Секция «Риски и методы воздействия на риск»

Кибер-риски: измерение и регулирование

Научный руководитель – Котлобовский Игорь Борисович

Амангельдиев Низамиддин Берикулы
Студент (магистр)
Московский государственный университет имени М.В.Ломоносова, Экономический факультет, Москва, Россия
E-mail: nizami_kz@mail.ru

Финансовый сектор является одним из целевых секторов кибер-атак из-за его зависимости от информации и главной роли в процессе кредитных операций. Более того, ввиду нормативных требований, касающихся операционного риска, финансовые учреждения с большей вероятностью собирают данные о кибер - инцидентах, чем нефинансовые корпорации.

Кибер-риск появился как системный риск, связанный с недавними кибер-инцидентами. Исследования за 1 квартал 2017 год указывают на кибер-риски, как главную проблему среди участников рынка, занимающие первое место в Барометре системного риска, опубликованным The Depositary Trust & Clearing Corporation (DTCC), а также второе место в новом обзоре DTCC, выпущенным в декабре 2018 года [5]. Успешные кибер-атаки, такие как Wannacry в мае 2017 года или NotPetya в июне 2017 года, показали, что кибер-атака может привести к серьезным сбоям и потерям.

Кибер-риск можно определить как операционный риск для информационных и технологических активов, который характеризуется как имущественный, так и риск ответственности, а также катастрофический и операционный риски [1]. Потери от реализации кибер-риска часто бывают малыми и независимыми, но они также могут иметь низкую частоту и высокий уровень воздействия (blackout).

Кибер-атаки могут воздействовать на компании через три основных аспекта информационной безопасности: конфиденциальность, целостность или интеграция и доступность. Три типа кибер-атак оказывают различное прямое воздействие на цели: сбой в работе бизнеса не позволяет фирмам работать, что приводит к убыткам; мошенничество приводит к прямым финансовым потерям; влияние нарушений, связанных с данными, требует больше времени для фиксации, так как к данному типу относят репутационный эффект, а также расходы на судебные разбирательства.

Основываясь на открытых данных, страны с развитой экономикой являются основными объектами кибер-атак, но и развивающиеся страны также подвержены кибер-рискам. 80 % успешных атак приходится на развитые экономики, такие как США (39%) и Великобритания (7%). Среди развивающихся стран на БРИКС приходится большая часть атак (17%): Россия (6%), Китай (4%) и Индия (3 %). В целом финансовые учреждения более чем в 50 странах стали жертвами кибер-атак за последние несколько лет. Среди финансовых учреждений на долю банков приходится основная часть атак (91%), за которыми следуют страховые компании (7%) [3].

Оценка кибер-риска

Для анализа статистических свойств кибер-атак используются инструменты из актуарной математики. Используется логнормальное распределение для тела распределения и теория экстремальных значений для хвоста. Далее проводится оценка распределения и частоты потерь через такие инструменты как value at risk - VaR и expected shortfall - ES, которые отражают средние показатели ущерба

Меры риска показывают, сколько капитала необходимо фирме для покрытия убытков с помощью определённого уровня доверия. Во-вторых, агрегированные потери вычисляются с помощью моделирования методом Монте-Карло, предполагая, что частота каждого кибер-события следует распределению Пуассона. Предложенный метод, конечно, является приблизительным и поверхностным, однако в целом может показать масштабность кибер-рисков.

Регулирование

В 2011 году SEC опубликовал руководство по раскрытию кибер-рисков для компаний, зарегистрированных на бирже, которое было пересмотрено в 2018 году, для того чтобы предоставить дополнительную информацию о том, как и когда фирмы должны раскрывать информацию инвесторам. Например, среди 4000 годовых отчетов американских компаний («форма 10-K»), опубликованных в 2017 году, только 7 процентов включали информацию о кибер-рисках, главным образом в секторах финансов и услуг [4].

В Европейском союзе вступил в силу Общий регламент по защите данных ЕС в мае 2018 года, который требует от компаний сообщать о нарушениях компетентному надзорному органу в течение 72 часов. Несоблюдение требований к отчетности может привести к штрафам до 20 млн. евро или 4 % годового оборота компании на мировом рынке (в зависимости от того, что выше). Особенность данного регламента заключается в экстерриториальном принципе действия, что подразумевает действие данного регламента и на американские, и на российские компании, которые обслуживают потребителей ЕС [2].

В регулировании кибер-рисков необходимо выделить роль страховщиков, которые выполняют немаловажную роль в уменьшении ущерба от кибер-атак, и цифровые технологии, способствующие предотвращению кибер-угроз. Инцидент с Wannacry продемонстрировал, что, даже если существует надежный рынок перестрахования, крупномасштабная кибер-атака может обанкротить страховые компании и перестраховщиков. Кибер-защита возрастает в эффективности благодаря технологии блокчейна. Блокчейн предотвращает мошенничество и обнаруживает фальсификацию данных. Помимо шифрования данных и транзакций, блокчейн способствует децентрализации, что решает проблему с DDoS атаками. Хакеры, пытающиеся централизовать или взломать блокчейн, оповестят всю систему.

В заключении надо подчеркнуть, что кибер-риск представляет собой новую угрозу для всех типов финансовых учреждений, включая центральные банки, а также фирмы-финтех. Своевременное регулирование и реагирование и инвестиции в технологии информационной безопасности будут способствовать сокращению кибер-угроз.

Источники и литература

1) 1. Eling, M. and J. H. Wirfs “Cyber Risk: Too Big to Insure? Risk Transfer Options for a Mercurial Risk Class” // Institute of Insurance Economics, University of St. Gallen, 2016 [Электронный ресурс]. – Режим доступа: https://www.ivw.unisg.ch/∼/media/internet/content/dateien/instituteundcenters/ivw/studien/cyberrisk2016.pdf 2. General data protection regulation (GDPR) [Электронный ресурс]. – Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:43:FIN 3. International Monetary Fund Working paper [Электронный ресурс]. – Режим доступа: imf.org 4. Securities and Exchange Commission «Commission Statement and Guidance on Public Company Cybersecurity Disclosures» [Электронный ресурс]. – Режим доступа: https://www.sec.gov/rules/interp/2018/33-10459.pdf 5. Systematic Risk: Systematic Risk Barometer Surveys [Электронный ресурс]. – Режим доступа: http://www.dtcc.com/systemic-risk/systemic-risk-barometer-surveys