Мовкебаева Г.А.,
Отызбаева Ж.М.

Информационные операции США в контексте обеспечения кибербезопасности

Широкомасштабное развитие в конце XX – начале XXI века информационных технологий, всеохватывающая информатизация правительственных и общественных структур, а также вооруженных сил в значительной степени трансформировали методы и способы, характер информационной деятельности государств. Понятие кибербезопасности трактуется неоднозначно многими экспертами. В статье предлагается анализ американских подходов к рассмотрению понятия киберпространства и кибербезопасности. На основе анализа американских исследований и официальных документов в сфере обеспечения кибербезопасности раскрываются понятия киберпространства, кибербезопасности, информационных операций. США являются безусловным лидером в киберпространстве. Именно поэтому представляется важным рассмотреть структуры ведомостей США, занимающихся информационными операциями. И, наконец, выявляются факторы уязвимости американских информационных систем, приоритетные направления развития информационных операций.

Ключевые слова: информационные операции, кибербезопасность, Соединенные Штаты Америки, киберпространство, информационная война.

Movkebayeva G.A.,
Otyzbayeva Zh.M.

US information operations in the context of cybersecurity

The information technologies' broad-scale development in the end of XX – beginning of XXI century, total computerization of government and public bodies, as well as of armed forces largely transformed the methods and techniques, the nature of the states' information activities. The concept of cyber security is not uniquely defined by different experts. The American approach to the concepts of cyberspace and cyber security is proposed in the article. The main cyber security concepts as cyberspace, cyber security, information operations are disclosed due to an analysis of American studies and official documents. The United States is the undisputed leader in cyberspace. So it is important to examine the US cyber structures. And finally, the paper explores American cyber insecurity factors.

Key words: information operations, cyber security, the United States, cyberspace, information warfare.

Мовкебаева Г.А.,
Отызбаева Ж.М.

Киберқауіпсіздікпен қамту контекстіндегі АҚШ ақпараттық операциялары

Ақпараттық технологиялардың XX ғасырдың соңы мен XXI ғасырдың басы аралығында кең ауқымды дамуы, үкіметтік және қоғамдық құрылымдардың және қарулы күштердің жалпылама ақпараттандыруы айтарлықтай дәрежеде мемлекеттердің ақпараттық қызмет тәсілдері мен әдістерін, сипатын өзгертті. Көптеген сарапшылар киберқауіпсіздік ұғымына әртүрлі мағынада түсінік береді. Бұл мақалада киберкеңістік пен киберқауіпсіздік ұғымдары американдық тәсілдеме шеңберінде зерттеледі. Американдық зерттеулер мен ресми құжаттардың негізінде киберкеңістік, киберқауіпсіздік, ақпараттық операциялар ұғымдары көрсетіледі. Америка Құрама Штаттары киберкеңістікте сөзсіз көшбасшы болып табылады. Сол үшін Америкадағы ақпараттық операциялармен айналысатын мекемелердің құрылымын зерттеп қарау қажет. Және де Американың ақпараттық жүйелерінің осалдық факторлары айқындалады.

Түйін сөздер: ақпараттық операциялар, киберқауіпсіздік, Америка Құрама Штаттары, киберкеңістік, ақпараттық соғыс.

УДК 327(73:004) 540

***Мовкебаева Г.А., Отызбаева Ж.М.**

Казахский национальный университет имени аль-Фараби,
Республика Казахстан, г. Алматы
*E-mail: gmovkebaewa@mail.ru

ИНФОРМАЦИОННЫЕ ОПЕРАЦИИ США В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

В настоящее время в мире происходит геостратегическое информационное соперничество в целях достижения безусловного превосходства в глобальном информационном пространстве.

Цифровые технологии, которые обычно называют кибер-системами, привели к парадоксу безопасности: они обеспечивают пользователей беспрецедентными возможностями, но в то же время подвергают их большей угрозе. Их коммуникативные возможности позволяют развивать сотрудничество и создание различных сетей, но при этом они открывают двери для тотального вмешательства в частную жизнь граждан и нарушают суверенитет государств. Концентрация данных и разнообразные манипуляции значительно повышают эффективность и масштаб операций, но эта концентрация, в свою очередь, экспоненциально увеличивает количество данных, которые могут быть украдены или будут разрушены в результате успешной кибератаки. Усложнение технического и программного обеспечения создает большие возможности, но вместе с тем порождает уязвимость сетей и снижает возможность противостоять кибервторжениям.

Известны миллиарды вирусов и вредоносных программ, обнаруженных в сети. Ежегодно количество подобных программ растет. Атаки в киберпространстве наносят ущерб в сотни миллиардов долларов [1].

Общий анализ проблематики защиты от подобных, вновь возникающих и продолжающих развиваться угроз, можно обозначить понятием «кибербезопасность».

США являются безусловным лидером в киберпространстве. Ведь военно-политическое руководство США первым начало рассматривать кибернетическое пространство как новую сферу ведения боевых действий наряду с наземной, морской и воздушно-космической сферами. При этом под киберпространством понимается сетевая инфраструктура, радиоэлектронные средства и средства распространения электромагнитных излучений, используемые для передачи информации, управления оружием, а также воздействия на объекты противника [2].

Военные операции в киберпространстве велись еще до появления Интернета. Официальное же создание воинских частей,

занимающихся проблемами киберпространства и кибероперациями, является особенностью 21-го века.

Данная статья ставит своей целью комплексное изучение этого явления для оценки динамичного характера операций в киберпространстве. Исследование основывалось на незасекреченной и открытой для общего доступа информации.

Доктринальные разработки ведения информационной войны в США начались практически после завершения войны в Персидском заливе (1991 г.), где американцы впервые применили новейшие информационные технологии.

Дальнейшая теоретическая разработка этих вопросов была продолжена в виде официального издания доктрин, согласно одной их которых «информационная операция – это комплекс мероприятий по манипулированию информацией в целях достижения и удержания всеобъемлющего превосходства над противником посредством воздействия на информационные процессы, происходящие в системах управления» [3].

Обновленная «Четырехлетняя программа развития обороны США» в 2001 году придала киберпространству статус пятого театра военных действий, а «Национальная военная стратегия для операций в киберпространстве», принятая в 2006 году, сформировала принципы ведения информационных оборонительных и наступательных операций в киберпространстве.

«Стратегия Министерства обороны США по операциям в киберпространстве» в 2011 году пересмотрела оборонительные позиции и сделала акцент на наступательные операции в киберпространстве.

Что касается структур, непосредственно занимающихся осуществлением информационных операций, то за проведением наступательных и оборонительных операций в компьютерных сетях в рамках министерства обороны отвечают Командование совместных информационных операций (Joint Information Warfare Command – JIOWC) и Командование боевых действий в киберпространстве (US Cyber command), входящие в состав объединенного стратегического командования (ОСК) ВС США.

Реальные возможности и конкретные направления деятельности этих структур строго засекречены, однако, они тесно сотрудничают с ЦРУ, АНБ, ФБР, а также привлекают к своей работе гражданских и военных специалистов государств-партнеров, например из стран НАТО. Среди ведомств, ответственных за приоритетные направления деятельности, так или иначе связанные с защитой критически важных объектов инфраструктуры, нужно выделить: Министерство обороны – отвечает за национальную оборону, государственный департамент – ответственен за международные отношения, ЦРУ – за разведку, и министерство юстиции и ФБР – за законодательное обеспечение этой деятельности [5].

Все ведомства характеризуются взаимосвязанностью. В структуре других министерств и ведомств также функционируют подразделения информационной безопасности. Кроме того, американское руководство привлекает к работе по обеспечению защиты киберпространства и негосударственные структуры.

В целях достижения информационного перевеса перед соответствующими структурами ставились две задачи – широкомасштабное использование коммерческих технологий и дальнейшая разработка эффективных наступательных и оборонительных информационных действий для защиты информационных систем от кибератак.

По мнению экспертов, спустя десятилетие после окончания Холодной войны Соединенные Штаты столкнулись с драматическим изменением характера окружающей геополитической среды. Диапазон новых угроз, помимо традиционных государств – вероятных противников, включает сегодня и деятельность негосударственных, транснациональных групп, точные границы которых трудно определить [6].

Сегодня сложно выявить степень нарушения информационной безопасности со стороны традиционных акторов, поскольку новые технологии проникновения в компьютерные сети не позволяют точно определить, когда же была пересечена граница лояльности.

Аналитики Пентагона отмечают, что, несмотря на существенное технологическое, экономическое и военное превосходство США, целый ряд региональных держав и межнациональных коалиций обладают потенциалом, позволяющим угрожать национальным интересам страны в сфере кибербезопасности. В современных условиях количество, разнообразие, непрозрачность, степень и скорость интерактивности акторов в киберпространстве являются беспрецедентными.

Джеймс Клэппер, директор Национальной разведки, в 2013 году поставил киберугрозу на первое место, выделив среди остальных государств Россию и Китай как основных потенциальных соперников в киберпространстве [7].

Потенциальные конкуренты освоили опыт действий армии США и НАТО в Югославии и в других конфликтах и адаптировались к новым условиям. Огромную угрозу безопасности представляет ИГИЛ.

В этих условиях противники будут искать возможности достичь цели прежде, чем США смогут ответить на вызов. Как считают аналитики Пентагона, действия противников будут включать как открытые военные действия, террористические акты, так и атаки на компьютерные сети. При этом исполнителей этих акций будет достаточно сложно обнаружить.

Среди основных угроз информационной безопасности США, кроме использования террористами преимуществ информационного прогресса, кибератаки со стороны других государств и других акторов, можно выделить также утечку секретной информации. Самые громкие скандалы рассекречивания документов под грифом «секретно» связаны с именами Джулиана Ассанжа, Брэдли Мэннинга и Эдварда Сноудена.

В связи с этим следует отметить три фактора незащищенности США в киберпространстве.

1. Конкурентная среда в киберпространстве.

Киберпространство – конкурентная среда, насыщенная различными акторами международных отношений.

Когда вооруженные силы США и НАТО в Ираке и Афганистане смогли дать адекватный ответ на атаки террористов, те усовершенствовали методы и приемы ведения террористической и антитеррористическим силам снова пришлось адаптироваться.

При обнаружении посягательства на систему безопасности, атакующими быстро зондируются средства и меры защиты.

2. Границы американского доминирования.

Американские структуры национальной безопасности беспрецедентно развивались в течение последних десятилетий, и можно констатировать, что американская система безопасности достигла технологического доминирования, но это преимущество не может сохраняться бесконечно. Правительство США не может контролировать кибер-угрозы, используя традиционные инструменты, предназначенные для укрепления национальной безопасности в пределах географических границ Америки. Многие кибератаки исходят с американской территории, но еще больше – извне. Соединенные Штаты имеют мало возможностей для создания киберконтроля на своих границах. Ведь, как уже упоминалось ранее, в киберпространстве успешно действуют другие государства, преступные организации, террористические группировки и т.д.

И, наконец, значительная часть оборонной власти американской нации сосредоточена теперь в частных руках. Как обороноспособность, так и инновации в этой сфере контролируются больше рынком частного сектора, маркетинговыми ходами и коммерческих приоритетами, нежели приоритетами Министерства обороны.

3. Скорость изменений.

Коммуникационные возможности Интернета изменили финансовую, военную, индустриальную и социальную системы, увеличив их киберзависимость. Цифровые информационные системы и их порождение, Интернет, обладают не меньшей мощью, чем в свое время изобретение пороха. Они требуют сопоставимых изменений. Но если на развитие и распространение пороховых технологий ушло приблизительно два столетия, то кибертехнологии получили широкое распространение примерно в течение двух десятилетий.

Подводя итоги, при разработке оборонительных планов в киберпространстве Соединенным Штатам следует учесть некоторые факторы уязвимости информационных систем.

Во-первых, возросшая конкуренция препятствует американскому прогрессу в сфере кибербезопасности.

Во-вторых, американское доминирование в сфере кибертехнологий не может считаться неоспоримым.

В-третьих, государственная власть США ограничена тем фактом, что частный сектор является двигателем инноваций внутри этой страны, и более того широкие возможности находятся за пределами американских границ. Новизна, скорость и непредсказуемость информационных технологий осложняют контроль над ними, их регулирование на основе долгосрочных научно-исследовательских программ.

Таким образом, приоритетным направлением для США является расширение информационных операций (в первую очередь наступательных) и модернизация киберструктур в целях обеспечения контроля и уменьшения рисков, внутренних и внешних угроз кибернетического характера.

Литература

1 Norton Cybercrime Report, 2012. //http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf)

2 Информационные войны в киберпространстве: Часть 1 – США // http://genadiafanassjev.blogspot.ru/2011/03/1_25.html

3 Joint Doctrine for Information Operations. Joint Publication 3-13. Washington. Joint Chiefs of Staff. October 1998 // http://www.c4i.org/jp3_13.pdf

4 Роговский Е.А. Политика США по обеспечению безопасности киберпространства // США – Канада. – 2012. – №6. – С. 3-22.

5 Официальный сайт АНБ // http://www.nsa.gov/about/mission/index.shtml

6 Lynn W. The Pentagon's Cyberstrategy, One Year Later Defending Against the Next Cyberattack // Foreign Affairs. September 28, 2011 // http://www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later

7 Jim Garamone. Clapper Places Cyber at Top of Transnational Threat List American Forces Press Service. Washington, March 12, 2013 // http://www.defense.gov/news/newsarticle.aspx?id=119500

References

1 Norton Cybercrime Report, 2012. //http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf)

2 Informacionnye voiny v kiberprostranstve: Chast 1 – SSHA // http://genadiafanassjev.blogspot.ru/2011/03/1_25.html

3 Joint Doctrine for Information Operations. Joint Publication 3-13. Washington. Joint Chiefs of Staff. October 1998 // http://www.c4i.org/jp3_13.pdf

4 Rogovskii E.A. Politika SSHA po obespecheniyu bezopasnosti kiberprostranstva // SSHA – Kanada. – 2012. – № 6. – S. 3-22.

5 Oficialnyi sait ANB // http://www.nsa.gov/about/mission/index.shtml

6 Lynn W. The Pentagon's Cyberstrategy, One Year Later Defending Against the Next Cyberattack // Foreign Affairs. September 28, 2011 // http://www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later

7 Jim Garamone. Clapper Places Cyber at Top of Transnational Threat List American Forces Press Service. Washington, March 12, 2013 // http://www.defense.gov/news/newsarticle.aspx?id=119500

Безопасность это процесс, а не результат.

Брюс Шнайер