П.А. ШАРИКОВ*

ЭВОЛЮЦИЯ ГОСУДАРСТВЕННОЙ СТРАТЕГИИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Во второй половине XX – начале XXI века развитие человечества было в значительной степени подвержено влиянию информационной революции. Значительные массы населения всей планеты смогли воспользоваться её плодами. Благодаря персональным компьютерам и Интернету участники глобального информационного обмена получили практически неограниченный доступ к анализу, применению и созданию новой информации, моментально распространяя её повсюду.

Эффективное использование возможностей, открывающихся при помощи информационных технологий (ИТ), во многом стало фактором экономического роста, повышения благосостояния населения, военного превосходства и многих других составляющих мощи государства.

С начала информационного бума прошло уже более 50 лет, однако спрос на его продукты не уменьшается, информационная революция продолжается. Возможно, в скором времени, информационное пространство будет включать в себя все данные, накопленные в течение всей истории существования земной цивилизации. Развитие технологий направлено на облегчение доступа человека к информации, в частности за последнее десятилетие были значительно усовершенствованы средства мобильной и беспроводной связи. Эта тенденция была обусловлена необходимостью войти в информационное пространство в любой точке планеты независимо от степени развития местной инфраструктуры. В результате появились технические средства, позволяющие пользоваться Интернетом посредством космических систем, сотовой связи, а возможности обработки и передачи данных на мобильных устройствах не уступают мощности обычных персональных компьютеров.

Одновременно с развитием технологий и их внедрением и использованием в различных сферах деятельности американского общества осложнялись и угрозы информационной безопасности. Уже в середине 1990-х годов американское правительство обратило внимание на возрастающее количество преступлений, совершаемых при помощи информационных технологий. Обнаружилась

* **ШАРИКОВ Павел Александрович – кандидат политических наук, научный сотрудник ИСКРАН.**

потенциальная уязвимость экономической и военной безопасности Соединённых Штатов в информационной сфере.

Во второй половине XX века в Соединённых Штатах были созданы благоприятные условия для развития информационных технологий, в результате чего именно в этой стране появились первые компьютеры. США – одна из первых стран, в которой информационные технологии стали стратегическим ресурсом, широко развитым и используемым в экономике, политике, вооружённых силах и многих других областях. Понятие «информационная безопасность» в американских реалиях в большей степени связана с информационной инфраструктурой, технологиями, информационным пространством, чем в других странах. В силу этих обстоятельств в Соединённых Штатах впервые политика государства в области регулирования информационной сферы стала **приоритетом** в обеспечении безопасности.

Возрастающая зависимость современного общества от информационных технологий значительно осложнила вопросы безопасности. Само понятие информационной безопасности имеет два аспекта: с одной стороны, безопасность самих инфоресурсов – информации и технологий; к этой категории следует отнести вопросы обеспечения стабильного функционирования информационной инфраструктуры, защиты от несанкционированного доступа, вредоносных программ и пр. Этот аспект в основном носит технический характер, так как связан с умышленным или случайным воздействием на информацию или информационную инфраструктуру.

Другой, более широкий, включает, в первую очередь такие категории, как информационные ресурсы, обеспечивающие безопасность в целом, эффективность применения информационных технологий, и пр. ИТ нашли широкое применение практически во всех сферах национальной безопасности, с этим связана актуальность зашиты информационных ресурсов. Воздействие на информацию или информационную инфраструктуру иной раз имеет катастрофические последствия на ту сферу, в которой они применяются. Таким образом, ко второму аспекту следует отнести не просто безопасность информационных ресурсов, но вопросы обеспечения различных аспектов национальной безопасности в информационной сфере.

Очевидно, что два эти аспекта крайне важны и тесно взаимосвязаны между собой. Информационные ресурсы играют важнейшую роль в развитии личности, общества, бизнеса, государства и международных отношений в целом. Одновременно с этим, информационные технологии нашли широкое применение в военной, экономической, социальной, энергетической и прочих сферах деятельности человека. Значение информационных ресурсов и обеспечение информационной безопасности в этих сферах возросло и продолжает оказывать большое влияние на все субъекты безопасности.

Скорее всего техническое понимание информационной безопасности первично. К примеру, возможность поражения компьютера вредоносной программой является угрозой информационной безопасности. Однако поражение вирусом системы, обеспечивающей электроснабжение, это информационная угроза энергетической безопасности. Повсеместное внедрение ИТ привело к тому, что

этот аспект стал актуален практически во всех сферах общества. Рассуждая дальше, можно прийти к выводу о том, что следует обращать внимание только на информационные аспекты различных сфер безопасности. Автор рассматривает ряд общих принципов функционирования инфраструктуры, на основе которых обеспечивается информационная безопасность, но, безусловно, каждый аспект национальной безопасности имеет свою специфику в информационной сфере.

К общим принципам обеспечения информационной безопасности следует отнести, прежде всего, то, что на современном этапе развития информационные технологии объединяются в единое пространство. Этого могло бы не произойти, если бы не универсальные для всех стран стандарты связи, передачи и хранения данных.

Во многом стандартизация информационного пространства – заслуга Соединённых Штатов, именно там появились многие стандарты передачи данных. К примеру, когда создавался Интернет, в США был принят стандарт передачи данных – протокол контроля передачи данных – Интернет-протокол (*Transmission Control Protocol/Internet Protocol, TCP/IP*). Этот стандарт во многом является основой пространства, на базе которого функционирует всемирная информационная сеть Интернет. В ходе распространения технологий в мире, остальные страны были вынуждены принять этот стандарт, иначе возник бы конфликт технической совместимости их национальных информационных ресурсов с Интернетом.

В настоящее время разрабатывается новый стандарт Интернет связи – Интернет-протокол передачи данных версии 6 (*Transmission Control Protocol Internet Protocol Version 6*, *TCP/Ipv6*). Разработчики утверждают, что этот протокол связи надёжнее, удобнее и быстрее чем предыдущий[1]. Переход на новый стандарт будет сопровождаться необходимостью устанавливать новое программное обеспечение, а иногда и приобретать новые технические устройства. По-видимому, это может стать серьёзной угрозой информационной безопасности. В некоторых сферах использование различных стандартов продолжается, однако в этих случаях (например, форматы трансляции и воспроизведения видеоданных *PAL, SECAM* и *NTSC*) несовместимость технологий не является серьёзным препятствием для развития и внедрения ИТ.

Уникальной особенностью информационных ресурсов, отличающих их от прочих аспектов национальной безопасности, является сетевая организация информационного пространства. Глобальная сеть не имеет системы централизованного иерархического управления. Потенциал участников общества определяется не законом, а уровнем технологического развития, возможностью доступа к информационным ресурсам. В условиях рыночной экономики они в значительной степени коммерциализированы, что сильно осложняет создание механизма государственного или международно-правового регулирования этой сферы.

[1] http://www.ipv6.org/

Узкое понимание информационной безопасности ограничивается вопросами зашиты информационного пространства, широкое же понимание подразумевает негативные последствия, возникающие в результате воздействия на информационные ресурсы в других сферах безопасности, в которых они используются.

Гарантировать безопасность (не только информационную) государство может только в том случае, если оно обладает возможностью максимального контроля или управления ресурсами. К примеру, государство гарантирует безопасность граждан от внешних военных угроз за счёт того, что они сами соблюдают законодательство (подчиняются государству), платят налоги, которые среди прочего идут на обеспечение армии. Армия, в свою очередь, подчиняется главнокомандующему, т.е. государственной власти, которая берёт на себя обязательство обеспечивать национальную безопасность.

Если речь идёт об информационной безопасности, государство вряд ли сможет взять на себя такие гарантии, так как информационные ресурсы, как правило, распределены между государством, бизнесом, обществом, отдельными личностями и даже международными акторами. Информационное пространство глобально, поэтому отдельное государство не может взять на себя ответственность за информационную безопасность в пределах своих национальных границ.

Вместе с тем, необходимо заметить, что как информация (знания, данные, ноу-хау), так и ИТ, как правило, в большой степени принадлежат частному бизнесу. Коммерческий спрос на информацию был одним из основных факторов стремительного экономического роста развитых стран (прежде всего США, Японии и Западной Европы). Государственное обеспечение информационной безопасности означало бы установление жёсткого регулирования или даже национализацию всех информационных ресурсов. Этот факт является лишним доказательством того, что государство не может гарантировать обеспечение информационной безопасности, но и не значит, что оно должно абстрагироваться от этого процесса.

Современный этап развития человечества характеризуется значительно возросшей зависимостью от информационных ресурсов, однако на данном этапе нельзя сказать, что все государства зависят от них в равной степени. Нарушение информационной безопасности будет иметь разные последствия для национальной безопасности государств с высокой и низкой степенью зависимости от ИТ.

Попытки создания иерархической системы информационной безопасности

В середине 1990-х годов в США началась разработка различных способов противодействия информационным угрозам. Основное внимание государственного руководства было обращено на угрозу криминального использования информационных технологий. Были приняты законы, устанавливающие наказание за использование ИТ в преступных целях.

Новые возможности, появившиеся в результате развития информационных технологий, создали для пользователей большие соблазны для нарушения имущественных прав. Обнаружился существенный разрыв в правовой базе, обусловленный технической отсталостью правоохранительных органов и возможностями совершения информационных преступлений. Проблема осложнялась тем, что уязвимость информационной безопасности возросла в государственном и частном секторе, а также и среди отдельных граждан. Кроме того, большая часть государственных и экономических предприятий находилась в острой зависимости от использования информационных технологий.

Помимо противодействия компьютерным преступлениям, не менее остро стояла проблема защиты критически важных элементов инфраструктуры. В мае 1998 г., президент США У. Клинтон выпустил директиву СНБ-63, которая устанавливала основные направления государственной политики в области противодействия угрозам критически важных элементов американской национальной инфраструктуры.

В документе отмечалась потенциальная возможность того, что ведение военных действий против Соединённых Штатов со стороны государств или других субъектов маловероятно, так как США нет равных в мире в военной сфере. Агрессия против США, по мнению авторов доклада, будет происходить нетрадиционными способами, включая атаки, исходящие с территории Соединённых Штатов, в силу того, что американская экономика всё больше зависит от взаимосвязанной информационной инфраструктуры. Поэтому нетрадиционные атаки на инфраструктуру и информационные системы могут принести значительные потери как в военной сфере, так и в экономике. В директиве признавалось, что для того, «чтобы выполнить поставленную цель – уничтожить возникшую угрозу, необходимы совместные усилия государства и частного сектора, но при этом государственное регулирование не должно препятствовать свободной экономической деятельности»[2].

Согласно директиве, в каждой государственной организации ответственность за противодействие информационным преступлениям возлагалась на директора по информационным технологиям, который устанавливал внутриорганизационные правила, направленные на обеспечение безопасности.

Кроме того, в директиве говорилось о необходимости сформировать специальный Центр защиты национальной инфраструктуры (*National Infrastructure Protection Center, NIPC*) в рамках Федерального бюро расследований. Созданный в 1998 г. Центр защиты национальной инфраструктуры тесно работал с частным бизнесом. В его задачи входило:

- выявлять случаи незаконного использования компьютеров и информационных технологий, ставящие под угрозу безопасность инфраструктуры США, предупреждать об этом соответствующие органы, пресекать их и заниматься их расследованием;
- расследовать дела, связанные с хакерами;

[2] Presidential Decision Directive/NSC-63, Subject: Critical Infrastructure Protection. The White House, Wash., 22.05.1998.

- оказывать помощь в расследовании дел, касающихся внешней контрразведки и борьбы с терроризмом и при этом связанных с незаконным использованием компьютеров;
- предупреждать руководителей служб, отвечающих за национальную безопасность, о тех случаях, когда попытка проникновения в инфраструктуру США является не обычным уголовным преступлением, а организованной из-за рубежа компьютерной атакой;
- координировать обучение следователей из государственных и частных структур, занимающихся расследованием компьютерных преступлений.

По сравнению с традиционными методами совершения правонарушений, компьютерное проще совершить и сложнее расследовать. При этом нападение может быть осуществлено из-за рубежа, а его жертвами в одинаковой степени могут оказаться любые компьютерные системы, а следовательно, простые граждане и частные предприятия, а также государственные инфраструктуры.

Правительство и Конгресс США предприняли попытки создать противодействия информационным правонарушениям. Были приняты законы, устанавливающие уголовную ответственность за совершение информационных преступлений, созданы государственные учреждения, на которые возложена ответственность за обеспечение информационной безопасности. Впервые в истории попытались создать иерархическую систему обеспечения информационной безопасности. Однако, несмотря на подобные законодательные, административные и организационные меры, противодействие угрозам продолжало оставаться неэффективным.

С приходом к власти администрации Дж. Буша-мл. политика США в области национальной безопасности была существенно пересмотрена. С распадом Советского Союза в международных отношениях сложились условия, в которых Соединённые Штаты стали претендовать на статус единственной сверхдержавы. Этот курс был начат ещё при администрации У. Клинтона, однако Дж. Буш-мл. продолжил закрепление за Соединёнными Штатами статуса единственной сверхдержавы другими методами, включающими военное применение силы. Важнейшую роль в обеспечении национальной безопасности США при его администрации играли и информационные ресурсы.

Вопросы информационной безопасности стояли настолько остро, что потребовалось дополнить «Стратегию национальной безопасности» другим документом – «Стратегией защиты киберпространства». Жизнь каждого американца стала слишком сильно зависеть от информационных технологий, от различных составляющих национальной инфраструктуры, которые оказались весьма уязвимыми для кибертеррористов. Многочисленные исследования свидетельствовали о том, что «государство было не готово противостоять информационным угрозам, оно просто не в состоянии обеспечить соответствующими системами компьютерной безопасности все частные банки, энергетические компании, предприятия транспорта и другие компоненты частного сектора»[3].

[3] National Strategy to Secure Cyberspace. Wash., September 2002.

Администрация Дж. Буша-мл. обратила внимание на то, что одной из центральных оказалась проблема неэффективности американской правоохранительной системы. Законодательство США не соответствовало масштабу сформировавшихся угроз информационной безопасности. Более того, в стратегии признавалось, что дальнейшее продвижение в направлении рыночной либерализации сферы развития ИТ без адекватных средств защиты национального киберпространства, повышения технического уровня правоохранительной и судебной системы не только нерационально, но даже опасно. Для обеспечения информационной безопасности – защиты критических элементов инфраструктуры от кибертеррористов, противодействия компьютерному мошенничеству, создания системы безопасности конфиденциальной информации, интеллектуальной собственности на элементы ИТ и авторских прав – потребовалось существенное развитие всей правоохранительной системы.

В стратегии подробно рассматривались угрозы нанесения возможного ущерба, приводились рекомендации по его избежанию. Исходя из того, что только пользователь знает слабые места используемого им участка киберпространства, в обеспечении информационной безопасности частных лиц, компаний, а также ресурсов национальной инфраструктуры правительство, согласно стратегии, ориентировалось на совместные усилия правительства, бизнеса и частных пользователей.

В качестве таких пользователей можно рассматривать: домашних пользователей и мелких предпринимателей, крупные компании, правительственные и неправительственные структуры, вузы, структуры национального и глобального уровня.

Значительное внимание в стратегии уделялось не только методам противодействия угрозам информационных атак, но и вопросам использования правительством информационных ресурсов против угроз национальной безопасности в целом. В частности, детально рассматриваются полномочия директора национальной разведки, Федерального бюро расследований, Административно-бюджетного управления и Бюро по научно-технической политике при президенте США, Государственного департамента и других правительственных агентств и ведомств.

Республиканская администрация Дж. Буша-мл. инициировала существенную реформу системы обеспечения защиты инфраструктуры. В декабре 2003 г., президент выпустил директиву Департамента внутренней безопасности, посвящённую приоритетам в области защиты критически важных элементов инфраструктуры (*Homeland Security Presidential Directive*-7). Она заменяла директиву СНБ-63.

В отличие от предыдущего документа, в новой директиве признавалось, что в силу специфики угрозы информационных атак, её полное уничтожение невозможно. Таким образом, сохраняя лидерство американского государства в области противодействия информационным атакам, особое внимание в директиве уделялось деятельности правительства в области максимального уменьшения последствий потенциальных атак.

В отличие от директивы администрации Клинтона, в новой редакции не было сказано ни слова про обеспечение конфиденциальности (*privacy*) личности. Если документ 1998 г. давал значительную свободу коммерческим компаниям и отдельным государственным учреждениям в области противодействия информационным атакам, новый возлагал большую долю ответственности на государственное руководство.

Должность координатора, который занимался вопросами взаимодействия различных государственных учреждений в области информационной безопасности, сохранялась. Однако ответственность за обеспечение защиты критически важных элементов инфраструктуры возлагалась на созданное Министерство внутренней безопасности. Созданный У. Клинтоном Центр по защите национальной инфраструктуры трансформировался в один из его отделов.

Ответственность Министерства внутренней безопасности включала следующие направления:

– развитие всеобъемлющего национального плана по защите критически важных элементов национальной инфраструктуры, включающего вопросы информационной безопасности;

– обеспечение сотрудничества и координации усилий в сфере информационной безопасности между органами государственной власти на федеральном, местном и уровне штатов и частным сектором;

– улучшение и укрепление процесса обмена информацией о кибератаках, угрозах и уязвимостях в сфере информационной безопасности между органами государственной власти и частными предприятиями;

– разработку и укрепление государственного потенциала в области анализа и предупреждения информационных угроз;

– разработку механизмов противодействия и устранения последствий информационных атак;

– идентификацию и оценку информационных атак и уязвимостей;

– поддержку НИОКР в области укрепления безопасности информационного пространства;

– развитие системы предупреждения об информационных угрозах;

– обучение и подготовку экспертов;

– укрепление информационной безопасности в органах государственного управления на федеральном, местном и уровне штатов;

– укрепление международной информационной космической безопасности;

– интеграцию механизмов противодействия информационным угрозам в обеспечение национальной безопасности[4].

Администрация Дж. Буша-мл. значительно усовершенствовала систему обеспечения информационной безопасности государственных учреждений. Проблема защиты критически важных элементов инфраструктуры требовала больших усилий, президент подписал документ под названием «Стратегия физической защиты критически важных элементов инфраструктуры», в котором

[4] Homeland Security Presidential Directive-7. Critical Infrastructure Identification, Prioritization, and Protection. White House. Wash., 17.12.2003.

признавалось, что действий правительства недостаточно, потому что инфраструктура состоит как из государственных, так и из частных институтов в различных секторах экономики. В стратегии были выделены 13 элементов инфраструктуры, критически важных для национальной безопасности. В документе утверждалось, что для стабильного функционирования инфраструктуры необходимо, прежде всего, унифицировать и стандартизировать действующие требования к обеспечению безопасности внутри всех государственных учреждений. Кроме того, отдельно отмечалась, особая роль информационного пространства, которое является «нервной системой» Соединённых Штатов.

Доверить полностью безопасность федеральных информационных ресурсов коммерческим компаниям правительство не могло, это противоречило интересам национальной безопасности, а политика активной государственной поддержки ИТ создала условия, при которых бизнес имел значительное информационное превосходство над государством. Обеспечение безопасности федеральных информационных ресурсов было нескоординированным и характеризовалось значительной разобщённостью требований к этим проблемам. Многочисленные исследования показывали, что деятельность государственного руководства США в области информационной безопасности неэффективна[5].

Перспективы политики по информационной безопасности

После победы Б. Обамы на выборах, но до его официального вступления в должность, американский Центр по изучению международных стратегических исследований (*Centre for Strategic International Studies*), представил доклад, посвящённый вопросам информационной безопасности. Авторы этого доклада под названием «Защита киберпространства при администрации 44-го президента США» (*Securing Cyberspace for the 44th presidency*) приходят к неутешительным выводам о том, что в этой области Бараку Обаме будет необходимо принять ряд неотложных мер для того, чтобы не допустить обострения угрозы национальной безопасности США.

В частности, авторы доклада говорят о «необходимости укрепления государственной политики в области обеспечения информационной безопасности, например посредством создания Национального управления по кибербезопасности (*National Office for Cybersecurity*), об увеличении расходов на кибербезопасность из федерального бюджета США, о реформировании принятого законодательства об информационной безопасности федеральных ведомств, о необходимости отказаться от «добровольного обеспечения информационной безопасности» и ввести обязательное привлечение государственных, коммерческих, международных ресурсов и ресурсов гражданского общества для этих целей. Авторы также отмечают важность участия гражданского общества в этом процессе для того, чтобы не допустить превышения полномочий прави-

[5] См.: GAO Report № 08-64T Critical Infrastructure Protection Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies Statement of David A. Powner Director, Information Technology Management Issues. 31.10.2007.

тельства в области нарушения конфиденциальности. Участие же бизнеса необходимо, чтобы сократить разрыв между предложением коммерческих продуктов в области информационной безопасности и необходимыми требованиями, определяемыми правительством[6].

Б. Обама отреагировал на эти рекомендации и одним из первых своих указов приказал провести полную ревизию системы информационной безопасности. Президент обязал[7] в 60-дневный срок (к середине апреля) подготовить специальный доклад с изложением программ, планов и деятельности федерального правительства в области обеспечения информационной безопасности. Руководить подготовкой доклада, было поручено Мелиссе Хэтэвэй, которая занимала должность координатора отдела по кибербезопасности в Управлении национальной разведки США.

Множество фактов свидетельствует о том, что подход к стратегии в администрации Б. Обамы будет значительно отличаться от позиции администрации Дж. Буша-мл.: в первую очередь это касается позиции президента США по борьбе с терроризмом: в своей риторике Б. Обама старается избегать формулировок Дж. Буша. Необходимость решения финансово-экономических проблем отодвинули актуальность войны против терроризма на второй план. Очевидно, что президент Б. Обама стремится разделить разрешение военных конфликтов в Ираке и в Афганистане, не объединяя их под общей идеей войны против терроризма. Примечательно, что угрозы информационной безопасности в период правления Дж. Буша-мл. в основном относились к проблемам внутренней безопасности.

Многие действия нынешней администрации свидетельствуют о том, что теперь информационные угрозы отнесены к уровню национальной безопасности. В частности, в конце февраля президент Б. Обама отправил в Конгресс проект бюджета на 2010 г.[8] Впервые там появляются некоторые контуры расходов на разведывательную деятельность. В проекте бюджета, в статье расходов на специальные службы, президент увеличивает расходы на кибербезопасность. Причём, в отличие от документов администрации Дж. Буша-мл., в 2010 г. нет ни одного упоминания о расходах на противодействие кибертерроризму.

Кроме того, о растущих информационных угрозах национальной безопасности США говорили и высокопоставленные представители американского разведывательного сообщества. В ежегодной оценке угроз национальной безопасности в Комитете по разведке Палаты представителей США директор Управления по внешней разведке Дэннис Блэр отметил актуальность информационных угроз. Среди основных проблем в этой области он указал на уязвимость информационных элементов американской национальной инфра-

[6] Securing Cyberspace for the 44th Presidency (http://www.csis.org/media/csis/pubs/081208_securingcyberspace_44.pdf).

[7] President Obama Directs the National Security and Homeland Security Advisors to Conduct Immediate Cyber Security Review (http://www.whitehouse.gov/the_press_office/AdvisorsToConductImmediateCyberSecurityReview/).

[8] A New Era of Responsibility Renewing America's Promise, p. 58 (http://www.whitehouse.gov/omb/assets/fy2010_new_era/A_New_Era_of_Responsibility2.pdf).

структуры от кибератак. Директор Управления отметил, что эта угроза исходит не только от государств, но и от отдельных индивидов. В контексте информационных угроз он уделил особое внимание проблеме международной организованной преступности[9].

Принципиальным отличием президента Б. Обамы от позиции администрации Дж. Буша-мл. является то, что вопросы информационной безопасности относятся не к внутренней безопасности, а к национальной. Соответственно, ответственность за противодействие этим угрозам возложена не только на Федеральное бюро расследований или Министерство внутренней безопасности, но и на ЦРУ, Управление национальной разведки и Совет национальной безопасности.

По-видимому, изменится и позиция США по вопросам международной информационной безопасности. Внешнеполитическая стратегия администрации Дж. Буша-мл. в сфере информационной безопасности заключалась в том, чтобы избежать и не допустить принятия норм международного права, запрещающих военное использование информационных технологий. Более того, многие действия политики Буша свидетельствовали о том, что США стремятся к достижению абсолютного доминирования в информационной сфере.

В марте президент Б. Обама учредил пост федерального директора по информационным технологиям в Белом доме и назначил на эту должность директора по ИТ округа Колумбия В. Кундру. Вступив в должность, В. Кундра развернул активную деятельность, направленную, прежде всего, на максимальную открытость действий правительства, а также на ужесточение требований в сфере информационной безопасности государственных ведомств Соединённых Штатов.

Должность директора по информационным технологиям существует практически в каждой организации – государственной и коммерческой. Его полномочия заключаются в том, чтобы максимально эффективно распределять и использовать информационные ресурсы (в основном технические). Применительно к деятельности правительства, в распоряжении директора по информационным технологиям в каждом отдельном ведомстве находятся информационные ресурсы, которые должны быть использованы максимально эффективно, чтобы ведомство выполняло свои задачи. Создание подобной должности на общефедеральном уровне, возможно, лишит части полномочий директоров по ИТ в системе государственной власти США. Полномочия в сфере обеспечения информационной безопасности среди обязанностей директоров по ИТ прописаны не чётко.

По словам Кундры, он стремится обеспечить доступ граждан к государственной информации, значительно увеличив количество рассекречиваемых данных. Особое внимание Кундра посвящает инновациям, а также скорости обмена информации и технологическим нововведениям, используемым американским государством для исполнения своих функций.

---

[9] Annual Threat Assessment of the Intelligence Community for the House Permanent Select Committee on Intelligence, Dennis C. Blair Director of National Intelligence, 25.02.2009 (http://www.dni.gov/testimonies/20090225_testimony.pdf).

Одним из первых шагов в этом направлении стала разработка сайта data.gov, предназначенного не только для предоставления информации гражданам США, но и для обмена мнением и вовлечения населения в государственную деятельность.

Другим направлением работы нового директора стала реформа системы закупок информационных технологий. Кундра не раз заявлял о том, что существующая система закупок несовершенна, требует значительных финансовых ресурсов и неэффективна в деятельности правительства. Среди прочего, Кундра даже планирует обеспечить федеральные ведомства собственными провайдерами Интернет-связи.

Кундра стремится изменить сложившуюся ситуацию, в которой информационные ресурсы коммерческих предприятий намного превосходят государственные. По его мнению, государство должно взять больше полномочий в сфере регулирования информационной сферы, распределения информационных ресурсов[10].

Если в обязанности В. Кундры входит обеспечение информационной безопасности федеральных ведомств Соединённых Штатов, то другим направлением политики администрации Обамы в этой сфере является активное вовлечение военных. Примечательно, что демократическая администрация подходит к этому вопросу совершенно с иных позиций, чем администрация Дж. Буша.

В мае 2009 г. официальные представители Пентагона объявили о возможности создания нового военного киберкомандования, которое обеспечит безопасность не только военных, но и гражданских информационных систем. На слушаниях в Комитете по вооружённым силам Палаты представителей, директор Агентства национальной безопасности заявил, что новое командование будет совмещать оборонительные и наступательные информационные средства Министерства обороны и Агентства национальной безопасности[11]. Кроме того, посредством создаваемого органа АНБ планирует поддерживать Министерство внутренней безопасности, в чьи обязанности в настоящее время входит обеспечение информационной безопасности Соединённых Штатов. АНБ не хочет брать на себя настолько обширные полномочия и обязательства, однако вполне в силах помочь МВБ. Для того, чтобы более эффективно противостоять информационным угрозам, военные должны теснее сотрудничать с частным сектором и Министерством внутренней безопасности.

В преддверии публикации доклада по информационной безопасности Соединённых Штатов, был опубликован ряд предложений по совершенствованию системы обеспечения информационной безопасности другими правительственными и неправительственными организациями.

---

[10] K u n d r a : IT Procurement Needs Improving. – «Federal Computer Week», 23.04.2009.

[11] Statement for the Record Lieutenant General Keith Alexander Commander Joint Functional Component Command for Network Warfare before the House Armed Services Committee Terrorism, Unconventional Threats, and Capabilities Subcommittee, 5.05.2009.

В частности, интерес представляет доклад разведывательного альянса по национальной безопасности (*Intelligence and National Security Alliance*). В этом докладе представлены предложения по ключевым вопросам[12].

Основной тезис заключается в определении роли государства в обеспечении информационной безопасности, особенно от угроз бизнесу. Примечательно, что авторы этого доклада считают, что создание должности (отдела), наделённой широкими полномочиями в этой сфере – наиболее оптимальное решение. Подобные попытки уже были предприняты при администрациях Клинтона и Буша. Принципиальным отличием данной инициативы является то, что полномочиями по обеспечению информационной безопасности будет наделён не существующий орган, в обязанности которого входит широкий круг прочих полномочий, а планируется новое ведомство, которое не будет заниматься никакими другими вопросами (необходимо отметить, что полномочия В. Кундры ограничены только правительственными учреждениями).

Одним из важнейших направлений в совершенствовании системы обеспечения информационной безопасности по мнению разведывательного альянса является развитие в этой области сотрудничества между государством и бизнесом.

По-видимому, Соединённые Штаты откажутся от планов, связанных с установлением глобального информационного доминирования, однако курс, обеспечивающий лидерство страны в информационной сфере сохранится. Произойдёт отход от чрезмерного упора на военно-силовое применение информационных технологий в области наступательных методов, направленных на обеспечение национальной безопасности, приоритетное значение могут получить методы экономического и невоенного влияния Соединённых Штатов в информационной сфере.

60-дневный срок на подготовку доклада закончился в конце апреля, однако доклад был опубликован только в середине мая. Официальные представители Белого дома утверждали, что обнародование доклада было отложено в связи с развернувшейся эпидемией «свиного гриппа».

Во многом в документе были приняты к сведению ключевые положения доклада Центра по изучению международных стратегических исследований. Планируется, что основным направлением развития системы информационной безопасности США в ближайшей перспективе станет создание специальной должности в Белом доме. Планировалось, что эту должность займёт Мелисса Хэтэвэй, у которой будет двойное подчинение – советнику по национальной безопасности и Совету экономических помощников.

Однако фактически не успев приступить к исполнению обязанностей, «киберцарица» была вынуждена уйти в отставку. Пресса сообщает, что это связано с тем, что идеи М. Хэтэвэй относительно реформы системы информационной безопасности в частном секторе, направленной на то, чтобы ответствен-

[12] Critical Issues for Cyber Assurance Policy Reform An Industry Assessment. Intelligence and National Security Alliance (http://insaonline.org/assets/files/INSA_CyberAssurance_Assessment.pdf).

ность за информационную безопасность лежала на самих компаниях. Эти идеи противоречили взглядам демократической администрации Барака Обамы.

Очевидно, что администрация президента Б. Обамы совершит новую попытку создания централизованной системы обеспечения информационной безопасности в США. Возможно, будет создан новый государственный орган, в функции которого будет входить координация всех усилий по обеспечению информационной безопасности США.

Создаваемое военной кибер-командование будет, прежде всего, заниматься защитой информационных систем Министерства обороны, органов государственной власти, разведки, а, возможно, и обеспечением безопасности гражданских ИТ.

Важнейшим аспектом в политике администрации Б. Обамы в сфере информационной безопасности будет еще более тесное сотрудничество государства и бизнеса, направленное в первую очередь на защиту государственных информационных ресурсов, а также всего американского киберпространства. Для этого потребуется большее вмешательство американского государства в информационную сферу, в том числе в информационный сектор экономики. Тем не менее, видимо, произойдет отказ от наиболее одиозных методов внутреннего шпионажа.

Вместе с тем значительной коррекции может быть подвергнута внешнеполитическая стратегия Вашингтона в этой сфере. Можно предположить, что американская позиция по управлении Интернетом вопросу будет пересмотрена, и США пойдут на компромисс с передачей Европейскому Союзу часть полномочий в сфере управления Интернетом. Кроме того, есть предпосылки к тому, что Соединённые Штаты не будут столь жёстко, как при Дж. Буше-мл., противодействовать разработке международно-правовых норм, обеспечивающих основу военного и разведывательного использования информационных технологий.