CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

О СОЗДАНИИ МЕЖДУНАРОДНО-ПРАВОВОЙ НОРМЫ В ЦЕЛЯХ ЗАЩИТЫ ОТ ДЕСТРУКТИВНОГО ВОЗДЕЙСТВИЯ НА ЦЕЛОСТНОСТЬ ФИНАНСОВЫХ ДАННЫХ

ТИМ МАУРЕР, АРИЭЛЬ (ЭЛИ) ЛЕВИТ И ДЖОРДЖ ПЕРКОВИЧ

ВВЕДЕНИЕ

18 марта 2017 года министры финансов и управляющие центральными банками двадцати ведущих экономик мира — «Большой двадцатки» (G20) — выпустили коммюнике, в котором подчеркнули:

> «Злонамеренное применение и использование информационных и коммуникационных технологий (ИКТ) может нарушить процесс оказания финансовых услуг, критически важных для национальных и международных финансовых систем, подорвать доверие к этим системам и их безопасность, а также поставить под угрозу финансовую стабильность. Мы будем содействовать повышению надежности финансовых услуг и усилению способности финансовых институтов в странах „Большой двадцатки“ противостоять злонамеренному применению ИКТ, в том числе со стороны государств, не входящих в G20. В целях укрепления нашего международного сотрудничества мы, в качестве первого шага, призываем Совет по финансовой стабильности проанализировать практику банковского надзора и регулирования в наших юрисдикциях, а также международные инструкции, для того, чтобы выявить эффективные подходы. Совет по финансовой стабильности должен подготовить информацию о своей деятельности в этой области к саммиту лидеров стран „Большой двадцатки“, который состоится в июле 2017 года, и представить полный отчет к октябрю 2017 года»[1].

Необходимо выразить признательность министрам финансов и управляющим центральными банками стран «Большой двадцатки» за то, что они призывают к повышению устойчивости мировой финансовой системы. Однако правительства не должны ограничиваться обращениями к частному сектору с просьбой умножить усилия; они сами способны содействовать уменьшению потенциальной опасности, угрожающей финансовому сектору. Лидеры «Большой двадцатки» могли бы от имени своих стран принять недвусмысленное обязательство отказаться от использования агрессивных кибернетических методов для нанесения удара по целостности данных в финансовой системе. Они также могли бы пообещать, что будут сотрудничать в случае, если подобные кибератаки произойдут.

Финансовый кризис 2007 года показал, как сильно глобальная финансовая система нуждается во взаимном доверии и насколько уязвимой и хрупкой она может быть. Проникновение в информационную систему Центрального банка Бангладеш в 2016 году высветило новую угрозу финансовой стабильности и беспрецедентный масштаб риска для финансовых институтов в случае предумышленных хакерских атак[2]. Использование кибероперацій для нарушения целостности данных чревато не только похищением денежных средств и данных

ОБ АВТОРАХ

Тим Маурер — *один из руководителей программы «Инициатива в области киберполитики» Фонда Карнеги за Международный Мир. Исследует проблемы киберпространства в контексте международных отношений, включая вопросы кибербезопасности, прав человека во Всемирной сети и управления интернетом.*

Ариель (Эли) Левит — *внештатный старший научный сотрудник программы «Ядерная политика» Фонда Карнеги. В 2002–2007 годах занимал должность первого заместителя генерального директора по вопросам политики в Комиссии по атомной энергии Израиля.*

Джордж Перкович — *вице-президент по науке в Фонде Карнеги за Международный Мир. Основные направления его исследований: ядерная стратегия и нераспространение ядерного оружия; киберконфликты; новые подходы к государственно-частному сотрудничеству в сфере управления технологиями стратегического значения.*

— оно создает больше очевидных системных рисков, чем любые иные формы финансового давления. Комплексный и взаимозависимый характер финансовых систем, действие которых распространяется дальше физических или национальных границ, означает, что специальное или нецеленаправленное деструктивное воздействие на данные финансовых учреждений может поставить под угрозу финансовую стабильность и устойчивость всей международной системы. Важно отметить, что в отличие от того, что наблюдалось во время мирового экономического кризиса 2007–2008 годов, этот риск существует вне зависимости от фундаментальных экономических факторов и он будет только нарастать по мере того, как все большее число стран принимают твердое решение перейти к экономике, основанной на безналичных расчетах[3].

В 2015 году Группа правительственных экспертов ООН (UNGGE) по международной информационной безопасности и стран «Большой двадцатки» уже предлагала рассмотреть всеобъемлющие принципы противодействия нападениям на жизненно-важные гражданские объекты инфраструктуры в мирное время. В сегодняшних условиях министры финансов и управляющие центральными банками «Большой двадцатки» выделили актуальность угроз финансовой стабильности. В связи с этим в этой публикации мы предлагаем такие рекомендации: используя существующие договоренности и соглашения как фундамент для их сотрудничества, главы государств обязывались не нарушать целостность данных и алгоритмы финансовых институтов в мирное и военное время[4] и не позволяли делать это[5] своим гражданам.

Мы предлагаем включить в текст такого соглашения следующие формулировки и, разумеется, приглашаем заинтересованных лиц к обсуждению и внесению уточнений:

> «Ни одно государство не должно осуществлять, или сознательно поддерживать любые действия, которые предполагают целенаправленное воздействие на целостность данных и алгоритмов финансовых институтов в любом месте, где бы они ни хранились, или в процессе транзитной передачи.
>
> В случаях, установленных законодательством, государство обязуется безотлагательно отвечать на запросы другого государства для того, чтобы можно было воспрепятствовать действиям, совершенным с целью повлиять на целостность данных и алгоритмов финансовых институтов, в тех случаях, когда такие действия осуществляются, или инициируются на территории этого государства, или совершаются его гражданами».

Государства уже продемонстрировали значительную сдержанность в применении информационных и коммуникационных технологий для получения несанкционированного доступа к данным финансовых институтов. Поэтому такое соглашение позволило бы конкретно и недвусмысленно определить, что именно может рассматриваться, как формирующаяся государственная практика. Четкое определение могло бы:

- стать ясным сигналом того, что стабильность мировой финансовой системы зависит от обеспечения целостности финансовых данных в мирное и военное время и, что международное сообщество расценивает посягательство на эти данные как незаконное;
- укрепить доверие между государствами, уже проявляющими умеренность в этой области, и тем самым, дать им дополнительные возможности для эффективной мобилизации международного сообщества в случае нарушения указанного принципа;
- придать политический импульс более активному расширению сотрудничества в области противодействия негосударственным субъектам, использующим ИКТ для подрыва деятельности финансовых учреждений;
- дополнить и сделать более действенными существующие договоренности и усилия, а именно: заявление лидеров «Большой двадцатки» в 2015 году, отчет Группы правительственных экспертов ООН (UNGGE) от 2016-м и инструкции по кибербезопасности, разработанные Комитетом по платежным системам и рыночным инфраструктурам и Международной организацией комиссий по ценным бумагам (CPMI — IOSCO).

Хотя в коммюнике министров финансов и управляющих центральными банками стран «Большой двадцатки», опубликованном 18 марта, отсутствует определение «злонамеренного применения и использования информационных

и коммуникационных технологий (ИКТ)», вполне разумно полагать, что в этом документе особое внимание уделено целостности и доступности финансовых данных. Дело в том, что правоохранительные и разведывательные органы неизбежно и отнюдь не со злым умыслом могут нарушать конфиденциальность информации банков и прочих финансовых учреждений в целях борьбы с терроризмом, распространением оружия и преступностью. В этой публикации объясняется, почему для обеспечения стабильности системы международных отношений, столь важно установить запрет на повреждение данных в глобальной финансовой системе и закрепить это как норму.

Государства, как ожидается, будут выполнять эти обязательства в соответствии с ограничениями и требованиями национальных и международного законодательств, каждое из которых может в конечном итоге быть скорректировано так, чтобы отразить суть предложенных здесь норм. Кроме того, предполагается, что государства будут использовать существующие инструкции и передовую практику, такие как вышеупомянутые инструкции по кибербезопасности, разработанные CPMI и IOSCO[6].

В настоящее время у глав государств «Большой двадцатки» есть возможность принять эти обязательства и обратиться к Совету по финансовой стабильности с просьбой обеспечить их последовательное выполнение вместе с органами, которые устанавливают стандарты, организациями частного сектора, правоохранительными структурами и Группой реагирования на компьютерные чрезвычайные происшествия (CERT). Такое решение могло бы опираться на прецедент, созданный в 2015 году, когда «Большая двадцатка» решила включить вопросы кибербезопасности в совместное коммюнике руководителей стран-участниц, а также на прецедент, относящийся к действиям G20 после финансового кризиса 2007-го; также можно сослаться и на коммюнике министров финансов и управляющих центральными банками стран «Большой двадцатки».

КРАТКИЙ ОБЗОР СИТУАЦИИ

В 2015 году Группа правительственных экспертов ООН, включающая представителей пяти постоянных членов Совета Безопасности ООН, отметила в своем согласованном докладе следующее: «Государство не может осуществлять или сознательно поддерживать деятельность в области информационных и коммуникационных технологий, которая противоречит его обязательствам в рамках международного права и которая целенаправленно нарушает работу ключевых инфраструктур или иным образом мешает использованию или функционированию ключевых инфраструктур, обслуживающих население»[7].

Несколько позднее эта декларация была одобрена высшими руководителями государств на саммите «Большой двадцатки»[8]. Политические заявления такого рода можно только приветствовать. Тем не менее, исторический опыт показывает, что главы государств зачастую дают несбыточные обещания и позднее не выполняют их. Одна из проблем связана с неоднозначностью понятий: государства могут по-разному понимать, что такое «ключевая инфраструктура». При этом, все больше экспертов выражают скептицизм относительно эффективности процесса, инициированного Группой правительственных экспертов ООН[9]. Кроме того, формулировки, разработанные UNGGE, в основном касаются результатов кибератак и игнорируют конкретный контекст — мировую финансовую систему с ее высокой степенью взаимозависимости. Поэтому будет полезным подготовить более подробное соглашение, в котором формулировки и термины были бы уточнены и разъяснены в свете специфических операций, способных оказать разрушительное воздействие на международную систему.

Финансовая система представляет собой особенно перспективное направление такой работы, учитывая наличие общих интересов у большей части государств. Эта система отличается от большинства прочих видов ключевой инфраструктуры, например, транспорта или энергосетей, поскольку она характеризуется глобальным уровнем взаимозависимости. Ведущие державы признают это по существу и на деле, несмотря на фундаментальные разногласия. Согласно имеющимся сведениям, правительство США воздержалось от использования кибератак против финансовой системы Саддама Хуссейна, а также при проведении военных учений, имитирующих гипотетический конфликт с Китаем[10]. В предложенном Россией в 2011 году проекте конвенции ООН «Об обеспечении международной информационной

безопасности» четко говорится: «Каждое государство-участник принимает необходимые меры для обеспечения невмешательства в деятельность международных информационных систем управления... финансовыми потоками»[11]. Китай также заинтересован в этой системе — достаточно упомянуть его успешную деятельность, направленную на включение юаня в корзину мировых резервных валют Международного валютного фонда[12]. В тоже время, страны по всему миру создают или укрепляют существующие группы, в обязанности которых входит реагировать на компьютерные чрезвычайные происшествия в финансовом секторе. Индия, которая создала такую группу в феврале 2017 года[13], — один из примеров этого.

Глобальная взаимозависимость делает финансовый сектор более уязвимым, чем прочие ключевые инфраструктуры, и при этом порождает общую заинтересованность разных стран в защите этого сектора. Разрушительный эффект несанкционированного вмешательства в работу объектов электро-энергетической инфраструктуры, или предприятий нефтегазового сектора будет в основном ограничен территорией одной страны, или её стран-соседей. Однако географический фактор отнюдь не всегда помогает сдержать распространение последствий удара по целостности и безопасности данных финансового учреждения. Результаты такого вмешательства очень трудно понять и, следовательно, предусмотреть и предсказать. Деструктивное воздействие на систему обработки платежных поручений способно напрямую сорвать сделку. Последствия повреждения данных финансового учреждения могут косвенным образом привести к его банкротству, и, как результат, произвести международный кризис. Например, банкротство Lehman Brothers в 2008 году создало неожиданный «домино» эффект, который продемонстрировал, что банкротство даже одного финансового учреждения может значительно повлиять на другие финансовые учреждения. Азиатский финансовый кризис 1997-го года, обусловлен обвалом таиландской валюты, создал такой же эффект в масштабе всего региона. Такие «эффекты второго порядка» весьма сложно прогнозировать. Более того, даже организаторы атаки порой не включают их в оценку характера и степени ущерба.

Международный опыт в сфере борьбы с изготовлением фальшивых денег может оказаться весьма полезным. Государства соблюдают договоренность о запрете фальшивомонетничества и содействуют ее выполнению, так как осознают взаимную уязвимость перед лицом этой опасности. И поскольку запрет действует во многих государствах, страны-нарушительницы, скорее всего, будут призваны к ответу. Разумеется, негосударственные субъекты в ряде случаев продолжают подделывать валюту (например, в Северной Корее и нескольких других странах), однако эта практика достаточно ограниченна и не угрожает стабильности международной финансовой системы[14].

Еще одна историческая аналогия показывает, почему крупные экономические державы, по крайней мере такие, как страны «Большой двадцатки», заинтересованы в утверждении и соблюдении специальных норм, направленных на борьбу с деструктивным воздействием на финансовые данные в мирное и военное время. В 1914 году правительство Великобритании, пользуясь своим доминирующим положением в мировой торговле и финансовой системе, начало экономическую войну против Германии. Великобритании удалось серьезно разладить мировую экономику, однако уже через три месяца Лондон отринул эту стратегию. Ее негативные последствия проявились гораздо более интенсивно и быстрее, чем ожидалось, и среди прочего включали в себя протесты британских предпринимателей, рабочего класса и политических деятелей, а также давление со стороны союзников[15]. Высокий уровень международной экономической интеграции не позволил Великобритании избежать неблагоприятной реакции на экономическую войну против Германии.

Разумеется, в XXI веке лишь некоторые страны, относительно обособленные от мировой экономики, и негосударственные субъекты, которые могут быть или не быть связаны с ними, имеют потенциальные возможности для кибератак на финансовые учреждения. Разумеется, представители такого рода деструктивных сил не будут соблюдать предложенные выше обязательства. Однако государства, однозначно поддержавшие эти нормы, станут более сплоченными, у них появятся основания для того, чтобы требовать и принимать ответные меры в отношении нарушителей, будь то государства, террористы или киберпреступники, и их выгода от этих действий станет более очевидной. Иными словами, предложенное четко сформулированное соглашение могло бы стать основой для разработки коллективных действий

против любых злоумышленников. (Некоторые государства, заявившие о своей приверженности соглашению, могут не удержаться от соблазна проявить терпимость к частным посредникам или прочим агентам и использовать их для атак на финансовые учреждения. Однако и в этом случае наличие соглашения даст дополнительные возможности и рычаги, которые могут быть использованы для давления на режимы, в которых присутствуют преступные намерения.)

ОСНОВА СОГЛАШЕНИЯ — СУЩЕСТВУЮЩИЕ ПРАВОВЫЕ НОРМЫ И МЕЖДУНАРОДНОЕ ЗАКОНОДАТЕЛЬСТВО

Четко сформулированное соглашение о предотвращении действий, направленных на подрыв целостности данных финансовых учреждений, может базироваться на результатах недавно предпринятых международных усилий по разработке правил поведения в киберпространстве и на основополагающих нормах международного права, которые применяются против изготовителей фальшивых денег. Кроме того, такие соглашения помогут заполнить пробел в праве вооруженных конфликтов (также известном как международное гуманитарное право).

На сегодняшний день самое важное достижение международного сообщества в деле разработки «правил игры» в киберпространстве — процесс, инициированный Группой правительственных экспертов ООН и одобренный главами стран «Большой двадцатки» в 2015 году.

Однако, во-первых, в декларации 2015 года и в заявлении о ее поддержке руководителей государств — членов G20 не оговариваются детали и конкретные шаги, позволяющие превратить эти документы в эффективный и надежный инструмент обеспечения режима безопасности. Во-вторых, амбициозные формулировки UNGGE могут быть применены в мирное, но не в военное время и не могут дополнить действующее международное гуманитарное право. Кроме того, в декларации существует пробел в том, что касается специфических случаев кибератак на финансовые учреждения.

Деструктивное воздействие на целостность финансовых данных во многом аналогично изготовлению фальшивой валюты. В связи с этим Международная конвенция по борьбе с подделкой денежных знаков, принятая в 1929 году, может служить правовой базой для дальнейших шагов[16]. В 2004-м году Франсуа Джанвити, который был в то время главным советником по правовым вопросам Международного валютного фонда, отметил: «Право государства на выпуск своей валюты защищено от иностранных государств. По этой причине, иностранное государство не может подделывать валюту другого государства (обычное международное право и женевская Международная конвенция по борьбе с подделкой денежных знаков от 20 апреля 1929 года)[17]. Запрет на подделку валюты нарушался редко, что говорит об эффективности нормы на протяжении несколько десятилетий[18]. Это отражает тот факт, что главы государств единодушно признали: изготовление фальшивых денег нарушает целостность финансовой системы и подрывает доверие к ней, в то время как очень многое, если не все, зависит от стабильности этой системы.

Однако руководители государств пока еще не обсудили и не решили, надо ли и каким образом использовать запрещающую фальшивомонетничество норму в цифровую эпоху. Другими словами, может и должна ли Международная конвенция по борьбе с подделкой денежных знаков применяться к электронным деньгам и (или) к финансовым данным? Если целостность финансовых данных в XXI веке так же важна, как целостность валюты, то недвусмысленное заявление об этом через принятие специального нового соглашения послужило бы интересам всего мира. Прецедент установления режима противодействия подделке денежных знаков мог бы улучшить понимание пользы этой меры и укрепить убежденность в том, что установить правовую норму, запрещающую деструктивное воздействие на финансовые данные, возможно.

В международном гуманитарном праве в настоящее время также не оговорены характер и важность данных. В этом отношении можно отметить, как минимум, два важных вопроса. Первый связан с *jus ad bellum* (нормами права, регулирующими вступление в войну). Законоведы не пришли к единому мнению относительно того, можно ли квалифицировать деструктивное воздействие на финансовые данные (независимо от тяжести и масштаба потенциальных последствий такого воздействия) как применение силы. Статья 2(4) Устава ООН запрещает только использование вооруженной силы, но не возбраняет политическое или экономическое принуждение[19]. В более

общем плане можно отметить, что с появлением гибридной и информационной войны международное сообщество сегодня размышляет над вопросом о том, необходимо ли и каким образом юридически квалифицировать акты принуждения, которые осуществляются без применения военной силы. Этой теме уделено основное внимание в опубликованном в 2017 году Таллинском руководстве 2.0 по применению юридических норм международного права к военным действиям в киберпространстве.

Более актуальным является вопрос, связанный с *jus in bello* (правилами ведения войны): допустимо ли и нужно рассматривать данные как объект, который не может быть целью поражения?

Мнения экспертов по правовым вопросам в этой области расходятся. Например, группа экспертов — авторов Таллинского руководства по применению юридических норм международного права к военным действиям в киберпространстве от 2013 года — утверждала, что данные, как таковые, не являются объектом и что по этой причине существующее международное гуманитарное право и оговоренные в нем принципы и защитные меры не распространяются на наступательные кибероперации, проводимые с целью оказать деструктивное воздействие на финансовые данные[20]. Таким образом, статус финансовых данных в рамках международного права является предметом спора.

Кроме того, отнесение финансовых учреждений к гражданским или военным объектам зависит от того, определяет ли та или иная страна понятие «военный объект» в узком смысле (учитывая только его боевые возможности), или, как это принято в США, в широком смысле (принимая во внимание как боевые возможности, так и военно-экономический потенциал)[21]. Во втором случае, финансовые учреждения и их данные могут рассматриваться в военное время как законные цели для нанесения удара (хотя, как отмечалось выше, до настоящего времени США воздерживались от нападения на такие объекты)[22].

Таким образом, четко сформулированное соглашение о запрете деструктивного воздействия на целостность финансовых данных могло бы показать, хотя бы в этой ограниченной сфере, в каком направлении страны, присоединившиеся к такому соглашению, намереваются развивать международное право.

ПРЕДЛАГАЕМОЕ СОГЛАШЕНИЕ

Современные тенденции развития международных отношений дают основания предполагать, что кибератаки на объекты инфраструктуры в большей степени вероятны в так называемой серой зоне — в период между миром и вооруженным конфликтом[23]. Соглашения, которое предусматривало бы защиту целостности финансовых данных лишь в мирное время, было бы недостаточно, учитывая жизненную важность финансовой системы для стабильности и благополучия всех стран и обществ. Потенциальные непреднамеренные негативные последствия взлома данных, включая ответные действия, перевешивают любые предполагаемые выгоды от таких действий. Более того, в случае вооруженного конфликта денежные средства могут потребоваться для восстановления ущерба и выплаты репараций. Поэтому было бы желательным и возможным для всех государств заключить соглашение о запрете деструктивного воздействия на целостность финансовых данных в любых обстоятельствах.

Столь пристальное внимание к вопросам целостности данных не уменьшает важность защиты их доступности и конфиденциальности. Однако можно сказать, что удар по целостности данных имеет более серьезные внутренние и международные последствия, чем нарушение конфиденциальности, и устранить их технически более сложно, чем справиться с проблемами, возникающими вследствие временного прекращения доступа к данным. Восстановить целостность поврежденных данных чрезвычайно трудно. Кроме технических сложностей, появляются дополнительные препятствия, связанные с правовыми нормами, специфическими для финансовой системы, например, окончательные расчеты. По этим и другим причинам утрата целостности данных является гораздо более серьезной проблемой, чем потеря их доступности. Последнее, но не менее важное обстоятельство: хотя эксперты могут иметь разные мнения относительно того, что именно является «системным риском» для финансовой системы, они практически единодушны в том, что нарушение целостности данных представляет собой самую большую угрозу.

Атаки типа «распределенный отказ в обслуживании» (DDoS-атаки) стали привычным явлением. Они носят временный и обратимый характер, поскольку их последствия можно предотвратить или смягчить с помощью определенных технических решений. Кроме того, государства и международное сообщество (через механизмы ООН) периодически применяют санкции в отношении финансовых учреждений, что в некоторой степени напоминает отказ в доступе к ресурсам этих учреждений для их владельцев и пользователей. Операции, влияющие на доступность данных, могут оказаться под запретом, когда происходит или планируется нарушение целостности сделок, как, например, в случае вмешательства посторонних лиц в процесс заключения договора. То же самое относится и к доступности данных, касающихся определенных ключевых систем. Чтобы понять, следует ли и каким образом затрагивать в предлагаемом соглашении проблему деструктивного воздействия на доступность таких данных, потребуется провести более широкие консультации с экспертами. «Большая двадцатка» должна поручить Совету по финансовой стабильности действовать совместно с органами и экспертами, которые устанавливают стандарты, и выработать рекомендации, которые будут рассмотрены в ходе дальнейшей работы.

Что касается вопросов конфиденциальности, некоторые государства продолжат применять ИКТ для сбора разведывательной информации о банках и финансовых институтах. Такие разведывательные действия критически важны для успешной борьбы с распространением оружия, терроризмом, отмыванием денег, наркоторговлей и прочими видами незаконной деятельности. Они не запрещены международными обычаями и правом[24]. Если норма, запрещающая кибероперации в отношении финансовых учреждений, будет распространена на сбор разведданных, ее принятие окажется нецелесообразным и (или) возникнут сомнения в ее эффективности.

Поэтому другие страны начали обсуждать возможные ограничения разведывательных кибероперций. Также необходимо рассмотреть технический аспект проблемы для того, чтобы определить, насколько реально провести грань между проникновением в компьютерные сети финансовых структур для сбора разведывательной информации и вторжением в них для деструктивного воздействия на

Рисунок 1. Три опоры эффективного самоусиливающегося режима

данные. Тайная загрузка информационного наполнения, способного повлиять на целостность финансовых данных, должна быть запрещена.

Учитывая эти соображения, предлагаемое соглашение будет содержать три взаимосвязанных и взаимо-усиливающих компонента:

> Ни одно государство не должно осуществлять или сознательно поддерживать любые действия, которые предполагают целенаправленное воздействие на целостность данных и алгоритмов финансовых институтов в любом месте, где бы они ни хранились, или в процессе транзитной передачи[25].
>
> В установленных законодательством случаях государство обязуется безотлагательно отвечать на соответствующие запросы другого государства для того, чтобы можно было воспрепятствовать действиям, совершенным с целью повлиять на целостность данных и алгоритмов финансовых институтов, в случаях когда такие действия осуществляются или инициируются на территории этого государства или совершаются его гражданами.

Эти положения также основаны на отчете Группы правительственных экспертов ООН от 2015 года, в котором говорится: «Государства не должны использовать посредников для совершения на международном уровне

неправомерных действий с использованием ИКТ и должны стремиться к тому, чтобы исключить возможность использования их территории негосударственными субъектами для совершения таких действий»[26].

Важная черта этих положений состоит в том, что в них сочетаются негативное (государство обязуется не совершать определенных действий) и положительное (государство обязуется совершать определенные действия) обязательства. Кроме того, предполагается, что государства внедрят существующие стандарты проведения комплексной экспертизы («дью дилидженс») и передовую практику, описанную, в частности, в инструкциях по кибербезопасности, разработанных Комитетом по платежным системам и рыночным инфраструктурам и Международной организацией комиссий по ценным бумагам в 2016 году. Соединение этих трех элементов позволит повысить эффективность указанного нормативного режима в целом, как показано на рисунке 1. Взаимосвязь соглашения, регулирующего поведение государства, и ожиданий в отношении внедрения стандартов проведения дью дилидженс в частном секторе призвана способствовать решению потенциальных проблем, обусловленных наличием риска недобросовестных действий. То, что государства будут обязаны предоставить по запросу помощь и информацию позволяет обойти проблему атрибуции атак, поскольку бремя расследования будет переложено с жертвы кибератак на государства, которые проявили интерес оказать помощь в расследовании этих преступлениях и целью которых является предотвратить такие нападения в будущем. Государства, как ожидается, будут выполнять эти обязательства в соответствии с ограничениями и требованиями национального и международного законодательств, каждое из которых может в перспективе быть скорректировано так, чтобы отразить суть предложенных здесь норм.

Для того чтобы соглашение эффективно соблюдалось всеми участниками и было признано государствами — членами ООН, оно не должно ограничиваться лишь отдельными финансовыми структурами, например, глобальными системно -значимыми банками (перечень которых приведен Советом по финансовой стабильности), действующими в десятках стран. Чтобы укрепить международную стабильность и заручиться поддержкой значительного числа государств, целесообразно рассмотреть вопрос о том, должны ли меры защиты распространяться на финансовые институты всех государств. Дело в том, что кибероперации, угрожающие целостности данных и алгоритмов любого финансового учреждения, могут создавать прецеденты и сеять страхи, угрожающие всем государствам.

Информация о предполагаемом запрете будет передаваться от государства к государству. Запрет не будет распространяться на негосударственных субъектов (например, террористов), действующих на территории, где номинальный верховный орган не способен поддерживать порядок и законность. Хотя более широкий масштаб был бы желательным во многих отношениях, практические соображения вынуждают сузить круг участников соглашения. Первоначально будет трудно получить согласие государств без привлечения негосударственных субъектов. Если и только когда ключевые государства начнут одобрять документ, подобный предложенному в этой публикации, можно будет приступить к работе над расширением состава участников и целей соглашения.

ПРОЦЕСС: ВОЗМОЖНЫЕ СЛЕДУЮЩИЕ ШАГИ

Если ключевые государства воспримут предложенное соглашение, как те, которые отвечают их национальным и глобальным интересам, возникнут вопросы: как закрепить соглашение; каким образом уточнить детали его применения и где искать единомышленников. «Большая двадцатка» представляется оптимальной площадкой для обсуждения и решения вопросов, упомянутых в данной публикации. Одно или несколько государств могут выступить в роли активных поборников этой идеи и предложить другим странам усовершенствовать и поддержать ее. Кроме того, можно было бы представить это предложение на обсуждение на нескольких международных форумах и мероприятиях с участием многосторонних организаций.

Если главы государств «Большой двадцатки» признают целесообразность предложенного соглашения, можно было бы предпринять следующие шаги:

- Включить формулировки, предлагаемые в настоящей публикации (или улучшенные), в коммюнике руководителей стран — членов «Большой двадцатки».

- Поручить Совету по финансовой стабильности:
  - — выработать меры по реализации и внедрению соглашения вместе с соответствующими органами по установлению стандартов и организациями частного сектора, включая Комитет по платежным системам и рыночным инфраструктурам, Международную организацию комиссий по ценным бумагам и Базельский комитет (это предполагает аналитическое рассмотрение некоторых из нижеуказанных позиций, а именно: следует ли включать в документ вопрос доступности определенных данных и систем; все ли виды данных подпадают под действие соглашения, в том числе такие, как данные о транзакциях и операционные данные, а также записи в главной бухгалтерской книге/данные о собственниках);
  - — подготовить для рассмотрения на следующем форуме «Большой двадцатки» доклад с отчетом о проделанной работе и дорожной картой, в которой будут намечены дальнейшие шаги.

В отличие от мер, осуществленных после финансового кризиса 2007–2008 годов, принятие и реализация соглашения, подобного предложенному в данной публикации, потребует взаимодействия с учреждениями и специалистами из разных стран, занимающимися вопросами национальной безопасности, и группами реагирования на компьютерные чрезвычайные происшествия. В настоящее время международная площадка для такого взаимодействия отсутствует. Однако Совет по финансовой стабильности может взять на себя организацию такого процесса и действовать в сотрудничестве с прочими неправительственными организациями и при их поддержке.

Комитет по платежным системам и рыночным инфраструктурам и Международная организация комиссий по ценным бумагам также могли бы подключиться к этой работе, особенно с учетом их деятельности в последнее время. Международный валютный фонд — еще один институт, который мог бы внести свой вклад, поскольку он представляет собой один из немногих форумов, привлекающих к своей работе представителей министерств финансов и центральных банков — двух важных групп, заинтересованных в предложенном здесь соглашении.

Нынешний интерес Всемирного экономического форума к этой теме, а также тот факт, что он уже занимался вопросами кибербезопасности в прошлом, дают возможность вовлечь высших руководителей компаний частного сектора. Их участие потребуется для того, чтобы надлежащим образом рассмотреть и проанализировать технические аспекты повышения эффективности предложенных норм и усиления контроля за их соблюдением. Институт международных финансов — еще одна организация, которая может взаимодействовать с мировой финансовой индустрией в этой области.

И наконец, совершенно очевидно, что в каждой стране официальные представители учреждений, занимающихся вопросами национальной безопасности, готовы в некоторой мере сотрудничать с зарубежными правительствами и экспертами из финансового сектора. В свете этого обстоятельства возможно предположить, что международное соглашение, заключенное главами стран — членов G20, в дальнейшем может быть дополнено целым рядом односторонних деклараций отдельных правительств или их военных ведомств в поддержку заявления руководителей государств «Большой двадцатки». Такой сценарий мог бы повысить действенность соглашения. Односторонние декларации могут стать достаточно простым способом выразить свою поддержку и солидарность с позицией «Большой двадцатки» для стран, которые не входят в эту организацию.

ВОПРОСЫ, ТРЕБУЮЩИЕ РАССМОТРЕНИЯ И РЕШЕНИЯ

Работая над этим предложением, мы включили ремарки и отзывы официальных представителей правительственных учреждений, профильных международных организаций и финансовых учреждений ряда стран, включая США, Россию, Китай, Великобританию, Сингапур и Израиль. Их отзывы в целом положительны; основополагающие допущения в этом меморандуме были подтверждены или скорректированы в процессе последующего совершенствования исходного текста. Чтобы предлагаемые нормы получили широкую поддержку и использовались на практике, необходимо прояснить ряд вопросов и всесторонне рассмотреть их в ходе переговоров по соглашению и на этапе его реализации. Мы предлагаем

читателям изучить эти вопросы и направить ответы авторам и (или) прочим заинтересованным сторонам.

1. Какой должна быть сфера действия финансовых учреждений? Являются ли достаточными следующие определения и сфера действия — или же они должны быть более узкими или более широкими?[27] В список терминов включены уже согласованные определения в области международной торговли, в частности окончательные формулировки, обсуждавшиеся в рамках Транстихоокеанского партнерства (ТТП) и международного финансового сообщества:

   - «Любой финансовый посредник или иное предприятие, имеющее право заниматься деловой деятельностью и являющееся объектом регулирования или надзора в качестве финансового учреждения по законодательству Стороны, на территории которой расположена эта организация» (это определение «финансового учреждения» в окончательном тексте ТТП в части, касающейся финансовых услуг);

   - «Финансовое учреждение, включая филиал, расположенное на территории Стороны, которое находится под контролем лиц другой Стороны» (определение «финансового учреждения другой стороны» в окончательном тексте ТТП в части, касающейся финансовых услуг);

   - «Любой неправительственный орган, включая биржу ценных бумаг или фьючерсный рынок/фьючерсную биржу, клиринговую организацию или же иную организацию или ассоциацию, которая осуществляет функции регулирующего или надзорного органа в отношении поставщиков финансовых услуг или финансовых учреждений по нормам статутного права или же на основании делегирования полномочий центральным или региональным правительством» (определение «самоуправляемой организации» в окончательном тексте ТОП в части, касающейся финансовых услуг)[28];

   - «Многосторонняя система участвующих учреждений и институтов, включая оператора системы, используемой для целей клиринга, расчетов или отражения платежей, ценных бумаг, производных финансовых инструментов или прочих финансовых операций» (определение термина «инфраструктура финансового рынка» в документе Банка международных расчетов / Международной организации комиссий по ценным бумагам 2012 года, озаглавленном «Принципы инфраструктуры финансового рынка»)[29].

2. Учитывая, насколько существенно отсутствие доступа к некоторым данным и системам может повлиять на систему в целом, каким образом можно обеспечить доступность данных и сочетать это с необходимостью уделять пристальное внимание целостности данных? Кроме того, бывают ли случаи злонамеренной деятельности в отношении доступности данных, влияющей на целостность транзакций, и если это так, то какие контрмеры могут быть приняты?

3. В контексте вооруженных конфликтов и международных гуманитарных войн можно ли провести различие между ударом по финансовым учреждениям как физическим объектам и ударом по их информации? Иначе говоря, если считается допустимым использовать обычные средства ведения войны, чтобы нанести удар по банку и тем самым физически уничтожить хранящиеся там деньги, то не надо ли запретить нападения на банки с применением ИКТ ввиду побочных негативных последствий и ответного удара в форме наступательных кибероперациий?

4. В современных условиях, когда финансовые учреждения используют облачные технологии для того, чтобы передать некоторые функции управления их данными другим компаниям, способна ли предложенная формулировка «в любом месте, где бы они ни хранились» в достаточной ли мере отразить такую тенденцию? Является ли это необходимым?

5. Будет ли такое соглашение касаться только тех государств, которые согласились заключить его, или же государства, признавшие установленные в соглашении

нормы, должны руководствоваться его требованиями и ограничениями в отношениях со странами, которые не приняли такие же обязательства?

6. В более общем плане, при наличии некоей нормы, отвергающей узко специфическую деятельность, каким образом государствам удается сделать так, чтобы не создавалось впечатления, будто они проявляют терпимость к прочим действиям, которые также могут являться вредоносными? Или, напротив, не является ли ограниченная норма более приемлемым вариантом, чем полное отсутствие формулировки в некоей сфере?

7. Когда возникает инцидент, связанный с деструктивным воздействием на целостность данных финансового учреждения, какие формы сотрудничества можно ожидать от государства?

   а. Какие недостатки существуют в настоящее время в отношениях между группами реагирования на инциденты информационной безопасности и правоохранительными органами?

   б. Какую информацию должно государство предоставлять своим партнерам?

   в. Стоит ли ожидать, что государства будут готовы согласиться с участием в расследовании совместной следственной группы?

   г. Будут ли государства принимать новые законы или вносить в старые законы поправки, согласно которым такая деятельность будет расцениваться на их территории как противозаконная и все их граждане, занимающиеся такой деятельностью, будут считаться нарушителями вне зависимости от того, где они ее осуществляют?

   д. Поддержат ли государства карательные меры Совета Безопасности ООН в случае нарушений со стороны какого-либо государства? Должно ли это государство являться участником соглашения или соглашение должно быть дополнено резолюцией Совета Безопасности ООН, чтобы оно стало применимым ко всем членам ООН?

   е. Какие передовые практики, которые используются государствами, подписавшими Конвенцию о киберпреступности, могут быть применены к этому типу инцидентов?

   ж. Какие меры, кроме существующих механизмов сотрудничества участников Конвенции о киберпреступности, следует включить в текст соглашения?

   з. Как мог бы выглядеть шаблон, который отражает все эти рекомендации?

8. Можно ли разработать методы для выявления случаев проникновения в компьютерные сети, в результате которых происходит нарушение целостности данных финансовых институтов? И можно ли найти способы, позволяющие провести различие между проникновением для сбора разведывательной информации и кибероперациями, которые также способны навредить данным?

9. Какие требования к уведомлениям и режиму уведомления должны быть установлены для того, чтобы государства узнали о таких инцидентах? Какие защитные меры должны применяться?

И наконец, мы констатируем, что информация, касающаяся прочих секторов экономики, например, телекоммуникационной отрасли и энергетики, а также целостность данных в прочих системах имеют огромное значение для финансовой системы. Однако любые соглашения, относящиеся к этим отраслям, являются еще более сложными с точки зрения ведения переговоров и эффективности их применения. В связи с этим мы рассматриваем это предложение как начало того, что, вероятно, станет долгим процессом, продолжающимся до тех пор, пока не утвердится эффективный всеобъемлющий режим безопасности.

Таблица 1. Субъекты международных отношений и организации, которые могут быть вовлечены в процесс

Постоянные члены Совета Безопасности ООН	Страны — участницы «Большой двадцатки»	Участники процесса, инициированного Группой правительственных экспертов ООН (UNGGE) в период 2014–2015 годов	Участники процесса, инициированного Группой правительственных экспертов ООН (UNGGE) в период 2016–2017 годов	Базельский комитет по банковскому надзору	Страны, имеющие глобальные системно-значимые банки	Страны, имеющие глобальные системно значимые страховые компании	Государства — члены «Большой семерки»
Китай	Китай	Китай	Китай	Китай	Китай	Китай	
Франция	Франция	Франция	Франция	Франция	Франция	Франция	Франция
Россия	Россия	Россия	Россия	Россия			
Великобритания	Великобритания	Великобритания	Великобритания	Великобритания	Великобритания	Великобритания	Великобритания
США	США	США	США	США	США	США	США
	Аргентина			Аргентина			
	Австралия		Австралия	Австралия			
	Бразилия	Бразилия	Бразилия	Бразилия			
	Канада		Канада	Канада			Канада
	Германия	Германия	Германия	Германия	Германия	Германия	Германия
	Индия		Индия	Индия			
	Индонезия		Индонезия	Индонезия			
	Италия	Италия		Италия	Италия		Италия
	Япония	Япония	Япония	Япония	Япония		Япония
	Мексика	Мексика	Мексика	Мексика			
	Саудовская Аравия			Саудовская Аравия			
	ЮАР			ЮАР			
	Южная Корея	Южная Корея	Южная Корея	Южная Корея			
	Турция			Турция			
		Беларусь					
		Колумбия					
		Египет	Египет				
		Эстония	Эстония				
		Гана					
		Израиль					
		Кения	Кения				
		Малайзия					
		Пакистан					
		Испания		Испания	Испания		
			Нидерланды	Нидерланды	Нидерланды	Нидерланды	
			Швейцария	Швейцария	Швейцария		
				Бельгия	Бельгия		
				Швеция	Швеция		
			+ Ботсвана, Куба, Финляндия, Казахстан, Сербия, Сенегал	+Гонконг*, Люксембург, Сингапур			

ПРИЛОЖЕНИЕ

КИБЕРАТАКИ НА ФИНАНСОВЫЕ УЧРЕЖДЕНИЯ И ДРУГИЕ ОРГАНИЗАЦИИ В 2007–2016 ГОДАХ

В этом разделе рассказывается в общих чертах о масштабных атаках с применением ИКТ, которым подверглись финансовые учреждения в разных странах мира в период с 2011-го по декабрь 2016 года, а также о серьезных киберинцидентах в 2007–2011 годах. Отметим, что в общедоступных источниках нет информации о фактах, которые указывали бы на причастность тех или иных государств к каким-либо инцидентам, связанным с деструктивным воздействием на целостность данных финансовых институтов. Это свидетельствует в пользу того, что до настоящего времени государства воздерживались от таких действий, — если не учитывать атаку в целях стирания данных с диска, проведенную в 2013 году против финансовых институтов Южной Кореи предположительно КНДР, и, возможно, низкоуровневую распределенную атаку типа «отказ в обслуживании» против российских финансовых учреждений в декабре 2016-го.

Перечисленные в таблице инциденты включают искажение страниц веб-сайтов, DDoS-атаки и проникновение в системы, осуществленные с использованием усовершенствованных хакерских программ. Целью нападений были преимущественно банки, однако в обзоре также фигурирует одна фондовая биржа и одна платежная система. В число стран, финансовый сектор которых попал под удар хакеров, входят Бангладеш, Бельгия, Бразилия, Грузия, Ливан, Польша, Россия, США, Украина, Эстония и Южная Корея. Во многих случаях представляется затруднительным точно определить, кто именно осуществил кибератаку, однако круг предполагаемых взломщиков охватывает как независимые преступные и хакерские группировки, так и хакеров, действующих при государственной поддержке, или даже государства как таковые. Результаты этого обзора, составленного авторами, подтверждают предположение, что государства уже проявляют значительную сдержанность в этой области, несмотря на значительные технические возможности, которыми они располагают.

Таблица 2. Краткий перечень и даты кибератак

Краткое описание	Дата
DDoS-атака на российские банки	Конец 2016 г.
Ограбление Центрального банка Бангладеш	Начало 2016 г.
DDoS-атака на Национальный банк Бельгии	Начало 2016 г.
Резкий обвал котировок на Шанхайской фондовой бирже (неподтвержденный случай атаки с применением ИКТ)	2015 – 2016 г.г.
Хищение средств собственных клиентов российскими банками	Конец 2015 г.
Продажа и покупка валюты от имени российского банка с использованием вредоносной программы	Начало 2015 г.
Применение хакерской программы Metel против российских банков	2015 г.
Утечка данных Министерства финансов Украины	Середина 2015 г.
Взлом компьютерной сети Варшавской фондовой биржи	Конец 2014 г.
Проникновение в базу данных украинского банка	Середина 2014 г.
Применение хакерской программы Carbanak против различных банков	2013 – 2015 г.г.
Применение вируса Dark Seoul против южнокорейских банков	Начало 2013 г.
Утечка данных из JPMorgan Chase в результате операций преступной группировки	2012 – 2015 г.г.
Серия DDoS-атак против бразильских банков	2012 г. и 2014 г.
Хакерская атака на бразильскую платежную систему	2012 – 2014 г.г.
DDoS-атака на финансовые учреждения США	2012 – 2013 г.г.
Воздействие на данные Шанхайской фондовой биржи (неподтвержденный случай атаки с применением ИКТ)	Середина 2012 г.
Заражение компьютерным вирусом Gauss в банках Ливана	2011 – 2012 г.
Применение вредоносной программы против южнокорейского банка	Середина 2011 г.
Проникновение в систему NASDAQ	Конец 2010 г.
Искажение страниц веб-сайта в период российско-грузинской войны	Середина 2008 г.
Серия DDoS-атак против Эстонии, в частности эстонских банков	Середина 2007 г.

DDoS-атака на российские банки в 2016 году

2 декабря 2016 года Федеральная служба безопасности России объявила, что она получила информацию о планируемых кибератаках на «ряд крупнейших российских банков» в период с 5 декабря[30]. Серверы и центры управления, которые, предположительно, привлекались для проведения этих кибератак, были расположены в Нидерландах и принадлежали украинской хостинговой компании BlazingFast. Директор этой компании Антон Оноприйчук сообщил, что не располагает информацией о какой-либо кибератаке и что его компания не обнаружила никаких вредоносных данных. Министерство безопасности и правосудия Нидерландов заявило, что они знают, что их инфраструктура может быть использована хакерами для проведения кибератак во всем мире, а также отметило, что, «если в понедельник действительно состоится такая атака, решение о том, надо ли проводить расследование, должны принимать российские власти... При необходимости они могут обратиться к голландским следственным органам с просьбой о содействии в таком расследовании»[31].

9 декабря российский оператор связи «Ростелеком» выступил с заявлением о том, что 5 декабря он блокировал атаки типа «отказ в обслуживании», направленные против пяти крупнейших банков и финансовых учреждений России. Их максимальная мощность достигала 3,2 млн пакетов в секунду, что является относительно низким показателем по сравнению с другими недавними DDoS-атаками, самая длительная из которых продолжалась несколько часов. Кроме того, «Ростелеком» отметил, что часть атак была совершена с помощью бот-сетей, подобных тем, что применялись в предшествующие недели против компаний Deutsche Telekom (Германия) и Eircom (Ирландия), чему способствовала уязвимость домашних маршрутизаторов[32].

На участие в кибератаке каких-либо государственных субъектов ничто не указывало, хотя ФСБ России заявила, что кибернападение было организовано «иностранными разведывательными органами», и на основании местоположения и гражданства владельца компании высказывались предположения о том, что за акцией стояла Украина[33]. Согласно заявлению ФСБ России, они ожидали, что кибератаки будут сопровождаться текстовыми публикациями в социальных сетях и блогах, содержащими провокационное сообщение о «кризисе российской кредитно-финансовой системы, банкротстве и отзыве лицензий у ведущих федеральных и региональных банков», и что «эта кампания будет направлена против нескольких десятков российских городов»[34]. По всей видимости, предполагалось подтолкнуть население к массовому изъятию депозитов из российских банков и тем самым вызвать финансовый кризис. Однако помимо кибератак как таковых отсутствуют какие-либо факты и доказательства попыток спровоцировать финансовый кризис.

Ограбление Центрального банка Бангладеш 2016 года

В феврале 2016 года средства массовой информации сообщили: хакеры проникли в компьютерную сеть Центрального банка Бангладеш и после этого отправили в Федеральный резервный банк Нью-Йорка 35 сфальсифицированных запросов на перевод денежных средств на общую сумму 1 млрд долларов США[35]. Четыре запроса банк удовлетворил, в результате чего хакеры смогли перевести 81 млн долларов США на счета на Филиппинах. Это стало одним из крупнейших ограблений банков в истории[36]. Пятый запрос на 20 млн долларов США, которые мошенники собирались перевести на банковский счет в Шри-Ланке, был задержан. Подозрение вызвала ошибка в наименовании получателя: вместо Shalika Foundation было написано Shalika Fandation[37]. Оставшиеся переводы, на общую сумму примерно 850–870 млн долларов США, также были приостановлены[38].

Хакеры использовали вредоносные программы для взлома сервера Центрального банка Бангладеш, а также программу — клавиатурный шпион, что позволило им получить доступ к идентификационным кодам для использования платежной системы Swift. Хакеры также применили вредоносное программное обеспечение, которое нарушило нормальную работу Alliance Access — системы управления счетами клиентов SWIFT — и позволило скрыть следы преступления[39]. С его помощью злоумышленники удалили учетные записи запросов на перевод денежных средств, обошли проверку на достоверность, удалили сведения о логине, произвели манипуляции с данными об остатках денежных средств и остановили подсоединенные принтеры, чтобы не допустить распечатку журнала транзакций. Хотя использованная вредоносная программа была специально

предназначена для этой кражи, она может быть применена и против других банков, которые подключены к системе SWIFT, использующей программное обеспечение Alliance Access.

Киберпреступники отслеживали повседневную деятельность банка, чтобы их сфальсифицированные запросы на перевод денежных средств выглядели как подлинные. Они выбрали для кражи оптимальное время: когда Федеральный резервный банк Нью-Йорка направил в Дакку запросы в связи с сомнительными переводами, в Бангладеш был конец рабочей недели, а когда служащие Центрального банка Бангладеш дали американским коллегам указание отменить операции, в Нью-Йорке уже наступили выходные дни.

DDoS-атака на Национальный банк Бельгии в 2016 году

22 февраля 2016 года группа хакеров DownSec (Бельгия) посредством атаки типа «отказ в обслуживании» парализовала работу веб-сайта Национального банка Бельгии на большую часть первой половины дня[40]. Сообщения об этой атаке были немногословными, однако известно, что ей предшествовала серия осуществленных той же группировкой схожих кибернападений на веб-сайты Бельгийского федерального агентства по ядерному контролю, Кризисного центра и Группы реагирования на чрезвычайные ситуации в сфере кибербезопасности. DownSec заявляет, что ее цель — борьба против коррупции в государственных органах.

Резкий обвал котировок на Шанхайской фондовой бирже в 2015 году (неподтвержденный случай атаки с применением ИКТ)

С 12 июня 2015 года начался обвал Шанхайского составного индекса, и уже к 19 июня он снизился на 13 %[41]. Падение на китайских фондовых биржах продолжалось в июле и августе, а затем возобновилось в январе и феврале 2016-го[42]. Хотя в открытых источниках нет доказательств, высказывались предположения, что внезапный обвал котировок вызван кибератакой[43].

Хищение средств собственных клиентов российскими банками в 2015 году

В настоящее время имеется лишь ограниченная информация об этом происшествии, однако британский журнал SC Magazine UK недавно сообщил, что Центральный банк России отозвал лицензии трех российских банков по результатам расследования, в рамках которого было установлено, что действующие и бывшие сотрудники банка использовали ИКТ для снятия денежных средств со счетов своих вкладчиков, а также покрывали прочие преступления и правонарушения в этих банках[44]. Центральный банк России сообщил, что только за последний квартал 2015 года со счетов клиентов ряда банков было украдено свыше 20 млн долларов США, причем, возможно, с ведома и при прямом участии самих банков. ЦБ России также сообщил, что действия хакеров, скорее всего, стали результатом масштабных сокращений в финансовом секторе России в предыдущем году. Эти сокращения вызвали недовольство бывших сотрудников банков и подтолкнули их к сотрудничеству с хакерами, в то время как банки не желали или не могли пойти на дополнительные расходы по укреплению кибербезопасности.

Продажа и покупка валюты от имени российского банка с использованием вредоносной программы в 2015 году

Русскоязычные хакеры использовали троян Corkow для проникновения в компьютерные системы российского «Энергобанка» в сентябре 2014 года[45]. Они смогли собрать идентификационные данные, запустить собственное торговое программное обеспечение и 27 февраля 2015 года разместили средства на сумму свыше 500 млн долларов США по нерыночным ставкам, что привело к резким колебаниям обменного курса в диапазоне 55–66 рублей за доллар США на протяжении четырнадцати минут[46]. Интересно отметить, что хакеры, по всей видимости, не извлекли значительной выгоды из этой операции, хотя вполне возможно, что они использовали свою инсайдерскую информацию для обогащения на других рынках. Кроме того, нельзя исключать, что это было своего рода подготовкой к следующим кибератакам. «Энергобанк» заявил, что из-за действий злоумышленников он потерял 3,2 млн долларов США.

Применение хакерской программы Metel против российских банков в 2015 году

Группа киберпреступников использовала ранее разработанную вредоносную программу Metel, чтобы похищать деньги непосредственно из банков, а не у конечных пользователей банковских услуг. Преступная группировка, в которую, предположительно, входило менее десяти человек, использовала целевые фишинговые письма или уязвимости

браузеров для проникновения в определенные части банковских систем, имевшие доступ к денежным операциям, например к компьютерам, используемым операторами центра обработки звонков или банковских служб поддержки. Оказавшись внутри компьютерной сети, Metel автоматически отменяла последнюю команду в банкомате. Это позволяло злоумышленникам использовать карты взломанных банков для снятия фактически неограниченных денежных сумм: каждый раз, когда они снимали деньги, остаток на счете не менялся. Такого рода махинации не были замечены за пределами России[47].

Утечка данных Министерства финансов Украины в 2015 году

В мае 2015 года пророссийские хакеры-активисты («хактивисты») — группа, называющая себя «КиберБеркут», — заявили о том, что смогли проникнуть в сети Министерства финансов Украины[48]. В качестве доказательства неспособности Украины обслуживать свой внешний долг они опубликовали то, что назвали документами, похищенными ими из сети министерства. Насколько заявление «КиберБеркута» соответствует действительности, а также каким образом группа якобы получила доступ к документам ведомства, неизвестно. Более подробную информацию о деятельности группы «КиберБеркут» см. в параграфе «Проникновение в базу данных украинского банка в 2014 году».

Взлом компьютерной сети Варшавской фондовой биржи в 2014 году

В октябре 2014 года группа, объявившая о своей связи с так называемым «Исламским государством», смогла проникнуть во внутренние сети Варшавской фондовой биржи и опубликовала учетные данные онлайновых брокеров[49]. Способы, использованные группой для проникновения в сети биржи, остаются неизвестными, однако, согласно имеющимся данным, она смогла проникнуть в блок инвестиционного моделирования и в веб-портал для управления процессом перехода биржи на новую трейдинговую систему, а также закрыть доступ к веб-порталу на два часа[50]. По сообщениям служащих биржи, трейдинговая система не была взломана. Несколько позднее представители НАТО в частном порядке сообщили, что заявление хакерской группы о ее принадлежности к «Исламскому государству» являлось «операцией под чужим флагом», а на самом деле проникновение совершила группа «APT 28», которая, по мнению многих исследователей в области безопасности, связана с Россией[51].

Проникновение в базу данных украинского банка в 2014 году

В июле 2014 года пророссийская группа хакеров-активистов «КиберБеркут» заявила о том, что смогла взломать компьютерную сеть «ПриватБанка», одного из крупнейших коммерческих банков Украины, и опубликовала данные его вкладчиков в российской социальной сети «ВКонтакте»[52]. Способ проникновения в базу данных остается неизвестным. Есть мнение, что «КиберБеркут» выбрал «ПриватБанк» в качестве цели потому, что Игорь Коломойский, совладелец этого банка, предложил награду 10 000 долларов США за поимку российских боевиков на территории Украины[53]. «КиберБеркут» предупредил клиентов «ПриватБанка» о том, что им лучше перевести свои денежные средства в государственные банки. Возможно, что «КиберБеркут» на самом деле имеет связи с российским правительством, однако относительная незамысловатость их хакерских атак приводит некоторых экспертов к мнению, что наличие у «КиберБеркута» официальных связей с российскими государственными органами маловероятно[54].

Применение хакерской программы Carbanak против различных банков в 2013–2015 годах

Группа преступников использовала вредоносную программу Carbanak для кибератаки на финансовые учреждения, включая банки и системы электронных платежей, почти в 30 странах. Эта программа предоставляла удаленный доступ к атакуемым серверам и снабжала хакеров видеоматериалами и фотографиями, позволяя отслеживать ежедневные банковские операции в течение месяцев[55]. Затем злоумышленники могли, имитируя действия сотрудников банка, дать банкоматам команду на выдачу наличных или осуществить перевод денежных средств. Однако самые крупные суммы денег были похищены, когда преступники, действуя в роли сотрудников банка, взламывали банковские информационные системы и завышали количество денег на текущих счетах клиентов банка. Возникшие таким образом деньги перечислялись на счета преступников, после чего

баланс счета возвращался к исходному значению. Жертвами мошенников стали Австралия, Бразилия, Болгария, Великобритания, Германия, Гонконг, Индия, Ирландия, Исландия, Испания, Канада, Китай, Марокко, Непал, Норвегия, Пакистан, Польша, Россия, Румыния, США, Тайвань, Украина, Франция, Чешская Республика и Швейцария[56].

Применение вируса Dark Seoul против южнокорейских банков в 2013 году

Эта хакерская атака произошла 20 марта 2013 года. Злоумышленники использовали вирус Dark Seoul в целях проникновения в компьютерные сети трех южнокорейских банков — Shinhan, Nonghyup и Jeju, что привело к стиранию данных и сбоям в работе банкоматов и мобильных платежных систем[57]. Дистанционное банковское обслуживание Shinhan Bank было заблокировано на протяжении части рабочего дня, что не позволяло клиентам выполнять онлайновые сделки, при этом работа некоторых филиалов банков Nonghyup и Jeju была парализована в течение двух часов после того, как компьютерный вирус разрушил файлы зараженных компьютеров. Четвертый банк — Woori, заявивший о хакерской атаке, не пострадал от ее последствий. Несколько корейских медиакомпаний также подверглись нападению хакеров: их компьютеры были блокированы, но вещание тем не менее не прекратилось[58]. Власти Южной Кореи возложили ответственность за инциденты на КНДР[59].

Утечка данных из JPMorgan Chase в результате операций преступной группировки в 2012–2015 годах

В августе 2014 года банк JPMorgan Chase заявил о масштабной утечке данных, в результате которой хакеры получили доступ к контактным данным свыше 80 млн держателей счетов, что является самым масштабным в истории случаем утечки данных из финансового учреждения США[60]. Хотя первоначально высказывались предположения об участии российских властей в этой кибератаке[61], в ноябре 2015 года федеральные органы предъявили четырем лицам обвинение в проникновении в базу данных, которое, по заявлению властей, было частью крупной хакерской операции: злоумышленники проникали в сети других финансовых учреждений, занимались мошенничеством с ценными бумагами и онлайновыми биржевыми спекуляциями, что принесло им чистую прибыль в размере 100 млн долларов США[62]. Преступники использовали адреса электронной почты, полученные ими в результате атаки на JPMorgan, для махинаций с ценой акций; кроме того, они рассчитывали учредить свою собственную брокерскую фирму, используя украденные данные для установления контакта с потенциальными клиентами[63]. Хотя хакерское нападение на JPMorgan было самой крупной операцией этой группировки, преступники также взломали базы данных шести других финансовых учреждений: Scottrade, E-Trade, Dow Jones (материнская компания, владеющая изданием The Wall Street Journal), еще одной организации, занимающейся финансовой информацией, а также нескольких онлайновых брокерских организаций[64].

Серия DDoS-атак против бразильских банков в 2012 и 2014 годах

В январе 2012 года хакерская группа Anonymous использовала атаки типа «отказ в обслуживании» для взлома веб-сайтов некоторых крупнейших банков в стране, заявив, что это сделано в знак протеста против коррупции и неравенства в Бразилии[65]. В результате атак, получивших название #OpWeeksPayment, были на несколько часов заблокированы веб-сайты целого ряда банков, включая, в частности, Banco do Brasil, Itaú Unibanco и Bradesco[66].

В июне 2014 года группа провела еще одну серию атак того же типа в знак протеста против проведения чемпионата мира по футболу[67]. Эти атаки, названные #OpHackingCup, обрушили несколько бразильских веб-сайтов, включая веб-сайт Центрального банка Бразилии. Мишенью хакеров стали также веб-сайты правительства Бразилии, компании Hyundai Brazil и официальный веб-сайт чемпионата мира по футболу[68].

Хакерская атака на бразильскую платежную систему в 2012–2014 годах

Киберпреступники использовали вредоносную программу «Человек-в-браузере» для атаки на популярную в Бразилии платежную систему Boleto Bancario, которая позволяет копаниям выпускать бумажные или онлайновые билеты (boletos) со штрихкодом, которые клиенты могут использовать для перевода денег в банк[69]. Вредоносная программа проникла в браузеры почти 200 000 зараженных вирусом компьютеров, получив возможность перехватывать и

изменять подлинные болето таким образом, чтобы перенаправлять денежные платежи на счета хакеров[70]. В результате хакерской атаки было нарушено нормальное функционирование системы безопасности и были поставлены под угрозу транзакции на сумму 3,75 млрд долларов США. Однако остается неизвестным, какую часть этой суммы преступникам удалось успешно разместить на своих собственных счетах[71].

DDoS-атака на финансовые учреждения США в 2012–2013 годах

Имели место две скоординированные волны хакерских атак типа «отказ в обслуживании» на веб-сайты финансовых учреждений США: первая волна наблюдалась в период с сентября по октябрь 2012 года, а вторая — с декабря 2012-го по январь 2013-го[72]. Группа исламских хактивистов «Кибервоины Изз ад-Дин аль-Кассам» взяла на себя ответственность за эти нападения, которые она назвала «операция „Ababил“»[73]. Однако представители правительства США в частном порядке проинформировали СМИ о том, что, по их мнению, нападение — дело рук Ирана[74]. Масштаб атак был беспрецедентным с точки зрения количества пострадавших финансовых учреждений и объема трафика, заполнившего сайты. Один из исследователей прокомментировал эти события так: «Никогда раньше столь большое число финансовых учреждений не оказывалось под воздействием столь серьезного шантажа»[75]. Хотя в обоих случаях хакеры заранее объявили об атаках и их целях, банки не смогли защититься, что привело к нарушению работы веб-сайтов многих финансовых учреждений США, включая Bank of America, Citigroup, Wells Fargo, U.S. Bancorp, PNC, Capital One, Fifth Third Bank, BB&T и HSBC[76]. Оборонительные и восстановительные мероприятия обошлись банкам в миллионы долларов[77]. «Кибервоины Изз ад-Дин аль-Кассам» объявили о еще двух волнах кибератак в 2013 году, но те оказались менее эффективными[78].

Воздействие на данные Шанхайской фондовой биржи в 2012 году (неподтвержденный случай атаки с применением ИКТ)

Четвертого июня 2012 года Шанхайский составной индекс открылся на отметке 2346,98 и упал на 64,89 пункта к закрытию торгов[79]. В этот день исполнилась очередная годовщина печально известного подавления студенческих выступлений на площади Тяньаньмэнь в 1989 году. В связи с этим многие в КНР предположили, что оба числа, возможно, неслучайны и содержат намек на трагедию в Пекине[80]: цифра 2346,98 может быть прочитана в обратном порядке и указывать на дату — год, месяц и день — события, а цифра 23 напоминает о том, что разгон акций протеста на площади Тяньаньмэнь произошел 23 года назад. Аналогичным образом многие обозреватели в Китае предполагают, что 64,89 пункта, на которые упали котировки фондового рынка в тот день, также могут обозначать дату студенческих выступлений — 6/4/89. Очевидное совпадение цифр породило распространенное, хотя и недоказанное предположение о том, что биржевой индекс, возможно, стал объектом хакерской атаки и манипулирования, чтобы вывести на экран биржи указанные цифры. Нумерология играет очень важную роль в китайской культуре, и китайские граждане в прошлом уже использовали цифры в качестве утонченной формы протеста.

Заражение компьютерным вирусом Gauss в банках Ливана в 2011–2012 годах

9 августа 2012 года «Лаборатория Касперского», российская компания, специализирующаяся на системах защиты от различных киберугроз, объявила об обнаружении вируса Gauss, который был разработан для хищения данных из ливанских банков, включая Bank of Beirut, EBLF, BLOM Bank, Byblos Bank, Fransabank и Credit Libanais, а также со счетов пользователей Citibank и PayPal[81]. Эксперты «Лаборатории Касперского» пришли к выводу, что это вредоносное программное средство спонсировалось государством и было разработано создателями вирусов Stuxnet, Flame, Duqu и шпионских троянов[82]. Свыше 2500 компьютеров, принадлежавших клиентам «Касперского», были поражены вирусом в двадцати пяти странах (1660 из которых находятся в Ливане), однако «Лаборатория Касперского» предупреждает, что общее количество зараженных компьютеров может исчисляться десятками тысяч[83].

Как только персональный компьютер оказывается заражен, троян инициирует кражу подробной информации — историю просмотров браузера, пароли, куки, конфигурацию системы и данные учетной записи интернет-банкинга, а также устанавливает шрифт Palida Narrow, цель использования

которого остается неясной[84]. Любопытно, что вирус Gauss содержит закодированное информационное наполнение, которое специалисты по ИТ-безопасности не могут расшифровать. Это указывает на наличие важного вредоносного кода, эксплуатирующего уязвимости в программном обеспечении, защиту которого создатели вируса сочли весьма существенной[85]. Ввиду того что Ливан является финансовым центром всего Ближнего Востока, а отсутствие прозрачности в деятельности банков в этой стране часто вызывает нарекания со стороны органов финансового регулирования, стремящихся пресечь финансирование терроризма и легализацию незаконных доходов, представляется вероятным, что этот вирус мог быть разработан для мониторинга и (или) блокировки денежных потоков, которые расцениваются как угроза национальной безопасности государства-спонсора[86].

Применение вредоносной программы против южнокорейского банка в 2011 году

Кибератака, предпринятая с целью оказать воздействие на банковские операции южнокорейской Национальной федерации сельскохозяйственных кооперативов (Нонхёп), произошла 12 апреля 2011 года. Изначально вредоносная программа инфицировала ИТ-системы организации в сентябре 2010-го, когда субподрядчик случайно загрузил вирусы в персональный компьютер, что было использовано хакерами для распространения вредоносных программ по всем сетям банка[87]. В результате оказались уничтожены данные кредитных карт многих клиентов и начались перебои в обслуживании, которые продолжались три дня и отрицательно сказались на работе банкоматов, онлайн- и мобильного банкинга, а также использовании кредитных карт. Южная Корея посчитала, что за этой атакой стояла КНДР[88].

Проникновение в систему NASDAQ в 2010 году

О несанкционированном проникновении в сети NASDAQ первоначально сообщили в эксклюзивной статье, опубликованной Bloomberg Business в 2014 году[89]. В октябре 2010-го ФБР обнаружило факт взлома серверов NASDAQ. Программа, инфицировавшая серверы, использовала две уязвимости нулевого дня и походила на вредоносную программу, ранее разработанную главной российской спецслужбой, ФСБ. Сначала она проникла в систему Directors Desk, с помощью которой сотни компаний обмениваются конфиденциальной информацией с членами совета директоров. В заявлении NASDAQ сообщалось, что нападению подверглась только эта система, однако, по данным Bloomberg, злоумышленникам удалось проникнуть гораздо глубже в сети биржи, хотя хакерам и не удалось получить доступ к самой торговой площадке.

Агентство национальной безопасности первоначально полагало, что эта хакерская программа могла вызвать масштабный сбой в компьютерной сети NASDAQ и даже стереть данные во всех системах биржи. Кроме того, присутствовали признаки кражи большого количества данных, хотя у следствия было мало фактов, свидетельствующих о том, что именно пропало в результате хакерской атаки. Несколько позднее ЦРУ заявило, что программа была менее разрушительной, чем первоначально считалось, и не смотря на то что она не могла полностью уничтожить компьютерную систему NASDAQ, программа могла получить контроль над определенными функциями и использовать их для нарушения работы сети. Согласно выводу следствия, основной целью несанкционированного проникновения было похищение запатентованной технологии, важной для России, для того чтобы использовать ее на российских фондовых биржах и тем самым способствовать превращению Москвы в глобальный финансовый центр. Публичный анализ использованной хакерской программы не проводился, и в сообщении Bloomberg было изложено мало подробностей, так что в открытых публикациях отсутствует дополнительная техническая информация об этой вредоносной программе и ее возможностях.

Искажение страниц веб-сайта в период российско-грузинской войны в 2008 году

Атаки с использованием ИКТ начались в Грузии 20 июля 2008 года, незадолго до начала военных действий, и продолжались вплоть до прекращения конфликта в середине августа[90]. Это был первый в истории случай одновременного применения кибер- и кинетического оружия. Предположительно, кибератака была проведена одной из государственных структур России или российскими хакерами, связанными с государством[91]. В день начала боевых действий на российских веб-сайтах появились списки грузинских сайтов, которые могли бы

стать мишенью для кибератак, подробные инструкции как можно взломать эти сайты и формы отчетов о уже предпринятых хакерами действиях, что убедительно показало: к конфликту готовились заранее и знали о его начале[92]. Операции включали искажение страниц сайтов (дефейс) и атаки типа «отказ в обслуживании», а среди объектов нападения упоминались веб-сайт президента Грузии и другие сайты правительственных организаций страны. Что касается финансового сектора, то здесь был отмечен единственный случай кибератаки — дефейс веб-сайта Национального банка Грузии[93].

Серия DDoS-атак против Эстонии, в частности эстонских банков, в 2007 году

Серия скоординированных кибератак типа «отказ в обслуживании» против веб-сайтов правительства Эстонии, эстонских банков, университета и сайтов ряда газет началась 26 апреля и продолжалась три недели[94]. В течение первой недели целью атак были только серверы электронной почты и веб-сайты государственных органов и политических партий, а в ходе второй недели нападению подвергались и веб-сайты эстонских новостных изданий[95]. Чтобы вернуть зараженные сайты в режим онлайн, сетевым администраторам пришлось отключить их от международного трафика, что по иронии судьбы ограничило возможности эстонских СМИ информировать внешний мир о происходивших в стране событиях.

Третья волна кибератак, объектом которых стал эстонский банковский сектор, началась 9 мая и оказалась самой мощной[96]. Нападения вынудили два ведущих эстонских банка — включая Hansabank, крупнейший в стране, — временно приостановить онлайновые банковские операции. Было нарушено подключение банковских сетей к банкоматам, и клиенты, находившиеся за пределами страны, не могли воспользоваться эстонскими дебетовыми карточками[97]. Самыми напряженными днями были 9–10 мая, после чего кибератаки медленно пошли на спад и прекратились 19 мая, когда срок действия контракта с хакерами, по всей видимости, истек[98].

Кибероперациями занимались российские хактивисты. Они открыто общались в русскоязычных чатах, где получали четкие инструкции. Эстония заявила, что заказчиком является российское правительство, однако в Таллине не смогли подкрепить свое обвинение однозначными доказательствами[99].

Авторы этой публикации выражают признательность Тейлору Бруксу, Стивену Найкосу и Элизабет Уитфилд за их содействие в подготовке данной публикации. Мы также благодарны более чем пятидесяти представителям власти и экспертам более чем из десяти стран, которые предоставили нам свои отзывы и ценную информацию по этой теме.

ПРИМЕЧАНИЯ

1. G20 Finance Ministers and Central Bank Governors, Communiqué. — University of Toronto. — March 18, 2017 // http://www.g20.utoronto.ca/2017/170318-finance-en.html.
2. Более подробный рассказ об этом и других кибернападениях на финансовые учреждения см. в приложении. *Das K. N., Spicer J.* The SWIFT Hack — How the New York Fed Fumbled Over the Bangladesh Bank Cyber-Heist. — Reuters. — July 21, 2016 // http://www.reuters.com/investigates/special-report/cyber-heist-federal/.
3. Зависимость государств от устойчивости финансовых данных и взаимозависимость ИТ-систем, вероятно, будут возрастать. Например, в декабре 2015 года газета The New York Times опубликовала статью о попытках правительства Швеции полностью перевести страну на экономику, основанную на безналичных расчетах; ООН также поддерживает усилия стран по переходу на безналичные расчеты через альянс «Лучше, чем наличные». Правительство Индии также стремится к созданию безналичной экономики. См. Alderman L. In Sweden, a Cash-Free Future Nears. — New York Times. — April 26, 2015 // http://www.nytimes.com/2015/12/27/business/international/in-sweden-a-cash-free-future-nears.html?_r=0; Better Than Cash Alliance [accessed April 21, 2016] // https://www.betterthancash.org/; From Eradicating Black Money to Cashless Economy: PM Modi's Changing Narrative Since Demonetisation. — Indian Express. — December 22, 2016 // http://indianexpress.com/article/india/demonetisation-modi-cashless-economy-black-money-narratives-4439843/.
4. Сюда же можно включить вредоносные программы, предназначенные для стирания информации с диска. Вместе с тем усилия по расшифровке тайнописи, как часть сбора разведывательных данных, не подпадают под это соглашение. Мы также предлагаем государствам рассмотреть возможность потенциального включения в текст соглашения функции доступности данных определенных критически важных систем, однако рекомендуем рассмотреть этот вопрос в ходе последующей контрольной проверки, учитывая имеющиеся трудности в формулировании определений.
5. Мы не принадлежим к числу тех, кто первым предложил заключить такое соглашение, однако считаем, что эта публикация на сегодняшний день представляет собой наиболее подробный и всесторонний анализ и столь же подробное и комплексное предложение. Например, Ричард Кларк и Роберт Нейк предложили ввести схожую норму в своей публикации 2011 года; см.: *Clarke R. A., Knake R. K.* Cyber War: The Next Threat to National Security and What to Do About It. — N.Y.: HarperCollins, 2011. — P. 269. Грег Остин и Эрик Каппон из Института «Восток — Запад» также написали на эту тему небольшую статью, в которой они провели аналогию с Конвенцией 1997 года о преступлениях против лиц, пользующихся международной защитой; см.: *Austin G., Cappon E.* Internationally Protected Facilities in Cyberspace: The Examples of Stock Exchanges and Clearing Houses. — EastWest Institute. — December 2014.
6. Риск недобросовестных действий в связи с таким международным соглашением теоретически может существовать, но он - маловероятен в свете значительной угрозы со стороны негосударственных субъектов. Кроме того, уже оказывается давление с целью повысить запас прочности за счет комплексной проверки, и поэтому международное соглашение, которое вынуждает государства к сдержанному поведению, в последующем будет принято и дополнит механизмы, которые уже существуют.
7. United Nations General Assembly, A/70/174. — Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. — July 22, 2015 // https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement.
8. G20 Leaders' Communiqué Antalya Summit, 15–16 November 2015. Press release. — European Council. — November 16, 2015 // http://www.consilium.europa.eu/en/press/press-releases/2015/11/16-g20-summit-antalya-communique/.
9. *Uchill J.* Israel Cyber Head: US-Backed Cyber Norms Too Broad. — Hill. — September 13, 2016 // http://thehill.com/policy/cybersecurity/295651-israel-cyber-head-us-supported-cyber-norms-too-broad.
10. *Markoff J., Shanker T.* Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk. — New York Times. — August 1, 2009 // http://www.nytimes.com/2009/08/02/us/politics/02cyber.html.
11. Russian Ministry of Foreign Affairs: Convention on International Information Security. — September 22, 2011 // http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666.
12. *Fahey M., Wells N.* Charts: Who Loses When the Renminbi Joins the IMF Basket? — CNBC. — December 2, 2015 // http://www.cnbc.com/2015/12/02/who-loses-when-the-renminbi-joins-the-imf-basket.html.
13. *Dangwal S.* Budget 2017: Computer Emergency Response Team to Be Set Up to Check Cyber Frauds. — India. — February 1, 2017 // http://www.india.com/news/india/budget-2017-computer-emergency-response-team-to-be-set-up-to-check-cyber-frauds-1802854/.
14. Что касается подделки валюты в военное время, главный советник по правовым вопросам Международного валютного фонда Франсуа Джанвити в статье 2004 года написал: «Применим ли запрет на подделку валюты в военное время? Существуют примеры таких мер». Например, Германия в годы Второй мировой войны провела операцию «Бернхард», направленную на подрыв британской экономики. Согласно некоторым сообщениям, правительство США занималось подделкой вьетнамской и иракской валюты во время войн с этими странами. *Mann F. A.* The Legal Aspect of Money, 5th ed. — Oxford: Oxford University Press, 1992; Nazi Fake Banknote 'Part of Plan to Ruin British Economy'. — Telegraph. — September 29, 2010 // http://www.telegraph.co.uk/history/world-war-two/8029844/Nazi-fake-banknote-part-of-plan-to-ruin-British-economy.html; *Suiter L., Hucke J., Schultz C.* The War at Home: A Look at Media Propaganda in WWII, Vietnam, and the War in Iraq. Final paper. — Stanford EDGE program. — December 2004; *Ibrahim*

Y. M. Fake-Money Flood Is Aimed at Crippling Iraq's Economy. — New York Times. — May 27, 1992 // http://www.nytimes.com/1992/05/27/world/fake-money-flood-is-aimed-at-crippling-iraq-s-economy.html?pagewanted=all.
15. *Lambert N. A.* The Strategy of Economic Warfare: A Historical Case Study and Possible Analogy to Contemporary Cyber Warfare / *Goldman E. O., Arquilla J.* (eds.) Cyber Analogies. — Monterey: Naval Postgraduate School, 2014 // http://calhoun.nps.edu/bitstream/handle/10945/40037/NPS- DA-14-001.pdf?sequence=1.
16. Конвенцию подписали и ратифицировали более восьмидесяти стран. Китай, Индия и США находятся в числе государств, которые подписали, но не ратифицировали ее.
17. *Gianviti F.* Current Legal Aspects of Monetary Sovereignty. — International Monetary Fund. — May 24, 2004 // https://www.imf.org/external/np/leg/sem/2004/cdmfl/eng/gianvi.pdf.
18. Самым последним и документально подтвержденным примером нарушения этой нормы является «супердоллар» — подделка денег Северной Кореей; *Mihm S.* No Ordinary Counterfeit. — New York Times. — July 23, 2006 // http://www.nytimes.com/2006/07/23/magazine/23counterfeit.html.
19. *Hathaway O., et al.* The Law of Cyber Attack. — California Law Review 100. — 2012 // http://digitalcommons.law.yale.edu/fss_papers/3852/.
20. *Schmitt M. N. (ed.)* Tallinn Manual on the International Law Applicable to Cyber Warfare. — Cambridge: Cambridge University Press, 2013. — P. 56–57.
21. Например, в январе 2016 года вооруженные силы США разрушили здание в Мосуле, в котором находились миллионы долларов, с целью расшатать финансовое положение «Исламского государства». В отличие от подделки валют в военное время это служит примером уничтожения физических денег; *Dunlap C.* The Loyola Conference and the Evolving Definition of Military Objective. — Lawfire (blog), Duke University. — February 14, 2016 // http://sites.duke.edu/lawfire/2016/02/14/the-loyola-conference-and-the-evolving-definition-of-military-objective/.
22. Кто-то может утверждать, что соглашение не потребует внесения изменений в американскую концепцию обеспечения ведения боевых действий, если будет рассматривать финансовые учреждения (в их физической форме) как потенциально разрешенные цели нападения и запрещать действия, направленные на нарушение целостности финансовых данных.
23. *Clapper J. R.* Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community. — Senate Armed Services Committee. — February 9, 2016 // http://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf.
24. *Clarke, Knake*. Cyber War. P. 202–203.
25. Например, предоставляя информацию об уязвимостях финансовых данных другим сторонам, осуществляющим злонамеренные действия, или игнорируя незаконные действия негосударственных субъектов.
26. United Nations General Assembly, A/70/174.
27. Policy Measures to Address Systemically Important Financial Institutions. — Financial Stability Board. — November 4, 2011 // http://www.fsb.org/wp-content/uploads/r_111104bb.pdf?page_moved=1.
28. Trans-Pacific Partnership. Chapter 11: Financial Services. — Office of the United States Trade Representative // https://ustr.gov/sites/default/files/TPP-Final-Text-Financial-Services.pdf.
29. Committee on Payment and Settlement Systems, Technical Committee of the International Organization of Securities Commissions: Principles for Financial Market Infrastructures. — Bank for International Settlements and IOSCO. — April 2012 // http://www.bis.org/cpmi/publ/d101a.pdf.
30. FSB Reports Foreign Special Services Preparing Massive Cyber Attacks. — TASS. — December 2, 2016 // http://tass.com/politics/916315.
31. *Kottasova I.* Russia: Foreign Hackers Are Trying to Take Down Our Banks. — CNN. — December 2, 2016 // http://money.cnn.com/2016/12/02/technology/russia-hack-banks-foreign/.
32. Ibid.
33. Ibid.
34. FSB Reports, TASS.
35. *Herman S.* Historic Bangladesh Bank Heist Muddled in Mystery. — Voice of America. — March 24, 2016 // http://www.voanews.com/content/historic-bangladesh-bank-heist-muddled-in-mystery/3252379.html; Gladstone G. Bangladesh Bank Chief Resigns After Cyber Theft of $81 Million. — New York Times. — March 15, 2016 // http://www.nytimes.com/2016/03/16/world/asia/bangladesh-bank-chief-resigns-after-cyber-theft-of-81-million.html?_r=0.
36. Reuters: Spelling Mistake Prevented Hackers Taking $1bn in Bank Heist. — Guardian. — March 10, 2016 // http://www.theguardian.com/business/2016/mar/10/spelling-mistake-prevented-bank-heist.
37. Gladstone: Bangladesh Bank Chief.
38. Reuters: Spelling Mistake.
39. *Shevchenko S.* Two Bytes To $951m. — Bae Systems Threat Research Blog. — April 25, 2016 // http://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html.
40. *Cerulus L.* Belgian Government Plagued by Hackers. — Politico. — February 22, 2016 // http://www.politico.eu/article/belgium-government-agencies-plagued-hackers-downsec-ddos-attacks-cybercrime/.
41. *Riley C.* China Stocks Plunge as Bubble Fears Grow. — The Open (blog), CNN. — June 19, 2015 // http://money.cnn.com/2015/06/19/investing/china-stocks-shanghai-correction/.
42. Chinese Stocks Tumble for a Second Day After Global Fall. — BBC. — August 25, 2015 // http://www.bbc.com/news/business-34048084; Alter D. What Today's China Stock Market Crash Means for Your Money in 2016. — Money Morning. — February 25, 2016 // http://moneymorning.com/2016/02/25/what-todays-china-stock-market-crash-means-for-your-money-in-2016/.
43. *Vicens A. J.* The Shocking Truth About Wednesday's Apocalypse Involving Wall Street, China, ISIS, and United Airlines. — Mother Jones. — July 8, 2015 // http://www.motherjones.com/politics/2015/07/nyse-glitch-hack-china-cia-cyber-isis.
44. *Gerden E.* Russian Bank Licences Revoked for Using Hackers to Withdraw Funds. — SC Magazine UK. — February

17, 2016 // http://www.scmagazineuk.com/russian-bank-licences-revoked-for-using-hackers-to-withdraw-funds/article/474464/.
45. *Cluley G.* Corkow — the Lesser-Known Bitcoin-Curious Cousin of the Russian Banking Trojan Family. — We Live Security. — February 11, 2014 // http://www.welivesecurity.com/2014/02/11/corkow-bitcoin-russian-banking-trojan/; How malware moved the exchange rate in Russia. — We Live Security. — February 12, 2016 // http://www.welivesecurity.com/2016/02/12/malware-moved-exchange-rate-russia/.
46. *Rudnitsky J., Khrennikov I.* Russian Hackers Moved Ruble Rate With Malware, Group-IB Says. — Bloomberg. — February 8, 2016 // http://www.bloomberg.com/news/articles/2016-02-08/russian-hackers-moved-currency-rate-with-malware-group-ib-says?mod=djemRiskCompliance.
47. *Kochetkova K.* Dozens of Banks Lose Millions to Cybercriminals Attacks. — Kaspersky Lab Daily (blog). — February 8, 2016 // https://blog.kaspersky.com/metel-gcman-carbanak/11236/.
48. Cyberberkut Hacked the Site of Ukrainian Ministry of Finance: The Country Has No Money. — SouthFront. — May 25, 2015 // https://southfront.org/cyberberkut-hacked-the-site-of-ukrainian-ministry-of-finance-the-country-has-no-money/.
49. *Bennett C.* Hackers Breach the Warsaw Stock Exchange. — Hill. — October 24, 2014 // http://thehill.com/policy/cybersecurity/221806-hackers-breach-the-warsaw-stock-exchange.
50. *Riley M., Robertson J.* Cyberspace Becomes Second Front in Russia's Clash With NATO. — Bloomberg. — October 14, 2015 // http://www.bloomberg.com/news/articles/2015-10-14/cyberspace-becomes-second-front-in-russia-s-clash-with-nato.
51. Ibid.
52. 'Cyber Berkut' Hackers Target Major Ukrainian Bank. — Moscow Times. — July 4, 2014 // http://www.themoscowtimes.com/business/article/cyber-berkut-hackers-target-major-ukrainian-bank/502992.html.
53. Pro-Russian Hackers Mug Key Ukrainian Bank. — ThreatWatch (blog), Nextgov. — July 4, 2014 // http://www.nextgov.com/cybersecurity/threatwatch/2014/07/stolen-credentials-network-intrusion-data-dump-pro/1225/.
54. *Gertz B.* Russian Cyber Warfare Suspected in Bank Attacks. — Flash//CRITIC Cyber Threat News. — August 30, 2014 // http://flashcritic.com/russian-cyber-warfare-suspected-bank-attacks-sophisticated-hackers/.
55. *Sanger D. E., Perlroth N.* Bank Hackers Steal Millions via Malware. — New York Times. — February 14, 2015 // http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html?_r=0.
56. Kaspersky Lab's Global Research and Analysis Team: The Great Bank Robbery: The Carbanak APT. — Securelist (blog), Kaspersky Lab. — February 16, 2015 // https://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/.
57. *Hang-Sun C.* Computer Networks in South Korea Are Paralyzed in Cyberattacks. — New York Times. — March 20, 2013 // http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html; *Zarate J. C.* The Cyber Financial Wars on the Horizon. — Foundation for Defense of Democracies. — July 2015 // http://www.defenddemocracy.org/content/uploads/publications/Cyber_Financial_Wars.pdf, p. 12–13.
58. Ibid.
59. *Kwon K. J.* Smoking Gun: South Korea Uncovers Northern Rival's Hacking Codes. — CNN. — April 22, 2015 // http://www.cnn.com/2015/04/22/asia/koreas-cyber-hacking/.
60. *O'Toole J.* JPMorgan: 76 Million Customers Hacked. — CNN. — October 3, 2014 // http://money.cnn.com/2014/10/02/technology/security/jpmorgan-hack/?iid=EL; *Pagliery J.* JPMorgan's Accused Hackers Had Vast $100 Million Operation. — CNN. — November 10, 2015 // http://money.cnn.com/2015/11/10/technology/jpmorgan-hack-charges/.
61. *Riley M., Robertson J.* FBI Said to Examine Whether Russia Tied to JPMorgan Hacking. — Bloomberg. — August 27, 2014 // http://www.bloomberg.com/news/articles/2014-08-27/fbi-said-to-be-probing-whether-russia-tied-to-jpmorgan-hacking.
62. *Zetter K.* Four Indicted in Massive JP Morgan Chase Hack. — Wired. — November 10, 2015 // http://www.wired.com/2015/11/four-indicted-in-massive-jp-morgan-chase-hack/.
63. Ibid.
64. Ibid; *Pagliery*. JPMorgan's Accused Hackers.
65. *Cowley M.* Brazilian Banks' Websites Face Hacker Attacks. — Wall Street Journal. — January 31, 2012 // http://www.wsj.com/articles/SB10001424052970204740904577194930748478316?cb=logged0.12500478560104966.
66. *Israel E.* Hackers Target Brazil's World Cup for Cyber Attacks. — Reuters. — February 26, 2014 // http://www.reuters.com/article/us-worldcup-brazil-hackers-idUSBREA1P1DE20140226.
67. #OpWorldCup: Anonymous wages cyber attacks against Brazil govt. — RT. — June 12, 2014 // https://www.rt.com/news/165444-anonymous-brazil-world-cup/.
68. *Cooper P.* Anonymous Lives Up to Threats: FIFA World Cup Hacks Get Underway. — IT Pro Portal. — June 13, 2014 // http://www.itproportal.com/2014/06/13/anonymous-lives-up-to-threats-fifa-world-cup-hacks-get-underway/#ixzz41DPxOwdR.
69. *Lemos R.* Cyber-Attacks Seen Defrauding Brazilian Payment System of Billions. — eWeek. — July 6, 2014 // http://www.eweek.com/security/cyber-attacks-seen-defrauding-brazilian-payment-system-of-billions.html.
70. *Marcus E.* RSA Uncovers Boleto Fraud Ring in Brazil. — RSA. — July 2, 2014 // https://blogs.rsa.com/rsa-uncovers-boleto-fraud-ring-brazil/.
71. Boleto Malware May Lose Brazil $3.75bn. — BBC. — July 3, 2014 // http://www.bbc.com/news/technology-28145401.
72. *Iasiello E.* Cyber Attack: A Dull Tool to Shape Foreign Policy (paper presented at the 2013 5th International Conference on Cyber Conflict) // https://ccdcoe.org/cycon/2013/proceedings/d3r1s3_Iasiello.pdf, p. 11.
73. *Goldman D.* Major Banks Hit With Biggest Cyberattacks in History. — CNN. — September 28, 2012 // http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/.

74. *Slavin B*. US Withholds Evidence for Iran Cyberattacks. — Al-Monitor. — January 17, 2013 // http://www.al-monitor.com/pulse/originals/2013/01/cyber-attacks-us-iran-ddos.html.
75. *Perlroth N., Hardy Q*. Bank Hacking Was the Work of Iranians, Officials Say. — New York Times. — January 8, 2013 // http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html.
76. Ibid.
77. *Slavin*. US Withholds Evidence.
78. *Schwartz M. J*. Bank Attackers Restart Operation Ababil DDoS Disruptions. — Dark Reading. — March 6, 2013 // http://www.darkreading.com/attacks-and-breaches/bank-attackers-restart-operation-ababil-ddos-disruptions/d/d-id/1108955.
79. *Sweeney P., Ruwitch J*. June 4 Crackdown Remembered in China Stock Index, or Chance? — Reuters. — June 4, 2012 // http://www.reuters.com/article/us-china-stocks-tiananmen-idUSBRE8530F720120604.
80. *Bradsher K*. Market's Echo of Tiananmen Date Sets Off Censors. — New York Times. — June 4, 2012 // http://www.nytimes.com/2012/06/05/world/asia/anniversary-of-tiananmen-crackdown-echos-through-shanghai-market.html.
81. Kaspersky Lab Discovers 'Gauss' — A New Complex Cyber-Threat Designed to Monitor Online Banking Accounts. Press release. — Kaspersky Lab. — August 9, 2012 // http://usa.kaspersky.com/about-us/press-center/press-releases/2012/kaspersky-lab-discovers-gauss-new-complex-cyber-threat-desi.
82. *Goodin D*. Puzzle Box: The Quest to Crack the World's Most Mysterious Malware Warhead. — Ars Technica. — March 14, 2013 // http://arstechnica.com/security/2013/03/the-worlds-most-mysterious-potentially-destructive-malware-is-not-stuxnet/.
83. *Zetter K*. Flame and Stuxnet Cousin Targets Lebanese Bank Customers, Carries Mysterious Payload. — Wired. — August 9, 2012 // http://www.wired.com/2012/08/gauss-espionage-tool/all/.
84. Kaspersky Lab Discovers 'Gauss'.
85. *Goodin*. Puzzle Box; *Zetter K*. Suite of Sophisticated Nation-State Attack Tools Found With Connection to Stuxnet. — Wired. — February 16, 2015 // http://www.wired.com/2015/02/kapersky-discovers-equation-group/.
86. *Zarate*. Cyber Financial Wars; *Zetter*. Flame and Stuxnet Cousin.
87. *Harlan C., Nakashima E*. Suspected North Korean Cyber Attack on a Bank Raises Fears for S. Korea, Allies. — Washington Post. — August 29, 2011 // https://www.washingtonpost.com/world/national-security/suspected-north-korean-cyber-attack-on-a-bank-raises-fears-for-s-korea-allies/2011/08/07/gIQAvW-wIoJ_story.html; North Korea 'Behind South Korean Bank Cyber Hack'. — BBC. — May 3, 2011 // http://www.bbc.com/news/world-asia-pacific-13263888.
88. Prosecution Says N. Korea Behind Nonghyup's Network Breakdown. — Yonhap. — May 3, 2011 // http://english.yonhapnews.co.kr/national/2011/05/03/23/0302000000AEN20110503007100315F.HTML?1a7c6120.
89. *Riley M*. How Russian Hackers Stole the NASDAQ. — Bloomberg. — July 21, 2014 // http://www.bloomberg.com/bw/articles/2014-07-17/how-russian-hackers-stole-the-nasdaq.
90. *Markoff J*. Before the Gunfire, Cyberattacks. — New York Times. — August 12, 2008 // http://www.nytimes.com/2008/08/13/technology/13cyber.html.
91. *Smith D. J*. Russian Cyber Capabilities, Policy and Practice / inFOCUS Quarterly 5, № 1. Winter 2014 // http://www.jewishpolicycenter.org/4924/russian-cyber-capabilities?utm_content=bufferbb5cd&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer; Markoff. Before the Gunfire, Cyberattacks.
92. *Smith*. Russian Cyber Capabilities, Policy and Practice.
93. *Markoff*. Before the Gunfire, Cyberattacks.
94. *Richards J*. Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security. — International Affairs Review 18, № 2. 2009 // http://www.iar-gwu.org/node/65.
95. Cyberwarfare 101: Case Study of a Textbook Attack. — Stratfor. — April 18, 2008 // https://www.stratfor.com/analysis/cyberwarfare-101-case-study-textbook-attack; *Richards*. Denial-of-Service.
96. Ibid.
97. Ibid.
98. Cyberwarfare 101; *Davis J*. Hackers Take Down the Most Wired Country in Europe. — Wired. — August 21, 2007 // http://www.wired.com/2007/08/ff-estonia/.
99. Ibid.

ФОНД КАРНЕГИ ЗА МЕЖДУНАРОДНЫЙ МИР

Фонд Карнеги за Международный Мир — это уникальная глобальная сеть центров политических исследований в России, Китае, Европе, на Ближнем Востоке, в Индии и США. Миссия Фонда, которой он следует уже более ста лет — способствовать делу мира посредством анализа и выработки новаторских политических идей, прямого диалога и сотрудничества с руководителями государств, бизнеса и гражданского общества. Работая совместно, наши центры обеспечивают неоценимое преимущество — разнообразие национальных точек зрения по двусторонним, региональным и глобальным проблемам.

 **@CarnegieEndow**

 **facebook.com/CarnegieEndowment**