



Оценка кибер-риска для финансового сектора

[Кристин Лагард](#)

22 июня 2018 года



Потери финансовых организаций от кибератак в среднем могут составлять несколько сот миллиардов долларов в год (фото: EtiAmmos/iStock by Getty Images).

Кибер-риск стал серьезной угрозой для финансовой системы. В результате моделирования, проведенного персоналом МВФ, получены оценки, согласно которым потери финансовых организаций от кибератак в среднем могут составлять несколько сот миллиардов долларов в год, что уменьшает прибыль банков и потенциально угрожает финансовой стабильности.

Как показали последние случаи, эта угроза является реальной. Успешные атаки уже привели к утечкам данных, в результате которых воры получили доступ к конфиденциальной информации и совершили мошенничество, например, на бирже криптовалюты Coincheck было похищено 500 млн долларов. Существует

также опасность, что организация, являющаяся объектом атаки, окажется не в состоянии функционировать.

Неудивительно, что опросы регулярно демонстрируют, что риск-менеджеры и другие руководители финансовых организаций больше всего беспокоятся о кибератаках, как показано на графике ниже.

В опросах кибер-риск занимает первое место

Риск-менеджеры и другие финансовые руководители усматривают растущую угрозу кибератак, создающую большие риски, чем геополитические события и новые нормативные акты.

(В процентах респондентов)



Источник: Survey by Depository Trust & Clearing Corp., опубликовано как DTCC Systemic Risk Barometer 2017Q1.



Уязвимость финансового сектора

Финансовый сектор особенно уязвим по отношению к кибератакам. Финансовые организации являются привлекательными объектами из-за их важнейшей роли как посредников в движении денежных средств. Успешная кибератака на одну организацию может быстро распространиться через весьма взаимосвязанную финансовую систему. Многие организации все еще пользуются устаревшими системами, которые, возможно, не являются устойчивыми по отношению к кибератакам. Успешная кибератака может иметь прямые существенные

последствия в виде финансовых убытков, а также косвенных издержек, таких как ухудшение репутации.

Недавние широко известные случаи все чаще приводят к тому, что кибер-риск включается в повестку дня официального сектора, в том числе [международных организаций](#). Однако количественный анализ кибер-риска все еще находится на ранней стадии, особенно из-за отсутствия данных о потерях от кибератак и трудностей моделирования кибер-риска.

[Недавнее исследование МВФ](#) создает основу для анализа возможных потерь от кибератак с упором на финансовый сектор.

Оценка потенциальных убытков

В основе моделирования применяются методы актуарной науки и оценки операционного риска для расчета совокупных убытков от кибератак. Это требует оценки частоты кибератак на финансовые организации и представления о распределении убытков от таких событий. Числовое моделирование затем может быть использовано для расчета распределения совокупных убытков от кибератак.

Для иллюстрации нашей основы мы используем набор данных, охватывающих недавние убытки от кибератак в 50 странах. Это служит примером того, как можно рассчитать потенциальные убытки для финансовых организаций. Эта процедура является сложной, ее дополнительно затрудняют серьезные недостатки данных о кибер-риске. Кроме того, к счастью, пока еще не было успешной крупномасштабной кибератаки на финансовую систему.

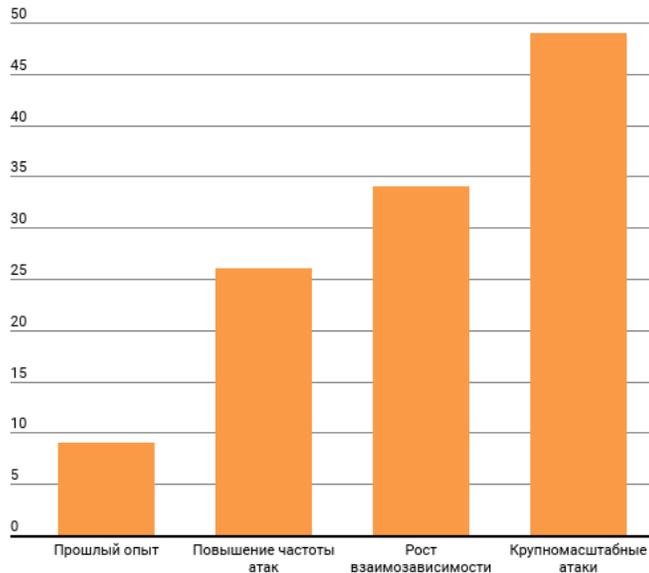
Поэтому наши результаты следует рассматривать как иллюстративные. Если считать их верными, они указывают на то, что годовые потенциальные убытки от кибератак могут быть значительными и приближаться к 9 процентам чистого дохода банков или составлять примерно 100 млрд долларов. При крайне неблагоприятном сценарии (когда частота кибератак будет в два раза выше, чем раньше, и при более широком распространении последствий) убытки могут быть в 2½–3½ раза больше или достичь 270–350 млрд долларов.

Эта основа может использоваться для изучения сценариев с более серьезным риском, предусматривающих массированные атаки. Распределение собранных нами данных означает, что в таких сценариях, составляющих 5 процентов наихудших случаев, средние потенциальные убытки могут достичь даже половины чистого дохода банков, что создаст угрозу для финансового сектора.

Возможные последствия для прибыли банков

Финансовые организации во всем мире могут понести убытки от кибератак в диапазоне от 9% чистого дохода (на основе имеющегося опыта) до половины прибыли (при крайне неблагоприятном сценарии).

(В процентах чистого дохода)



Источник: оценки персонала МВФ.



Такие оценки убытков на несколько порядков превышают текущий размер рынка страхования от кибер-рисков. Несмотря на рост в последнее время, страховой рынок защиты от кибер-рисков остается небольшим, в 2017 году величина премий составляла около 3 млрд долларов. Большинство финансовых организаций даже не имеет страховки от кибер-рисков. Покрытие является ограниченным, и страховщики испытывают трудности с оценкой риска в силу неопределенности подверженности киберугрозам, недостаточности данных и возможной цепной реакции.

Дальнейшие действия

Имеются значительные возможности для совершенствования оценок рисков. Сбор государственными органами более детальных, последовательных и полных данных о частоте и последствиях кибератак поможет оценить риск для финансового сектора. Требования сообщать об утечках данных (например, рассматриваемые в рамках Общего регламента ЕС о защите данных) должны

привести к улучшению информированности о кибератаках. Анализ сценариев может использоваться для всесторонней оценки возможных путей распространения кибератак и разработки достаточных ответных мер со стороны частных организаций и государственных органов.

Требуется также продолжить работу для понимания того, как повысить устойчивость финансовых организаций и инфраструктуры, как в целях уменьшения шансов успешной кибератаки, так и в целях содействия плавному и быстрому восстановлению работы. Во многих регионах мира необходимо также развивать потенциал официального сектора для мониторинга и регулирования таких рисков.

В целом, требуется усиление систем регулирования и надзора для защиты от кибер-рисков, принимаемые меры должны быть сосредоточены на действенной практике надзора, реалистичной проверке уязвимости и восстановления и планировании на случай непредвиденных обстоятельств. МВФ оказывает государствам-членам техническую помощь для совершенствования их систем регулирования и надзора.



Кристин Лагард — директор-распорядитель Международного Валютного Фонда. После завершения первого пятилетнего срока на этом посту в июле 2016 года она получила назначение на второй срок. Г-жа Лагард — гражданка Франции, в прошлом министр финансов Франции с июня 2007 года по июль 2011 года, она также занимала должность государственного министра внешней торговли Франции в течение двух лет.

Г-жа Лагард также имела продолжительную и примечательную карьеру юриста по антимонопольным и трудовым вопросам и была партнером в международной юридической фирме Baker & McKenzie, где в октябре 1999 года была избрана председателем. Она занимала высшую должность в этой фирме до июня 2005 года, когда была назначена на свою первую должность министра во Франции. Г-жа Лагард имеет ученые степени из Института политических наук и юридического факультета в Университете Париж X, где она также читала лекции до перехода на работу в Baker & McKenzie в 1981 году.

Более полную биографию читайте [здесь](#).

Ссылки по теме:

[Киберзащита должна иметь глобальный характер](#)