезопасности как необходимой меры управления финансовой устойчивостью и безопасностью функционирования банковских организаций должны стать приоритетной задачей (для всех участников финансового рынка стра-

ны), решение которой позволит наметить эффективные пути по обеспечению финансовой стабильности в стране, в т. ч. в случае возникновения нестандартных (кризисных) ситуаций.

Таким образом, принимаемые банковским регулятором инициативы с учетом международного опыта в данной области будут способствовать повышению эффективности системы обеспечения стабильности финансового сектора как необходимого условия устойчивого социально-экономического развития Республики Беларусь.

Список использованных источников

1. Innovation-Driven Cyber-Risk to Customer Data in Financial Services [Electronic resource]: World Economic Forum, 2017. – Mode of access: https://www.oliverwyman.com/content/dam/oliverwyman/v2/publications/2018/march/WEF_Cyber_Risk_to_Customer_Data.pdf. – Date of access: 02.10.2018.
2. The Global Risks Report 2018 [Electronic resource]: World Economic Forum, 2018. – Mode of access: <http://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/the-global-risks-report-2018.pdf>. – Date of access: 10.10.2018.
3. Which countries have the worst (and best) cybersecurity? [Electronic resource] // Comparitech, 2019. – Mode of access: <https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/>. – Date of access: 08.02.2019.
4. Cyber-resilience: range of practices [Electronic resource] // The Basel Committee on Banking Supervision, 2018. – Mode of access: <https://www.bis.org/bcbs/publ/d454.pdf>. – Date of access: 02.02.2019.
5. Стратегия развития финансового рынка Республики Беларусь до 2020 года [Электронный ресурс]: постановление Совета Министров Респ. Беларусь и Национального банка Респ. Беларусь, 29 марта 2017 г., № 229/6 // Национальный банк Респ. Беларусь. – Режим доступа: http://www.nbrb.by/finsector/P229_6.pdf. – Дата доступа: 06.08.2018.
6. О внесении изменения и дополнений в постановление Правления Национального банка Республики Беларусь от 29 октября 2012 г. № 550 [Электронный ресурс] // Банковский вестник, информационный выпуск, май 2018 г. – Режим доступа: http://www.nbrb.by/bv/Arch/suppl_75.pdf. – Дата доступа: 23.09.2018.
7. О ходе реализации стратегического проекта Национального банка «Создание системы мониторинга и противодействия компьютерным атакам в кредитно-финансовой сфере (FinCERT)» [Электронный ресурс] // Банковский вестник. – 2018. – №10 (октябрь). – Режим доступа: <http://www.nbrb.by/bv/articles/10561.pdf>. – Дата доступа: 13.11.2018.
8. Итоговый документ XV Международного форума по банковским информационным технологиям «БанкИТ'2018» [Электронный ресурс] // Банковский вестник, декабрь 2018. – Режим доступа: <http://www.nbrb.by/bv/articles/10585.pdf>. – Дата доступа: 13.01.2019.
9. Обеспечение финансовой стабильности в 2018 году и задачи на 2019 год [Электронный ресурс] // Банковский вестник. – 2019. – №1 (январь). – Режим доступа: <http://www.nbrb.by/bv/articles/10589.pdf>. – Дата доступа: 11.02.2019.
10. О предварительных итогах реализации денежно-кредитной политики в 2018 году и основных задачах деятельности Национального банка на 2019 год [Электронный ресурс] // Банковский вестник. – 2018. – №12 (декабрь). – Режим доступа: <http://www.nbrb.by/bv/articles/10578.pdf>. – Дата доступа: 08.02.2019.

ПРОБЛЕМЫ ФИНАНСИРОВАНИЯ ИННОВАЦИОННОГО РАЗВИТИЯ В УКРАИНЕ

Гузар Б. С., Уманский национальный университет садоводства,
г. Умань, Украина

Одной из составляющих обеспечения динамики роста экономики Украины является внедрение инновационной модели развития. Именно такой путь дает возможность нашей стране сохранить и наиболее эффективно использовать существующий научно-технический