УДК 336.71

КИБЕР–РИСК КАК НОВАЯ УГРОЗА ФИНАНСОВОЙ СТАБИЛЬНОСТИ

Григорьева Яна Ивановна, аспирант,
Белорусский государственный университет
Grigoreva Yana, Belarusian State University, yana.2007@list.ru

Аннотация. Оценка кибер–риска “на упреждение” формирует преимущественное право на стабильную финансовую устойчивость и жизнеспособность банковского сектора в долгосрочной перспективе.

Ключевые слова: финансовые технологии, финтех, кибер–риск, киберинцидент, кибербезопасность.

Быстрое внедрение инновационных технологий в банковские операционные процессы и появление новых бизнес–моделей становятся источником принципиально новых угроз, негативно влияющих на безопасное функционирование банковской организации. Современные информационные технологии превращаются в потенциально негативный фактор, источник которого может исходить как из внешней, так и из внутренней среды. В подобных условиях усиливается роль обеспечения безопасности и высоких стандартов соответствия при применении инноваций в банковском секторе.

В последние годы на финансовом рынке наблюдается стремительное внедрение так называемых финансовых технологий или финтех (financial technology или fintech). На этом фоне Базельский комитет по банковскому надзору опубликовал новый документ “Sound Practices: implications of fintech developments for banks and bank supervisors”, в котором использует рабочее определение финансовой стабильности для понятия **финтех (fintech)** как “технологически обеспеченные финансовые инновации, которые могут привести к появлению новых бизнес–моделей, процессов или продуктов с соответствующим материальным эффектом на финансовых рынках и в учреждениях, предоставляемых финансовые услуги” [1, с.9]. Данный документ разработан, в первую очередь, с целью способствования

общему пониманию новых рисков и возможностей, связанных с активным внедрением финансовых технологий в банковском секторе, путем описания наблюдаемых практик, прежде чем выступать в качестве самостоятельного документа с конкретными техническими рекомендациями, обязательными к исполнению.

Характер и масштабы банковских рисков, которые традиционно имеют место быть из–за особенностей банковской деятельности, претерпевают изменения соразмерно увеличению внедряемых передовых финансовых технологий. Эти события могут привести как к открытию новых возможностей для клиентов, так и к новым и дополнительным рискам для банков. К основным рискам, связанным с появлением финтеха, наряду со стратегическим и операционным рисками, риском соблюдения требований (комплайенс–риск), также относят и **кибер–риск (cyber risk)** [1, с.6].

После участившихся в последнее время атак на финансовые учреждения [2] все больше международных экспертов сходятся во мнении, что именно кибер–риск становится ключевой угрозой финансовой стабильности. Актуальность новой угрозы возрастает с учетом того, что данные о кибер–инцидентах скудны, а их количественного анализа недостаточно по причине отсутствия в финансовом секторе единых стандартов оценки кибер–риска. Как правило, усредненный анализ проводят путем изучения различных типов киберинцидентов (утечка данных, мошенничество и нарушение бизнес–процессов) и выявления закономерностей с использованием различных наборов данных [3].

Сущность относительно нового для банковской практики понятия "**кибер–риск**" следует рассматривать как потенциальные финансовые потери или вред (урон), причиненный технической инфраструктуре и информационным системам организации. При переходе банковских организаций от старых систем к новым цифровым платформам, новая оцифрованная среда может нести реальную угрозу кибербезопасности и проявляться в различных формах. Источник кибер–риска может исходить как от самой организации (внутренняя угроза может исходить от сотрудников, подрядчиков организации), так и располагаться за ее пределами (киберпреступники, партнеры–поставщики). Также не редки ситуации умышленных действий хакера (или их группы), осуществляющего атаку с целью заражения информационных систем. Однако они также могут быть непреднамеренными, например, ошибка пользователя или системного администратора, которая делает систему временно недоступной.

Высокая взаимосвязь между участниками рынка может создать преимущества для банков и потребителей, и, вместе с тем, потенциально сделать банковскую систему более уязвимой для кибер–угроз и подвергнуть большие объемы конфиденциальной информации преднамеренному воздействию заинтересованных лиц. Это подчеркивает необходимость того, чтобы банки, финтех–фирмы и органы банковского надзора способствовали обеспечению эффективного управления и контроля кибер–риска. Так, например, в мае 2018 г. перечень основных видов операционного риска банков был дополнен кибер–риском [4, с.8].

Вместе с тем, следует подчеркнуть, что новые технологии и бизнес–модели могут увеличить кибер–риск, если средства и способы управления им не будут успевать за все новыми технологическими изменениями. Таким образом, **система мониторинга и контроля кибер–риска должна быть динамичной и адаптивной**.

Безопасность, надежность и финансовая стабильность могут быть усилены за счет осуществления регулятором в лице центральных (национальных) банков надзорных процедур. Целью таких мероприятий являются оценка наличия и эффективности функционирования созданной банком системы внутреннего контроля, инструменты которой позволяют оперативно идентифицировать, контролировать и надлежащим образом противостоять рискам, связанным с использованием финансовых технологий, включая новые бизнес–модели, процессы, банковские продукты и услуги.

Список использованных источников:

2. Sound Practices: implications of fintech developments for banks and bank supervisors [Electronic resource] : Basel Committee on Banking Supervision, 2018. – Mode of access: https://www.bis.org/bcbs/publ/d431.pdf. – Date of access: 11.08.2018;

2. The Biggest Cyber Attacks of 2017 [Electronic resource] : Vircom, 2017. – Mode of access: https://www.vircom.com/blog/biggest–cyber–attacks–of–2017/. – Date of access: 12.09.2018;

3. Cyber Risk for the Financial Sector: A Framework [Electronic resource] : IMF Working Paper No. 18/143, 2018. – Mode of access: http://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber–Risk–for–the–Financial–Sector–A–Framework–for–Quantitative–Assessment–45924. – Date of access: 14.09.2018;

4. Инструкция об организации системы управления рисками в банках, открытом акционерном обществе “Банк развития Республики Беларусь”, небанковских кредитнофинансовых организациях, банковских группах и банковских холдингах [Электронный ресурс] : постановление Правления Национального банка Респ. Беларусь, 29 окт. 2012 г., № 550 // Национальный правовой Интернет–портал Республики Беларусь. – Режим доступа: http://www.nbrb.by/Legislation/documents/PP_550_2016.pdf. – Дата доступа: 06.09.2018.