КИБЕРРИСКИ — РАСТУЩАЯ УГРОЗА ДЛЯ МАКРОФИНАНСОВОЙ СТАБИЛЬНОСТИ

На фоне растущей цифровизации, развития технологий и усиления геополитической напряженности за последние два десятилетия, и особенно с 2020 года, значительно участились инциденты, связанные с киберугрозами, в особенности со злым умыслом. Серьезные инциденты в крупных финансовых учреждениях могут представлять немалую угрозу макрофинансовой стабильности из-за утраты доверия, перебоев в работе критически важных услуг и распространения вторичных эффектов на другие учреждения в силу технологических и финансовых взаимосвязей.

Как следует из выводов главы, хотя киберинциденты до сих пор не носили системного характера, риск чрезвычайных прямых потерь — в размере не менее 2,5 млрд долларов США — для компаний в результате таких инцидентов возрос. Более того, косвенные убытки от киберинцидентов также значительны и, как правило, существенно превышают заявленные компаниями прямые потери.

Понимание факторов, способствующих возникновению или предотвращению киберинцидентов, имеет решающее значение для разработки надежных регламентов и стратегий в области кибербезопасности. Как показывает проведенный в главе анализ, в результате цифровизации и геополитической напряженности значительно повышается риск киберинцидентов, тогда как более совершенное законодательство в области кибербезопасности и более эффективное управление киберрисками в компаниях могут помочь снизить такой риск.

Финансовый сектор весьма подвержен киберугрозам; так, почти пятая часть всех инцидентов затрагивает финансовые компании. Учитывая высокую концентрацию рынка и низкую взаимозаменяемость, особенно в случае критически важных услуг, таких как платежные услуги и депозитарное банковское хранение, киберинциденты в финансовых компаниях могут стать особенно разрушительными; в этой связи задача по укреплению кибербезопасности и операционной устойчивости становится особенно важной. Деятельность финансовых компаний часто зависит от общих сторонних поставщиков ИТ-услуг, что также повышает риск общих потрясений и вторичных эффектов.

Серьезный киберинцидент в финансовом учреждении может подорвать доверие к финансовой системе, а в крайних случаях повлечь за собой распродажу на рынке или массовое изъятие вкладов из банков. Несмотря на то что масштабного изъятия вкладов из-за киберинцидентов пока не произошло, эмпирический анализ указывает на небольшой, но довольно устойчивый отток депозитов из некрупных банков в США после кибератаки.

В условиях, когда глобальная финансовая система сталкивается со значительными и растущими киберугрозами, принципы политики и управления должны идти в ногу со

временем. Однако, как показывает опрос центральных банков и органов надзора в странах с формирующимся рынком и развивающихся странах, основы политики кибербезопасности зачастую остаются недостаточными.

Устойчивость финансового сектора к киберрискам следует укреплять посредством разработки надлежащей национальной стратегии кибербезопасности, соответствующей нормативно-правовой и надзорной базы, квалифицированных кадров в области кибербезопасности, а также национальных и международных соглашений об обмене информацией. Чтобы обеспечить более эффективный мониторинг киберрисков, необходимо усилить отчетность о киберинцидентах. Органам надзора следует возложить на членов советов директоров ответственность за управление кибербезопасностью в финансовых компаниях, формирование корпоративной культуры, способствующей борьбе с рисками, поддержание кибергигиены и проведение мероприятий по обучению и повышению осведомленности. В целях ограничения потенциально дестабилизирующего воздействия на финансовую систему финансовым компаниям следует разрабатывать и тестировать процедуры ответных действий и восстановления после инцидентов. Государственным органам стран следует разрабатывать эффективные протоколы ответных действий и принципы кризисного управления.

МВФ активно помогает странам-членам укреплять свои системы кибербезопасности с помощью Программ оценки финансового сектора и инициатив по развитию потенциала. С полным текстом доклада на английском языке можно ознакомиться по адресу http://IMF.org/GFSR-April2024