IMFBlog
INSIGHTS AND ANALYSIS ON ECONOMICS & FINANCE

Киберзащита должна иметь глобальный характер

Эмануэль Копп, Линкольн Каффенбергер и Кристофер Уилсон

26 октября 2017 года

Для кибернетического риска нет географических границ, и угроза носит глобальный характер, поэтому роль международных организаций принципиально важна (solarseven/iStock by Getty Images).

Кибератаки на финансовые организации становятся более распространенными и существенно более изощренными. Получившие широкую огласку случаи, такие как взлом системы Equifax, нарушивший конфиденциальность кредитной информации 143 миллионов американцев, и кража 81 миллиона долларов США из Банка Бангладеш являются лишь двумя примерами недавних случаев несанкционированных проникновений хакеров в финансовой отрасли.

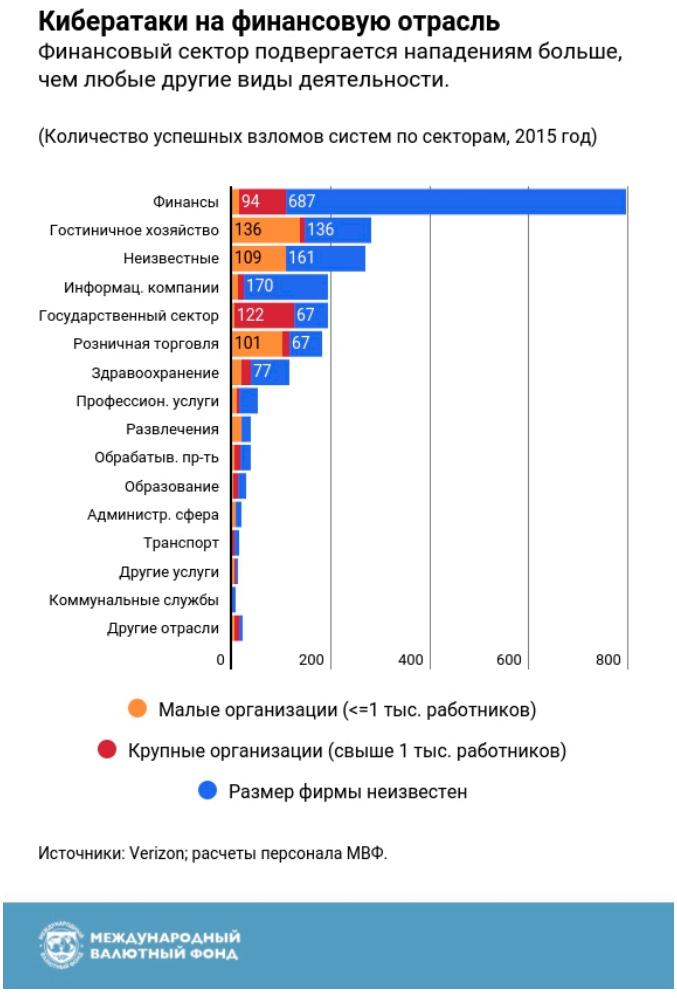
Сегодня кибер-риск представляет собой постоянную угрозу для финансовых организаций и надлежащего функционирования в высокой степени взаимосвязанной финансовой системы. Банки всех размеров подвергаются кибератакам каждый день. Взломы систем отдельных фирм могут вызывать негативные эффекты домино для других финансовых и нефинансовых компаний и создавать системный риск, представляющий собой новое, неизученное измерение кибер-риска.

Недавний Рабочий документ МВФ указывает на то, что международные организации, такие как Банк международных расчетов, Совет по финансовой стабильности и МВФ, могут сыграть важнейшую роль в поддержке процесса распространения информации, разработке координированных мер политики, содействии разрешению споров и сдерживании системного риска.

Изощренные атаки

Некоторые из наиболее опасных кибератак включают злонамеренные действия в отношении операций по переводу денег и работы банкоматов, введение вредоносных программ в банковские системы, уничтожение файлов и вычислительной техники и действия, носящие характер вымогательства и нарушающие внутренние операции.

Однако в условиях сложившейся на сегодня мозаики различных национальных норм регулирования и внутренних мер политики отрасли отсутствуют комплексные данные, и высока вероятность недооценки риска.



Компании сами усиливают неопределенность, поскольку из опасений ущерба для своей репутации и деятельности они часто утаивают информацию о происходящих с ними киберсобытиях. Во многих случаях информация о случаях взлома раскрывается через многие месяцы, а иногда через годы после произошедшего инцидента.

Границы безопасности

Как действовать в отношении столь широкой и сложной угрозы? Меры безопасности, такие как системы сетевой защиты, кодирование данных, обучение персонала и планирование для обеспечения бесперебойной деятельности, хотя и являются необходимыми, могут быть связаны со значительными затратами и способны затруднять для компании ведение повседневной коммерческой деятельности. Внесение изменений в продукты или процессы может способствовать уменьшению риска, но новые методы работы могут создавать новые факторы уязвимости.

Фирмы могут передавать риск третьим сторонам, таким как страховые компании или внешние поставщики услуг кибербезопасности. Но асимметрия информации и ее недостаточность у этих сторон, а также в целом малый опыт в работы с данным видом экономического риска, ограничивают возможности частного сектора по уменьшению кибер-риска в финансовой системе. Фирмы, как правило, недооценивают свою подверженность кибер-риску и завышают свои способности защититься от него, а также покрытие, предоставляемое полисами страхования от кибер-рисков. По сравнению с другими поддающимися страхованию рисками, кибер-риск недостаточно понятен, поэтому страховые компании закладывают в страховые премии дополнительную защиту, чтобы учесть неопределенность.

Системный риск

Сами эти третьи стороны могут стать объектом хакеров. И если на рынке есть всего несколько страхователей или поставщиков услуг кибербезопасности, эта концентрация может стать источником системного риска по всей финансовой системе.

Системный риск может также возникать в силу концентрации информационных технологий в финансовой системе, фирмы которой используют общие операционные системы и программы, облачные серверы и электронные сетевые узлы. Подключения через межбанковские рынки и рынки денежных переводов могут позволять шокам быстро распространяться по всей финансовой системе. Популярность полисов киберстрахования создала быстро растущий рынок, но продолжающееся накопление кибер-рисков в страховом секторе может само стать системным риском.

Государственный сектор, очевидно, должен заниматься обеспечением того, чтобы убытки, возникающие вследствие кибератак, не создавали системный риск.

Программа мер в сфере регулирования

Официальные органы стран должны создавать стимулы к обеспечению того, чтобы компании оперативно и точно сообщали о кибератаках, и чтобы данные об убытках систематически собирались. Поскольку кибератаки имеют криминальный характер, органы банковского регулирования должны быть в состоянии оперативно координировать свою работу с правозащитными органами. Крайне важно, чтобы органы регулирования имели возможность и полномочия быстро адаптировать свои ответные меры по мере эволюции киберугроз.

Для кибер-риска не существует географических границ, и создаваемая им угроза носит глобальный характер, поэтому международные организации играют здесь принципиально важную роль. Пришло время для правительств рассмотреть вопрос о принятии согласованных мер в ответ на системный кибер-риск. Международные структуры, такие как Совет по финансовой стабильности, и международные форумы, такие как Группа семи, возглавляют работу по распространению информации среди своих членов и укреплению координации деятельности между странами. Представляется, что они имеют все возможности для того, чтобы содействовать решению некоторых из вопросов информационного характера и международной координации, создаваемых системным кибер-риском.

*****

Эмануэль Копп — старший экономист в Отделе стран Северной Америки, занимающийся вопросами экономики США. До этого он был сотрудником Департамента денежно-кредитных систем и рынков капитала МВФ, где он работал над различными программами оценки финансового сектора (в том числе по Германии, Италии, Дании и Колумбии), а также над программой экономической корректировки для Португалии. В сферу исследовательских интересов г-на Коппа входят вопросы макрофинансового риска, финансовой стабильности и регулирования, инвестиций и макроэкономического прогнозирования. Он имеет степень магистра по финансам и степень доктора экономики от Венского экономического университета (Австрия).

Крис Уилсон — старший эксперт по финансовому сектору в *Департаменте денежно-кредитных систем и рынков капитала*. Он специализируется на банковском надзоре и регулировании в целом. Особый интерес для него представляют стандарты системы Базель-III в отношении ликвидности, и он выступал руководителем миссий технической помощи по этому вопросу. До МВФ он работал в Управлении пруденциального регулирования Австралии и Управлении финансовых услуг Соединенного Королевства в сфере банковского надзора и регулирования, в том числе надзора над крупнейшими банками и региональными банками. В последнее время он занимался вопросами введения системы Базель-III на национальном уровне. Он имеет

степень бакалавра по экономике и степень магистра в области политических наук и государственной политики Университета Маккуори и диплом о высшем образовании Института финансовых услуг Австралазии (FINSIA).

Линкольн Каффенбергер — специалист по информационной безопасности в МВФ. Он имеет более десяти лет опыта помощи различным организациям в понимании угроз, с которыми они сталкиваются, и принятии информированных, основанных на риске решений.