IV. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 323.285

© Савин Л.В.
Savin L.

БРИТАНСКАЯ СТРАТЕГИЯ ПО КИБЕРБЕЗОПАСНОСТИ

BRITISH STRATEGY ON CYBERSECURITY

Аннотация. *В статье подробно рассмотрена рабочая модель британской стратегии по кибербезопасности, ее положения и дорожная карта действий правительства.*

Annotation. *SIn publication defined working model of the strategy on cybersecurity of UK., it's and roadmap of the government's actions.*

Ключевые слова. *Кибербезопасность, Великобритания, экономика, полиция, государство, частный сектор, коммуникации.*

Key words. *Cybersecurity, UK., economy, police, state, private sector, communications.*

Развитие информационных технологий неумолимо приводит к тому, что экономика многих государств становятся зависимой от киберпространства. Британия не является исключением. 6% ВВП Британии зарабатывается с помощью манипуляций, которые так или иначе связаны с Интернет. Британская экономика - одна из самых развитых онлайн экономик в мире, которая оценивается в сто миллиардов фунтов стерлингов в год, и эти показатели будут расти в ближайшее время. Ожидается, что в перспективе она превысит даже доходы от агропромышленного сектора, а в течение следующих пяти лет 365 тысяч британцев получат рабочие места, связанные непосредственно с Интернет-заработками. Конечно же, в связи с этим правительство Британии намерено создать надлежащие условия для нового бизнеса и помочь в организации индустрии кибербезопасности. При этом правительство Объединенного Королевства не занимается «алармизмом» по поводу киберугроз, как это делают их коллеги из США, а планомерно проводит свою работу. Хотя военные занимаются кибербезопасностью отдельно, а гражданские отдельно, государство и частный сектор вместе работают над созданием синергетического потенциала в этой сфере.

В конце прошлого года премьер-министр Великобритании Дэвид Кэмерон заявил, что кибербезопасность является высшим приоритетом правительства, которое намерено тесно работать с полицией, службами безопасности, международными партнерами и частным сектором для того, чтобы показать, что Великобритания остается одним из самых безопасных мест в мире для ведения бизнеса.

Тогда же была представлена новая стратегия по кибербезопасности. Министр по кибербезопасности Великобритании Фрэнсис Мод, представляя эту стратегию, отметил, что «развитие Интернет революционизировало нашу каждодневную жизнь, что обещает ранее невиданные социальные и экономические возможности в дальнейшие годы. Эта стратегия должна помочь нам получить полную выгоду из осетевленного мира с помощью создания надежного цифрового окружения, которому мы можем доверять и которое защищало бы общество от мошенничества онлайн, так же как и необходимую инфраструктуру от кибератак» [1].

Непосредственно согласно киберстратегии Великобритании правительство намерено реализовать ряд проектов.

Савин Леонид Владимирович – главный редактор журнала «Геополитика», кафедра социологии международных отношений социологического факультета МГУ им. М.В. Ломоносова, тел. (495) 514- 65-16.

Savin Leonid – editor-in-chief of "Geopolitika" magazine, Department of Sociology of international relations, Sociology Faculty of the Moscow State University named after M.V. Lomonosov, tel. (495) 514-65-16.

• Запустить новые общественные/частные "хабы" (узлы) по кибербезопасности. Это позволит правительству и частному сектору обмениваться полезной информацией о киберугрозах и управлять ответами на кибератаки. Пилотный проект был запущен в декабре 2011 г. с участием пяти бизнес-секторов: обороны, телекоммуникаций, финансов, фармацевтики и энергетики.

• Изучить методы, с помощью которых опыт Центра правительственной связи может способствовать экономическому росту: ЦПС является родоначальником экспертизы мирового класса по кибербезопасности. Правительство будет изучать методы, в которых этот опыт может более непосредственно способствовать экономическому росту и поддержке развития сектора кибербезопасности Великобритании без ущерба для основных задач агентства по безопасности и разведке. Например, варианты могут включать в себя работу с партнерами из частного сектора с целью изучения потенциала коммерческих приложений для уникального опыта в ЦПС. Кроме того, предполагается совместная работа с Британской информационной службой, Советом технологической стратегии и Советом по исследованиям в области инженерии и физики для изучения стратегических носителей, направленных на объединение промышленных, научных кругов и правительства по использованию новейших достижений в области кибербезопасности в целях повышения благосостояния и безопасности Великобритании в киберпространстве. Кроме того, есть идея создания модели венчурного капитала при поддержке правительства для того, чтобы разблокировать инновации по кибербезопасности в малом и среднем бизнесе.

• Поддержать малый и средний бизнес. Правительство обеспечит роль более мелких компаний в качестве двигателей новых идей и инноваций путем привнесения предложений в рамках программы "Обзор развития" для оказания помощи малому и среднему бизнесу в полном доступе к государственным закупкам. Ожидается, что не менее 25% от стоимости государственных контрактов, связанных с кибербезопасностью, будет направлено в малый и средний бизнес.

• Поддержать внедрение основных промышленных стандартов по кибербезопасности для компаний частного сектора. Предприятия Великобритании могут использовать это как конкурентное преимущество путем продвижения себя в качестве сертифицированных агентов по кибербезопасности. Британская информационная служба будет работать с отечественными, европейскими и глобальными коммерческими организациями по стандартизации для того, чтобы ускорить эту работу и содействовать кибербезопасности британской промышленности за рубежом. Департамент торговли и инвестиций Соединенного Королевства будет работать с торговыми ассоциациями в секторе безопасности, чтобы увеличение внутреннего роста помогало британским фирмам в зарубежных продажах.

Базовые положения стратегии по кибербезопасности предполагают следующее.

• Создание подразделения «киберспециалистов» для того, чтобы помочь полиции решать проблемы киберпреступности. Центральное подразделение полиции по электронной преступности (PCeU) лондонской полиции уже осуществило новаторское задействование спецполиции с соответствующей квалификацией для помощи в решении киберпреступлений. Планируется, что правительство будет поощрять все полицейские силы по задействованию «киберспециалистов».

• Формирование подразделения по киберпреступности в рамках Национального агентства по борьбе с преступностью к 2013 г. Это поможет решать самые серьезные киберпреступления на национальном уровне и также сможет частично применяться для крупных национальных инцидентов. Оно будет работать вместе с отделом по электронным преступлениями Агентства по борьбе с организованной преступностью и центральным подразделением полиции по электронной преступности, а также обеспечивать поддержку всех элементов национального агентства по борьбе с преступностью и всех полицейских подразделений.

• Поощрение полиции и судов более широко использовать существующие санкции в отношении киберпреступлений. Уже введены дополнительные полномочия, которые применяются в тех случаях, когда есть все основания полагать, что осужденный склонен к совершению дальнейших серьезных киберпреступлений. Например, различные сроки заключения, ограничение доступа к сети Интернет и запрет на использование служб мгновенных сообщений уже применялись для ограничения деятельности организованных преступных групп, совершавших онлайновые мошенничества. Правительство также опубликует новые рекомендации, направленные на повышение применений санкций за киберпреступления.

• Упрощение докладов по финансово-мотивированной киберпреступности путем создания единой системы отчетности для предприятий и общественности. Национальный отчет по мошенничеству и консультационный пункт при национальной администрации по вопросам мошенничества станут центральным порталом для отчетов по любому финансово-мотивированному

киберпреступлению.

Стратегия по кибербезопасности также включает задачу укрепления информационных коммуникационных систем и баз данных Великобритании для защиты от возможных угроз, повышение общественной осведомленности по данной проблематике, а также образовательные и исследовательские инициативы.

Хотя в первой половине 2012 г. специалисты по кибербезопасности Великобритании признавали, что их страна отстает от Франции и Германии в этом вопросе, Олимпийские игры послужили хорошим поводом для проведения тестовых инициатив и анализа ситуации. Команда экспертов по кибербезопасности заранее начала заниматься этими вопросами в преддверии Олимпийских игр в Лондоне. Ими был учтен опыт проведения Олимпийских игр в Пекине, во время которых произошло около 12 миллионов кибератак и, по словам министра Фрэнсиса Мода, Британия готова обеспечить надежные и безопасные игры, хотя сети правительства Великобритании по-прежнему служат целью для иностранных разведок или групп, работающих от их имени [2].

В технологическом секторе также идет соответствующая работа. Например, компания Forensic Pathways разработала и в мае 2012 г. представила инновационное обеспечение, которое автоматически в течение нескольких секунд позволит полиции идентифицировать запрещенный видео контент, а также цифровые изображения в сети, имеющие отношение к терроризму или детской порнографии [3].

Эти достижения демонстрируют реализацию шагов, предложенных в стратегии по кибербезопасности. Следует ожидать, что в дальнейшем остальные пункты программы также будут реализованы.

В России на уровне властей также начинают высказывать идеи о необходимости выработки концепции кибербезопасности. Вице-премьер Дмитрий Рогозин, в частности, в марте 2012 г. заявил о необходимости создания кибервойск, которые займутся обеспечением безопасности всей соответствующей инфраструктуры государства [4]. Вряд ли в ближайшее время в России будет по силам создать структуру, идентичную киберкомандованию в США, однако направление для будущей работы выбрано верно. Несмотря на повсеместный рост значения информационных технологий, этот сектор в нашей стране значительно проседает. Однако британский опыт, вместе с опытом других стран, а также взаимодействие по линии международного сотрудничества, связанного с предотвращением организованных транснациональных преступлений, включая кибердеятельность, могли бы способствовать лучшему пониманию возможных угроз и уязвимостей, а также ограничить отток капитала из России, сделав более благоприятный климат для мелкого и среднего бизнеса в этой отрасли как в плане создания отечественной информационно-технологической продукции, так и для обеспечения адекватных условий работы.

Литература

1. Government publishes all-new strategy for boosting cyber security. 25 Nov 11. http://www.info4security.com/story.asp?sectioncode≠51&storycode≠4128432&c≠1.

2. Fuentes Chavarriga, Julio. Preparacion para la Proteccion de los Juegos Olimpicos de Londres, con ciber-equipo de contra ataqu. 16.05.2012 http://www.inteligenciaholistica.org/preparacion-para-la-proteccion-de-los-juegos-olimpicos-de-londres-con-ciber-equipo-de-contra-ataqu.

3. New software to detect child pornography and terrorist material. 02 May 12 of data and identify illegal content. http://www.info4security.com/story.asp?sectioncode≠11&storycode≠4128993&c≠1.

4. Рогозин рассказал о планах создать киберкомандование,// Ведомости, 21.03.2012. http://www.vedomosti.ru/tech/news/1547405/rogozin_rasskazal_o_planah_sozdat_kiberkomandovanie.

Материал поступил в редакцию 27. 09. 2012 г.