УДК 004.056.5(73)
ББК 32.973.202

Селянин Ярослав Владиславович*, научный сотрудник Центра военно-политических исследований РИСИ.

Роль Пентагона в обеспечении кибербезопасности США

В настоящее время идёт активное развитие и распространение информационно-коммуникационных технологий (ИКТ), что создаёт серьёзные вызовы безопасности для отдельных пользователей этих технологий и для государственных структур по всему миру, которые сегодня в своей деятельности всё больше зависят от компьютерной техники и доступа к информационным сетям. По официальным данным, в США сложилась достаточно сложная ситуация с обеспечением кибербезопасности[1] федеральных агентств, включая Министерство обороны.

Положение дел с кибербезопасностью в США на современном этапе

Согласно стенограмме выступления руководителя направления по вопросам информационной безопасности Счётной палаты США (U.S. Government Accountability Office, GAO) перед президентской комиссией по вопросам укрепления национальной кибербезопасности за период 2006–2015 фин. гг. годовое число инцидентов в киберпространстве, о которых сообщили федеральные агентства США, выросло с 5503 до 77 183.

По оценке Счётной палаты США, американские федеральные системы и сети находятся под постоянным риском в связи с их высокой сложностью, неоднородностью и географической рассредоточенностью. Причём они содержат огромное количество уязвимостей, как уже известных, так и неизвестных. Например, ежедневно пополняемая национальная база данных по состоянию на 15 сентября 2016 г. содержала информацию о 78 907 известных уязвимостях. Усложняет ситуацию то, что федеральные

* yaroslav.selyanin@riss.ru

[1] *Кибербезопасность* — это способность обеспечить защищённое от кибератак использование киберпространства. *Кибератака* — атака, осуществляемая посредством использования киберпространства, с целью: разрушения, отключения, уничтожения или злонамеренного управления вычислительной средой / инфраструктурой; нарушения целостности данных или кражи контролируемой информации. *Киберпространство* — пространство внутри информационной среды, состоящей из взаимозависимых сетей и включающей инфраструктуру информационных систем, таких, как интернет, телекоммуникационные сети, компьютерные системы и встроенные процессоры и контроллеры. См.: National Information Assurance (IA) Glossary (CNSSI 4009) // National Counterintelligence and Security Center (NCSC). URL: https://www.ncsc.gov/nittf/docs/CNSSI-4009_National_Information_Assurance.pdf (дата обращения: 01.11.2016).

системы и сети часто взаимосвязаны с другими внутренними и внешними системами и сетями, включая интернет. При этом Счётной палатой США за последние 7 лет было дано около 2,5 тыс. рекомендаций правительственным структурам по повышению уровня информационной безопасности. Однако по состоянию на 16 сентября 2016 г. около 1 тыс. из них не было реализовано[2].

Данное ведомство полагает, что это создаёт угрозу нормальному функционированию информационной и коммуникационной инфраструктуры, необходимой для работы энергосистемы, системы здравоохранения, правоохранительной системы и для обеспечения национальной обороны[3].

По мнению Счётной палаты, неэффективная защита подобных систем и сетей может привести к невозможности выполнения ими своих функций и как результат к следующим последствиям[4]:

– утеря или кража компьютерных ресурсов, активов и денежных средств;

– несанкционированный доступ, раскрытие, изменение и уничтожение чувствительной информации, касающейся национальной безопасности, а также персональных данных и частной бизнес-информации;

– разрушение критической инфраструктуры (КИ), обеспечивающей национальную оборону и действия аварийно-спасательных служб;

– срыв выполнения государственными структурами своих функций, что может привести к инцидентам, подрывающим уверенность общества в правительстве;

– несанкционированное использование компьютерных ресурсов, в том числе для проведения атак на иные системы;

– нанесение ущерба сетям и оборудованию;

– высокие затраты на восстановление.

В то же время, в доктринальных документах США киберпространство рассматривается как полноценная сфера ведения военных действий, требующая принятия серьёзных мер для обеспечения защиты американских интересов и противодействия угрозам национальной безопасности США. Пентагон рассматривает силы и средства для решения задач в этой среде как полноценный инструмент защиты американских национальных интересов наряду с дипломатическими, информационными, военными, экономическими, финансовыми, правоохранительными инструментами, и работает над отработкой их согласованного совместного использования[5].

---

[2] См.: GAO-16-885T. September 19, 2016. FEDERAL INFORMATION SECURITY: Actions Needed to Address Challenges. Testimony Before the President's Commission on Enhancing National Cybersecurity. P. 1–3 // United States Government Accountability Office. URL: http://www.gao.gov/products/GAO-16-885T (дата обращения: 01.11.2016).

[3] См.: GAO-15-758T. July 8, 2015. INFORMATION SECURITY. Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies. Testimony Before the Subcommittees on Research and Technology and Oversight, Committee on Science, Space, and Technology, House of Representatives. P. 2 // United States Government Accountability Office. URL: http://www.gao.gov/products/GAO-15-758T (дата обращения: 01.11.2016).

[4] Ibid.

[5] См.: U.S. National Security Strategy 2015. P. 7, 12–13. // National Security Strategy Archive. URL: http://nssarchive.us/wp-content/uploads/2015/02/2015.pdf (дата обращения: 01.11.2016); DOD Cyber Strategy 2015. P. 2 // U.S. Department of Defense. URL: http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (дата обращения: 01.11.2016).

При этом сложность обеспечения кибербезопасности самого Пентагона обусловлена значительным количеством пользователей и чрезвычайной рассредоточенностью и неоднородностью сетей и систем. Так, согласно официальным данным, по состоянию на 2015 г. в МО США служили более 1,4 млн военнослужащих, 718 тыс. гражданского персонала, около 1,1 млн человек личного состава Национальной гвардии и резервистов. Объекты МО США располагались в 5 тыс. пунктов и баз. Число компьютеров только в несекретных сетях составляло около 4 млн ед.[6]

Ввиду важности проблемы кибербезопасности в апреле 2015 г. вышла уже вторая по счёту стратегия МО США, определяющая политику Пентагона в отношении действий в киберпространстве — Киберстратегия Министерства обороны США (The Department of Defense Cyber Strategy, далее — Киберстратегия-2015). Одной из основных тем документа является вопрос обеспечения кибербезопасности ВС США и критической инфраструктуры, необходимой для выполнения ими своих задач. А в июле 2016 г. было опубликовано исследование "Общая оперативная обстановка 2035" (Joint Operating Environment 2035, JOE-2035), подготовленное управлением J-7 Комитета начальников штабов американских ВС, в котором авторы на основе существующих в настоящий момент тенденций развития ситуации в мире рассматривают вероятные условия, в которых к 2035 г. придётся действовать ВС США. Основная задача данного исследования — дать старт обсуждению шагов, необходимых для формирования облика американских ВС, адекватного будущей обстановке. Это своего рода набросок модели угроз, отталкиваясь от которого авторы документа предлагают начать выработку необходимого направления развития ВС США, в том числе в отношении действий в киберпространстве, чему в докладе уделено большое внимание.

Эти документы дают достаточно полное представление о взглядах специалистов американского военного ведомства на существующие и потенциальные угрозы, связанные с использованием информационно-коммуникационных технологий.

В качестве потенциальных противников американские ВС рассматривают:

– Россию и Китай, которые, по мнению авторов, работают над созданием перспективных средств для действий в киберпространстве;

– Иран и КНДР, которые, по мнению американских военных, хотя и не обладают серьёзными возможностями, но демонстрируют враждебное отношение к США и американским интересам в киберпространстве;

– негосударственных акторов — отдельных лиц или террористические организации — такие, как запрещённая в России группировка ИГИЛ / ДАИШ, использующая киберпространство для рекрутирования новых членов и распространения пропаганды, а также стремящаяся, по мнению Пентагона, к получению средств проведения кибератак[7].

---

[6] См.: Frequently-Asked-Questions // Department of Defense Chief Information Officer. URL: http://dodcio.defense.gov/About-DoD-CIO/Frequently-Asked-Questions/ (дата обращения: 01.11.2016).

[7] См.: DOD Cyber Strategy 2015. P. 9; Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World. P. 33 // The Defense Technical Information Center. URL: http://www.dtic.mil/doctrine/concepts/joe/joe_2035_july16.pdf (дата обращения: 14.03.2017).

Стоит отметить, что в рассмотренном выше отчёте Счётной палаты США дан иной список противников (как по содержанию, так и по степени их опасности), к которым отнесены: операторы ботнетов[8]; криминальные группы; хакеры / хактивисты[9]; инсайдеры; иностранные государства; террористы[10]. Как представляется, это более точный список, ввиду деполитизированности указанного отчёта, в отличие от Киберстратегии Министерства обороны США.

Как полагают в Пентагоне, потенциальные противники могут использовать кибертехнологии в криминальных и политических целях. При этом государства могут использовать негосударственных акторов в качестве прикрытия, что серьёзно усложняет задачу выявления основных заказчиков атаки. Проблемой также является не только создание вредоносного программного обеспечения (ПО), для чего требуются специалисты, но и возможность его приобретения на "чёрном" рынке. При этом, по оценке МО США, сегодня и государственные, и негосударственные акторы активно привлекают экспертов к поиску и разработке средств для использования уязвимостей в ПО, что создаёт неконтролируемый рынок, обслуживающий различных участников международной системы. И далее эта угроза будет только усугубляться[11].

Важность киберпространства для США и глобальной экономики оценивается авторами доклада чрезвычайно высоко. Отказ в доступе или разрушение его частей может, по их мнению, вызвать настолько серьёзные угрозы безопасности, что государство будет вынуждено принимать срочные меры. При этом отсутствие согласованной общепринятой терминологии и норм международного права, регулирующих использование данной среды (особенно в военных целях), чревато серьёзными разногласиями и разночтениями, в том числе в отношении оценки ущерба, нанесённого кибератаками и вышедшего за рамки непосредственно киберпространства[12]. В связи с этим авторы доклада ожидают усиления соперничества государств в вопросах выработки общепринятых международных норм, что, по их мнению, может значительно осложнить сотрудничество стран в рамках международных институтов по вопросам регулирования действий в киберпространстве и, в конечном счёте, привести к началу гонки вооружений в данной сфере[13].

---

[8] *Ботнет* (botnet) — сеть компьютеров с запущенными ботами — программами, которые устанавливаются на компьютер жертвы без её ведома и дают злоумышленнику возможность выполнять некие действия с использованием ресурсов заражённого компьютера. Ботнет используется для рассылки спама, хищения личных данных пользователей или осуществления сетевых атак. Подключение компьютера к ботнету происходит посредством заражения системы вирусом через уязвимость ПО, введение пользователя в заблуждение или использование санкционированного доступа к компьютеру. См.: Ботнет // SecurityLab.ru. URL: http://www.securitylab.ru/news/tags/%E1%EE%F2%ED%E5%F2/ (дата обращения: 01.11.2016).

[9] *Хактиви́зм* (англ. hacktivism; словослияние от хакер и активизм) — использование компьютеров и компьютерных сетей для продвижения политических идей, свободы слова, защиты прав человека и обеспечения свободы информации.

[10] См.: GAO-15-758T. INFORMATION SECURITY. Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies. P. 3–5.

[11] См.: DOD Cyber Strategy 2015. P. 9–10.

[12] См.: Joint Operating Environment 2035... P. 34.

[13] Ibid. P. 8.

Основной возможной причиной стратегического соперничества государств в киберпространстве названо их желание обеспечить его чёткое разграничение на части, на которые распространяется суверенитет того или иного государства, и на части, находящиеся в общем пользовании. То есть фактически речь идёт о том, что вопросы *установления границ и защиты суверенитета в киберпространстве*, по мнению американских военных, станут одним из новых поводов для войн и конфликтов в будущем[14].

Действия многих государств в данной среде будут направлены, в том числе, и на внесение раскола в стан их соперников, посредством воздействия на их систему принятия решений. Более того, высока вероятность повышения персонализации кибератак, заключающаяся в попытках оказать влияние на ключевых американских политических, военных руководителей и бизнесменов, используя полученные данные в информационных кампаниях[15].

В связи со всё большей взаимосвязью киберпространства и физической реальности авторы доклада указывают на угрозу появления такого типа конфликтов, когда посредством использования киберпространства осуществляется воздействие на критическую инфраструктуру (КИ) противника (вплоть до её физического разрушения) и защита собственной. Осложняет ситуацию то, что подобные системы зачастую крайне уязвимы перед кибератаками. Кроме того, физическая инфраструктура, обеспечивающая существование киберпространства, является крайне уязвимой перед атаками с использованием некоторых видов вооружения (например, электромагнитного оружия)[16].

По мнению авторов, развитие кибертехнологий и использование киберпространства являются очень привлекательными для держав, достигших доминирования в собственном регионе и желающих проецировать силу и оказывать влияние на ход событий по всему миру, одновременно обеспечив собственную защиту[17]. Один из основных мотивов использования противником данной среды будет состоять в том, чтобы "обойти" необходимость столкновения с ВС США и воздействовать непосредственно на процесс выработки решений политическим и военным руководством[18]. В связи с этим американские ВС ожидают роста числа государств, создающих наступательный потенциал для действий в киберпространстве, который (в дополнение к воздействию на КИ) будет использоваться для: воздействия на финансовую, правовую и техническую инфраструктуру; провоцирования социальных волнений; стратегической разведки, включая промышленный и научный шпионаж; выявления ключевой инфраструктуры, военного персонала и их семей внутри и за пределами США; в конечном счёте, для получения экономических, военных и политических преимуществ[19].

Вероятность того, что иностранные военные получат возможность на тактическом и оперативном уровне принимать решения о проведении

---

[14] См.: Joint Operating Environment 2035... P. 34.
[15] Ibid. P. 35.
[16] Ibid. P. 36.
[17] Ibid. P. 29.
[18] Ibid. P. 7.
[19] Ibid. P. 24, 35.

кибератак против ВС США с целью подрыва их боеготовности, американские военные расценивают как высокую. При том, что действия в киберпространстве, как предполагается, станут вполне обычной составляющей военных операций, поскольку особенности данной среды расширяют их диапазон от воздействия на отдельное конкретное устройство до глобального уровня[20].

Кроме того, результатом распространения информационных технологий, по мнению Пентагона, станет то, что силы противников — от государств до повстанцев и иррегулярных вооружённых формирований — будут располагать самыми современными системами управления, командования, связи, разведки, наблюдения и рекогносцировки (Command, Control, Communication, Intelligence, Surveillance and Reconnaissance, C3/ISR) и пытаться использовать уязвимости в аналогичных системах ВС США и их союзников[21].

Сети и системы самого Пентагона сегодня уязвимы для вторжений и атак, в том числе потому, что представляют собой "лоскутное одеяло" из тысяч сетей по всему миру. Это создаёт проблему определения необходимой организационной структуры, требуемой для эффективной защиты данных сетей[22].

Кроме того, по американским оценкам, более 90 % сетей и инфраструктуры в киберпространстве принадлежат частному сектору, который рассматривается Пентагоном как первая линия обороны, в то время как роль правительства США в этом вопросе официально признана достаточно ограниченной. В связи с этим одной из важнейших проблем является вопрос усиления собственной кибербезопасности частными компаниями, так как кража оперативной информации и интеллектуальной собственности американских министерств, ведомств и юридических лиц могут негативно сказаться на ВС США, а кибератаки на критическую инфраструктуру, используемую Пентагоном, могут ударить по их возможности действовать в особой обстановке[23].

Важным штрихом к описанию сложившейся ситуации является и то, что молодое поколение, выросшее после окончания "холодной войны" и приходящее сегодня на военную службу, привыкло к наличию постоянного доступа к информации и средствам коммуникации, являющимся важнейшей частью повседневной жизни молодёжи. Лишение их возможности пользования данными инструментами (например, в результате действий противника) может привести к срыву выполнения поставленной задачи[24].

Рекомендации руководящих документов

Описанная ситуация вызывает серьёзное беспокойство руководства Соединённых Штатов. Среди прочего, вслед за опубликованной в 2011 г. первой Стратегии МО США в отношении действий в киберпространстве

[20] Joint Operating Environment 2035... P. 36.
[21] Ibid. P. 18–19.
[22] DOD Cyber Strategy 2015. P. 7.
[23] Ibid. P. 5, 10, 13–14.
[24] Ibid. P. 4–5.

(Department of Defense Strategy for Operating in Cyberspace), американский президент подписал ряд директив, определяющих политику государства по вопросам, связанным с этой сферой, и распределяющих зоны ответственности конкретных министерств и ведомств. Среди них:

– директива № 20 от 16 октября 2012 г. (Presidential Policy Directive / PPD-20 "U.S. Cyber Operations Policy"), определяющая политику правительства США в области проведения операций в киберпространстве;

– директива № 21 от 12 февраля 2013 г. (Presidential Policy Directive / PPD-21 "Critical Infrastructure Security and Resilience"), определяющая государственную политику США по обеспечению безопасности и устойчивости критической инфраструктуры;

– директива № 41 от 26 июля 2016 г. (Presidential Policy Directive / PPD-41 "United States Cyber Incident Coordination"), определяющая координацию действий американских министерств и ведомств в отношении инцидентов в киберпространстве, затрагивающих интересы США.

Кроме того, достаточно подробно планируемые действия по обеспечению кибербезопасности Пентагона прописаны в Киберстратегии-2015.

В целом, выделено три основных направления работы[25].

Первым является защита сетей, систем и информации МО США. Министерство обороны назначено ответственным за обеспечение безопасности собственной информационной сети (Department of Defense Information Network, DoDIN)[26], включая снижение рисков, ответные действия в отношении субъектов кибератак и восстановительные работы в случае инцидентов[27].

В связи с признаваемой невозможностью защитить каждую сеть и систему от всех типов вторжения в силу масштабности DoDIN, перед Пентагоном поставлена задача по выявлению и защите наиболее важных сетей и данных, а также по планированию и отработке действий в условиях полного или частичного отсутствия доступа к киберпространству как в результате успешной атаки противника на сети или данные МО США, так и в случае разрушения элементов критической инфраструктуры, используемой американскими военными. Для этого рекомендовано внедрить новые технологии, включая создание и применение более защищённой архитектуры сети в рамках реализации концепции Единой информационной среды (Joint Information Environment, JIE)[28]. Пентагон назначен

---

[25] DOD Cyber Strategy 2015. P. 3.

[26] Информационная сеть Министерства обороны США (Department of Defense Information Network, DoDIN) включает в себя: несекретные (unclassified), секретные (Secret fabric), совершенно секретные (Top Secret, TS) и вспомогательные информационные системы МО США. См.: DoD Cybersecurity Discipline. Implementation Plan. P. 4 // Department of Defense Chief Information Officer. URL: http://dodcio.defense.gov/Portals/0/Documents/Cyber/CyberDis-ImpPlan.pdf (дата обращения: 01.11.2016).

[27] См.: Presidential Policy Directive / PPD-41 "United States Cyber Incident Coordination" // Federation of American Scientists. URL: https://fas.org/irp/offdocs/ppd/ppd-41.html (дата обращения: 14.03.2017); Presidential Policy Directive / PPD-21 "Critical Infrastructure Security and Resilience". P. 2 // Federation of American Scientists. URL: https://fas.org/irp/offdocs/ppd/ppd-21.pdf (дата обращения: 14.03.2017).

[28] *Единая информационная среда* (Joint Information Environment, JIE) – концепция по созданию более защищённой и менее затратной ИТ-среды посредством централизации, обновления сетей, используемых информационных технологий и коммуникаций.

ответственным (sector-specific agency, SSA) за обеспечение безопасности критической инфраструктуры (КИ) американского военно-промышленного комплекса (defense industrial base, DIB)[29].

В соответствии с этими предписаниями, в октябре 2014 г. заместитель министра обороны США по приобретению, технологии и материально-техническому обеспечению направил в Научный совет МО США (Defense Science Board, DSB) запрос о проведении исследования по теме "Управление обороной в киберпространстве" (Cyber Defense Managment), целью которого было выявление методов управления системами и сетями МО США, обеспечивающих им достаточный уровень кибербезопасности.

Рабочая группа, проводившая исследование, констатировала, что большинство систем МО США всё ещё не имеют адекватной защиты от киберугроз[30], и что требуются следующие немедленные действия:

– обеспечение постоянного мониторинга состояния систем, своевременное обновление ПО, удаление не санкционированно установленного ПО и оборудования, повышение навыков и бдительности как лиц, ответственных за обеспечение информационной безопасности, так и пользователей. Всё это объединено термином "кибергигиена" (cyber hygiene)[31];

– обеспечение прозрачности происходящих в системе процессов для системных администраторов[32];

– повышение уровня кибербезопасности самих систем и сетей.

Рабочая группа указала на то, что МО необходимо проводить непрерывный сбор и анализ данных о совершённых на их сети и системы кибератаках (свидетельств проведения такой работы исследователи не обнаружили) для повышения эффективности защитных мер[33].

Указана необходимость повысить автоматизацию управления сетью, которое в настоящее время в значительной степени осуществляется в ручном режиме. Автоматизации подлежат операции от обновления и конфигурирования программного обеспечения до анализа первичных данных о текущем состоянии безопасности, так как это позволит сократить время, требуемое для ликвидации обнаруженных уязвимостей. Интересно, что прежде чиновники МО в ряде случаев мотивировали отказ от модернизации систем тем, что в таком случае будет утеряна часть их функциональных возможностей[34]. Заместителю министра обороны по приобретению,

---

Конечными целями являются: обеспечение доверенного обмена информацией, сотрудничества и совместимости как в рамках МО, так и с внешними партнёрами; усиление защиты от киберугроз и уязвимостей; снижение прямых и косвенных затрат на ИТ-инфраструктуру. Внедрение данной концепции призвано упростить, стандартизировать, консолидировать и автоматизировать ИТ-инфраструктуру Пентагона. См.: Frequently-Asked-Questions.

[29] См.: PPD-21. P. 11; PPD-41.

[30] См.: DSB Task Force Report on Cyber Defense Management. P. 8 // Federation of American Scientists. URL: https://fas.org/irp/agency/dod/dsb/cyberdef.pdf (дата обращения: 14.03.2017).

[31] Ibid. P. 9.

[32] Ibid.

[33] Ibid. P. 10–11.

[34] Ibid. P. 12–13.

технологии и материально-техническому обеспечению также рекомендовано обеспечить, чтобы все ИТ-системы, которые МО США будет закупать в перспективе, по умолчанию имели бы необходимую степень автоматизации процессов управления. Исключение признано оправданным только в случае, если предварительный анализ рисков указывает, что внедрение этих возможностей в систему влечёт появление рисков ещё более серьёзных[35].

В рекомендациях рабочей группы подчёркнуто, что необходимо обеспечить кибербезопасность не только сетей МО США, но и систем вооружения и управления войсками на поле боя. Игнорирование этого направления ставит под угрозу выполнение поставленных задач в случае столкновения с противником, имеющим соответствующие современные силы и средства. Отмечено, что этот процесс необходимо начинать немедленно и завершить его в ближайшие 2–3 года[36].

Рекомендовано также использовать моделирование, чтобы выявить элементы систем, наиболее уязвимые на данный момент перед кибератаками. Предлагается использовать опыт работы с аналогичными системами в коммерческой сфере, а в качестве лидера в разработке таких моделей названа RAND Corp[37].

При этом указано, что Пентагону необходимо стимулировать своих поставщиков к повышению уровня защищённости их продукции, что называется, "из коробки". Теоретически это может быть обеспечено в том числе с помощью требования о наличии в закупаемых системах только требуемых Министерству обороны функций[38]. Кроме того, подчёркивается необходимость проведения специалистами МО экспертизы поставляемой продукции, так как в настоящий момент МО США не в состоянии этого сделать, а требование о минимизации количества уязвимостей к кибератакам закупаемого вооружения и военной техники рекомендовано сделать обязательным[39].

В качестве важнейшего направления работы МО США рассматривается снижение угрозы от действий инсайдеров посредством проведения непрерывного мониторинга сетей, повышения знаний личного состава в сфере кибербезопасности, развития методов идентификации, оповещения и отслеживания подозрительного поведения[40].

Вместе с тем, деятельность правительства США, включая Пентагон, в киберпространстве далеко не ограничивается только защитой собственных систем и сетей. Использование данной среды признаётся необходимым для ведения разведки, сдерживания и противодействия противнику, угрожающему национальным интересам США как в мирное время, так и в период войн и кризисов[41].

---

[35] См.: DSB Task Force Report on Cyber Defense Management. P. 14.
[36] Ibid.
[37] Ibid. P. 16–17.
[38] Ibid. P. 18.
[39] Ibid. P. 19.
[40] DOD Cyber Strategy 2015. P. 22.
[41] См.: Presidential Policy Directive / PPD-20 "U.S. Cyber Operations Policy". P. 4 // Federation of American Scientists. URL: https://fas.org/irp/offdocs/ppd/ppd-20.pdf (дата обращения: 14.03.2017).

В целом, в президентской директиве PPD-20 выделены следующие виды активности:

Защита сетей (network defense) — "действия, проводимые непосредственно на компьютерах, в сетях или информационно-коммуникационных системах самим владельцем, либо с его ведома с целью защиты: указанных компьютеров, сетей и систем; хранимых, обрабатываемых или передаваемых через них данных; физической и виртуальной инфраструктуры, контролируемой данными компьютерами, сетями и системами. Защита сетей не предполагает и не требует доступа или осуществления действий на компьютерах, сетях и системах без получения санкции со стороны их владельца или превышения прав доступа, санкционированных владельцем"[42].

Сбор информации (cyber collection) — "действия, тайно проводимые правительством США в киберпространстве или в его интересах, либо с его помощью, с целью сбора разведывательной информации и предполагающие отсутствие санкции владельца компьютеров, сетей и систем на проведение таких действий, а также включающие принятие мер по противодействию их детектированию или атрибутированию противником"[43].

Оборонительные кибероперации (Defensive Cyber Effect Operations, DCEO) — "действия, не включающие защиту сетей или сбор данных, проводимые правительством США в киберпространстве или в его интересах, либо с его помощью, с целью сделать возможным или непосредственно оказать воздействие на компьютеры, информационно-коммуникационные системы, сети, физическую или виртуальную инфраструктуру, ими контролируемую, за пределами сетей правительства США, с целью защиты от готовящихся или уже осуществляемых атак или враждебной активности в киберпространстве против национальных интересов США как внутри, так и вне киберпространства"[44].

Неинтрузивные оборонительные контрмеры (nonintrusive defense countermeasures, NDCM) — "действия, являющиеся подклассом оборонительных кибероперацій, которые не требуют доступа к компьютерам, информационно-коммуникационным системам или сетям, несанкционированного их владельцем или оператором, и оказывающие воздействие на компьютеры, информационно-коммуникационные системы, сети, физическую или виртуальную инфраструктуру, ими контролируемую, минимально необходимое для уменьшения опасности враждебных действий"[45].

Наступательные кибероперации (Offensive Cyber Effect Operations, OCEO) — "действия, не включающие защиту сетей, сбор данных или оборонительные кибероперации, проводимые правительством США в киберпространстве или в его интересах, либо с его помощью, с целью сделать возможным или непосредственно оказать воздействие на компьютеры, информационно-коммуникационные системы, сети, физическую или виртуальную инфраструктуру, ими контролируемую, за пределами сетей, принадлежащих правительству США"[46].

---

[42] См.: Presidential Policy Directive / PPD-20 "U.S. Cyber Operations Policy". P. 2.
[43] Ibid. P. 2–3.
[44] Ibid. P. 3.
[45] Ibid.
[46] Ibid.

Стоит отметить, что термин "кибероперации" включает в себя только сбор информации, оборонительные (включая неинтрузивные) и наступательные операции в киберпространстве[47].

При этом наступательные (OCEO) и оборонительные (DCEO) операции рассматриваются как ещё один инструмент обеспечения и защиты национальных интересов США наряду с дипломатией, военной силой и экономическими рычагами[48]. Оборонительные операции предполагается осуществлять, в том числе, в рамках использования права государства на самооборону[49]. При проведении DCEO министерствам и ведомствам рекомендовано сотрудничать с ИТ-отраслью, а также с иностранными государствами и различными организациями[50].

Министерству обороны вместе с другими министерствами и ведомствами предписано принять участие в разработке предложений по созданию потенциала для проведения оборонительных и наступательных операций, включая ответные действия, как в случае готовящейся, так и в условиях уже осуществляемой атаки на США и на интернет[51]. В том числе, обеспечить подготовку к проведению OCEO: выявить потенциальные цели (системы, процессы и инфраструктуру), определить условия, при наступлении которых возможно проведение данных операций, и необходимые для этого ресурсы и порядок действий, и обеспечить их взаимную интеграцию с иными инструментами наступательного характера[52]. При этом, согласно исследованию JOE-2035, наступательные операции в будущем могут включать в себя выявление, захват и даже ликвидацию личного состава сил противника, обеспечивающих его действия в киберпространстве[53].

Отдельно предусмотрен вариант проведения экстренных действий в киберпространстве (Emergency Cyber Actions, ECA) как в условиях уже осуществляемой противником атаки, так и *превентивно*, с целью ликвидации угрозы. В данном случае уполномоченные на проведение ECA министерства и ведомства могут действовать без получения санкции президента[54]. При этом МО США уполномочено проводить оборонительные операции в киберпространстве в качестве ECA, если:

– они проводятся в рамках осуществления права США на самооборону;

– невозможно обеспечить защиту сетей или правопорядка в случае соблюдения предусмотренного обычного порядка действий;

– с достаточной степенью вероятности они не приведут к значительным последствиям (significant consequences)[55];

---

[47] См.: Presidential Policy Directive / PPD-20 "U.S. Cyber Operations Policy". P. 3.
[48] Ibid. P. 6, 9.
[49] Ibid. P. 8.
[50] Ibid.
[51] Ibid. P. 16.
[52] Ibid. P. 9, 15.
[53] Joint Operating Environment 2035... P. 50.
[54] PPD-20. P. 15.
[55] Значительные последствия: гибель людей, значимые ответные действия против Соединённых Штатов, существенный материальный ущерб, серьёзные неблагоприятные

– они не приведут к гибели людей;

– они будут ограничены по масштабам и продолжительности уровнем, необходимым для снижения угрозы или смягчения последствий атаки со стороны противника[56].

Рассмотренные предписания определяют ещё два направления работы МО США в киберпространстве.

Так, вторым является защита территории и национальных интересов США от кибератак, которые могут вызвать значительные последствия[57]. В подобной ситуации американские ВС могут провести встречную кибероперацию для противодействия готовящейся либо осуществляемой кибератаке. Основным заявленным принципом является то, что проведение кибероперации — крайняя мера в случае отсутствия положительного результата от применения иных мер[58].

В то же время Пентагон указывает, что в силу отмеченной выше правовой неопределённости вокруг действий в киберпространстве противник может организовать нанесение удара по США так, чтобы атаку нельзя было использовать в качестве достаточного повода для военного ответа, даже если она представляет серьёзную угрозу для национальной безопасности Соединённых Штатов. Поэтому США оставляют за собой право предпринять ответные действия дипломатического и правового характера, а также применить экономические санкции против атакующих[59].

Третьим же направлением является использование сил и средств для действий в киберпространстве с целью проведения военных операций и действий в особой обстановке, а это, в свою очередь, подразумевает проведение кибероперации по разрушению сетей или инфраструктуры, используемых вооружёнными силами противника, а также для защиты американских интересов в зоне проведения операций ВС США. Целью является получение возможности контролировать эскалацию конфликтов и направлять развитие конфликтной обстановки на всех стадиях. Кроме того, американское Кибернетическое командование может провести совместную кибероперацию с иными федеральными агентствами с целью сдерживания или ликвидации стратегических угроз вне киберпространства[60].

Необходимо отметить, что руководство США уделяет большое внимание информационному сопровождению своих действий. Так, советнику по национальной безопасности предписано провести ревизию коммуникационной стратегии правительства США, в том числе и руководства по связям с общественностью, в связи с включением DCEO и OCEO в число инструментов американской внешней политики[61].

последствия для американской внешней политики, либо серьёзное экономическое влияние на США. См.: PPD-20. P. 3.

[56] См.: PPD-20. P. 10–11.

[57] DOD Cyber Strategy 2015. P. 5.

[58] Ibid.

[59] Ibid. P. 12.

[60] Ibid. P. 5, 14.

[61] PPD-20. P. 15.

Практические действия

С целью обеспечения собственной безопасности в киберпространстве Пентагон в 2013 г. инициировал создание кибервойск (Cyber Mission Force, CMF), которые по его планам в течение 5 лет (считая с 2015 г.) должны достичь состояния полной готовности к выполнению задач[62]. Планируемая общая численность CMF составляет около 6,2 тыс. человек личного состава, включая военнослужащих, гражданский персонал и персонал подрядчиков Пентагона. Должно быть сформировано 133 подразделения трёх видов[63]:

– подразделения Cyber Protection Forces отвечают за защиту сетей и систем МО США;

– подразделения National Mission Forces отвечают за защиту США и их интересов от кибератак со значительными последствиями;

– подразделения Combat Mission Forces должны действовать в киберпространстве в интересах боевых командований для обеспечения реализации их оперативных планов и действий в особой обстановке.

Согласно планам, подразделения, относящиеся к Combat Mission Forces и Cyber Protection Forces, будут выполнять задачи в киберпространстве в поддержку действий боевых командований, а подразделения из состава National Mission Forces должны действовать под руководством командующего Кибернетического командования США. Тем не менее, при необходимости отдельные подразделения могут использоваться вне указанной структуры[64].

Согласно Киберстратегии-2015 основной задачей создаваемых кибервойск США является *сдерживание* противника от осуществления кибератак против американских интересов[65]. При этом в документе указано, что по состоянию на момент его опубликования (апрель 2015 г.) подавляющее большинство действий МО США в киберпространстве носило оборонительный характер и проводилось в собственной информационной сети[66].

В целом же, информация о практической реализации американским военным ведомством рекомендаций и требований руководящих документов в области кибербезопасности скудна.

Так, согласно проекту оборонного бюджета на 2017 фин. г., планируется получить 6,7 млрд дол. на оборонительные и наступательные кибероперации, создание средств для осуществления действий в киберпространстве и реализации целей Киберстратегии-2015. Данная сумма на 0,9 млрд дол. больше, чем было выделено в 2016 фин. г.[67] Эти средства

---

[62] DOD Cyber Strategy 2015. P. 13.

[63] Ibid. P. 6.

[64] Ibid.

[65] Ibid. P. 10–11.

[66] Ibid. P. 4.

[67] См.: Department of Defense (DoD) Releases Fiscal Year 2017 President's Budget Proposal // U.S. Department of Defense. URL: http://www.defense.gov/News/News-Releases/News-Release-View/Article/652687 (дата обращения: 01.11.2016); Defense Budget Overview Book. P. 5-5 // Under Secretary of Defense (Comptroller). URL: http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2017/FY2017_Budget_Request_Overview_Book.pdf (дата обращения: 01.11.2016).

планируется направить на финансирование деятельности по следующим направлениям[68]:

– продолжение работы по формированию 133 подразделений кибервойск, которые должны достичь состояния полной готовности к концу 2018 фин. г.;

– оборудование Центра объединённых операций (Joint Operations Center) для Кибернетического командования в форте Мидл (штат Мэриленд), начало функционирования которого запланировано на 2018 фин. г.;

– поддержка научно-технических программ и других исследований и проектов по разработке необходимых инструментов в интересах кибервойск;

– исследования в области создания виртуальной среды для проведения тренировок и "репетиций" выполнения заданий в киберпространстве;

– поддержка оборонных кибероперациий посредством обеспечения целостности и безопасности сетей Пентагона;

– поддержка действий боевых командований и проведения наступательных кибероперациий посредством обеспечения ВС США соответствующими средствами.

Среди основных военных учений вооружённых сил США, проведение которых предусмотрено на 2017 фин. г., три мероприятия непосредственно связаны с обеспечением кибербезопасности.

Во-первых, это ежегодные учения Стратегического командования США (USSTRATCOM) Cyber Guard, которые являются общенациональными учениями для отработки реагирования на внутреннюю кибератаку и разрушение киберпространства по причинам природного или антропогенного характера[69].

Предыдущие учения Cyber Guard 2016 состоялись (уже в 5-й раз) на базе центра Комитета начальников штабов в Саффолке, созданного для проведения военных натурных испытаний и учений. Среди участников были организации, управляющие инфраструктурой киберпространства и критической инфраструктурой, а также эксперты более 100 учреждений и организаций, включая правительство, академические круги, ИТ-индустрию и представителей союзников (Австралия, Канада, Великобритания). Руководство учениями совместно осуществляли Киберкомандование США, Министерство внутренней безопасности (DHS) и ФБР[70].

По сценарию учений от 1 до 10 млн домов и предприятий в США остались без электричества, в результате чего в Техасе и Луизиане произошёл разлив нефти на прибрежных НПЗ, а порт Лос-Анджелеса был закрыт[71].

---

[68] Defense Budget Overview Book. P. 5-5.

[69] Ibid. P. 3-15, 3-16.

[70] См.: Cyber Guard 16 Fact Sheet // U.S. Department of Defense. URL: http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Cyber-Guard-16-Fact-Sheet-FINAL.pdf (дата обращения: 01.11.2016); Cyber Guard 2016 Seeks to Manage Complexity in Invisible Domain // U.S. Department of Defense. URL: http://www.defense.gov/News/Article/Article/803018/cyber-guard-2016-seeks-to-manage-complexity-in-invisible-domain (дата обращения: 01.11.2016).

[71] См.: Cyber Guard 2016 Seeks to Manage Complexity in Invisible Domain.

Целями учений являлись: отработка взаимодействия силовых ведомств с гражданскими властями, проверка возможности МО США действовать в киберпространстве и продолжение работы по созданию Постоянной тренировочной среды (Persistent Training Environment, PTE) для кибервойск. PTE представляет собой закрытую сеть для проведения учений, планирования тренировок, управления и оценки, натурной отработки действий, с возможностью проведения полного спектра общенациональных учений и тренировок в киберпространстве[72].

Во-вторых, запланированы учения Стратегического командования США (USSTRATCOM) Cyber Flag, включающие отработку сочетания наступательных и оборонительных действий в киберпространстве с полным спектром военных операций Пентагона[73].

В-третьих, учения Транспортного командования (USTRANSCOM) Ultimate Guardian 2017, которые взаимосвязаны с учениями Тихоокеанского командования США (USPACOM) Pacific Century 17–2. Целью проведения учений является отработка действий USTRANSCOM и оценка его готовности к осуществлению оборонительных кибероперaций на стратегическом, операционном и тактическом уровнях. Сюда включается отработка процессов обнаружения, снижения ущерба и восстановления после кибератаки, а также отработка взаимодействия с подразделениями поддержки из состава кибервойск[74].

Таким образом, ВС США ведут достаточно активную подготовку к действиям с использованием возможностей киберпространства.

Одновременно продолжается работа по созданию кибервойск.

Так, 24 октября 2016 г. Пентагон объявил о том, что все 133 подразделения кибервойск Киберкомандования США достигли начального уровня оперативной готовности (initial operating capability), позволяющего им приступить к решению своих задач. В настоящее время численность личного состава кибервойск составляет около 5 тыс. человек из планируемых к концу 2018 фин. г. 6,2 тыс. человек. Полной готовности кибервойска должны достичь к 30 сентября 2018 г. Тем не менее, в настоящий момент примерно половина подразделений достигла этой стадии, и в целом они уже играют жизненно важную роль в защите США от кибератак. Командующий USCYBERCOM и директор АНБ адмирал М. Роджерс заявил, что нынешнее положение, когда вновь создаваемые подразделения сразу приступают к решению задач, является необычным для ВС США и вызвано высокой изменчивостью ситуации[75].

Информации об официальных оценках реального состояния дел в области кибербезопасности ВС США и с реализацией целей Киберстратегии-2015 также крайне мало. Так, например, на странице генерального инспектора Пентагона опубликованы лишь общие сведения об отчётах, подготовленных по результатам аудита положения с кибербезопасностью в МО. Однако тексты самих документов отсутствуют в свободном доступе.

---

[72] См.: Cyber Guard 16 Fact Sheet.

[73] См.: Defense Budget Overview Book. P. 3-15, 3-16.

[74] Ibid. P. 3-15, 3-16.

[75] См.: All Cyber Mission Force Teams Achieve Initial Operating Capability // U.S. Department of Defense. URL: http://www.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability (дата обращения: 01.11.2016).

Из краткой открытой аннотации известно, что один отчёт, опубликованный в 2015 г., является секретным, и в нём отмечается необходимость переоценки процессов развёртывания подразделений кибервойск[76].

Второй отчёт опубликован в 2016 г. и имеет гриф "для служебного пользования". Согласно краткой открытой аннотации, в нём представлены результаты проверки ПО, закупаемого в интересах программы создания перспективного боевого корабля прибрежной зоны ВМС США, на предмет выполнения требований об обязательном тестировании приобретаемого Пентагоном ПО с целью выявления возможных уязвимостей. Указано, что результаты проверки неудовлетворительные, так как данное ПО не обеспечивает все предусмотренные контрмеры. Таким образом, риск наличия уязвимостей в таком программном обеспечении растёт, что в конечном счёте может привести к невыполнению поставленных командованием задач. Заместителю министра обороны по приобретению, технологии и материально-техническому обеспечению рекомендуется исправить указанные недостатки[77].

Пентагон прорабатывает варианты использования методов повышения кибербезопасности, хорошо зарекомендовавших себя в частном секторе.

Так, следует отметить появление инициативы "Взломай Пентагон" (Hack the Pentagon), которая представляет собой программу привлечения специалистов из коммерческого сектора к поиску уязвимостей в публичных приложениях, сайтах и сетях американского военного ведомства. Данная инициатива является первым опытом федерального правительства США по использованию программ премирования внешних специалистов за сообщения об обнаруженных уязвимостях в программном обеспечении (Bug bounty). В то же время крупнейшие ИТ-компании достаточно активно и успешно привлекают профессионалов со стороны для повышения защищённости своих сетей, продуктов и цифровых сервисов.

Первое мероприятие в рамках данной инициативы Пентагона прошло в апреле–мае 2016 г. на базе компании HackerOne, базирующейся в Кремниевой долине. Участники получили доступ к предварительно выбранному сегменту информационной сети МО США. Иные сегменты сети, включая критически важные, в данном мероприятии не участвовали.

Пробная попытка признана успешной — получены "впечатляющие результаты, значительно превосходящие ожидания"[78]. Участники обнаружили 1189 уязвимостей (первая была обнаружена через 13 минут после старта мероприятия), 138 из которых признаны представляющими серьёзную угрозу и требующими срочного устранения. Общая сумма затрат Пентагона на проведение данного мероприятия составила 150 тыс. дол., примерно половина из которых пошла на вознаграждение участников.

---

[76] См.: DODIG-2015-117. Audit Report // Office of Inspector General, U.S. Department of Defense. URL: http://www.dodig.mil/pubs/report_summary.cfm?id=6440 (дата обращения: 01.11.2016).

[77] См.: DODIG-2016-082. Audit Report // Office of Inspector General, U.S. Department of Defense. URL: http://www.dodig.mil/pubs/report_summary.cfm?id=6938 (дата обращения: 01.11.2016).

[78] "Hack the Pentagon" Fact Sheet — June 17, 2016 // U.S. Department of Defense. URL: http://www.defense.gov/Portals/1/Documents/Fact_Sheet_Hack_the_Pentagon.pdf (дата обращения: 01.11.2016).

По полученным результатам Пентагон объявил о планах запуска новых инициатив[79]:

– создание механизма, позволяющего любому, кто имеет информацию об уязвимостях в системах, сетях, приложениях или сайтах Пентагона, сообщить о них, не опасаясь судебного преследования;

– распространение программы Bug bounty в рамках Пентагона.

Предполагается включить эти инициативы в закупочную политику МО США с целью повышения защиты данных американского военного ведомства.

Таким образом, можно заключить, что Пентагон явно предпринимает активные действия в этом направлении. Перечень таких мер включает интенсификацию усилий по завершению создания кибервойск, по применению и контролю за выполнением руководящих документов и инструкций, а также по адаптации к нуждам американского военного ведомства методов, хорошо зарекомендовавших себя в частном секторе.

* *
*

Подводя итог, можно констатировать, что в силу описанной выше сложной ситуации с обеспечением собственной кибербезопасности, направления работ и цели Пентагона в этой сфере на настоящий момент практически полностью состоят, согласно официальным документам, в обеспечении безопасности ведомственной информационной сети, систем вооружения и критической инфраструктуры (как собственной, так и американского ВПК) от киберугроз. Возможность проведения действий наступательного характера в киберпространстве предусмотрена, но, как представляется, не является для МО США основной.

Тем не менее, американские военные исходят из того, что в будущем Соединённым Штатам придётся оборонять собственное суверенное киберпространство, защищать свой доступ к использованию киберпространства общего пользования, в том числе обеспечивать контроль его ключевых частей[80]. Поэтому ведётся масштабная планомерная работа по оценке сложившейся ситуации, выработке рекомендаций по её исправлению и воплощению их в жизнь — от распределения зон ответственности между министерствами и ведомствами, определения задач и создания соответствующих сил и средств ВС США (в том числе наступательного характера) — до оценки и использования опыта обеспечения кибербезопасности, наработанного в коммерческой сфере.

---

[79] См.: Statement by Pentagon Press Secretary Peter Cook on DoD's "Hack the Pentagon" Cybersecurity Initiative // U.S. Department of Defense. URL: http://www.defense.gov/News/News-Releases/News-Release-View/Article/684106/statement-by-pentagon-press-secretary-peter-cook-on-dods-hack-the-pentagon-cybe (дата обращения: 01.11.2016); DoD Announces 'Hack the Pentagon' Follow-Up Initiative // U.S. Department of Defense. URL: http://www.defense.gov/News/Article/Article/981160/dod-announces-hack-the-pentagon-follow-up-initiative (дата обращения: 01.11.2016); "Hack the Pentagon" Fact Sheet — June 17, 2016.

[80] Joint Operating Environment 2035... P. 33.

Таким образом, можно заключить, что наличие у других субъектов международных отношений эффективных средств для проведения действий в кибепространстве является весомым аргументом для удержания американской стороны от осуществления активных враждебных действий в этой сфере.

Ключевые слова: *США — кибербезопасность — киберпространство — критическая инфраструктура — политика США в отношении действий в киберпространстве — кибервойска США.*

Keywords: *USA — cybersecurity — cyberspace — critical infrastructure — the U.S. cyberspace policy — the U.S. cyber forces.*

СПИСОК ЛИТЕРАТУРЫ

1. Ботнет // SecurityLab.ru. URL: http://www.securitylab.ru/news/tags/%E1%EE%F2%ED%E5%F2/ (дата обращения: 01.11.2016).

2. All Cyber Mission Force Teams Achieve Initial Operating Capability // U.S. Department of Defense. URL: http://www.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability (дата обращения: 01.11.2016).

3. Cyber Guard 16 Fact Sheet // U.S. Department of Defense. URL: http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Cyber-Guard-16-FactSheet-FINAL.pdf (дата обращения: 01.11.2016).

4. Cyber Guard 2016 Seeks to Manage Complexity in Invisible Domain // U.S. Department of Defense. URL: http://www.defense.gov/News/Article/Article/803018/cyber-guard-2016-seeks-to-manage-complexity-in-invisible-domain (дата обращения: 01.11.2016).

5. Defense Budget Overview Book // Under Secretary of Defense (Comptroller). URL: http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2017/FY2017_Budget_Request_Overview_Book.pdf (дата обращения: 01.11.2016).

6. Department of Defense (DoD) Releases Fiscal Year 2017 President's Budget Proposal // U.S. Department of Defense. URL: http://www.defense.gov/News/News-Releases/News-Release-View/Article/652687 (дата обращения: 01.11.2016).

7. DoD Announces 'Hack the Pentagon' Follow-Up Initiative // U.S. Department of Defense. URL: http://www.defense.gov/News/Article/Article/981160/dod-announces-hack-the-pentagon-follow-up-initiative (дата обращения: 01.11.2016).

8. DOD Cyber Strategy 2015. P. 2 // U.S. Department of Defense. URL: http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (дата обращения: 01.11.2016).

9. DoD Cybersecurity Discipline. Implementation Plan. P. 4 // Department of Defense Chief Information Officer. URL: http://dodcio.defense.gov/Portals/0/Documents/Cyber/CyberDis-ImpPlan.pdf (дата обращения: 01.11.2016).

10. DODIG-2015-117. Audit Report // Office of Inspector General, U.S. Department of Defense. URL: http://www.dodig.mil/pubs/report_summary.cfm?id=6440 (дата обращения: 01.11.2016).

11. DODIG-2016-082. Audit Report // Office of Inspector General, U.S. Department of Defense. URL: http://www.dodig.mil/pubs/report_summary.cfm?id=6938 (дата обращения: 01.11.2016).

12. DSB Task Force Report on Cyber Defense Management // Federation of American Scientists. URL: https://fas.org/irp/agency/dod/dsb/cyberdef.pdf (дата обращения: 14.03.2017).

13. Frequently-Asked-Questions // Department of Defense Chief Information Officer. URL: http://dodcio.defense.gov/About-DoD-CIO/Frequently-Asked-Questions/ (дата обращения: 01.11.2016).

14. GAO-15-758T. July 8, 2015. INFORMATION SECURITY. Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies. Testimony Before the Subcommittees on Research and Technology and Oversight, Committee on Science, Space, and Technology, House of Representatives. P. 2 // United States Government Accountability Office. URL: http://www.gao.gov/products/GAO-15-758T (дата обращения: 01.11.2016).

15. GAO-16-885T. September 19, 2016. FEDERAL INFORMATION SECURITY: Actions Needed to Address Challenges. Testimony Before the President's Commission on Enhancing National Cybersecurity. P. 1–3 // United States Government Accountability Office. URL: http://www.gao.gov/products/GAO-16-885T (дата обращения: 01.11.2016).

16. "Hack the Pentagon" Fact Sheet — June 17, 2016 // U.S. Department of Defense. URL: http://www.defense.gov/Portals/1/Documents/Fact_Sheet_Hack_the_Pentagon.pdf (дата обращения: 01.11.2016).

17. Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World // The Defense Technical Information Center. URL: http://www.dtic.mil/doctrine/concepts/joe/joe_2035_july16.pdf (дата обращения: 14.03.2017).

18. National Information Assurance (IA) Glossary (CNSSI 4009) // National Counterintelligence and Security Center (NCSC). URL: https://www.ncsc.gov/nittf/docs/CNSSI-4009_National_Information_Assurance.pdf (дата обращения: 01.11.2016).

19. Presidential Policy Directive / PPD-20 "U.S. Cyber Operations Policy" // Federation of American Scientists. URL: https://fas.org/irp/offdocs/ppd/ppd-20.pdf (дата обращения: 14.03.2017).

20. Presidential Policy Directive / PPD-21 "Critical Infrastructure Security and Resilience" // Federation of American Scientists. URL: https://fas.org/irp/offdocs/ppd/ppd-21.pdf (дата обращения: 14.03.2017).

21. Presidential Policy Directive / PPD-41 "United States Cyber Incident Coordination" // Federation of American Scientists. URL: https://fas.org/irp/offdocs/ppd/ppd-41.html (дата обращения: 14.03.2017).

22. Statement by Pentagon Press Secretary Peter Cook on DoD's "Hack the Pentagon" Cybersecurity Initiative // U.S. Department of Defense. URL: http://www.defense.gov/News/News-Releases/News-Release-View/Article/684106/statement-by-pentagon-press-secretary-peter-cook-on-dods-hack-the-pentagon-cybe (дата обращения: 01.11.2016).

23. U.S. National Security Strategy 2015 // National Security Strategy Archive. URL: http://nssarchive.us/wp-content/uploads/2015/02/2015.pdf (дата обращения: 01.11.2016).