УДК 32 +33 (73)

ГЛОБАЛЬНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ – ФАКТОР МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ

© 2010 г. **Е.А. Роговский***
Институт США и Канады Российской академии наук, Москва

Статья посвящена анализу политики информационной безопасности нынешней администрации США в свете создания уникального потенциала национальной киберобороны от новых угроз международной безопасности. Показано, что расширение информационного разрыва можно рассматривать в качестве одной из причин нестабильности современного мира.

Ключевые слова: *кибербезопасность, сверхмощные информационные системы, сдерживание кибертерроризма, информационная асимметрия, политический фактор.*

В XXI веке процветание американской экономики будет зависеть не только от того, в какой степени ИТ-инновации обеспечат бизнесу информационное превосходство над зарубежными партнёрами и конкурентами, но также и от того, насколько США удастся защитить своё информационное пространство.

Развитие ИТ-технологий сопровождается новыми угрозами. США наращивают потенциал кибербезопасности

Проблемы защиты страны от актуальных угроз привлекли серьёзное внимание администрации президента Дж. Буша-мл. после террористических актов 11 сентября 2001 г.: Америка почувствовала себя уязвимой, и была осознана потребность в повышении уровня национальной безопасности.

Но террористические нападения были совершены не только на башни Торгового центра в Нью-Йорке. Многие компьютеры в США подверглись кибератакам вирусов *NIMDA* и *Code Red*. Возникли другие киберугрозы. В новой «Стратегии национальной безопасности США отмечается, что «информационные технологии обеспечивают военное превосходство Соединённых Штатов, но делают американскую гражданскую экономику чрезвычайно уязвимой» [6], истощают ресурсы её надёжности. ИТ-преступления стали совершаться чаще, они стали более изощрёнными, причиняют бóльший ущерб [2]. В докладе ГКРУ, подготовленном по запросу Конгресса летом 2010 г. [14], приведены следующие определения типов кибератак (см. табл. 1):

* **РОГОВСКИЙ Евгений Александрович – кандидат экономических наук, руководитель Центра проблем военно-промышленной политики ИСКРАН.** E-mail: Rogowsky@mail.ru

Статья подготовлена в рамках проекта РГНФ № 09-03-00771 «Особенности глобализационной стратегии США и их влияние на политику безопасности России в многополярном мире».

Таблица 1

Типы кибератак

	Типы кибератак	Описание
1	Отказ обслуживания	Метод кибератаки, исходящей из одного источника, блокирующий авторизованным пользователям доступ к тому или иному компьютеру-жертве путём его «переполнения» внешними сообщениями. Этот метод может блокировать легальный трафик (т.е. обмен данных компьютера-жертвы с другими компьютерами).
2	Распределённый отказ обслуживания	Вариант кибератаки типа «отказ обслуживания», построенный на скоординированной атаке сразу со многих компьютеров. Для организации такой атаки участвующие в ней компьютеры часто предварительно заражаются специальными программами-«червями».
3	Инструменты взлома («отмычки»)	Публично доступные средства проникновения в системы различного уровня сложности с целью поиска в той или иной киберсистеме уязвимых мест и получения доступа к компьютеру-жертве.
4	Логические бомбы	Форма саботажа, когда программист вводит специально сконструированный код, вызывающий деструктивную работу выполняемой программы, в том числе её полное прекращение.
5	Фишинг	Создание и использование специальных электронных сообщений и web-сайтов, подобных хорошо известным пользователям легальным сайтам с целью дезориентации (обмана) пользователей, провоцирующие их раскрыть свои персональные данные, такие как пароли или информацию о финансовых счетах. «Фишеры» продают эту конфиденциальную информацию или используют её в криминальных мошеннических целях.
6	Сниффер	Программа, перехватывающая и фильтрующая информационный трафик (пакеты), выискивая в нём специальную информацию о пользователе, например, передаваемые пароли.
7	Трояны	Компьютерная программа, содержащая неявные вредоносные коды. Трояны обычно маскируются под обычные полезные программы, которые пользователь может использовать.
8	Вирусы	Программа, инфицирующая компьютерные файлы (обычно исполняемые программы) путём включения в них специальных команд. Эти команды, как правило, исполняются при загрузке инфицированного файла в оперативную память компьютера, что позволяет вирусу заражать и другие файлы. В отличие от компьютерных «червей», размножение вирусов требует вмешательства, хотя зачастую и неосознанного, человека (пользователя).
9	Вишинг	Метод фишинга, использующий дешевые Интернет-технологии передачи звуковых (в том числе голосовых) файлов и программное обеспечение так называемых «открытых кол-центров». Дешевизна позволяет мошенникам создавать собственные телефонные «кол-центры» и оттуда (от имени настоящих банков) посылать потенциальным жертвам голосовые или электронные сообщения «с просьбой, в связи с возникновением проблем в системе безопасности банка, для реактивации их кредитной (или дебитовой) карточки, позвонить по определенному телефону» или послать SMS и таким образом раскрыть мошенникам конфиденциальную информацию.

Продолжение табл. 1

	Типы кибератак	Описание
10	«Военное катание»	Метод получения несанкционированного доступа к компьютерным сетям, использующим «лэптопы» (ноутбуки) и применяющим для выхода в Интернет антенны и беспроводные сетевые адапторы, содержащие контролируемые локаторы.
11	«Черви»	Независимые компьютерные программы, распространяющиеся с помощью копирования по Интернету самих себя из одного компьютера в другой. В отличие от компьютерных вирусов, черви не требуют для своего размножения вмешательства человека.
12	Атака нулевого дня	Способ опережения киберзащиты. Угроза реализуется в тот же самый день, когда общественности становится известно о наличии в системе безопасности уязвимых мест, не имеющих адекватной киберзащиты.

Некоторые авторы выделяют также киберугрозы, имеющие целью захват контроля над компьютером, управляющим какой-либо реальной инфраструктурной или иной функциональной системой.

Данные ФБР об ущербе, нанесённом кибератаками, опубликованные на официальном сайте центра по противодействию компьютерной преступности ФБР (IC3, см. ниже), показывают, что рост компьютерной преступности продолжается стремительными темпами; особенно поражает резкий (почти в 2 раза!) скачок финансовых потерь от компьютерных преступлений, зарегистрированный в 2009 г. по отношению к 2008 г. Аналитики отмечают также, что последние годы около трети всего ущерба от компьютерных правонарушений приходится на финансовые кибермошенничества, осуществляемые с помощью кибератак различного типа.

Выступая в начале 2010 г. в музее журналистики в Вашингтоне госсекретарь США Х. Клинтон заявила: «Правительство и граждане США должны быть уверены в том, что сети, составляющие основу национальной безопасности и экономического процветания, являются безопасными и устойчивыми. Если мы не сможем полагаться на безопасность информационных сетей, на карту будет поставлена возможность пользоваться услугами банков в онлайновом режиме, вести электронную торговлю и обеспечивать защиту интеллектуальной собственности, которая стоит миллиарды долларов» [12]. Перед американским государством возникли задачи укрепления кибербезопасности страны, обеспечения уверенности в надёжной работе информационно-коммуникационных систем, восстановления их после возможных аварий, а также после случайных или несанкционированных вторжений.

В рамках борьбы с терроризмом США значительно увеличили использование мощных специальных информационных технологий, применение которых обеспечивает информационное доминирование США в мире. Имея в виду такую цель ещё президент У. Клинтон для стимулирования участия частного бизнеса в развитии информационных технологий рассекретил Интернет, вынес на аукционы ряд диапазонов радиочастот, а также создал условия для широкого коммерческого использования каналов космической связи в гражданских целях. Со своей стороны, президент Дж. Буш-мл. рассекретил «Новую космическую политику» США (подготовленную на основе доклада комиссии

Д. Рамсфелда) [7], а также ряд информационно-космических проектов. Теперь наступила очередь президента Б. Обамы, и он принял решение снять гриф секретности с принятой Дж. Бушем «Инициативы всесторонней национальной кибербезопасности» – ИВНКБ (*The Comprehensive National Cybersecurity Initiative – CNCI*).

Согласно опубликованным в декабре 2009 г. материалам ИВНКБ, США намерены управлять федеральной сетью ведомств как целостной системой и разместить в ней подсистему оповещения о проникновении хакеров. Кроме того, предполагается оптимизировать исследовательские и конструкторские работы, связанные с информационными технологиями, а также наладить взаимодействие центров быстрого реагирования на киберпреступления. Среди инициатив также есть распоряжения по разработке киберконтрразведки и повышению безопасности секретных сетей.

Анализируя ИВНКБ, важно не упускать из вида, что поставленных целей нельзя достичь без укрепления ряда ключевых функций правительства, таких как расследование криминальных преступлений, сбор, обработка и анализ разведывательной информации, а также общенациональные усилия в области обеспечения кибербезопасности. Инициативы ИВНКБ разрабатывались очень тщательно, с большим вниманием к проблемам конфиденциальности и гражданских свобод и с учётом консультаций с профильными экспертами правительства. Защита гражданских свобод и прав на конфиденциальность остаётся фундаментальной целью и при реализации ИВНКБ. По мнению администрации, инициативы ИВНКБ должны развиваться и стать ключевыми элементами более широкой обновлённой стратегии кибербезопасности США; они и дальше будут играть ключевую роль в определении основных положений политики президента Обамы.

Документ ИВНКБ [24] состоит из ряда взаимосвязанных инициатив:

– ***установить передовую линию обороны от непосредственных угроз*** путём расширения осведомлённости пользователей о реальной ситуации в сети в отношении её уязвимости, имеющихся угроз и возможностей федерального правительства – а также правительств штатов, местных властей и партнёров из частного сектора, – быстро сокращать уязвимые места и предотвращать проникновения;

– ***защититься от всего спектра угроз*** с помощью усиления контрразведки США и укрепления безопасности сети операторов по всем ключевым информационным технологиям;

– ***укрепить безопасность киберпространства*** путём расширения кибероборазования, координации и переориентации усилий федерального правительства в области НИОКР;

– ***разработать стратегию сдерживания враждебной*** (недружественной) ***деятельности в киберпространстве.***

Для достижения более высокого уровня общественного восприятия и поддержки федеральных усилий помощнику президента (координатору) по кибербезопасности Г. Шмидту было поручено раскрыть следующие общие характеристики 12 инициатив ИВНКБ:

1. Инициатива **«Надёжные соединения с Интернетом»**. **Управлять сетью федеральных предприятий как единой сетью предприятий, связанных надёжной Интернет-связью.** Эта инициатива, возглавляемая Административно-бюджетным управлением при президенте США, а также Министерством внутренней безопасности (МВБ), состоит в консолидации «точек» внешнего доступа (в том числе в/из Интернета) к сети федеральных предприятий и организаций. Консолидация обеспечивает общность решений в сфере безопасности, способствует сокращению точек доступа, создаёт в федеральных учреждениях базисный потенциал безопасности и обосновывает целесообразность его применения. Агентства, располагающие собственными возможностями, участвуют в этой инициативе через своих провайдеров; прочие могут заключать договоры с коммерческими провайдерами.

2. Инициатива **«Внедрение на федеральных предприятиях сенсорных систем выявления вторжений».** Системы выявления вторжений, основанные на пассивных сенсорах, составляют жизненно важную часть защиты правительственных сетей США – они идентифицируют тот момент времени, когда к этим сетям пытается получить доступ неавторизованный пользователь. Министерство внутренней безопасности в рамках проекта «Эйнштейн-2» внедряет сигнатурные сенсоры, способные контролировать входящий в федеральные системы Интернет трафик на предмет выявления попыток несанкционированного доступа и злонамеренного контента. Возможности «Эйнштейн-2» позволяют в ходе рутинных автоматических инспекций трафика анализировать эти информационные потоки сетей американского правительства с помощью особой сигнатурной технологии с целью выявления вторжений и потенциально опасной деятельности. При этом инвестиции в технологию должны осуществляться параллельно вложениям в человеческие ресурсы. Система «Эйнштейн-2» способна в реальном масштабе времени оповещать о наличии в трафике федеральных сетей злонамеренной или потенциально вредной деятельности, а также предоставлять визуализацию соответствующих производных данных. Благодаря этому аналитики отдела кибербезопасности МВБ[*] смогут существенно лучше понимать складывающуюся в сети обстановку, а также воспользоваться более широкой палитрой возможностей для преодоления обнаруженных слабых и уязвимых мест в системе безопасности федеральных сетей. В результате это подразделение приобретает бóльшую осведомлённость о ситуации и может более эффективно получать релевантную информацию о безопасности и делиться ею со всеми защитниками правительственных сетей США, с профессионалами в частном секторе и во всем американском обществе. В настоящее время Бюро по конфиденциальности (*Privacy Office DHS*) проводит оценку влияния программы «Эйнштейн-2» на конфиденциальность пользователей.

3. Инициатива «**Внедрение в государственных организациях систем предотвращения кибератак**». Этот проект совершенствования как коммерческих,

[*] Оперативное подразделение отдела национальной кибербезопасности (*National Cyber Security Division – NCSD*) Министерства внутренней безопасности США было создано для реализации задач, поставленных в «Национальной стратегии безопасности киберпространства» (*National Strategy to Secure Cyberspace*), принятой администрацией Дж. У. Буша в 2003 году.

так и специализированных правительственных информационных технологий, получивший название «Эйнштейн-3», имеет целью проведение в реальном масштабе времени полной инспекции всего пакета информации (включая сетевой трафик, входящий или исходящий из сети) того или иного ведомства, а также принятие решений, адекватных выявленным угрозам. Фактически целью проекта «Эйнштейн-3» является усиление ключевых функций защиты ведомственных информационных систем, а именно – идентификации и анализа злонамеренного сетевого трафика, повышение уровня осведомлённости о складывающейся ситуации и автоматического реагирования на киберугрозы до возникновения значимого ущерба. Поэтому данный проект можно считать системой динамической обороны, предотвращающей вторжения и снижающей уязвимость ведомственного киберпространства. Проект призван поддерживать усовершенствованный информационный обмен со всеми федеральными ведомствами, давая возможность автоматического оповещения об обнаруженных попытках вторжениях в сети и, когда это необходимо, посылать не раскрывающие контента уведомления в Агентство национальной безопасности (АНБ), что способствует выполнению санкционированных законом функций последнего. В соответствии с этой инициативой в национальный разведывательный потенциал будут вложены существенные долгосрочные инвестиции, которые увеличат возможности получения критически важной информации о внешних (из-за рубежа) киберугрозах и её оперативного использования во внутренних системах. Система позволит МВБ адаптировать для функций обеспечения кибербезопасности федеральных систем классификационные сигнатуры угроз, используемые внешней разведкой АНБ и Министерством обороны. Обмен информацией о кибератаках будет осуществляться в соответствии с законом и для предотвращения возможных нарушений конфиденциальности и прав граждан США будет охватывать только деятельность, связанную с обеспечением внутренней безопасности, разведкой и обороной.

В настоящее время МВБ проводит апробацию описанных в этой инициативе возможностей «Эйнштейн-3», опирающихся на разработанные в АНБ технологии «сжатия» процессов контроля и защиты информации, извлекаемой в ходе кибератак, направленных против гражданских ведомств. При этом ответственные за соблюдение конфиденциальности и гражданских свобод правительственные чиновники в ходе проектирования и оперативного внедрения проекта «Эйнштейн-3» будут работать в тесном контакте с АНБ и МВБ.

4. Инициатива «**Координация и переориентация исследований и разработок в области технологий кибербезопасности**». Как оказалось, в настоящее время ни одна из федеральных организаций не осведомлена о всех финансируемых правительством НИОКР, связанных с киберпространством. Эта инициатива состоит в разработке стратегии и структуры координации всех таких НИОКР (как секретных, так и открытых), спонсируемых правительством США (или непосредственно им осуществляемых), а также в их переориентации там, где это необходимо. Эта инициатива критически важна для исключения избыточного федерального финансирования исследований и разработок по тематике кибербезопасности, для определения разрыва в исследованиях и соответствующих приоритетов, а также для убеждения налогоплательщиков в

эффективном использовании их денег при формировании инвестиционной стратегии в этой области.

5. Инициатива «**Укрепление взаимодействия существующих операционных киберцентров с целью повышения уровня ситуационной осведомлённости**». Для гарантии обмена данными о злонамеренной деятельности против федеральных систем между правительственными подразделениями информационной безопасности и стратегическими операционными центрами необходимы дополнительные усилия. То же самое справедливо и в отношении защиты от пиратства, данных персональной идентификации, а также иной защищаемой информации. Поэтому, как это установлено законом, для обеспечения максимально возможной защиты национального киберпространства необходимо обеспечить лучшее понимание угроз правительственным системам и максимально использовать преимущества каждого отдельного подразделения. Эта инициатива должна предоставить ключевые средства, обеспечивающие обмен данными о складывающейся ситуации (ситуационную осведомлённость), и сотрудничество между шестью центрами, ответственными за поддержание уровня кибератвности США. В рамках этой инициативы усилия фокусируются на ключевых технологиях практического взаимодействия различных элементов кибератвности США, в том числе организационных решениях, инвестициях в обновление инфраструктуры, расширение частотного диапазона, инструменты и процедуры информационного обмена, повышающие уровень информационной осведомлённости с помощью обмена аналитическими технологиями, а также на так называемые «технологии сотрудничества».

В рамках этой инициативы ключевую роль в обеспечении безопасности правительственных сетей и систем будет играть Национальный центр кибербезопасности (*National Cybersecurity Center – NCSC*), координирующий и интегрирующий информацию шести национальных центров с целью обеспечения перекрёстной ситуационной осведомлённости, анализа, подготовки сводных докладов о состоянии информационных сетей и систем США, а также усиления их интеграции, взаимодействия и координации.

6. Инициатива «**Разработка и внедрение общеправительственного плана кибернетической контрразведки – ККР**» Такой план необходим для координации соответствующего вида работ во всех федеральных агентствах с целью выявления, сдерживания и противодействия спонсируемым из-за рубежа киберугрозам, направленным против государственных и частных информационных систем США. Для достижения этих целей план ККР учреждает и расширяет контрразведывательное образование, программы повышения уровня осведомлённости о внешних киберугрозах, а также разработки, направленные на интеграцию ККР во все кибероперации, повышение ответственности сотрудников в отношении киберугроз и усиление ККР-сотрудничества в правительстве. Кибернетический ККР-план сопрягается с «Национальной контрразведывательной стратегией США» (2007) и поддерживает программные элементы Инициативы всесторонней национальной кибербезопасности.

7. Инициатива «**Повышение безопасности закрытых (секретных) сетей**». Секретные сети содержат наиболее чувствительную информацию федерального правительства. Именно эти сети составляют информационную инфраструк-

туру, обеспечивающую проведение важнейших боевых, дипломатических, контртеррористических, правоохранительных и разведывательных операций, а также операций по обеспечению внутренней безопасности. Удачное проникновение или разрушение этих сетей может иметь исключительно тяжелые последствия для национальной безопасности. Обеспечение безопасности и целостности этих сетей, а также содержащихся в них данных требует постоянных тщательных усилий.

8. Инициатива «**Расширение образования в сфере кибербезопасности**». Обеспечение безопасности правительства США в киберпространстве зависит не только от миллиардов долларов, которые расходуются на новые технологии, но также и от людей, обладающих необходимыми знаниями, навыками, опытом и способностями внедрения и использования этих технологий. И в федеральном правительстве, и в частном секторе для реализации инициатив ИВНКБ имеющихся в настоящее время экспертов по кибербезопасности недостаточно. Более того, в сфере обеспечения кибербезопасности федеральных структур отсутствует адекватное поле для карьерного роста. Существующие программы подготовки персонала ограничены по своим целям и страдают из-за отсутствия унификации. Для *обеспечения технического преимущества США в сфере* кибербезопасности в перспективе необходимо систематически готовить технологически грамотных специалистов. Решение этой задачи потребует новой национальной стратегии, подобной той, что в 1950-х годах была использована для обновления научного и математического образования.

9. Инициатива «**Разработка перспективных прорывных технологий, стратегий и программ**». Одной из целей ИВНКБ является разработка технологий, обеспечивающих кибербезопасность, уровень которой на порядки превышает показатели существующих систем, при этом такие технологии должны быть внедрены уже в течение ближайших 5–10 лет. Эта инициатива потребует разработки стратегий и программ, направленных на активизацию финансируемых правительством НИОКР, ориентированных на высокорисковые/высокоэффективные решения критически важных проблем кибербезопасности. Федеральное правительство подготовило новый документ, адресованный исследовательскому сообществу под названием «Большие вызовы» (*Grand Challenges*), содержащий призыв содействовать в решении таких проблем, требующих нетрадиционного мышления. В работе с частным сектором правительство определяет общественные нужды, которые должны стимулировать и направлять взаимные инвестиции в ключевых сферах исследований.

10. Инициатива «**Разработка перспективных стратегий и программ сдерживания информационных угроз**». Высшие политики страны оперируют долгосрочными стратегическими понятиями, которые в современном мире зависят от надёжного использования киберпространства. До настоящего времени американское правительство использовало традиционные подходы к проблемам защиты этого пространства, а принимаемые им меры не обеспечивали необходимого уровня кибербезопасности. Эта инициатива направлена на формирование нового подхода к построению стратегии киберзащиты, который нацелен на сдерживание кибератак путём радикального совершенствования потенциала их предупреждения, чёткого определения ролей частного сектора, междуна-

родных партнёров, а также разработки адекватных реагирующих действий как для государственных, так и для негосударственных игроков.

11. Инициатива «**Разработка многофакторного подхода к управлению киберрисками в глобальных экономических системах**». Глобализация рынка коммерческих информационных и коммуникационных технологий создаёт огромные возможности для тех, кто намерен нанести ущерб США путём проникновения в глобальные экономические системы с целью получения несанкционированного доступа к данным, их модификации или прерывания коммуникаций. Риски, возникающие в этой связи как в национальных, так и в глобальных экономических системах, должны всесторонне оцениваться со стратегической точки зрения и учитывать весь жизненный цикл продукта, системы или услуги. Управление такими рисками потребует бóльшей осведомлённости об угрозах, уязвимых местах и последствиях, связанных с приобретением такой продукции (системы или услуги); внедрения и эксплуатации инструментов и ресурсов с тем, чтобы технически и операционно учитывать связанные с этим продуктом риски в течение всего его жизненного цикла (от задумки до утилизации); разработки новой политики и практики государственных закупок, которая отражала бы сложности глобального рынка; партнёрства с частной промышленностью с целью разработки и внедрения передового экономического опыта и стандартов управления рисками. Эта инициатива должна расширить палитру используемых федеральным правительством инструментов и процедур и предоставить ведомствам, испытывающим инструментальный дефицит, возможности лучшего менеджмента и адекватного учёта экономических рисков на уровне, соответствующем критической значимости их систем и сетей.

12. Инициатива «**Определить роль федерального правительства в укреплении кибербезопасности критически важных инфраструктурных систем**». Правительство США в исполнении своих общественных функций зависит от множества критически важных объектов инфраструктуры, находящихся в частной собственности и управляемых частными операторами. В свою очередь, работа этих объектов опирается на эффективное функционирование информационных систем и сетей, которые чувствительны к злонамеренным киберугрозам. Эта инициатива строится на существующем партнерстве между федеральным правительством и операторами общественных организаций и частного сектора, управляющими объектами критически важной инфраструктуры (КВИ) и ключевыми ресурсами. МВБ и его партнёры из частного сектора разработали жёсткий поэтапный план совместных действий. Он включает краткосрочные и долгосрочные рекомендации, учитывающие как предшествующие достижения и неудачи, так и текущую деятельность. План содержит меры обеспечения кибербезопасности, имеющие целью увеличение гибкости и операционного потенциала всего инфраструктурного сектора; он сфокусирован на общественно-частном обмене информацией о киберугрозах и инцидентах, имеющих место как в правительственном секторе, так и в секторе критически важной инфраструктуры.

Причём, к сектору отраслей критически важной инфраструктуры (КВИ-сектору), наряду с отраслями водо- и энергоснабжения, отнесён Интернет.

Таблица 2

Центры обеспечения кибербезопасности

Центры (Cyber Ops Centers)		Задача (пример)	Принадлежность
Объединенная группа «Глобальные сетевые операции»	Joint Task Force-Global Network Operations (JTF-GNO)	Руководство стратегическими, оперативными и тактическими действиями Глобальной информационной решётки (ГИР) и её защита при поддержке всего спектра боевых, разведывательных и бизнес- операций МО.	Стратегическое командование США (СТРАТКОМ)
Военный центр киберпреступности	Defense Cyber Crimes Center (DC3)	Разработка стандартов цифровой обработки и анализа данных об инцидентах для всех расследований МО, требующих судебной поддержки.	Министерство обороны, Министерство ВВС
Национальная группа Центр операций по контролю угроз	National Task Force Threat Operations Center	Ситуационный контроль чрезвычайных ситуаций в области компьютерной безопасности	Агентство национальной безопасности
Компьютерный центр чрезвычайного реагирования	U.S. Computer Emergency Response Center» U.S. Computer Emergency Readiness Team (US-CERT)	Оперативная поддержка и защита от кибератак гражданских федеральных органов исполнительной власти (.gov), их информационный обмен с местными властями, бизнесом и зарубежными партнерами.	Министерство внутренней безопасности
Центр разведывательного сообщества по реагированию на инциденты	Intelligence Community Incident-Response Center (IC-IRC)	Непрерывный (24/7) обмен данными о киберсобытиях между членами разведывательного сообщества с цель защиты их способности собирать, анализировать и распространять разведывательную информацию по своим сетям. Этот центр отвечает за координацию с другими организациями, участвующими в реагировании на киберинциденты, предоставляя им прогнозные индикаторы потенциальных угроз.	Разведывательное сообщество США
Объединённая национальная кибернетическая исследовательская группа	National Cyber Investigative Joint Task Force (NCIJTF)	Содействует координации, интеграции и обмену информацией о киберугрозах с разведывательным сообществом и правоохранительными органами.	Федеральное бюро расследований

В середине 2008 г., было объявлено о создании военного киберкомандования в рамках ВВС (*AFCYBER*). Планировалось, что в рамках нового военного командования будут развиваться и поддерживаться возможности вооружённых сил в киберпространстве – «проведение интегрированных военных операций с применением электромагнитных технологий». Было объявлено, что новое

киберкомандование будет обладать возможностями «сдерживания, разрушения, обмана, разубеждения и поражения врагов при помощи различных средств наступления и обороны» [9]. Оно также должно заниматься преимущественно наступательными операциями.

Фактически реформа системы обеспечения информационной безопасности началась сразу же после прихода в Белый дом нового президента США. Помимо Министерства внутренней безопасности, значительно усилилась роль Агентства национальной безопасности, Совета по национальной разведке, ЦРУ и других специальных служб, входящих в разведывательное сообщество США[*]. Одновременно с реформой системы обеспечения информационной безопасности, администрацией Обамы были приняты другие организационные и законодательные меры, направленные на закрепление за Соединёнными Штатами статуса информационной супердержавы.

Так, уже в мае 2009 г. Пентагон объявил о намерении создать новое киберкомандование, призванное обеспечить безопасность не только военных, но и гражданских информационных систем. 23 июня 2009 г. министр обороны США Р. Гейтс опубликовал меморандум, в котором говорилось о создании нового киберкомандования [19], но не в системе ВВС, а в рамках Стратегического командования. Первоочередной задачей нового командования является поддержка военных информационных ресурсов, включая как средства обеспечения безопасности (обороны), так и средства нападения. Именно на это командование будет возложена ответственность за защиту военных компьютерных сетей и проведение наступательных кибероперацій против вражеских сил [20]. Возглавил новое командование генерал-лейтенант армии США К. Александер, покинувший пост главы АНБ. На слушаниях в комитете по вооружённым силам Палаты представителей было заявлено, что новое командование будет совмещать оборонительные и наступательные информационные средства МО и АНБ [10].

В системе кибероборонь США ключевые места занимают показанные в табл. 2 профильные центры, которые одновременно определяют характер взаимодействия федеральных ведомств, бизнеса и общества в целом по вопросам, связанным с кибербезопасностью [28].

Деятельность этих центров в общем виде можно охарактеризовать по пяти направлениям: 1) общий ситуационный мониторинг и анализ чрезвычайных ситуаций в области кибербезопасности, 2) обмен информацией о киберинцидентах и мерах защиты между государственными и частными организациями, 3) анализ военных аспектов национальной безопасности, защита военной информационной инфраструктуры, разработка наступательных операций в киберпространстве, а также определение того, что именно в киберпространстве можно считать актом военного нападения, 4) внешняя разведка, 5) борьба с киберпреступностью и контрразведка.

[*] О составе разведслужб см.: «США ❖ Канада», 2009, № 7. с. 67–84. – *Ред.*

Сверхмощный информационный потенциал может стать причиной политического кризиса

Оснащение государственных ведомств специальными информационными системами, а также их постоянное совершенствование могут привести к тому, что инновационные возможности практического применения этого сверхмощного информационного потенциала (в том числе баз данных) значительно превысят потребности, обоснованные необходимостью решения задач проведения военных операций и борьбы с терроризмом. В результате уникальная (не доступная конкурентам) информация может оказаться использованной «не по назначению». Так, несмотря на введение жестких требований в федеральных ведомствах США, состояние их информационной безопасности уже давно вызывает беспокойство. На проблемы обеспечения сохранности данных, обращающихся в ведомственных сетях, а также надёжности их предоставления авторизованным пользователям неоднократно обращало внимание Главное контрольное управление США [13; 14]. Это даёт основания предполагать, что спонтанная коммерциализация созданного потенциала специального назначения фактически уже происходит.

Как известно, президент Обама провозгласил информационную открытость (транспарентность) одним из ключевых принципов работы своей администрации. По его мнению, «во многих отношениях свобода информации никогда ещё не была столь значима. Появилось больше способов распространения большего количества идей среди большего числа людей, чем когда-либо в истории». «Чем свободнее льётся поток информации, тем сильнее становится общество» [21].

Однако отсутствие чётких критериев и целей дальнейшего развития сверхмощных ведомственных информационных систем, а также четкой оценки результатов их внедрения и использования порождает опасения, что Пентагон, разведывательное сообщество и иные привилегированные пользователи (в том числе бизнес) могут не только получить доступ к данным, весьма чувствительным с внутриполитической точки зрения (например, об информации, так или иначе связанной с конкретными политическими деятелями), но и использовать подобную информацию, так сказать «в собственных интересах».

Что здесь можно сделать? Первый путь – предотвращать возникновение таких ситуаций, второй – выявлять случаи нелегального использования служебной информации и наказывать виновных. (Судя по отношению американского общества к финансовым мошенничествам предпочтительным является второй путь.) Однако, по нашему мнению, в настоящее время ни государство, ни американское общество далеко не всегда успевают предотвращать возникновение (в том числе целенаправленное!) ситуаций информационного преобладания одних участников над другими, и далеко не всегда выявляют и наказывают виновных в нанесённом ущербе[*]. Более того, неясным остаётся вопрос:

[*] Как показывает опыт США, регулировать распространение и использование таких технологий на основе антимонопольных принципов защиты свободной конкуренции чрезвычайно сложно. Они становятся фактором информационного превосходства в конкурентной борьбе, в том числе на международном рынке. В известном смысле можно считать, что в настоящее время глобальное лидерство американского бизнеса во многом опирается именно на его информационное превосходство, иначе говоря, на использование в своих интересах сложившейся информационной асим-

какие именно из намеченных (или достигнутых) функциональных возможностей той или иной информационной системы специального назначения можно считать допустимыми с правовой точки зрения, а какие нет. (И специалисты, и политики стали отмечать, что в США расширяющиеся возможности и угрозы глобального применения новых информационных технологий обгоняют процесс национального законотворчества и уж тем более международного).

И пока не ясно, какая именно чрезмерная информированность привилегированных пользователей может привести к нарушению законов, остаётся некая «правовая неопределённость», в которой систематическое «нецелевое» использование данных может легко трансформироваться в устойчивое политическое преимущество технологических лидеров.

Вероятно, поэтому американцы и опасаются бесконтрольного роста разведывательного сообщества и того, что многочисленные специальные правительственные организации делают работу, результаты которой просто невозможно своевременно осмыслить. Так, например, в специальном аналитическом отчёте «Скрытый мир растёт без контроля», опубликованном летом 2010 г. в газете «Вашингтон пост», отмечается, что в 15 городах США работает 51 федеральная организация (в том числе военные командования) занимающиеся отслеживанием денежных потоков, имеющих то или иное отношение к финансовым операциям террористов [25].

Складывается впечатление, что неконтролируемое государством развитие ИТ-технологий может представлять большую опасность. Напомним в этом контексте высказывание государственного секретаря США Х. Клинтон. В своём выступлении по вопросам развития Интернета отметила, что прогресс в сфере информационных технологий развивается стремительными темпами, но при этом с неменьшими темпами появляются и новые угрозы информационной безопасности. «Достижения научно-технического прогресса необходимо синхронизировать с нашими принципами» – сказала Х. Клинтон [12]. Без такой синхронизации, то есть без принятия регулирующих мер, адекватных быстро расширяющимся возможностям использования новых информационных технологий, их распространение порождает множество новых угроз информационной безопасности; причём таких угроз, которые могут быть направлены на подрыв базисных принципов американского общества.

Здесь уместно сослаться на «Доктрину информационной безопасности России», утверждённую в 2000 г. тогдашним президентом РФ В.В. Путиным. В ней говорится: «Современный этап развития общества характеризуется возрастающей ролью информационной сферы... [которая], являясь системообразующим фактором жизни общества, активно влияет на состояние политической,

---

метрии международного рынка. Оборотной стороной лидерства становится такая угроза международной экономической безопасности, как финансовый кризис. Его основные причины тесно связаны с вовлечением в оборот огромной массы созданных компьютерными роботами, но информационно неполноценных («неадекватных») залоговых документов. (Об этой угрозе правительство США было предупреждено заранее [15], и тем не менее допустило глобальное обострение ситуации.) Подробнее экономические аспекты возникновения в американском обществе сильной информационной асимметрии (т.е. неравенства информационных потенциалов участников капиталистического рынка) рассмотрены в публикации «О постиндустриальных особенностях американского НТП [8].

экономической, оборонной и других составляющих национальной безопасности». Из этого положения ясно, что круг проблем информационной безопасности США шире проблем защиты их собственного киберпространства. Если применить к США определение «информационной безопасности», данное в Доктрине РФ, а именно, понимать под информационной безопасностью страны «состояние защищённости её национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства» [1], то такая расширенная трактовка понятия национальной информационной безопасности как раз и предполагает включение в круг угроз потенциальных возможностей «нецелевого» применения» специальных информационных систем и банков данных, которые способны дестабилизировать основы общества.

Особенно важно не упускать из вида то, что неадекватное применение ИТ-систем может осуществляться анонимно. М. Делл, глава американской компьютерной корпорации «Делл», выступая в начале мая 2010 г. в Далласе (штат Техас) на первом Всемирном саммите по вопросам кибербезопасности, подчеркнул, что «способность огромного количества киберпреступников ("плохих мальчиков") оставаться анонимными и с лёгкостью заметать следы» является главной, первоочередной проблемой и для государства, и для общества в целом. По мнению Делла, система, в которой людям позволено действовать анонимно (иначе говоря, безответственно) не может быть надежной. В конечном счёте сохранение анонимности пользователей системы, критически важной для экономики страны, связано с рисками, представляет серьёзную угрозу и становится вопросом безопасности [22]. Если такие угрозы неприемлемы, а риски чрезмерны, то США должны заранее их предвидеть и предотвращать. М. Делл подчеркнул, что именно усиление борьбы с анонимностью позволит повысить надёжность информационной инфраструктуры, и дал понять, что, обсуждая направления инновационного развития информационной инфраструктуры США, надо выбрать что-то одно – или надёжность системы, или анонимность пользователей.

Как оказалось, для противодействия кибертеррористам многие старые методы не подходят. В самом деле, сегодня, неприемлемыми могут оказаться киберугрозы, исходящие даже от отдельных лиц, которые с помощью компьютеров оказываются в состоянии сеять хаос, «не имея даже тех средств, которые нужны для покупки одного единственного танка» [11]. Иначе говоря, чисто финансовые ограничения слабо влияют на способность кибертерроризма создавать неприемлемые угрозы, а потому **созданная администрацией Дж. Буша мл. система противодействия финансированию террористов против кибертеррористов эффективно работать не может.**

Кроме того, против кибертеррористов практически бессмысленно использовать и старые методы экспортного контроля (запрет поставок потенциальным террористам техники технологий двойного назначения), которые устарели. В самом деле, ещё совсем недавно США ограничивали производительность вывозимых в другие страны компьютеров [7]. Сегодня, когда компьютеры легко объединяются в сети («облачная» Интернет-технология), мощность компьютера, на котором работает тот или иной пользователь, большого значения не имеет.

Сдерживание кибертеррористов требует принципиально иных, инновационных методов. Для того, чтобы понять их суть, следует обратить внимание не на сильные, а на слабые стороны новой «облачной» технологии. Эти слабые стороны тесно сопряжены с проблемами обеспечения информационной безопасности той задачи, которую решает пользователь, – если она несекретная (неконфиденциальная), то привлечение с помощью Интернета для её решения возможностей других компьютеров очень выгодно. Однако, если же решаемая задача так или иначе связана с «закрытой» информацией (в том числе государственными или коммерческими секретами), то решать такую задачу с помощью «интернет-облаков» слишком рискованно, поскольку эта информация может быть перехвачена теми, кто контролирует Интернет-трафик. Эти рассуждения применимы и к широко распространённым поисковым системам: если вы не хотите, чтобы кто-либо знал, что именно вас интересует, – ищите ответы на свои вопросы в книгах (в библиотеках), а не с помощью корпорации «Гугл», которая запоминает не только сам запрос, но и того, кто его сделал.

Концерн «Эппл» когда-то считался образцом защиты конфиденциальных данных. Но сегодня этот концерн хочет знать о своём клиенте практически все. Цепочка начинается при покупке гаджета *iPhone* – регистрируя, пользователь указывает свои фамилию и адрес. Далее, приобретая для гаджета музыкальную заставку, как правило, пользователь указывает номер своей кредитной карточки. «Эппл» может получать информацию: кто, когда и какие приложения загружает на свой *iPad*, какие фильмы и композиции в *iTunes* приобретает, какие книги читает. Кроме того, концерну становится известно точное место, где именно миллионы его клиентов используют свои телефоны-коммуникаторы, что позволяет судить об их передвижениях, а виртуальный архив предоставляемых интернет-услуг допускает хранение электронных писем, данных органайзера пользователя, его адресной книжки, фотоальбома, блокнота и других личных документов. Все это может быть продано компаниям, занимающимся адресной рассылкой рекламы, которые, основываясь на такого рода информации, формируют «портрет личности пользователя», «отражая» его вкусовые предпочтения в покупках, а также учитывая, что смотрит, что слушает, чем занимается пользователь. Причём в этом бизнесе концерн «Эппл» не одинок – и «Фейсбук», и «Гугл» зарабатывают деньги тоже, продавая информацию о своих клиентах. Более того, в начале 2010 г. корпорация «Гугл» открыто заявила о том, что «закрывает доступ к китайской версии поисковой системы (*www.google.cn*) из-за участившихся информационных атак на свои серверы» (как оказалось, эти атаки имели целью получить накопленную информацию о китайских активистах борьбы за права человека).

Все эти возможности могут быть использованы против кибертеррористов. Уязвимость, информационная небезопасность пользователя Интернетом – вот инновационный ключ для сдерживания киберпреступности. Логика сдерживания кибертеррористов может, например, состоять в следующем:

1) с помощью «облачных» технологий, социальных чатов, простоты и дешевизны коммуникаций и банковских расчётов вовлечь в Интернет как можно

больше людей, среди которых абсолютное большинство составляют «хорошие мальчики», не замышляющие никаких правонарушений*;

2) составить «портреты личности» пользователей и заархивировать их;

3) выделить тех, кто отличается нестандартным поведением (не регистрируется, использует что-либо нетипичное или интересуется чем-либо не соответствующим его статусу – это потенциальные «плохие мальчики»);

4) применить в отношении них специальные методы идентификации (разоблачения анонимности), иначе говоря, создать у «плохих мальчиков» впечатление (угрозу) реальности неотвратимого возмездия. По этой логике функцию сдерживания «кибертеррористов» должен выполнять страх раскрытия анонимности (т.е. идентификация злоумышленника, позволяющая применить к нему предусмотренные законом меры наказания). При этом правительство должно обеспечить поддержку такой борьбы с киберпреступниками со стороны элиты и абсолютного большинства «хороших мальчиков», которые не сочтут приведённые процедуры нарушением своих прав и гражданских свобод.

Вероятно, подобную схему и имел в виду упомянутый выше М. Делл, напрямую противопоставивший надёжность информационной инфраструктуры и анонимность киберпреступников.

В условиях нарастающего «цифрового разрыва» и в экономическом, и в политическом проигрыше могут оказаться пользователи (структуры, организации, страны), не располагающие собственными системами сбора и обработки информации, стремящиеся как можно шире использовать дешёвые «облачные технологии», чужие массивы данных, программное обеспечение и каналы связи. Такие технологии фактически лишают «бедных» пользователей так называемого «информационного суверенитета» (надёжной защиты своих каналов связи и банков данных), более того, заставляют их дополнительно платить коммерческим фирмам за сохранность своей чувствительной информации на чужих серверах. Все это очень важно не упускать из вида при анализе состояния современных международных отношений в целом и международной безопасности в частности. При этом следует также учитывать нарастающие различия в законах, регулирующих распространение и использование информационных технологий в различных странах мира.

О проблемах международной информационной безопасности

В этом контексте можно считать, что и вся сфера международной информационной безопасности тоже выходит за рамки киберпространства и распространяется также и на такие угрозы, как целенаправленное создание и использование в национальных интересах той или иной страны мощных систем сбора и обработки данных. По сути, такие системы во многом носят разведывательный характер и им, как в своё время спутникам-шпионам, абсолютное большинство стран мира нечего противопоставить просто не в состоянии. Именно такие системы и создают так называемые «ситуации информационно-

* Вице-президент «Гугл» Винтон Серф считает, что на 2010 г. число компьютеров, подключённых к Интернету, равняется 800 миллионам.

го доминирования», оказывающие на современную международную ситуацию колоссальное влияние.

Связанные с этим явлением угрозы носят глобальный характер, однако далеко не все страны мира в силу объективных обстоятельств, а также сложившейся политической или финансовой ситуации способны в настоящее время перейти на новые технологии (сетевые протоколы), позволяющие лучше контролировать (отслеживать) киберпреступников (т.е. подавлять их анонимность). Поэтому США во многом «взяли проблему борьбы с анонимностью на себя» и фактически создают систему глобального контроля Интернета, подобную системам глобального мониторинга мирового океана, воздушного или космического пространства.

В этом свете высказывание президента США Б. Обамы о том, что «чем свободнее льётся поток информации, тем сильнее становится общество», приобретает специфическую окраску. В самом деле, его можно понять так, что для укрепления американского общества США необходим свободный доступ к информационным ресурсам других стран[*].

И кибератаки террористов, и просто технические сбои в работе глобальной информационной системы «требуют скоординированных мер реагирования, как со стороны международного сообщества, так и правительств и частного сектора» [12]. По нашему мнению, это высказывание Х. Клинтон имеет непосредственное отношение к характеру трансграничного сотрудничества по информационной безопасности. Здесь соответствующие договорённости между странами достигнуты ещё далеко не везде. Европейский Союз считает американскую точку зрения (на доступность европейского информационного пространства) приемлемой.

Россия же, как и другие страны Шанхайской организации сотрудничества (ШОС), свободный доступ к своему киберпространству отвергает. Американские эксперты Дж. Марков и А. Крамер в статье, опубликованной в «Нью-Йорк таймс» в конце 2009 г., утверждали, что в ходе встречи по вопросам безопасности и контртерроризма, прошедшей в октябре 2009 г. в МГУ им. Ломоносова, генерал В. Шерстюк (директор Института проблем информационной безопасности МГУ) заявил, что Россия отвергает Конвенцию по киберпреступности Совета Европы (*Council of Europe Convention on Cybercrime*), поскольку одно из её положений разрешает зарубежным правоохранительным органам проведение Интернет-поиска внутри российских границ, что нарушает российскую Конституцию. Россия считает это вмешательство неприемлемым и потому не намерена подписывать Европейский договор о киберпреступности (*European Cybercrime Treaty*), содержащий такое положение [18].

И основания для данной позиции России есть. Летом 2009 г., практически сразу после программного выступления президента Б. Обамы по вопросам кибербезопасности (май 2009 г.), государства – члены ШОС заключили в Екатеринбурге Соглашение между правительствами о сотрудничестве в области

[*] Что, кстати, полностью соответствует сложившимся на рубеже веков схемам финансирования американской экономики за счёт эмиссии и распространения долларов на мировом финансовом рынке.

обеспечения международной информационной безопасности. В нём, в частности, говорится: «Реализуя сотрудничество в соответствии с настоящим Соглашением стороны исходят из наличия следующих основных угроз в области обеспечения международной информационной безопасности:

1) разработка и применение информационного оружия, подготовка и ведение информационной войны;

2) информационный терроризм;

3) информационная преступность;

4) использование доминирующего положения в информационном пространстве в ущерб интересам и безопасности других государств;

5) распространение информации, наносящей вред общественно политической и социально-экономической системам, духовной, нравственной и культурной среде других государств;

6) угроза безопасному, стабильному функционированию глобальных и национальных информационных инфраструктур, имеющие природный и (или) техногенный характер» [5].

В приложении 2 к этому Соглашению содержание перечисленных угроз уточняется. В частности, в отношении угрозы использования доминирующего положения в информационном пространстве в ущерб интересам и безопасности других государств, отмечается, что «источником этой угрозы является неравномерность в развитии информационных технологий в различных государствах и существующая тенденция к увеличению цифрового разрыва между развитыми и развивающимися странами. Некоторые государства, имеющие преимущества в развитии информационных технологий, умышленно ограничивают развитие прочих стран и получение доступа к информационным технологиям, что приводит к возникновению серьёзной опасности для государств с недостаточными информационными возможностями. Признаками этой угрозы являются монополизация производства программного обеспечения и оборудования информационных инфраструктур, ограничение участия государств в международном информационно-технологическом сотрудничестве, препятствующее их развитию и увеличивающее зависимость этих стран от более развитых государств; встраивание скрытых возможностей и функций в программное обеспечение и оборудование, поставляемое в другие страны, для контроля и влияния на информационные ресурсы и (или) критически важные структуры этих стране; контроль и монополизация рынка информационных технологий и продуктов в ущерб интересам и безопасности государств» [5].

Вместе с тем, в мире широко известна позиция президента России Д.А. Медведева, заявившего, что «Российское правительство в отличие от других стран вообще не занимается Интернетом», а также что «Россия не будет ограничивать возможности Интернета, поскольку он способствует развитию демократии в стране» [4].

Тем не менее, американцы стали больше опасаться расширения сферы конфликтности интересов государства и бизнеса, и в частности, инсайдеров, использующих служебную информацию в личных целях. Об этом свидетельствует, например, письмо руководства Коалиции финансового планирования (*Financial Planning Coalition*) руководителям комитетов Палаты представите-

лей Конгресса, в котором выражается их недоверие к бюрократам, устанавливающим стандарты финансовой отчётности [26].

Американцы стали больше опасаться слабости исполнительной власти администрации Обамы, столкнувшейся с незатухающим кризисом, с чрезмерным обострением межведомственной конкуренции, а также с нарастающим противостоянием правительства и многочисленных приверженцев свободного предпринимательства [23].

Как нам представляется, все эти проблемы побудили ряд сенаторов, активно участвующих в разработке законов, регулирующих вопросы информационной безопасности, накануне ноябрьских (2010 г.) выборов в Конгресс обратиться с открытым письмом к президенту США. Как отмечалось выше, мнение президента Б. Обамы о приоритетности этого аспекта национальной безопасности США ранее высказывалось неоднократно. Тем не менее, в своём письме к Б. Обаме руководители Сената США Гарри Рейд (лидер демократического большинства), Патрик Ли, Карл Левин, Джон Керри, Джон Рокфеллер IV, Джозеф Либерман и Диана Фейнштейн, возглавляющие влиятельные комитеты по обороне, торговле, науке и транспорту, по разведке международным отношениям, а также юридический комитет, ещё раз обращают внимание президента на то, что страна остаётся уязвимой для киберугроз и эти угрозы, несмотря на все принимаемые меры, только нарастают, а между тем всеобъемлющего законодательства по кибербезопасности пока нет [27].

Как уже отмечалось выше, круг инновационных возможностей, «недружественного» использования информационных технологий расширяется намного быстрее, чем законодатели успевают это осмыслить, и даже в США «оборонительные технологии» просто не поспевают за возникающими угрозами. Авторы этого письма считают сложившуюся ситуацию очень серьёзной и полагают, что именно высшая исполнительная власть должна сыграть ключевую роль в координации действий по обеспечению кибербезопасности страны (добиваясь максимально согласованных действий законодателей, военных, спецслужб, а также общественности, бизнеса и зарубежных партнёров).

Это письмо говорит о том, что, несмотря на усилия различных органов государственной власти, предпринимаемые до настоящего времени попытки укрепления информационной безопасности остаются в США недостаточно эффективными, а потому его авторы не доверяют вновь назначенному «киберцарю» и ощущают серьёзное беспокойство в отношении обеспечения информационной безопасности страны, федерального государства, а также, видимо, и своей собственной. Судя по всему, сенаторы хотят быть уверенными в том, что американское правительство, решая вопросы обеспечения кибербезопасности страны, сможет предотвратить применение в предвыборной борьбе сверхмощных информационных технологий, подобных Глобальной информационной решетке [7] или высокоэффективным информационно-поисковым и фильтрующим аналитическим системам типа «Эйнштейн-2», «Гугл» или весьма специфическим машинам для электронного голосования [25]. Складывается впечатление, что авторы этого письма просто настаивают на том, чтобы президент проявил инициативу и взял на себя личную ответственность за защиту информационной безопасности страны (причём в широком смысле).

Как оказалось, и в национальных границах сильно политизированного конкурентного общества мощный информационный потенциал, находящийся в распоряжении одного государственно-частного «клана», может стать инструментом подавления других структур. По нашему мнению, такая асимметрия информационных возможностей становится фактором, дестабилизирующим политическую обстановку в стране, и может послужить причиной серьёзного внутриполитического кризиса. Таким образом, можно заключить, что ***в постиндустриальном обществе кризис может быть информационным и обусловлен*** не кибератаками из-за рубежа, направленными против банков или иных критически важных объектов инфраструктуры, а ***доминированием информационного потенциала некоторых государственно-частных структур, которые «знают слишком много для того, чтобы общество оставалось демократическим***».

Таким образом, сегодня конкурентоспособность любого бизнеса, во многом зависит от возможностей его информационного преобладания над инвесторами, клиентами, покупателями. Это относится к созданию и поддержанию кредитоспособного имиджа, рекламе, подготовке финансовых отчетов и проч. Сегодня на бизнес опираются и международные связи (причём не меньше, чем на военную силу), особенно в таких сферах, как развитие глобального информационного общества и международная информационная безопасность. При этом различия в техническом уровне и защищённости национальной информационной инфраструктуры, подобно разнице электрических потенциалов, фактически представляют собой основу конкурентной борьбы одного участника рынка против другого. Отсюда следует важный политологический вывод: в ***современном обществе принцип равной (паритетной) информационной безопасности оказывается неприемлемым с экономической точки зрения, поскольку выравнивание информационных потенциалов различных стран нивелирует основные конкурентные преимущества лидеров.*** И они паритета не допустят.

Из сказанного выше следует, что, хотя номинальный «цифровой разрыв» между странами (например, по количеству компьютеров или сотовых телефонов на тысячу человек населения) со временем сокращается, реальная дифференциация стран по уровню защищённости (уязвимости) их информационного пространства постоянно нарастает. С этой тенденцией связан целый комплекс негативных международно-политических последствий. Прежде всего, это – ускорение поляризации мира, увеличение разрыва между богатыми и бедными, технологически отсталыми и передовыми странами во всех областях, увеличение числа стран-маргиналов, а также так называемых «несостоятельных» или «рухнувших» государств, не способных пресечь деятельность кибертеррористов в своём киберпространстве. Именно ***расширение информационного разрыва можно рассматривать в качестве одной из главных причин нестабильности***, питающей не только глобальную конкуренцию, но и конфликты, которые могут быстро обрести глобальные масштабы. Резко увеличивается военный потенциал передовых в научно-техническом отношении стран, приводящий к изменению глобального и регионального балансов сил. Это может спровоцировать озабоченность и даже враждебную реакцию «отстающих» государств, порождая таким образом новые очаги противостояния.

В определённом смысле можно считать, что изменяется само понятие безопасности. Современные международные конфликты приобретают новые формы, опираются на технические средства, формально не являющиеся оружием. Это могут быть войны без применения вооружений и военной техники и без осуществления силового воздействия в общепринятом традиционном понимании; войны, полностью основывающиеся на применении информационных и сетевых технологий. Такие формы противостояния могут быть не менее разрушительными, чем традиционные вооружённые конфликты [3].

В начале XIX века президент США Т. Джефферсон (1743–1826) известил мировую общественность о том, что его страна будет следовать принципу «свободы открытого моря» и защищать своё право на свободу торговли с любой страной мира. Тогда этот принцип был крайне важен для США: если бы они не могли свободно торговать, они просто не смогли бы экономически существовать. В настоящее время абсолютно преобладающая по стоимости масса торгуемых активов носит виртуальный характер (тогда как реальные ценности зачастую даже не перемещаются в пространстве). В самом деле, уже больше десяти лет главным «товаром», как вывозимым, так и ввозимым в США стали деньги. При этом подавляющее их количество перевозится не в дорожных сейфах, не в «коробках из-под ксерокса», а передаётся по компьютерным Интернет-каналам финансовых учреждений. В этом смысле можно говорить о том, что **деньги превратились в особый вид информации**, а принцип «свободы открытого моря» приобрёл ещё более широкую интерпретацию:– США фактически распространили его на так называемое виртуальное киберпространство.

Всё это означает, что **для современной торговли (и тем более для инвестиций) принцип «свободы перемещения такого рода информации – денег» оказывается значительно важнее принципа «свободы открытого моря»**, что финансовое «здоровье» США сегодня практически полностью зависит от обеспечения надежности и безопасности её киберинфраструктуры, с одной стороны, и от проницаемости информационного пространства («свободы Интернета») в странах-партнёрах – с другой.

В результате информационная инфраструктура в этом контексте становится стратегическим ресурсом, а её защита – приоритетным направлением обеспечения национальной безопасности.

В «Стратегии национальной безопасности Соединённых Штатов», обнародованной в мае 2010 г., содержится ряд существенных нововведений, которые позволяют говорить, что политика Вашингтона в сфере национальной безопасности претерпела значительные изменения. Так, теперь в борьбе как с внешними, так и с внутренними угрозами администрация Обамы собирается применять силу более осмотрительно, «используя вместо молотка скальпель». В этой связи в Стратегии впервые «предлагается интегрировать основные инструменты американской мощи: дипломатию, военную силу, экономические инструменты, разведку; силы обеспечения внутренней безопасности». В отношении информационных технологий в Стратегии отмечается, что они «обеспечивают военное превосходство Соединённых Штатов, но делают американскую гражданскую экономику чрезвычайно уязвимой» [6] (слишком «реактивной», как в своё время отметил бывший глава ФРС А. Гринспен). В определённом

смысле это означает: широчайшее распространение таких технологий в американской экономике во многом истощает ресурсы её надёжности, подрывает устойчивость, что следует рассматривать в качестве одной из приоритетных проблем национальной экономической безопасности страны.

Всё это стало причиной нарастания озабоченности мирового сообщества возможностями применения новых технологий в целях, не совместимых с задачами обеспечения международной стабильности. Уязвимость используемой информационной инфраструктуры, с одной стороны, и уникальные возможности наиболее передовых информационных технологий – с другой, способствовали появлению принципиально нового вида оружия – информационного, а также информационно-технологических угроз международной безопасности, связанных с его применением. Важнейшими угрозами здесь следует считать враждебное использование информационно-коммуникационных технологий в отношении критически важных элементов информационной инфраструктуры другого государства в политических, в том числе военных, целях, а также преступную и террористическую деятельность в киберпространстве.

В этом контексте можно считать, что сфера международной информационной безопасности распространяется за границы киберпространства, включая и такую угрозу, как целенаправленное создание и использование доминирующего положения той или иной страны в глобальном информационном пространстве в ущерб интересам безопасности других государств. И источник этой угрозы заключается в неравномерности развития информационных технологий в различных государствах, а также существующей тенденции к увеличению цифрового разрыва между развитыми и развивающимися странами. Некоторые государства, располагающие мощными системами сбора и обработки данных, добиваются в глобальной сети доминирующих позиций и под лозунгом «распространения западных демократических ценностей» претендуют на свободный доступ к информационным ресурсам других суверенных стран.

Однако круг возможностей, так сказать, «недружественного» применения всё более совершенных информационных технологий расширяется очень быстро, намного быстрее, чем политики и законодатели успевают этот процесс осмыслить. В этой сфере, по мнению авторитетных специалистов (например, М. Хатауэй, ещё совсем недавно «киберцарицы» в администрации Обамы) сегодня уже даже в развитых странах «оборонительные технологии» просто не поспевают за возникающими угрозами. Более того, в этой сфере создавать новые (наступательные) угрозы зачастую проще (и многократно дешевле), чем развивать оборону, адекватную существующим реальным угрозам [16].

С этой точки зрения и концепция национальной безопасности США может строиться не на основе достаточности средств защиты от существующих угроз, и даже не на основе их балансирования паритетными встречными угрозами, а на основе стратегии абсолютного информационно-технологического преобладания над потенциальным противником, которая включает: достижение проницаемости информационного пространства потенциальных противников, достаточной для заблаговременного выявления угрозы своим интересам; опережающее «изобретение» новых информационных угроз, неприемлемых

для потенциальных противников; надёжную защиту собственной информационной инфраструктуры.

В таких условиях даже для поддержания международной безопасности на прежнем уровне мировое сообщество в целом, в том числе и суверенные государства, вынуждены очень быстро совершенствовать свои «цифровые навыки». В этом контексте М. Хатауэй в своей фундаментальной работе, посвящённой стратегическим преимуществам США [16], обращает внимание на необходимость технологического перевооружения американского разведывательного и дипломатического сообщества (как это в своё время было сделано для решения задач по контролю над вооружениями и разоружению).

Однако очень многим участникам такой «гонки» вовремя решать соответствующие задачи, как правило, не удаётся. В результате может возникнуть и даже систематически воспроизводиться ситуация международной нестабильности (точнее, недостаточной безопасности), иначе говоря, ситуация расширения некомпенсированных угроз, в которой система международной безопасности строится не столько на основе прежнего объективного равновесия стратегических сил, сколько в существенной мере на субъективном анализе выявленных рисков.

Список литературы и источников

1. Доктрина информационной безопасности Российской Федерации. Утверждена указом Президента РФ 9 сентября 2000 г. № Пр-1895 (http://www.internet-law.ru/intlaw/laws/doctrina.htm).

2. Инновационные направления современных международных отношений / Учебное пособие для студентов вузов под ред. А.В. Крутских и А.В. Бирюкова. М.: Аспект Пресс, 2010. 295 с.

3. *Лавров С.* Приветствие министра иностранных дел России участникам научно-практической конференции «Наука, технологии и международные отношения в эпоху глобализации: роль образования и инноваций». Москва, МГИМО, 24.04.2006.

4. *Медведев Д.А.* Выступление на встрече с политологами в Ярославле 10.09.2010 (http://news.mail.ru/politics/4417809/).

5. Международная информационная безопасность: дипломатия мира / Сборник материалов под общей редакцией С.А. Комова. Москва, 2009.

6. *Рогов С.М.* «Стратегия национальной безопасности» администрации Обамы: американское лидерство в многополярном мире // Независимое военное обозрение. 11.06.2010.

7. *Роговский Е.А.* США: информационное общество. М.: Международные отношения, 2008. 408 с.

8. *Роговский Е.А.* О постиндустриальных особенностях американского НТП. М.: ИНП РАН, 2009. 78 с.

9. Air Force Cyber Command. Air Force Cyber Command Strategic Vision. March 2008 (http://www.afcyber.af.mil/shared/media/document/AFD-080303-054.pdf).

10. *Alexander K.* Statement for the Record before the House Armed Services Committee Terrorism. Unconventional Threats, and Capabilities Subcommittee. 05.05.2009
(http://armedservices.house.gov/pdfs/TUTC050509/Alexander_Testimony050509.pdf).

11. *Bush G.W.* The National Security Strategy of the United States of America (http://www.informationclearinghouse.info/article2320.htm).

12. *Clinton H.R.* Remarks on Internet Freedom. The Newseum. Washington. DC 21.01.2010 (http://www.state.gov/secretary/rm/2010/01/135519.htm).

13. GAO-04-858 The Global Information Grid and Challenges Facing Its Implementation (http://www.gao.gov/new.items/d04858.pdf).

14. GAO-10-606 CYBERSPASE United States Faces Challenges in Addressing Global Cybersecurity and Governance, July 2010.

15. *Hathaway M.E.* Strategic Advantage: Why America Should Care about Cybersecurity. Harvard Kennedy School. October 2009 (http://belfercenter.ksg.harvard.edu/files/Hathaway.Strategic%20Advantage.Why%20America%20Should%20Care%20About%20Cybersecurity.pdf).

16. *Goldfarb Z.* Government Had Been Warned for Months about Troubles in Mortgage Servicer Industry // The Washington Post. 10.10.2010.

16. *Kohno T., Stubblefield A., Rubin A D., Wallach D.* Analysis of an Electronic Voting System. John Hopkins University & Rice, July 2003. IEEE Symposium on Security and Privacy 2004. IEEE Computer Society Press, May 2004 (http://avirubin.com/vote.pdf).

17. *Markoff J., Kramer A.E.* In Shift, U.S. Talks to Russia on Web Security // The New York Times (http://www.nytimes.com/2009/12/13/science/13cyber.html?_r=1).

18. *Miles D.* Gates Establishes New Cyber Subcommand. Washington. 24.06.2009 (http://www.defenselink.mil/news/newsarticle.aspx?id=54890).

19. *Monroe J.S.* Cyber Command: So Much Still to Know // Federal Computer week (http://fcw.com/Articles/2009/07/06/buzz-cyber-command.aspx?p=1).

20. Open Government Directive. December 2009 (http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-06.pdf).

21. *Syed S.* Businesses, Governments and Consumers Must Work Together to Secure Cyberspace, Say Private- And Public-Sector Leaders (http://www.ewi.info/businesses-governments-and-consumers-must-work-together-secure-cyberspace-say-private-and-public-sec).

22. The 70-30 Nation // The Economist. Vol. 395, No. 8687. 19.06.2010.

23. The Comprehensive National Cybersecurity Initiative (http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative).

24. http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/

25. http://www.cfp.net/downloads/HR3817_Bachus001_Letter_2009-11-03.pdf

26. http://www.nationaljournal.com/congressdaily/issues/documents/Letter_President_on_Cyber_Security_Legislation_070110.pdf

27. http://www.whitehouse.gov/files/documents/cyber/CybersecurityCentersGraphic.pdf