АНАЛИЗ РАБОТЫ АППАРАТА КИБЕРБЕЗОПАСНОСТИ США И РЕКОМЕНДАЦИИ ПО УЛУЧШЕНИЮ ЕГО ДЕЯТЕЛЬНОСТИ

Рябов В.А.

Рябов Виктор Алексеевич – студент магистратуры,
направление «Международные отношения»,
кафедра № 65 «Анализ конкурентных систем», факультет управления и экономики высоких технологий,
Национальный исследовательский ядерный университет «МИФИ», г. Москва

Аннотация: *в статье анализируется работа аппарата кибербезопасности США, на основе анализа выявляются проблемы в работе его составляющих, а также даются рекомендации по их решению.*
Ключевые слова: *анализ, политика, США, безопасность, информационные технологии, международные отношения.*

За последние годы многие высокопоставленные чиновники и даже сам президент США публично обозначили кибербезопасность как один из важнейших аспектов национальной безопасности. Как следствие, был достигнут значительный прогресс в создании рамочных документов, в которых указано, как США будут бороться с динамично меняющимися киберугрозами. Созданная в 2008 году и изначально засекреченная Комплексная национальная инициатива по кибербезопасности (CNCI) [1] предложила стратегию, состоящую из восьми инициатив, направленных на усиление сплоченности общественного, частного, правового, оборонного и разведывательного секторов для улучшения кибербезопасности. Результатом этой инициативы стали два спорных законопроекта и одно постановление, что хоть и неплохо, но не дотягивает до уровня национального приоритета, как его обозначили политические лидеры. Несмотря на эти усилия, правительству США только ещё предстоит всерьез взяться за проблему киберугроз. Для начала у сильных мира сего не выйдет определить учреждение, которое целиком возьмет на себя эту ответственность, а также не получится распределить права и обязанности для накладывающихся друг на друга программ гражданской и военной кибербезопасности вкупе с расхождениями в бюджете. Правительству США необходимо реструктуризировать текущие организационные ресурсы, четко определить роли и обязанности вовлеченных учреждений независимо от их положения и размеров бюджета, а также поставить во главу этих учреждений надежных людей. Все это позволит укрепить кибербезопасность США с политической и управленческой точки зрения.

В настоящее время аппарат кибербезопасности США представляют собой никем не управляемое нагромождение подразделений, неэффективных совместных действий и бюрократии. Шестнадцать разведывательных агентств и еще больше гражданских и военных организаций пытаются организовать превентивные меры по профилактике и мониторингу киберугроз и/или выявлению и закрытию существующих сетевых угроз. Обмен деликатной информацией по данной тематике – дело весьма тонкое, особенно в тех случаях, когда такая информация попадает в руки влиятельных игроков на финансовом рынке. Так как большая часть данных правительства США проходит через частные сети, утечки нельзя исключать, поэтому, сотрудникам некоторых учреждений запрещено раскрывать информацию в зависимости от уровня секретности и деликатности. Тот факт, что многие из владельцев этих частных сетей относятся к производственным базам или к ключевым инфраструктурам, таким как системы диспетчерского управления и сбора данных (SCADA), доказывает, что усилия США в области кибербезопасности недостаточны. Из-за отсутствия утвержденной Конгрессом директивы и исполнительного порядка «ответственных» за кибербезопасность США продолжат терпеть неудачи в усилении национальной кибербезопасности не потому, что это недостижимая для них задача, а потому что правительство не заставляет погрязшие в бюрократии учреждения оставить эго и послужить благой цели. В скором времени Барак Обама (Barack Obama) собирается выпустить указ, направленный на то, чтобы «федеральные учреждения создали директивные материалы по кибербезопасности для владельцев энергетических, водных и других предприятий для исполнения на добровольной основе». Добровольный порядок исполнения этих директив показывает, насколько правительство не готово к столкновению с серьезными киберугрозами.

Большинство американцев согласны с тем, что бюрократическая система изжила себя и абсолютно неэффективна. В 2010 году представители исследовательского центра Пью (Pew Research Center) заявили, что около 80 процентов американцев не доверяют Вашингтону и не ждут того, что федеральное правительство разберется с национальными проблемами. Результаты опросов перед президентскими выборами показывают, что избиратели не питают надежд, что нынешние представители власти или их преемники приведут страну к успеху. Во многом именно бюрократия в государственных учреждениях позволяет людям понять, что все эти учреждения работают не на народ, а на то, чтобы получить больше власти.

Аксиома «сильные мира сего устанавливают правила» справедлива и для Вашингтона, где идет постоянная борьба за средства бюджета. К примеру, до того, как была создана Комплексная национальная инициатива по кибербезопасности (CNCI), существовало несколько киберорганизаций в гражданском и военном секторах. После создания CNCI на работу федеральных учреждений по кибернаправлению было выделены миллионы долларов. В 2011 году из федерального бюджета было запрошено 3.6 миллиарда долларов на программы CNCI. В 2012 году федеральные учреждения запросили еще больше денег. А в 2013 запрошено 140.8 миллиарда долларов на различные киберпрограммы. В итоге: государство выделило огромные деньги на решение проблемы, не имея планов, «дорожной карты» и надзорных органов, которые бы определили, что деньги используются по назначению, а не растрачиваются по другим направлениям.

Вопреки мнению большинства о том, что реорганизация не исправит недостатки в работе госучреждений, эффективное управление вкупе с установлением надзорных органов над ответственными учреждениями существенно повлияет на ситуацию. По правде говоря, не существует однозначного ответа на настолько обширную бесструктурную угрозу. Вдобавок, злоумышленников практически невозможно отследить. Тем не менее, отсутствие рамочных документов, в которых обозначены ответственные лица и их обязанности и права, будет продолжать отрицательно влиять на нашу способность ответить на эту новую угрозу.

Предложение ниже содержит советы по централизации национальной кибербезопасности и по реорганизации связанных с кибербезопасностью военных учреждений. Если принять во внимание то, что враждебные действия в киберпространстве занимают наносекунды, более централизованное управление позволит успешнее среагировать в случае инцидента.

В соответствии с рекомендациями «Cyberspace Policy Review» от 2009 года, президент США Барак Обама (Barack Obama) назначил специального координирующего советника по кибербезопасности, который возьмет на себя ответственность по заданию и координированию стратегии политики страны в области кибербезопасности. Советнику также придется проинспектировать, насколько выполняются директивы и меры по сохранению гостайны. Более того, в качестве части президентской администрации, координирующий орган сможет обращаться к Президенту напрямую за поддержкой словом и делом. Однако, пост советника не оправдал возложенных надежд из-за отсутствия реальной власти, и стал лишь номинальным, так как право давать рекомендации по тому или иному вопросу не имеет под собой законодательной базы для приведения этих рекомендаций в исполнение.

Рекомендации: Назначенный Президентом координатор сможет предлагать стратегические решения как внутри страны, так и на международной арене. Эти решения должны будут быть подтверждены Сенатом, что позволит конгрессменам управлять процессом. У координатора должны быть две важнейшие функции: (1) создание директивных материалов по кибербезопасности, которые должны быть применены на федеральном уровне и (2) участие в международных инициативах по кибербезопасности. Над директивами координатор должен работать совместно со следующими организациями: Национальный институт стандартов и технологий (National Institute of Standards and Technology), Управление по защите информации Агентства национальной безопасности (National Security Agency’s Information Assurance Directorate), Национальное управление кибербезопасности Министерства внутренней безопасности (Department of Homeland Security’s National Cyber Security Division (DHS NCSD)). В результате совместно должны быть выработаны «наиболее эффективные решения и стандарты» по кибербезопасности. После согласования чернового варианта одно из ответственных учреждений должно рассмотреть, внести правки и дополнения, которые позволят учесть интересы этих организаций. После рассмотрения Координатор совместно с DHS NCSD доведет директивы и планы с временем их введения до всех заинтересованных лиц. В случае, если учреждение не сможет исполнить директивы, Координатор имеет право обратиться к президенту с заявлением об исполнении директив в принудительном порядке, а затем и к Конгрессу с просьбой ограничить финансирование для не подчинившегося учреждения. Что касается международной составляющей, координатор будет представлять национальные интересы и контролировать взаимодействие Министерства обороны США (Department of Defense (DOD)), Министерства юстиции (Department of Justice) и Министерства иностранных дел (Department of State) с их иностранными коллегами по вопросам, касающимся кибербезопасности: заключению соглашений, меморандумов и договоров. Во время исполнения своих обязанностей, координатор удостоверяется, что поставленные в рамках усиления кибербезопасности достигаются своевременно, а также что субъекты внешней политики США работают на благо кибербезопасности. Наконец, являясь официальным представителем администрации президента, координатор должен присутствовать на Совете национальной безопасности США и обозначать все вопросы, касающиеся внутренней и международной кибербезопасности и требующие внимания президентского аппарата.

В настоящее время Министерство внутренней безопасности (Department of Homeland Security) осуществляет мониторинг государственных сетей, находящихся в публичном доступе (“.gov”), а также

предоставляет результаты аналитики владельцам и операторам частных сетей. Такое положение дел позволяет DHS производить мониторинг большинства частных сетей в США, включая сети ключевых инфраструктур, таких как энергетическая, газовая, водная и систем SCADA, которыми они управляются. Более того, в соответствии с информацией на официальном сайте, DHS стоит во главе центра по обработке информации, Национального управления кибербезопасности (National Cybersecurity and Communications Integration Center (NCCIC)) и нескольких других подразделений. Эти подразделения предоставляют техподдержку в случае инцидентов и в качестве профилактики безопасности частных сетей. NCCIC координирует информацию, полученную из различных источников, для создания дайджеста по работе всех киберподразделений государственного и частного сектора. DHS часто критикуют за некомпетентность и бюрократию. Тем не менее, работа министерства в области кибербезопасности постоянно осложнена недостатком полномочий над госучреждениями, которые они должны обезопасить. Хуже того, когда были атакованы важные американские сети, государство привычно обратилось за помощью к Агентству национальной безопасности (National Security Agency (NSA)), несмотря на то, что такими случаями в соответствии с законодательством должно заниматься DHS. По сути, DHS без официальных заявлений «отправили на скамейку запасных».

Рекомендации: DHS должно стать во главе кибербезопасности США в соответствии со своим уставом, миссией и правами защищать и обнародовать информацию частному сектору. Администрация президента и Конгресс должны предоставить DHS необходимые полномочия для управления госучреждениями в соответствии с рекомендациями координатора по кибербезопасности. У DHS будут полномочия, которые позволят инспектировать кибербезопасность данных госучреждений и предоставить координатор по кибербезопасности отчет. Вдобавок, DHS продолжит служить информационным буфером между общественным и частным сектором – будет собирать информацию, грифовать и предоставлять её частным заинтересованным лицам. И наконец, DHS сможет запрашивать у NSA поддержку в виде актуальной информации об активности в частных сетях. Также министерство сможет запросить у Федерального бюро расследований (Federal Bureau of Investigation (FBI)) помощь в расследовании киберпреступлений против частных сетей.

Подводя итог, стоит сказать, что в связи со сменой президента, аппарат кибербезопасности США ждут изменения. Однако, пока сложно сказать, пойдет ли новая администрация по пути исправления ошибок или попытается начать с чистого листа.

Список литературы

1. *Comprehensive National Cybersecurity Initiative. January 2008. Washington, DC.* [Electronic resource] URL: //nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-034.pdf/ (date of access: 01.03.2017).
2. *Конышев В.Н., Сергунин А.А.* Стратегия национальной безопасности Б. Обамы: состоялось ли радикальное обновление? // Обозреватель – Observer, 2010. № 12.