ГЛОБАЛЬНАЯ КИБЕРУГРОЗА

Число киберугроз финансовой системе растет, и мировое сообщество должно сотрудничать, чтобы защитить ее

Тим Маурер и Артур Нельсон

В феврале 2016 года хакеры атаковали центральный банк Бангладеш и, воспользовавшись уязвимыми местами основной системы сообщений об электронных платежах СВИФТ глобальной финансовой системы, пытались украсть 1 млрд долларов. И хотя большинство операций было заблокировано, 101 млн долларов все равно исчез. Это ограбление стало сигналом тревоги для мира финансов, что системные киберриски, существующие в финансовой системе, сильно недооценивались.

Сегодня оценка, согласно которой крупная кибератака представляет угрозу финансовой стабильности, является аксиомой и вопросом не того, *будет ли*, а того, *когда* будет предпринята такая атака. Однако правительства стран и компании во всем мире по-прежнему испытывают трудности со сдерживанием этой угрозы, поскольку остается неясно, кто является ответственным за защиту системы. Все более обеспокоенные ключевые голоса бьют тревогу. В феврале 2020 года председатель Европейского центрального банка и бывший руководитель Международного валютного фонда Кристин Лагард

Оценка, согласно которой крупная кибератака представляет угрозу финансовой стабильности, является аксиомой и вопросом не того, будет ли, а того, *когда* будет предпринята такая атака.

выступила с предостережением о том, что кибератака может спровоцировать серьезный финансовый кризис. В апреле 2020 года Совет по финансовой стабильности (СФС) предостерегал о том, что «крупный киберинцидент, если он не будет надлежащим образом сдержан, может серьезно нарушить функционирование финансовых систем, в том числе критически важной финансовой инфраструктуры, и повлечь за собой более масштабные последствия для финансовой стабильности». Потенциальные экономические издержки, связанные с такими событиями, могут быть огромными, а ущерб, причиненный доверию и уверенности общественности, — значительным.

Этот риск усугубляется двумя продолжающимися тенденциями. Во-первых, глобальная финансовая система претерпевает беспрецедентные цифровые преобразования, которые ускоряются пандемией COVID-19. Банки конкурируют с компаниями отрасли информационных технологий (ИТ), компании отрасли ИТ конкурируют с банками. В то же время пандемия увеличила спрос на финансовые услуги в режиме онлайн и сделала удаленную работу нормой. Центральные банки стран во всем мире рассматривают поддержку своим авторитетом цифровых валют и модернизацию платежных систем. В этот период преобразований, когда один инцидент может легко подорвать доверие и свести на нет такие инновации, кибербезопасность важна как никогда.

Во-вторых, злоумышленники используют этот процесс цифровых преобразований и представляют все большую угрозу глобальной финансовой системе, финансовой стабильности и уверенности в целостности системы. Пандемия даже предоставила хакерам новые мишени. Согласно данным Банка международных расчетов, финансовый сектор подвергается второй по величине доле кибератак, связанных с COVID-19, уступая только сфере здравоохранения.

Кто стоит за этой угрозой?

В будущем следует ожидать более опасных атак и вызванных ими потрясений. Наибольшее беспокойство вызывают инциденты, нарушающие целостность финансовых данных, например, учетных записей, алгоритмов и операций; в настоящее время существует мало технических решений в случае таких атак, которые способны подорвать доверие и уверенность в более широком плане. В число злоумышленников, стоящих за этим атаками, входят не только все более дерзкие преступники, такие как группа Carbanak, которая в 2013–2018 годы, атаковав финансовые организации, похитила более 1 млрд долларов, но и государства, а также злоумышленники, спонсируемые государствами (см. таблицу). Например, Северная Корея за последние пять лет похитила примерно 2 млрд долларов по крайней мере в 38 странах.

Это глобальная проблема. Если кибератаки в странах с высокими доходами, как правило, широко освещаются в средствах массовой информации, растущему числу атак на более легкие мишени в странах с низкими доходами и доходами ниже средних уделяется меньше внимания. Однако именно в этих странах наиболее выражено стремление обеспечить более широкий доступ к финансовым услугам, в связи с чем многие страны осуществляют быстрый переход к цифровым финансовым услугам, таким как мобильные платежные системы. Цифровые финансовые услуги действительно способствуют финансовой интеграции, но при этом создают среду с множеством мишеней для хакеров. Например, совершенный октябре 2020 года взлом крупнейших сетей мобильных банковских услуг MTN и Airtel в Уганде привел к серьезной дезорганизации операций этих сервисов, длившейся четыре дня.

Более детально о кибератаках

В число злоумышленников, которые стоят за этими инцидентами, входят не только все более дерзкие преступники, но и государства и группы, спонсируемые государствами, имеющие различные цели и побуждения.

ЗЛОУМЫШЛЕННИК	ПОБУЖДЕНИЯ	ЦЕЛИ	ПРИМЕРЫ
 **Государства, группы, спонсируемые государствами**	Геополитические, идеологические	Дестабилизация, разрушение, причинение ущерба, кража, шпионаж, финансовая выгода	Необратимое нарушение целостности данных, целенаправленное физическое повреждение, нарушение функционирования энергетической системы, дезорганизация платежной системы, мошеннические трансферты, шпионаж
 **Киберпреступники**	Обогащение	Кража/ финансовая выгода	Кража денежных средств, мошеннические трансферты, кража учетных данных
 **Террористические группы, хактивисты, инсайдерские угрозы**	Идеологические, недовольство	Дестабилизация	Утечки, клевета, распределенные атаки типа «отказ в обслуживании»

Источник: European Systemic Risk Board. 2020. "Systemic Cyber Risk." https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

ИЛЛЮСТРАЦИЯ: ISTOCK / YOUR_PHOTO

Если не будут приняты специальные меры, глобальная финансовая система будет становиться все более уязвимой в условиях, когда инновации, конкуренция и пандемия будут далее стимулировать цифровую революцию.

Пробел в сфере ответственности

Невзирая на то, что цифровая инфраструктура все шире используется в глобальной финансовой системе, неясно, кто является ответственным за защиту этой системы от кибератак. Отчасти это обусловлено быстро меняющимися условиями. Если не будут приняты специальные меры, глобальная финансовая система будет становиться все более уязвимой в условиях, когда инновации, конкуренция и пандемия будут далее стимулировать цифровую революцию. Многие злоумышленники сосредоточены на получении денег, но при этом растет число сугубо дестабилизирующих и разрушающих атак; кроме того, те, кто умеют совершать кражи, также узнают о сети и операциях финансовой системы, что позволяет им в дальнейшем предпринимать более дестабилизирующие и разрушительные атаки (или продавать эти знания и возможности другим). Эта быстрая эволюция ландшафта рисков ослабляет способность принимать ответные меры в остальном зрелой и хорошо регулируемой системы.

Повышение уровня защиты глобальной финансовой системы является в основном организационной задачей. Усилия по укреплению средств защиты и ужесточению регулирования имеют важное значение, но этого недостаточно, чтобы опередить возрастающие риски. В отличие от многих секторов, бóльшая часть сообщества сферы финансовых услуг не испытывает нехватки ресурсов или возможностей для внедрения технических решений. Главным вопросом является проблема коллективных действий: каков оптимальный способ организовать защиту системы в правительствах стран, органах финансового регулирования и отрасли, и каким образом обеспечить действенное и эффективное использование этих ресурсов.

Нынешняя фрагментация заинтересованных сторон и инициатив отчасти обусловлена особыми аспектами и меняющимся характером киберриска. Разные сообщества действуют разрозненно и решают эту проблему посредством своих соответствующих мандатов. Сообщество органов финансового надзора сосредоточено на устойчивости, дипломатов — на нормах поведения государства, ведомств по национальной безопасности — на попытках сдерживания злонамеренной деятельности, руководства отрасли — на рисках, специфических для компаний, а не этого сектора. По мере того как границы между компаниями сферы финансовых услуг и фирмами отрасли ИТ будут становиться все более нечеткими, границы ответственности за безопасность также будут становиться все более размытыми.

Наиболее значительно проявляется несоответствие между финансовым сектором, сферой национальной безопасности и дипломатическим сообществом. Органы финансового регулирования сталкиваются с особыми рисками, связанными с киберугрозами, однако их отношения с ведомствами по национальной безопасности, которые должны быть задействованы для эффективного преодоления этих угроз, остаются слабыми. Этот разрыв ответственности и сохраняющаяся неопределенность относительно функций и мандатов по защите глобальной финансовой системы повышают риски. Такая неопределенность отчасти обусловлена нынешним геополитическим климатом и высокими уровнями недоверия, что препятствует взаимодействию международного сообщества. Сотрудничество в области кибербезопасности затруднено, фрагментировано и часто ограничивается самыми узкими кругами доверия, поскольку затрагивает чувствительные вопросы равенства в сфере национальной безопасности. Международное сотрудничество с участием многих заинтересованных сторон не плюс, а необходимость.

Международная стратегия

Для достижения более действенной защиты глобальной финансовой системы от киберугроз Фонд Карнеги за международный мир в ноябре 2020 года опубликовал доклад под названием «International Strategy to Better Protect the Global Financial System against Cyber Threats» («Международная стратегия повышения уровня защиты глобальной финансовой системы от киберугроз»). В этом докладе, подготовленном в сотрудничестве со Всемирным экономическим форумом, рекомендуются конкретные меры по уменьшению фрагментации путем содействия более тесному взаимодействию как на международном уровне, так и между государственными ведомствами, финансовыми компаниями и фирмами отрасли ИТ.

Стратегия основывается на четырех принципах: во-первых, *необходимо повысить ясность относительно функций и ответственности*. Лишь в небольшом числе стран налажены действенные внутренние взаимосвязи между органами финансового регулирования, правоохранительными органами, дипломатами, другими соответствующими государственными субъектами и отраслью. Существующая фрагментация затрудняет международное сотрудничество и ослабляет коллективную устойчивость международной системы, а также ее возможности восстановления и реагирования.

Во-вторых, *настоятельно и срочно требуется международное сотрудничество*. Ввиду масштаба угрозы и взаимозависимого характера системы на глобальном уровне правительства отдельных стран, финансовые компании и фирмы отрасли ИТ, работая поодиночке, не могут обеспечить действенную защиту от киберугроз.

В-третьих, *уменьшение фрагментации поможет высвободить возможности для решения проблемы*. Реализуется много инициатив для повышения уровня защиты финансовых организаций, но эти инициативы остаются разрозненными. Некоторые из этих усилий дублируют друг друга, что увеличивает транзакционные издержки. Несколько из этих инициатив являются достаточно зрелыми для того, чтобы обмениваться ими, эффективнее координировать их и далее их интернационализировать.

В-четвертых, *защита международной финансовой системы может быть моделью для других секторов*. Финансовая система является одной из немногих сфер, в которой страны однозначно заинтересованы сотрудничать даже в условиях повышенной геополитической напряженности. Сосредоточение внимания на финансовом секторе служит отправным пунктом и может проложить путь для повышения в будущем уровня защиты других отраслей.

В числе мер по повышению киберустойчивости в докладе рекомендуется, чтобы СФС разработал базовую основу для надзора за управлением киберрисками в финансовых организациях. Правительства стран и отрасль должны укреплять безопасность путем обмена информацией об угрозах и создания групп реагирования на чрезвычайные ситуации, связанные с компьютерными системами, в сфере финансов (CERT) по образцу существующей в Израиле группы FinCERT.

Наряду с этим органам финансового регулирования следует устанавливать приоритетность повышения устойчивости финансового сектора к атакам на данные и алгоритмы. Это должно включать перенос защищенных, зашифрованных данных в резервные хранилища, что позволяет членам в течение ночи выполнять безопасное резервное копирование данных счетов клиентов. Следует регулярно проводить имитационное моделирование кибератак для определения слабых сторон и разработки планов действий.

Для усиления международных норм в докладе рекомендуется, чтобы правительства стран разъяснили, как они будут применять международное право к киберпространству и укреплять нормы по защите целостности финансовой системы. Первый шаг уже сделали правительства Австралии, Нидерландов и Соединенного Королевства, заявившие о том, что кибератаки из-за рубежа могут считаться незаконным применением силы или вмешательством во внутренние дела другого государства.

Киберустойчивость и более прочные международные нормы могут способствовать принятию коллективных ответных мер посредством правоохранительной деятельности и многостороннего реагирования отрасли. Ответные меры могут включать санкции, аресты, конфискацию активов.

Правительства стран могут содействовать этим усилиям путем создания организаций, помогающих оценивать угрозы и координировать ответные меры. Сбор разведывательных данных должен быть сосредоточен в том числе на угрозах в отношении финансовой системы, причем правительствам стран следует обмениваться этими данными с союзниками и государствами-единомышленниками.

Развитие потенциала

Изложенная в докладе Фонда Карнеги комплексная стратегия, в свою очередь, зависит от наращивания рабочей силы в сфере кибербезопасности, укрепления потенциала в области кибербезопасности в финансовом секторе и обеспечения сохранения достигнутого в процессе финансовой интеграции вследствие цифровых преобразований.

Возросшие вследствие пандемии уровни безработицы открывают важные возможности для подготовки и найма высококвалифицированных сотрудников с целью укрепить рабочую силу в сфере кибербезопасности. Компании отрасли финансовых услуг должны инвестировать в инициативы по подготовке талантливых кадров, в том числе в программах старших классов средней школы, профессиональной подготовки и университетов.

Наращивать потенциал в области кибербезопасности означает сосредоточиться на оказании помощи в случаях, когда она необходима. МВФ и другие международные организации получали много обращений государств-членов с просьбами об оказании содействия в области кибербезопасности, особенно после инцидента, имевшего место в 2016 году в Бангладеш. Правительства и центральные банки стран Группы 20-ти могли бы создать международный механизм для наращивания потенциала в области кибербезопасности финансового сектора при координации этих усилий назначенной международной организацией, такой как МВФ. Организация экономического сотрудничества и развития и международные финансовые организации должны сделать укрепление потенциала в области кибербезопасности одним из элементов пакетов помощи на цели развития и значительно увеличить объем помощи нуждающимся в ней странам.

Наконец, чтобы сохранить успехи, достигнутые в процессе финансовой интеграции, необходимо укреплять связи между финансовой интеграцией и кибербезопасностью. Эта задача является особенно неотложной в Африке в условиях, когда многие страны этого континента претерпевают серьезные преобразования в финансовом секторе вследствие расширения доступа к финансовым услугам и перехода к цифровым финансовым услугам. Должна быть создана сеть экспертов, которая сосредоточится специально на кибербезопасности в Африке.

Настало время международному сообществу, в частности, правительствам стран, центральным банкам, органам надзора, отрасли и другим соответствующим сторонам, сообща решать эту неотложную и важную задачу. Продуманная стратегия, подобная вышеуказанной, обеспечивает программу, которая поможет перейти от слов к действиям. ФР

ТИМ МАУРЕР — директор Инициативы по киберполитике, старший научный сотрудник Программы по информационным технологиям и международным вопросам Фонда Карнеги за международный мир. **АРТУР НЕЛЬСОН** — аналитик-исследователь Инициативы по киберполитике Фонда Карнеги.