УДК 070:34(063)

Некоторые аспекты международно-правового регулирования в информационной сфере

А.Н. Соломатин, *кандидат филологических наук, заместитель заведующего кафедрой телевидения и радиовещания АНО ДПО «Академия медиаиндустрии»; e-mail: alexns17@rambler.ru.*

В статье рассматриваются вопросы международно-правового регулирования информационно-коммуникативных технологий, особенности использования «информационного оружия», различные подходы в применении термина «агрессия». Автор анализирует возможности по выработке международных норм в сфере информационной безопасности, организации системы противодействия попыткам преступного и бесконтрольного использовании информационных и интернет-технологий. Показывается роль России и ее сторонников в процессе принятия решений по ограничению проведения трансграничных информационных атак, в развязывании межгосударственных конфликтов и создании с этой целью специального органа ООН.

Ключевые слова: *агрессия, информационное оружие, информационные атаки, кибервойна, киберпреступность, критическая информационная инфраструктура, международное право, межгосударственные военные конфликты, НАТО, ООН.*

За прошедшие 10–15 лет мир существенно изменился. Вопреки ожиданиям и надеждам он не стал более безопасным, более комфортным для проживания людей. Стремительный рост объемов информации и увеличение ее влияния на все сферы жизни человека в последние годы стали реальностью, с которой странам различного уровня развития приходится иметь дело в процессе обеспечения национальной безопасности. Возможности трансграничного оборота информации все чаще используются для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности. Все более сложными и изощренными становятся компьютерные атаки на объекты критически важных инфраструктур.

В 2018 году из-за хакерских атак, повлекших за собой утечки данных, организации и фирмы различного уровня по всему миру лишились трёх трлн. долларов. По данным компании Juniper Research, киберпреступники начинают использовать все более изощренные методы и инструменты. Среди них – искусственный интеллект, киберпреступ-

ность в социальных сетях и развитие таких технологий, как deepfake, которые позволяют создавать фейковые видеоролики с подменой лиц у действующих героев. В Juniper Research считают, что потери бизнеса от кибератак и последовавших от них утечек данных будут расти и превысят пять трлн. долларов[1]. К 2022 году, по прогнозу Всемирного экономического форума, сумма планетарного ущерба от кибератак может вырасти до восьми трлн. долларов[2].

Как заявляют эксперты, фокус перспективной разработки и инноваций в создании сложных вирусов, а также проведении многоступенчатых целевых атак сместился от финансово-мотивированных киберпреступников к проправительственным хакерам. Их действия направлены на обеспечение долговременного присутствия в сетях объектов критической инфраструктуры с целью саботажа или шпионажа за компаниями энергетического, ядерного, коммерческого, водного, авиационного и других секторов. Азиатско-Тихоокеанский регион по итогам 2017-2018 гг. стал самым активно атакуемым хакерами разных стран. За год здесь была зафиксирована активность 21 различных групп, что больше чем в США и Европе вместе взятых[3].

Атакам подвергаются ресурсы бизнес-сектора, государственных органов, общественных организаций и СМИ. Не так давно в США хакеры атаковали 50 финансовых компаний и получили доступ к информации ограниченного пользования IT-инфраструктуры дамбы в Нью-Йорке. Неоднократно фиксировались попытки взлома внутренней компьютерной сети немецкого бундестага и блокировки сайта канцлера ФРГ. В Польше отменялись более десятка рейсов крупнейшей авиакомпании «Лот» из-за вторжения в IT-систему аэропорта Варшавы. Подвергнув атаке сайт газеты «Лос-Анджелес таймс», хакеры получили возможность самовольно изменять содержание материалов издания.

Существенно обострились угрозы возникновения военных конфликтов в результате агрессивного или иного враждебного использования информации и современных информационно-коммуникационных технологий. В сочетании с экстремистскими, националистическими, расистскими действиями они способны дестабилизировать обстановку и устранить от власти любое правительство как в самом развитом, так и в отсталом государстве. Сегодня ни одна страна мира не может считать себя защищенной от трансграничных информационных угроз.

По данным российского Национального координационного центра

---

[1] Business Losses to Cybercrime Data Breaches to Exceed $5 trillion by 2024. URL: https://www.businesswire.com/news/home/20190826005013/en/Business-Losses-Cybercrime-Data-Breaches-Exceed-5 (дата обращения 01.11.2019).

[2] Там же.

[3] Group-IB представила отчет о киберпреступности и призвала рынок к хантингу. URL: https://www.group-ib.ru/media/hi-tech-crime-trends-2018/ (дата обращения: 01.10.2019)

по компьютерным инцидентам[1], в 2018 году было совершено более 4,3 млрд информационных воздействий на критическую информационную инфраструктуру РФ. Участились случаи скоординированных целенаправленных компьютерных атак из нескольких связанных между собой акций. В 2014-2015 годах количество таких атак составляло около 1,5 тысяч в год, а в 2018 уже превысило 17 тысяч.

В первой половине 2019 года предотвращено внедрение вредоносного программного обеспечения на более чем на 7 тысячах объектов критической информационной инфраструктуры. При этом целями атак становились объекты кредитно-финансовой сферы – 38 % от общего числа атак, органов государственной власти – 35 %, оборонной промышленности – 7 %, сферы науки и образования – 7 %, сферы здравоохранения – 3 %. Эти цифры говорят о колоссальной опасности, которую несут компьютерные атаки, т.к. атакуемые объекты обеспечивают повседневную жизнедеятельность общества и государства, безопасность граждан.

Информационные технологии могут стать детонатором развязывания межгосударственных военных конфликтов. При чем для создания конфликтной ситуации требуется гораздо меньше затрат, чем классическая подготовка традиционной войны. При этом не нужно создавать крупных группировок войск, концентрировать в определенных районах авиацию, артиллерию, противовоздушную оборону, подтягивать логистические подразделения и так далее.

Информационные воздействия являются бескровными, не разрушают окружающую среду и могут реализовываться через вполне мирные средства – СМИ, интернет, средства телекоммуникаций, информатики, связи и др. Посредством дезинформационных вбросов, публикаций и распространения экстремистских заявлений, проведения расистских или ксенофобских флэшмобов, трансграничных компьютерных атак на критически важные для жизни и деятельности общества объекты возможно «разогреть» ситуацию в любой стране до «социального взрыва». Подобные действия также способны поссорить несколько государств и довести их до состояния войны. На примерах «цветных» революций и волнений последнего десятилетия можно с уверенностью сказать, что такие технологии уже достаточно хорошо обкатаны.

Ситуацию осложняет и тот факт, что многими государствами для установления контроля над противником в информационной сфере, вмешательства в работу его автоматизированных систем и образцов вооружения, воздействия на командование и личный состав вооруженных сил, а также население и инфраструктуру разрабатываются специальные информационные технологии, средства и методы, называемые ин-

[1] Интервью заместителя секретаря Совета безопасности РФ О. Храмова «Российской газете» 15 августа 2019 года. URL: http://www.scrf.gov.ru/news/allnews/2629/ (дата обращения: 01.10.2019).

формационным оружием. Сегодня это понятие трактуется по-разному. Как видно из определения государств-членов ШОС, «информационное оружие – это информационные технологии, средства и методы, применяемые в целях ведения информационной войны»[1].

Ущерб от использования такого оружия может приводить к техногенным катастрофам на критически важных объектах промышленности, энергетики и транспорта, к финансовому коллапсу и системному экономическому кризису. С развитием информационных технологий будет расширяться линейка информационного оружия, а также увеличиваться перечень объектов, по которым предполагается его применение. Запретить разработку данного вида оружия, а главное – проконтролировать его наличие у государств, а тем более у террористических группировок практически невозможно. Но инициировать выработку механизма его нераспространения возможно. Кроме того, принятием международных правовых актов можно снизить вероятность применения информационного оружия по критически важным объектам государства (ядерная отрасль, энергетика, системы жизнеобеспечения и др.).

В ситуации юридической неурегулированности такого сложного вопроса западные государства пошли другим путем. В 2014 году на саммите НАТО в Уэльсе подтверждено, что в планах альянса рассматривать кибератаки на одного из членов НАТО как агрессию против блока в целом[2]. В Варшаве в 2016 году членами организации киберпространство признано новой «операционной средой», а киберзащита становится частью основной задачи НАТО по коллективной обороне[3]. При этом наиболее действенным ответом на нетрадиционные угрозы считается метод «сдерживания» геополитических соперников, основанный на демонстрации, а при необходимости и применении военной силы в информационном пространстве. Реагирование военной силой на какие-либо реальные или мнимые информационные угрозы может серьезно дестабилизировать ситуацию во всем мире.

Традиционно нарушение государственного суверенитета, территориальной неприкосновенности или политической независимости другого государства осуществляется в конкретных физических средах (наземном, морском и воздушном пространствах). Теперь появилась и «информационная сфера», в которой у каждого государства существуют свои интересы, подлежащие защите. В отличие от физических сред эта сфера не имеет явно выраженных государственных границ.

---

[1] Соглашению между правительствами государств–членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности // Бюллетень международных договоров. 2012. № 1. URL: www.mid.ru (дата обращения: 02.11.2019).

[2] Страны НАТО договорились об усилении обороны и создании спецсил. URL: https://ria.ru/world/20140905/1022950468.html (дата обращения: 16.05.2018).

[3] Cyber defence. URL: https://www.nato.int/cps/en/natohq/topics_78170.htm (дата обращения: 16.05.2018).

Деструктивное воздействие на объекты информационной сферы может осуществляться как с использованием традиционного оружия, так и с использованием информационных технологий, что можно квалифицировать как нарушение суверенитета, территориальной неприкосновенности или политической независимости другого государства, т.е. как агрессию.

В качестве примера можно рассмотреть гидро- или атомную электростанцию, которые являются критически важными объектами инфраструктуры государства. Если нанести по таким объектам удар любым из имеющихся современных вооружений, то это приведет к колоссальным разрушениям и массовой гибели людей. Это точно будет считаться актом агрессии. А если с использованием компьютерной атаки нарушена работа автоматизированной системы управления этого объекта, которая привела к тем же последствиям – данный факт будет считаться агрессией? С высокой степенью вероятности такие действия можно классифицировать как акт агрессии.

На наш взгляд, при проведении международно-правовой квалификации конкретного акта военного применения информационных технологий в соответствии с определением агрессии следует учитывать два основных фактора. Во-первых, агрессором может быть признано то государство, которое первым осуществило информационную атаку на другое государство для решения своих военно-политических задач. Во-вторых, для вынесения окончательного вердикта о том, является ли данная информационная атака актом агрессии или нет, следует оценить характер последствий этой атаки. В том случае, если последствия будут признаны катастрофическими, атака может быть квалифицирована как акт агрессии.

Однако на практике принять такое решение сейчас вряд ли удастся, так как для определения степени серьезности военного применения информационных технологий необходим соответствующий критериальный аппарат. В настоящее время роль такого аппарата в отношении применения традиционной вооруженной силы выполняет перечень возможных актов агрессии, приведенный в статье 3 Резолюции Генеральной Ассамблеи ООН «Определение агрессии» № 3314 (XXIX) от 14 декабря 1974 г.[1]. Все перечисленные в нем акты в той или иной мере

---

[1] Статья 3 Резолюции Генеральной Ассамблеи ООН «Определение агрессии» № 3314 (XXIX) от 14 декабря 1974 г.: «Любое из следующих действий, независимо от объявления войны, с учетом и в соответствии с положениями статьи 2, будет квалифицироваться в качестве акта агрессии:

a) вторжение или нападение вооруженных сил государства на территорию другого государства или любая военная оккупация, какой бы временный характер она ни носила, являющаяся результатом такого вторжения или нападения, или любая аннексия с применением силы территории другого государства или части ее;

b) бомбардировка вооруженными силами государства территории другого государства

могут применяться для квалификации агрессивного использования информационных технологий. Однако с 1974 года информационные технологии шагнули так далеко, что этого перечня в условиях цифровизации уже явно недостаточно.

По мнению начальника управления Генерального штаба РФ И. Дылевского, перечень актов агрессии можно дополнить положением о «применении вооруженными силами государства информационного оружия против критически важных объектов другого государства, которое повлекло за собой большие человеческие жертвы и разрушения»[1]. Представляется также необходимым разработать положение о применении технологий информационно-психологического воздействия, получивших широкое распространение в последнее время. С применением таких технологий, в частности, провоцируются «цветные» революции. В данное положение можно внести такие пункты, как «подстрекательские действия для свержения законно-избранных правительств, пропаганда войны и применения силы, распространение целенаправленной информации и дезинформации, способствующих дестабилизации внутригосударственной и международной обстановки, развязыванию и эскалации вооруженных конфликтов».

Стоит отметить, что в соответствии со статьёй 4 «Определения агрессии» СБ ООН государство может самостоятельно определять, какие акты представляют собой агрессию. Данный механизм также целесообразно использовать при определении виновника в агрессии.

Возможность применения права государств на самооборону и коллективную оборону (ст. 51 Устава ООН) в качестве реагирования на вооруженное нападение с использованием информационного оружия

или применение любого оружия государством против территории другого государства;

c) блокада портов или берегов государства вооруженными силами другого государства;

d) нападение вооруженными силами государства на сухопутные, морские или воздушные силы, или морские и воздушные флоты другого государства;

e) применение вооруженных сил одного государства, находящихся на территории другого государства по соглашению с принимающим государством, в нарушение условий, предусмотренных в соглашении, или любое продолжение их пребывания на такой территории по прекращению действия соглашения;

f) действие государства, позволяющего, чтобы его территория, которую оно предоставило в распоряжение другого государства, использовалась этим другим государством для совершения акта агрессии против третьего государства;

g) засылка государством или от имени государства вооруженных банд, групп, иррегулярных сил или наемников, которые осуществляют акты применения вооруженной силы против другого государства, носящие столь серьезный характер, что это равносильно перечисленным выше актам, или его значительное участие в них».

Доступ из справочно-правовой системы «КонсультантПлюс» (дата обращения: 31.01.2020).

[1] *И. Дылевский.* Выступление на дискуссионной секции № 2 «Безопасность информационного пространства и свобода доступа к информации: противоречивость взаимосвязи» // 6-я Конференция по безопасности в Минобороны РФ (MCIS-2017, 26.04.2017) URL: https://www.youtube.com/watch?v=m4W693_IVbA&feature=youtu.be (дата обращения: 11.10.2019).

тесно связана с вопросом об актах агрессии. В первую очередь, необходимо дать международно-правовое определение термину «вооруженное нападение с использованием информационного оружия». Не решив эту проблему в рамках ООН, нельзя говорить о возможности непосредственного применения существующей нормы. Но Североатлантический союз в обход ООН в своих документах уже закрепил данную норму.

На сегодня практическое признание трансграничных информационных воздействий «вооруженным нападением» представляется проблематичным. Во-первых, не разработаны методы и средства оперативного и точного определения местоположения и национальной принадлежности источников информационного нападения. Во-вторых, даже если эти источники идентифицированы, то возникает проблемный вопрос – как установить связь некоего сетевого сообщества с заинтересованными государственными структурами? Что если его члены действуют исключительно из патриотических или иных побуждений? Кто должен нести международную ответственность за результаты осуществления вредоносного информационного нападения? Против кого конкретно должны осуществляться ответные действия?

Войны развязывают и ведут государства с использованием вооруженных сил. Что касается иных физических и юридических лиц, то они могут считаться источником агрессии лишь в том случае, если действуют по заказу государственных структур. При этом лица, которые осуществляют трансграничные нападения, руководствуясь террористическими, экстремистскими или корыстными мотивами, не могут рассматриваться в качестве источника вооруженного нападения. В этом случае информационные нападения должны квалифицироваться как террористические, экстремистские или иные уголовные преступления.

Пока эти проблемы не решены, нет полной ясности относительно того, имеется ли основа для проведения ответных военных действий против государств, осуществляющих вооруженное нападение с использованием информационного оружия. Единственно верным правовым путем решения данной проблемы на сегодняшний день остается принятие соответствующего международно-правового акта ООН. Так как сейчас подобного документа не существует, может быть использовано обращение за помощью в Совет Безопасности ООН с тем, чтобы он квалифицировал информационное нападение как угрозу миру или агрессию и предпринял определенные меры, предусмотренные Уставом ООН. Поэтому если определенные виды таких информационных воздействий будут квалифицированы СБ ООН как вооруженное нападение, пострадавшая сторона будет иметь законное право на самооборону. Однако и в этом случае должен быть решен вопрос о проведении либо симметричных, либо несимметричных ответных действий с использованием информационного или обычного оружия.

Страны Запада рассматривают данный вопрос только применительно к кибератакам или по российской терминологии – компьютерным атакам. Информационно-психологические воздействия, например, приведшие к «цветным» революциям, ими не рассматриваются, хотя последствия от падения правительств для экономики страны, социальной сферы и других сфер жизнедеятельности гораздо разрушительнее, чем от поражения отдельных критически важных объектов.

В случае игнорирования норм международного права и принятия решений в обход ООН на роль агрессора странами НАТО может быть назначено любое неугодное для них государство. Достаточно будет только заявить о так называемой кибератаке на них, и в ответ применить военную силу.

В этой связи многие эксперты и аналитики остро ставят вопрос о том, в каком объеме должен осуществляться комплекс мер, призванных обеспечить сохранение государственного суверенитета на разных уровнях. Неограниченное распространение любой интернет-информации в странах Северной Африки и Ближнего Востока, а также в Латинской Америке, стало одной из причин подрыва стабильности и создания предпосылок для постепенного погружения мировой цивилизации в пучину хаоса. В этом случае интернет является, по существу, одним из дестабилизирующих факторов и контроль над его дальнейшим развитием жизненно необходим – опять же в интересах сохранения национального суверенитета государств, заинтересованных в поддержании стабильности на мировом уровне.

Кроме того, требует рассмотрения и проблема ответственности государства за действия в информационном пространстве уполномоченных ими лиц.

Нормы международного гуманитарного права устанавливают, что война должна вестись только между вооруженными силами соответствующих государств (комбатантами). Причем в состав вооруженных сил (регулярных и нерегулярных) входят силы милиции (полиции), безопасности, добровольческие отряды, отряды ополчения, партизаны, а также население, которое по собственной инициативе берется за оружие для борьбы с вторгающимися войсками, не успев сформироваться в регулярные части. Все указанные категории сражающихся рассматриваются в качестве законных участников войны, если они удовлетворяют следующим условиям, предусмотренным конвенциями: имеют во главе лицо, ответственное за своих подчиненных; имеют определенный и ясно видимый издали отличительный знак; открыто носят оружие; соблюдают в своих действиях законы и обычаи войны.

Очевидно, что некоторые из перечисленных пунктов не только не согласуются со спецификой проведения трансграничных информационных атак, но и не могут быть напрямую внедрены в практику расследования фактов их проведения. Таким образом, определение статуса «комбатанта» применительно к действующим в информпространстве

лицам также требует разработки и внедрения соответствующей юридической методологии. В противном случае, задача привлечения к ответственности конкретных государств и соответствующих должностных лиц представляется неразрешимой.

Квалификационные признаки событий в информационном пространстве, несущие в себе военно-политические угрозы, должны формулироваться на основе анализа положений существующих международно-правовых актов, норм национальных законодательств, а также информации о практике расследования инцидентов информационной безопасности в различных странах. До настоящего времени в мировой практике пока не зафиксировано ни одного случая квалификации таких событий.

Преступления в сфере информационно-коммуникационных технологий носят трансграничный характер. Однако законодательство государств является фрагментарным и не гармонизировано с точки зрения как материального, так и процессуального права. Ряд стран имеют возможность пользоваться региональными инструментами, однако их число и сфера географического охвата ограничены. Налицо необходимость углубления международного сотрудничества в этой области, выведения его на новый универсальный уровень.

В настоящее время формируется международный консенсус в отношении необходимости укрепить сотрудничество и выработать соответствующие правовые нормы, чтобы противостоять общим вызовам в сфере информационной безопасности. Однако США и их союзники призывают автоматически применять нормы и принципы международного права к регулированию военного использования информационно-коммуникационных технологий. По их мнению, это относится к возможности применения военной силы в ответ на трансграничное информационное воздействие. Отвергаются попытки регулирования в интернете, необходимость в хранении интернет-компаниями данных пользователей на своей территории, а также принятие резолюции ООН по борьбе с киберпреступностью, ссылаясь на то, что для такой борьбы уже есть все инструменты, заложенные в том числе и в Будапештской конвенции Совета Европы о компьютерных преступлениях 2001 года. Россию же не устраивает ст. 32 этой Конвенции («Трансграничный доступ к хранящимся компьютерным данным с соответствующего согласия или к общедоступным данным»), что позволяет спецслужбам без официального уведомления проводить операции в компьютерных сетях третьих стран.

Российская позиция состоит в том, что, не отрицая незыблемость права на самооборону, необходимо провести большую работу по созданию международно-правовой базы, с использованием которой можно будет адекватно осуществлять его реализацию применительно к спец-

ифике информационной сферы[1]. Необходимо исключить ситуации, когда какое-либо государство самостоятельно и без предъявления доказательств по собственному усмотрению определяет потенциальный источник киберугроз и наносит разрушительный карательный удар.

Страны Шанхайской организации сотрудничества (ШОС) на постоянной основе координируют свои подходы по международной информационной безопасности в ООН. В конце 2018 года по инициативе государств-членов была принята Резолюция Генассамблеи ООН под названием «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», где обозначены призывы к международному сообществу прилагать усилия к созданию мирного, безопасного, открытого и основанного на сотрудничестве упорядоченного информационного пространства. Подчеркивают центральную роль ООН в выработке универсальных международных норм, правил и принципов ответственного поведения государств в информационном пространстве, считая необходимым создать в рамках ООН на основе справедливого географического распределения рабочий механизм с целью выработки норм, правил и принципов ответственного поведения государств в информационном пространстве и их формализации путем принятия соответствующей резолюции Генеральной Ассамблеи[2].

Создание третейского органа по урегулированию конфликтов в киберсфере – одна из главных мер, которые предлагает Россия. Несмотря на противостояние ряда государств, в декабре 2019 года большинство стран-участниц Генассамблеи ООН поддержали резолюцию «О противодействии использованию информационно-коммуникационных технологий в преступных целях», соавторами которой вместе с Россией стали еще 47 государств. В поддержку российской инициативы выступили 79 стран (против – 60, еще 33 воздержались). Документ, голосование которого состоялось в Третьем комитете ООН, предусматривает создание специального межправительственного комитета экспертов из всех регионов.

Документы Генассамблеи ООН сами по себе не являются юридически обязывающими, однако могут запустить механизмы, результатом работы которых в итоге станет имеющая силу закона конвенция. Так это в свое время было, например, с Конвенцией ООН против коррупции и Конвенцией ООН против транснациональной организованной преступности.

---

[1] Десятый международный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности», Гармиш-Партенкирхен, Германия, 25–28 апреля 2016 года. URL: https://interaffairs.ru/virtualread/infosecurity/files/assets/downloads/publication.pdf. (дата обращения: 15.06.2019).

[2] Секретариат ШОС принял участие в работе Инфофорума Россия-Китай 2019. URL: http://rus.sectsco.org/news/20191026/589517.html (дата обращения: 01.11.2019.

Литература:

- *И. Дылевский.* Выступление на дискуссионной секции № 2 «Безопасность информационного пространства и свобода доступа к информации: противоречивость взаимосвязи» // 6 Конференция по безопасности в Минобороны РФ (MCIS-2017, 26.04.2017). URL: https://www.youtube.com/watch?v=m4W693_IVbA&feature=youtu.be.
- Десятый международный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности», Гармиш-Партенкирхен, Германия, 25–28 апреля 2016 года. URL: https://interaffairs.ru/virtualread/infosecurity/files/assets/downloads/publication.pdf
- Интервью заместителя Секретаря Совета Безопасности РФ О. Храмова «Российской газете» 15 августа 2019 года. URL: http://www.scrf.gov.ru/news/allnews/2629/.
- Секретариат ШОС принял участие в работе Инфофорума Россия-Китай 2019. URL: http://rus.sectsco.org/news/20191026/589517.html.
- Соглашение между правительствами государств–членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности // Бюллетень международных договоров.2012. № 1. URL: www.mid.ru.
- прав.- правовая система «КонсультантПлюс». URL: http://www.consultant.ru/.
- Страны НАТО договорились об усилении обороны и создании спецсил. URL: https://ria.ru/world/20140905/1022950468.html.
- Business Losses to Cybercrime Data Breaches to Exceed $5 trillion by 2024. URL: https://www.businesswire.com/news/home/20190826005013/en/Business-Losses-Cybercrime-Data-Breaches-Exceed-5.
- Cyber defence. URL: https://www.nato.int/cps/en/natohq/topics_78170.htm
- Group-IB представила отчет о киберпреступности и призвала рынок к хантингу. URL: https://www.group-ib.ru/media/hi-tech-crime-trends-2018/.

Поступила в редакцию 6 января 2020 года.