https://doi.org/10.5281/zenodo.3763255
УДК 327.2

Хлопов О.А.

Хлопов Олег Анатольевич, кандидат политических наук, доцент, Российский государственный гуманитарный университет, 125993, Россия, ГСП-3, Москва, Миусская площадь, д. 6. E-mail: rggu2007@rambler.ru.

Наступательные стратегии кибероружия как угроза международной безопасности

Аннотация. В статье рассматриваются подходы к понятию кибервойна и киберугрозы. Автором отмечается, что участники киберпространства предпочитают наступательные стратегии, в тоже время в киберпространстве со стороны многих государств доминируют киберзащитные действия. Это, в свою очередь, может служить основой для заключения эффективного международного соглашения о контроле над киберпростанством. В заключении подчеркивается необходимость принятия международной конвенции о применении кибероружия, а международный контроль над вооружениями и стремление укрепить индивидуальный потенциал государств могут служить основой для глобальной кибербезопасности.
Ключевые слова: киберугрозы, кибервойна, наступательная стратегия, США, международные отношения, международная безопасность.

Khlopov O.A.

Khlopov Oleg Anatolyevich, Candidate of Political Sciences, Associate Professor, Russian State Humanitarian University, 125993, Russia, GSP-3, Moscow, Miusskaya square, 6. E-mail: rggu2007@rambler.ru.

The Offensive Strategies of Cyber Warfare as Threat to International security

Abstract. The article discusses approaches to the concept of cyber war and cyber threat. The author argues that participants in cyberspace prefer offensive strategies, while at the same time in many countries cyber security dominates cyberspace. This, in turn, can serve as the basis for concluding an effective international agreement on the control of cyberspace. The conclusion emphasizes the need for an international convention on the use of cyber weapons, and international arms control and the desire to strengthen the individual capacities of states that can be the basis for global cyber security.
Key words: cyber threats, cyber warfare, offensive strategy, USA, international relations, international security.

Способность государств использовать современные информационные и коммуникационные технологии для нанесения серьезного вреда своим противника была в достаточной степени продемонстрирована в последние годы. Многие страны сообщают о широкомасштабных кибератаках против своих военных систем, водоснабжения и другой критически важной инфраструктуры. Способность государств использовать современные информационные и коммуникационные технологии (ИКТ) для нанесения серьезного экономического, политического и материального была наглядно продемонстрировано перед втор-

жением в Ирак в марте 2003 г. США нанесли «упреждающий удар»- отрезали иракские компьютерные сети и интернет-сеть, чтобы подорвать политическую и военную оборону режима.

Когда израильские истребители подвергли бомбардировке предполагаемый ядерный объект в Диая-аль-Сахир в Сирии, в 2007 г., они впервые взломали сирийские системы противовоздушной обороны, чтобы скрыться их от нападения. Позже в том же году Америка и Израиль использовали изощренное вредоносную программу «Stuxnet», чтобы отключить ядерный реактор в Натанзе, Иран. В 2017 г. Пентагон использовал кибердудары по ракетной программе Северной Кореи для саботажа испытательных пусков [1].

Между тем американские спецслужбы сообщают о множестве попыток кибератак на критически важную инфраструктуру в США, включая системы управления воздушным движением, спутниковые системы и национальные электрические сети. По мнению экспертов, Пекин успешно взломал американские базы данных и критическую инфраструктуру, такую как атомные и электрические электростанции и спутниковые системы. Северная Корея стремилась подавить электронные сигналы для управляемых США ракет, а хакеры, связанные с иранским правительством, взломали небольшую плотину в Нью-Йорке и сети AT & T, Bank of America и Нью-Йоркской фондовой [2].

Перспектива подобных атак на военные средства противовоздушной обороны, системы водоснабжения, химические и атомные электростанции или нефте- и газопроводы заставили политических и военных лидеров обратить внимание на необходимость приятия более эффективных средств кибер сдерживания. В 2009 г. в рамках Министерства обороны США было создано «Киберкомандование США», задача которого состоит в том, чтобы «проводить военные операции в киберпространстве полного спектра… [чтобы] обеспечить свободу действий США и союзников в киберпространстве и отрицать то же самое для наших противников» [3]. Подобные военные структуры были созданы во многих других странах. По крайней мере, 29 правительств в настоящее время имеют военные или разведывательные подразделения, специально предназначенные для наступательных кибероперациий, и более 60 стран разрабатывают кибероружие.

Сегодня в мире происходит развертывание международной гонки кибервооружений. Разработка ядерного оружия произвела революцию в стратегическом мышлении после Второй мировой войны и вызвала десятилетия гонки ядерных вооружений, которая лишь постепенно становилась под контролем благодаря интенсивной международной дипломатии и формальным соглашениям о контроле над вооружениями. Подобным образом новые кибертехнологии сегодня вызвали яростную борьбу за развитие кибертехнологий. наступательный вооружений и разработать новые стратегии для защиты от них [4].

История показывает, что гонку вооружений лучше всего контролировать с помощью официальных многосторонних соглашений, тщательно разработанных для уменьшения опасений и напряженности, повышения прозрачности и содействия взаимным сокращениям вооружений. От изобретения огнестрельного оружия до эволюции современного химического, биологического и ядерного оружия, внедрение новых военных технологий, как правило, приводит к усилиям и стремлениям со стороны международного сообщества для управления и ограничения их использования. Несмотря на нынешнюю гонку по размещению вооружений в киберпространстве, все призывы к международным договорам для регулирования кибервойн были решительно отклонены [5].

В настоящее время не существует согласованных международных правил или норм, регулирующих международные конфликты в киберпространстве. Многие правительства предпочитают не разраба-

тывать их, утверждая, что трудности проверяемости и проблемы, связанные с быстрыми технологическими изменениями, исключают соглашение о международной киберконвенции. Вместо этого страны предпочитают полагаться на неформальное сотрудничество и стратегическое сдерживание для ограничения прямого конфликта.

Очевидно, не стоит надеяться на то, что политические и военные лидеры откажутся от текущих целей укрепления киберинфрастуркутры своих государств в пользу особой опоры на международную дипломатию в борьбе с кибер соперничеством. Как и во время ядерного противостояния в годы «холодной войны», международный контроль над вооружениями и стратегическое сдерживание должны идти рука об руку с целью уменьшения рисков глобального киберконфликта.

Определения кибервойны.

В научной и общественно-политической литературе не существует четкого однозначного понимания содержания таких терминов, как «кибервойна» и «киберугрозы», и эксперты концентрируют внимание на различных проблемах или угрозах. Поэтому прежде чем продолжить, необходимо кратко определить ключевые концепции анализа.

Чтобы определить термины, относящиеся к анализу киберконфликта, мы должны сначала определить что есть «киберпространство». Киберпространство - это искусственная среда, состоящая из информации, данных и инфраструктуры управления – информационные и коммуникационные технологии (information and communication technology) ИКТ. Эта среда ежедневно используется сотнями миллионов людей для общения, поиска информации и проведения обычных деловых операций. В настоящее время, однако, киберпространство быстро «превращается в оружие». Это вооружение принимает две формы.

Во-первых, киберпространство становится оружием, поскольку в киберсреду вводятся наступательные вооружения, которые способны разрушать или повредить объекты в той же среде.

Во-вторых, само киберпространство все чаще рассматривается государствами как военный актив. Современные системы вооружений часто сильно зависят от инфраструктуры ИКТ, и поэтому киберпространство становится предметом горячих споров. О важности киберпространства как военной области свидетельствует заявление Министерства обороны США о том, что «Министерство будет выполнять кинетические задачи, чтобы сохранить свободу действий и стратегические преимущества в киберпространстве. Кинетические действия могут быть как наступательными, так и оборонительными и использоваться совместно с другими районами миссии для достижения оптимальных военных эффектов» [6].

Аналогичное заявление, но с большим упором на оборону, было сделано лидерами НАТО в 2016 г., когда они обозначили киберпространство как «оперативная область, в которой Североатлантический союз должен защищать себя так же эффективно, как и в воздухе, на суше и на море» [7].

Продолжающаяся вооруженная борьба с киберпространством значительно повышает риск возникновения международных конфликтов, возможно, поднимаясь до уровня кибервойны. В современной литературе термин «кибервойна» обычно используется для обозначения любого враждебного действия, которое происходит в киберпространстве или через него. Как отмечает Джозеф Най, киберпространство таит в себе широкий спектр угроз для государств и отдельных лиц - от кражи личных данных и кибершпионажа до различных форм электронных преступлений и саботажа низкого уровня посредством атак типа «отказ в обслуживании» или порчи интернет-сайты [8]. В то время как это враждебные и преступные действия, лишь немногие достигают уровня «военных действий».

Более узкое определение кибервойны как преднамеренного и враждебного ис-

пользования государством кибероружия с целью причинения телесных повреждений или смерти людям или значительного разрушения, повреждения или уничтожения стратегические активы другого государства или критическая национальная инфраструктура.

Это определение аналогично тому, которое предлагается в «Таллиннском руководстве» от 2013 г. (Talinn Manual) в котором кибератаки определяются как «наступательные или оборонительные кибердействия, которые, как ожидается, приведут к травмам или смерти людей или повреждению или разрушению объектов» [9]. Другое определение данное Метте Сангиованни отличается тем, что для того, чтобы квалифицировать акцию как кибервойна, кибератаки должны совершаться государственными субъектами и иметь целью уничтожение или повреждение объектов, имеющих стратегическое значение для страны. В содержании этого определения акцент делается на субъектности исполнителя – государство, которое обладает значительными ресурсами и преимуществами перед другими участниками.

Такое определение основывается на трех критериях, касающихся происхождения, средств и последствий враждебных действий в киберпространстве.

Первый критерий указывает, что кибервойна относится к враждебным действиям, совершаемым государствами и направленным против них. Некоторые исследователи не согласны с этим определением, делающим акцент на межгосударственный конфликтах, возражая, что многие нынешние киберугрозы исходят от негосударственных акторов. Но в то время как многие негосударственные акторы все больше разбираются в киберпространстве они, как правило, не имеют возможности самостоятельно проводить сложные кибер атаки против критической инфраструктуры. Среди кибер-экспертов растет понимание того, что негосударственные субъекты, такие как «хакеры и «кибер-ополченцы», в основном работают в тандеме или по указанию национальных правительств [10]. Кроме того, борьба с киберугрозами со стороны негосударственных акоторов представляет собой иной набор проблем для системы международного сотрудничества, нежели управление межгосударственными конфликтами.

Второй критерий указывает, что кибервойна относится к актам войны, совершаемым с использованием кибероружия. Кибероружие, в свою очередь, определяется как оружие, построенное в основном из программного обеспечения и данных, которые предназначены для нанесения целевого вреда или широкомасштабного уничтожения [11]. Отсюда следует, что кинетический удар по национальной инфраструктуре ИКТ не будет представлять собой акт кибервойны, но может представлять собой акт обычной войны.

Третий критерий предусматривает, что для того, чтобы считаться кибервойной, кибератака должна наносить серьезный ущерб. В дополнение к умышленным травмам или смерти людей это может включать стремление нанести значительный ущерб или разрушить стратегические активы другого государства или критически важную национальную инфраструктуру. «Стратегические активы» как определяют их эксперты, «жизненно важные активы, разрушение которых может оказать колоссальное влияние на национальную безопасность государства и его способность нормально функционировать» [10].

К ним могут относиться военные группировки государства, оборонно-промышленная база, спутниковая связь, электросеть, подключение к Интернету, центральная банковская система, фондовый рынок и правительственные учреждения.

Таким образом, можно отметить, что кибервойна относится к враждебным действиям, которые: а) совершаются государствами, в том смысле, что они направляются или контролируются государственными органами [8]; б) используется кибероружие; в) ее цель нанести

серьезный вред или ущерб людям или стратегическим объектам.

Как отмечает эксперт по кибербезопасности Лукас, вирус «Struxnet» уникален тем, что предлагает первый пример виртуального оружия, наносящего прямой физический урон по ценной стратегической цели в реальном мире, и поэтому его использование относительно легко классифицировать как акт военной киберагрессии [12].

Такое определение, однако, не предусматривает, что кибератаки должны вызывать физическое разрушение качества как акты войны. Виртуальные атаки на важные объекты (такие как правительственные учреждения или структуры военного командования) могут иметь одинаково разрушительные последствия, если им удастся отключить критически важную инфраструктуру или подорвать доверие к политической системе. Поэтому, трудно определить, когда виртуальная атака пересекает порог быть «эквивалентной применению вооруженной силы» в общепринятом смысле, и в настоящее время это один из самых горячих спорных вопросов среди юристов-международников [13].

Тем не менее, именно по этому вопросу необходимо выработать международное соглашение, чтобы избежать эскалации киберконфликта. Проведение этой линии в международном праве, несомненно, будет очень трудным и потребует долгих и трудных переговоров с участием экспертов по правовым и техническим вопросам.

Ложные преимущества кибернаступления

Ученые в области международной безопасности и военные и широко согласны с тем, что киберпространству присущи наступательные стратегии и операции нежели оборонительные [14]. Согласно традиционной теории нападения/защиты, когда при наступлении имеются явные преимущества, то относительно легче «продвигаться вперед, разрушать и завоевывать территорию», чем защищаться и защищать ее [15].

Эксперты перечисляют три основные причины, по которым наступательные стратегии в киберпространств превосходят оборонительные.

Во-первых, атаки в киберпространстве происходят с большой скоростью, подвергая оборону огромному давлению, «поскольку атакующий должен быть успешным только один раз, тогда как защитник должен быть успешным все время» [16].

Во-вторых, перспектива запуска атак с относительной анонимностью и, следовательно, безнаказанностью, снижает ожидаемую стоимость наступательных стратегий в киберпространстве.

В-третьих, физическое расстояние относительно неважно в виртуальном мире. Кибератаки могут возникать практически из любого места, предоставляя злоумышленникам значительные возможности захватить инициативу и застать защитников врасплох [16]. При этом кибертехнологии приводят к значительному улучшению мобильности и достижению силы - оба эти фактора используются для увеличения наступательных преимуществ.

Теория международных отношений указывает на четыре основных стратегических последствия наступательного доминирования. Во-первых, когда наступление является сильным по отношению к обороне, для государств становится обязательным быстрое и решительное реагирование на возникающие угрозы, поскольку даже небольшое первоначальное изменение в соотношении возможностей может привести к решающему сдвигу в способности субъектов превалировать в конфликте.

В киберпространстве принуждение к быстрым действиям и реакциям еще больше усиливается изменяющейся уязвимостью большинства киберцелей. Кибероружие состоит из сложного программного обеспечения, разработанного для использования уязвимостей, присутствующих в другом программном обеспечении, таких как компьютерные операционные системы или промышленные

системы управления. Смысл наступления, по мнению многих кибер-экспертов, заключается в том, что «если вы не будете действовать быстро, вы, возможно, не сможете действовать вообще» [11].

Вторым следствием наступательных преимуществ является поощрение гонок вооружений. Как объясняют эксперты Глейзер и Кауфман, когда наступление является сильным, государства могут обнаружить, что силы одинакового размера не способны поддержать оборонительную стратегию. Вместо этого они, скорее всего, придут к выводу, что им требуется существенное преимущество в военной силе для защиты от нападений. [17, с 48] Это вызывает динамику конкурентного наращивания вооружений, когда даже государства, которые просто хотят отстоять статус-кво, стремятся наращивать свои военные арсеналы быстрее, чем их конкуренты, для обеспечения адекватной защиты.

Третий эффект наступательного преимущества - это увеличение вознаграждения за первый удар, что увеличивает вероятность упреждающих или превентивных атак. Киберстимулы для атаки на врагов преимущественно возникают отчасти из-за того, что действия в киберпространстве движутся настолько быстро, что у целевых государств остается мало времени для защиты. Мотивация нанести первый удар может быть дополнительно усилена перспективой использования тщательно нацеленных киберударов для нейтрализации обычных систем обороны противника и, таким образом, ограничения его ответных возможностей.

В-четвертых, согласно теории международным отношениям, когда нападение является сильным по отношению к защите, способность сдерживать атаки, в отличие от попыток защиты от них, становится жизненно важной. Логично, что в стратегической среде, которая, как считается, благоприятствует наступательным операциям, способность сдерживать агрессоров в решающей степени зависит от способности сигнализировать или демонстрировать превосходные наступательные возможности. *Следовательно, в соответствии с традиционной теорией нападения/защиты, самый надежный способ достижения эффективного стратегического киберсдерживания состоит в том, чтобы развить сильные наступательные возможности, которые обещают сокрушительный ответный удар против потенциальных злоумышленников.*

Подводя итог, можно сказать, что общепринятая теория международных отношениях указывает на четыре стратегических значения кибернаступательных преимуществ: 1) акцент на быстрые действия, 2) тенденция к гонки вооружений, 3) сильные стимулы для упреждающих атак, 4) акцент на усиление сдерживания путем усиления наступательных возможностей.

Важность принятия фактических мер подчеркивается в ведущих национальных стратегиях кибербезопасности. Согласно американской «Национальной военной стратегии для киберпространства» киберпространство предоставляет командирам возможность быстро принимать решения, проводить операции и создавать эффекты на скоростях, которые ранее были непостижимы. Кроме того, увеличение скорости процесса принятия решений потенциально приведет к большей эффективности возможностей киберпространства [18].

Во многих стратегических документах и в публичных заявлениях представителей обороны четко отражена осознанная необходимость в усилении наступательных возможностей в качестве средства усиления сдерживания. Командующий военным киберкомандованием адмирал Майкл С. Роджерс неоднократно указывал на необходимость «увеличить наши возможности в атакующей стороне, чтобы достичь этой точки сдерживания» [19]. Администрация Трампа также продемонстрировала агрессивную киберпозицию. Во время своей президентской кампании Дональд Трамп неоднократно обещал расширить наступательные ки-

бернетические возможности Америки - обязательство, за которым последовали планы увеличения военных расходов на кибербезопасность на 15% в бюджете Министерства обороны США на 2017 г. [20].

Другие страны делают аналогичные выводы. Россия, Иран и Северная Корея имеют военные подразделения, специально предназначенные для наступательных кибероперациий. С 2005 г. Китай начал включать операции наступательных компьютерных сетей в свои военные учения, в первую очередь в комплексных первых ударах по сетям противника, и китайцы недавно признали существование чисто наступательных киберподразделений в НОАК. Немцы публично заявили, что они разрабатывают наступательное кибероружие, Аргентина, Франция, Дания и Нидерланды также запустили программы по развитию возможностей кибернаступления [21].

Таким образом, нынешние политические и военные лидеры в подавляющем большинстве сосредоточены на совершенствовании потенциала своих стран в области кибернаступления и, похоже, исходят из того, что национальные стратегии кибербезопасности основаны на твердой уверенности в том, что защитные стратегии недостаточны для сдерживания врагов в киберпространстве.

Опасность, возникающая из наступательных преимуществ, заключается в том, что оно увеличивает риск простых недоразумений, ведущих к непреднамеренной эскалации кризиса. Это может привести к тому, что решения будут основаны на предположениях «наихудшего сценария» о намерениях злоумышленника.

Тенденция реагировать на вторжения агрессивными контрмерами до того, как станут известны даже базовые факты, определятеся как активная киберзащита (АКБ), которая относится к «упреждающим электронным мерам», предназначенным для «обнаружения, анализа и устранения нарушений безопасности сети в режиме реального времени» и для принятия «агрессивных, наступательных контрмер против сетей злоумышленника» [22].

По сути, АКБ включает в себя настройку систем для обнаружения и автоматического удара по атакующим компьютерным системам с целью прекращения кибератак в середине потока до того, как будет точно известен точный источник или характер атаки.

Хотя активная киберзащита может помочь защитить критически важную инфраструктуру и может достичь некоторой степени сдерживания путем эффективного «отказа от инициативы», этот подход сопряжен с высокими рисками непреднамеренной эскалации кризиса [23]. Нанося удар по злоумышленникам без разбора, АКБ расширяет возможности для ошибок. Более того, активная киберзащита ограничивает возможности для снижения эскалации, выпуская четкие предупреждения или реагируя на вторжения небольшими, но постепенно усиливающимися контрмерами, чтобы убедить претендента отступить, тем самым ограничивая возможности для активного кризисного управления.

Это подразумевает явную угрозу перехода от киберконфликта к кинетической войне, где США сильно опережают большинство потенциальных противников. В то же время предполагаемое наступательное преимущество также побуждает государства быть более скрытными в своих военных возможностях и планах. Эта комбинация воинственной и скрытной дипломатии увеличивает риск конфликта из-за неправильного расчета возможностей или интересов других и порождает призрак непреднамеренного перехода от случайного кибератаки к полномасштабной кинетической войне посредством последовательности полу- или полностью автоматических контратак.

Подводя итог, можно сказать, что культ кибернаступления создает нестабильную стратегическую среду со значительными рисками быстрого обострения кризиса. На самом деле есть веские основания полагать, что оборонительные

стратегии кибербезопасности окажутся в целом сильнее, чем наступательные. Большинство случаев военного соревнования и гонки вооружений в конечном итоге обусловлены политическими соображениями и выбором. История учит нас тому, что гонка вооружений лучше всего сдерживаются официальными международными соглашениями, тщательно разработанными для того, чтобы уменьшить страх и неуверенность и умерить вооруженную конкуренции путем установления четких правил для приемлемого поведения.

Во время самого враждебного периода «холодной войны» постоянно существовавший риск ядерной войны решался двумя основными стратегиями: стратегическим ядерным сдерживанием, основанным на доктрине взаимно гарантированного уничтожения, и контролем над вооружениями, что проявлялось в подписанных двусторонних и многосторонних соглашениях.

Однако в современной киберсфере активно реализуется только одна стратегия предотвращения конфликтов, а именно стратегическое сдерживание посредством ответных мер. Односторонняя зависимость от стратегического кибер сдерживания продиктована современным технологическим состоянием, которое, поддерживает наступательные стратегии и исключает согласованные решения конфликта. Хотя технологический импульс может играть важную роль в формировании международного конфликта, технологические факторы редко бывают определенными. Политический выбор может и должен изменить соотношение нападение/защита в пользу более оборонительных стратегий. Всем странам необходимо принять ограничения на использование кибероружия и начать переговоры по заключению договора о международной конвенции о запрете его применения.

СПИСОК ЛИТЕРАТУРЫ

1. Sanger D. E. William J. B. Trump Inherits a Secret Cyberwar against North Korean Missiles // New York Times. March, 4. 2017. URL: https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html.
2. Damian P., Yadron D, Valentino-Devries J. Cyberwar Ignites a New Arms Race // Wall Street Journal. 2015
3. Cyber Command Fact Sheet. U.S. Department of Defense. 21 May 2010. URL: https://web.archive.org/web/20140416192156/http://www.stratcom.mil/factsheets/2/Cyber_Command/
4. Sanger D. E., Markoff Jh., Shanker Th. U.S. Steps up Effort on Digital defenses // NY Times, April 27. 2009.
5. Singer P. W., Friedman, A. Cybersecurity and Cyberwar: What Everyone Needs to Know? Oxford: Oxford University Press. 2014
6. US DOD, National Military Strategy for Cyber Operations, Dec. 11, 2006. URL: http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf.
7. Cyber Defence / NATO. Last updated: 17 Mar. 2020. URL: https://www.nato.int/cps/en/natohq/topics_78170.htm
8. Nye Joseph S. International Norms in Cyberspace. Project Syndidate, May, 11. 2015. URL: https://www.project-syndicate.org/commentary/international-norms-cyberspace-by-joseph-s--nye-2015-05?barrier=true
9. Tallinn Manual on the International Law Applicable to Cyber Warfare. 2013. URL: https://ccdcoe.org/tallinn-manual.html
10. Saltzman, I. Cyber Posturing and the Offense-Defense Balance // Contemporary .Security Policy. 2013 # 34(1), Pp. 40–63.
11. Clarke, R. A., Knake, R. K. Cyber War: the Next Threat to National Security and What to Do About it. New York: Harper Collins. 2010.

12. Lucas, G. Ethics of Cyber Warfare. The Quest for Responsible Security in the Age of Digital Warfare. Oxford: Oxford University Press. 2017.
13. Schmitt M. N., Liis Vihul The Emergence of International Legal Norms for Cyberconflict. In Fritz Allhoff, Adam Henschke and Bradley J. Strawser (eds.), Binary Bullets. The Ethics of Cyberwarfare (pp. 34–55). Oxford University Press, 2016.
14. Lonergan Sh. W. Cooperation Under the Ccybersecurity Dilemma" in Confronting Inequality: Wealth, Rights, and Power, eds. Hugh Liebert, Thomas Sherlock, and Cole Pinheiro. New York: Sloan, 2016.
15. Evera, V., Stephen. . The Cult of the Offensive and the Origins of the First World War // International Security, 1984 # 9(1), Pp. 58–107.
16. Sheldon , J. B. Deciphering Cyberpower Strategic Purpose in Peace and War // Strategic Studies Quarterly. 2011
17. Glaser, C. L., Kaufmann, C. . What is the Offense-Defense Balance and Can We Measure it? // International Security, 1998 # 22(4), pp.44–82.
18. United States Department of Defense. National Military Strategy for Cyber Operations. December 11, 2006. URL: http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf.
19. Statement by Admiral Michael S. Rogers Commander US Cyber Command before the Senate Committee on Armed Services. 19 March 2015.
20. Gady Franz-Stefan. Trump and Offensive Cyber Warfare. // The Diplomat, January 16. 2017. URL: http://thediplomat.com/2017/01/trump-and-offensive-cyber-warfare
21. Limnéll Jarno. Offensive Cyber Capabilities are Needed Because of Deterrence. In the Fog of Cyber Defence, eds. Jari Rantapelkonen and Mirva Salminen. Helsinki: Juves Print. 2013. pp 200–208.
22. Dewar R. S. The "Triptych of Cyber Security": a Classification of Aactive Cyber Defence. 6th Intl Conference on Cyber Conflict. Tallinn: NATO CCD COE Publications. 2014.
23. Schelling T. C. The Strategy of Conflict. Cambridge, MA: Harvard University Press. 1994.

Поступила в редакцию 13.04.2020.
Принята к публикации 16.04.2020.

Для цитирования:
Хлопов О.А. Наступательные стратегии кибероружия как угроза международной безопасности // Гуманитарный научный вестник. 2020. №3. С. 51-59. URL: http://naukavestnik.ru/doc/2020/03/Khlopov.pdf