РИСКИ И УГРОЗЫ КИБЕРБЕЗОПАСНОСТИ ЗИМНИХ ОЛИМПИЙСКИХ ИГР В СОЧИ

Бондаренко С.В.,
доктор социологических наук,
Ростов-на-Дону

Введение

Связанные с проведением зимних Олимпийских игр в Сочи краткосрочные угрозы кибербезопасности безусловно важны для имиджа страны, однако гораздо важнее долгосрочные вызовы, обусловленные низкой защищенностью критической инфраструктуры. Олимпиада как всемирно значимое событие предоставляет многим, в том числе и делинквентно ориентированы акторам, как «окно возможностей». Возможностей, в первую очередь, влияния на общественное мнение и пропаганды экстремистских идей через медийный контент, а также возможностей подрыва легитимности своих политических противников.

Поэтому в большей мере все, что далее будет сказано о кибербезопасности Олимпиады, может быть отнесено и к иным масштабным проектам компьютеризации России. По замыслу автора основная цель настоящей статьи состоит не в теоретическом осмыслении проблем кибербезопасности или перечислении возможных многочисленных киберугроз, а в постановке в публичном дискурсе проблемы информационной защиты предстоящей Олимпиады. Проблема чрезвычайно актуальна, поскольку выявленные нами факты свидетельствуют о нарастании игнорируемой чиновниками угрозы национальной безопасности России. Теоретические же основы онтологических проблем кибербезопасности будут отражены в других наших публикациях.

1. Постановка проблемы существования террористических киберугроз проведению Олимпийских игр

«Вы приведите мне 10 хакеров,
и в течение 90 дней я поставлю эту страну на колени»
Джим Сеттл[1]

События 11 сентября 2001 года привели к фундаментальным изменениям в сфере безопасности во всех сферах жизни общества, в том числе и в вопросах организации и проведения Олимпийских игр. По заключению экспертов по безопасности, каждая Олимпиада представляет собой новую цель для терактов, формы и особенности организации которых становятся все более изощренными.

Не случайно в общественных науках появился термин «террористический капитал»[2], размеры которого увеличиваются при совершении терактов в местах проведения массовых мероприятий. Олимпийские игры в этом отношении представляют идеальный объект для атаки, поскольку на соревнованиях присутствуют сотни тысяч туристов, спортсменов и вспомогательного персонала, а также международные лидеры и международные масс-медиа. Ежедневные телевизионные трансляции, чаще всего осуществляемые в режиме реального времени, создают возможности относительно свободного доступа террористов к глобальной аудитории. Эксперт по современному терроризму Брюс Хоффман (Bruce Hoffman) утверждает, что делинквентно

[1] Jim Settle, бывший глава ФБР. Цит. по: Verton D. Black Ice: The Invisible Threat of Cyber-Terrorism. California: McGraw-Hill, 2003.
[2] Toohey K., Taylor T. Perceptions of Terrorism Threats at the 2004 Olympic Games: Implications for Sports Events // Journal of Sport and Tourism, 2007, vol. 12, № 2. P. 100.

ориентированные акторы в последнее десятилетие добавили «к своему арсеналу новое оружие типа мини видеокамер, DVD, компьютеров и мобильных телефонов»[3].

Широкий спектр угроз безопасности включает не только различные формы террористических действий со стороны хорошо организованных групп экстремистов, но и спонтанные действия со стороны недовольных граждан или лиц с психическими отклонениями. Характер угроз меняется с течением времени и никогда нельзя ставить точку в плане обеспечения информационной безопасности.

Поэтому вполне естественны перманентные изменения модели обеспечения безопасности международных спортивных мероприятий, как в вопросах планирования, так организации системных процессов и управления рисками. Системные изменения должны происходить не только с точки зрения используемых технологий, но и в ментальности должностных лиц, в том числе и не отвечающих напрямую за обеспечение безопасности. Вот этого как раз и не могут понять в кабинетах, где обсуждаются вопросы информационной защиты предстоящей Олимпиады в Сочи.

Приведем несколько фактов напрямую не связанных с Олимпиадой, которые, тем не менее, иллюстрирующих масштаб существующих сегодня киберугроз. Достаточно показательно, что в США создана и действует группа экстренного реагирования на кибератаки. В 2009 году она была развернута один раз, в 2010г. уже 6 раз, а восемь месяцев 2011г. указанной группе приходилось включаться в работу уже 7 раз. В России помощь пострадавшим от кибератак организована куда менее эффективно, чем в странах с развитыми системами киберзащиты.

С угрозами информационной безопасности за последний год столкнулись 96% российских компаний. Для каждой второй организации эти инциденты закончились потерей конфиденциальных данных. Исследование, проведенное аналитиками "Лаборатории Касперского" совместно с международным агентством B2B International в 14 странах мира, включая Россию, выявило неприятную тенденцию: из 1700 опрошенных компаний почти половина указали на увеличение количества кибератак. Главными угрозами своей безопасности IT-специалисты этих компаний считают вирусы и вредоносные программы, позволяющие злоумышленникам получить доступ к корпоративной сети, а также фишинговые и DDOS-атаки, нарушающие работу серверов и сайтов. Исследование показало также, что чаще всего сбои в системе безопасности приводят к потере данных о платежах (13%), интеллектуальной собственности (13%), клиентских баз (12%) и информации о сотрудниках (12%).

Таким образом, не приходится говорить о том, что российские бизнес-структуры плохо осведомлены об угрожающих опасностях. Более того, практически все участники упомянутого исследования назвали информационную стратегию компании одной из важнейших в современных условиях, оценив ее даже выше маркетинговой и кадровой составляющей. Проблема заключается в другом: большинство компаний начинают вкладывать средства в системы защиты только после того, как сами подвергнутся нападению. В целом же 31% компаний в России до сих пор в полной мере не внедрили защиту от вредоносных программ (для примера: в Великобритании она установлена в 92% организаций), а установкой различных уровней доступа к IT-системам озаботились лишь в 47% компаний.

Ближайшее будущее аналитики рынка оценивают с определенным скепсисом. "Доля расходов на IT-безопасность в последние три года увеличивается в общей структуре расходов компании на IT. Это международный и российский тренд, - признает руководитель управления исследований "Лаборатории Касперского" А. Ерофеев. - Другое дело, что рост расходов на IT-безопасность не поспевает за ростом числа угроз. Злоумышленники сегодня "инвестируют" в свой бизнес гораздо больше, чем IT-менеджеры в информационную безопасность. Поэтому пока приоритеты не изменятся, то

[3] Hoffman B. Inside Terrorism, revised and expanded edition. New York: Colombia University Press, 2006. P. 197.

есть пока специалисты по инфобезопасности не поймут, что должны вкладывать в системы защиты по крайней мере не меньше, чем преступники в свои инструменты, ситуация не изменится"[4]. На самом деле стоимость инструментария для кибератак многократно ниже стоимости систем защиты и даже крупные компании не выделяют соответствующих ресурсов для киберзащиты о чем свидетельствуют факты, представленные нами далее.

В США в 2011 году хакеры успешно атаковали сайты платежных систем PayPal и Mastercard, а одна из криминальных групп заявила о взломе около 70 сайтов правоохранительных органов США. Ведущие корпорации японского военно-промышленного комплекса в 2011 году подверглись спланированной атаке со стороны неизвестных компьютерных взломщиков. Самый серьезный ущерб причинен крупнейшей компании отрасли Mitsubishi heavy industries, серверы которой оказались на время во власти хакеров и у которой, судя по всему, были похищены закрытая документация и технологические секреты. Эта компания производит по американским лицензиям боевые самолеты F-15, ракетно-зенитные комплексы Patriot, другую технику и снаряжение[5]. На регулярной основе из-за DDoS-атак становятся недоступными сайты политиков, коммерческих структур и масс-медиа в России и других странах.

К примеру, сайт посольства РФ в Великобритании в сентябре 2011 года подвергся предположительно кибератаке DDoS (англ. - *distributed denial of service*) и был выведен из строя в преддверии официального визита в Россию британского премьер-министра Дэвида Кэмерона. Сотрудникам дипмиссии РФ пришлось создать зеркальный веб-сайт чтобы удовлетворить возросший интерес к происходящим событиям общественности и масс-медиа.

Кибератаки с политическими целями осуществляются не только на государственные, но и на коммерческие структуры. К примеру, с 30 марта по 6 апреля 2011 года на блог-хостинг «Живой Журнал» (ЖЖ, LiveJournal) пришлось три мощные DDoS-атаки, которая заключается в том, что сайт оказывается перегружен обращениями с других компьютеров. Тогда недоступен для пользователей оказался даже блог президента России Д.А. Медведева. Российский президент назвал хакерские атаки "возмутительными и незаконными", которые способствуют тому, что интернет-пользователи в DDoS-атаках видят "происки власти, ФСБ, администрации президента".

Во всем мире наблюдается непрерывный рост числа кибератак. Их число увеличивается примерно на 55 процентов ежегодно. Было бы наивно ожидать, что киберугроз избежит Олимпиада в Сочи. Поэтому вопрос не в реальности киберугроз, а в уровне защищенности Олимпийских игр.

2. Опыт предыдущих Олимпиад

«Три пути ведут к знанию:
размышление — путь самый благородный,
подражание — путь самый легкий,
опыт — путь самый горький»
Конфуций

2.1. Развитие инфраструктуры кибербезопасности Олимпийских игр

В последние десятилетия возросла роль в функционировании инфраструктуры Олимпийских игр телекоммуникаций, которые все чаще становятся объектом цифровых атак. Инфраструктура Олимпийских игр является частным случаем национальной критической инфраструктуры, в которую входят объекты, задействованные в

[4] Закиев Р. К вам хакер. Количество кибератак на компании растет // Российская бизнес-газета, 2011, №817 (35). 04.10.
[5] Головнин В. В японской оборонке поработали хакеры // Коммерсантъ, 2011, №177 (4718), 22.09.

предоставлении населению таких услуг как водо- и газоснабжение, электроэнергии, телекоммуникаций, а также услуг банковского сектора. Сегодня все вышеупомянутые сферы в значительной мере используют ИКТ и потому априори являются объектами для осуществления кибератак. Еще при проведении в 2006 году зимней Олимпиады в Турине были выявлены факты взлома компьютерных сетей и нарушения целостности хранившихся данных[6].

Достаточно показательна ситуация с распространением в 2010 году компьютерного вируса Stuxnet, когда в Иране на объектах даже не подключенных к глобальным компьютерным сетям, эта компьютерная программа вывела из строя атомные центрифуги. Поскольку невозможно исключить влияние человеческого фактора, стало ясно, что не срабатывает философия киберзащиты, основанная на «бункеризации», когда объекты не подключены к сети Интернет и потому якобы защищены на 100%.

Кроме того, высокотехнологичный вирус Stuxnet, созданный по некоторым данным государственными акторами, был разобран хакерами на части и куски опасного компьютерного кода стали доступны практически любому. Соответственно, резко повысилось качество инструментария используемого для кибератак. Этот факт как и многие аналогичные необходимо учитывать организатором Олимпиад в Лондоне в 2012 году и в Сочи в 2014 при развертывании инфраструктуры этих крупнейших международных соревнований.

В таких условиях с каждым годом становится все труднее проводить различие между цифровыми и физическими системами охраны общественной безопасности. Если до недавнего времени компьютерные системы использовались в основном для хранения результатов соревнований и координации деятельности персонала, то уже при проведении в 2004 году летних Олимпийских игр в Афинах была создана цифровая инфраструктура для фиксации изображений с камер видеонаблюдения, использовавших формат MPEG4. Через четыре года на Олимпиаде в Пекине применялись усовершенствованные алгоритмы мониторинга, включая распознавание лиц и шаблоны обнаружения подозрительной активности в общественных местах.

При этом тотальной безопасности системы видеонаблюдения не обеспечивают. Концептуальная проблема не только в отсутствии высокоэффективных интеллектуальных систем распознавания образов, но и в большом количестве участников и зрителей спортивных мероприятий. Для решения такого рода вопросов при проведении в 2012 году Олимпиады в Лондоне разрабатываются планы использования меток радиочастотной идентификации (RFID), а также систем глобального спутникового геопозиционирования.

Хотя технологии обеспечения цифровой безопасности постоянно совершенствуются, тем не менее, в силу постоянного роста сложности возникающих угроз, на настоящий момент отсутствует оптимальная модель защищенности инфраструктуры олимпийских объектов. Поэтому развитие системы кибербезопасности Олимпийских игр, по определению, является нетривиальной задачей, решение которой основывается на стратегии управления рисками.

2.2. Управление рисками

На онтологическом уровне управление рисками при организации и проведении Олимпийских игр необходимо рассматривать с позиций:

- функционирования «общества риска» в трактовке Ульриха Бека;
- возрастания террористических рисков при проведении мегасобытий, привлекающих большое внимание, как граждан, так и глобальных средств массовой информации;

---

[6] Man Threatens to Attack Olympic Computers: Would Be Hacker Under Investigation // Associated Press, 2006, 13-th February.

- геофизического и геополитического положения страны, принимающей Олимпийские игры;

- практик функционирования современной бюрократии, уклоняющейся как от возможной ответственности, так и от проявлений инициативы;

- просчетов организаторов игр и руководства международным Олимпийским движением.

Учет вышеупомянутых позиций должен происходить как при разработке планов обеспечения кибербезопасности, так и при их реализации. При этом неизбежно столкновение с реальностью в виде ограниченного бюджета на осуществление мероприятий и постоянно растущими требованиями дополнительного ресурсного обеспечения. Необходимо учитывать гетерогенность состава акторов, которые будут осуществлять делинквентные действия: от искателей острых ощущений от взлома компьютерных систем, этнически ориентированных компьютерных вандалов и промышленных шпионов, до организованных преступных групп террористов и разведывательных служб. Приходится признать невозможность тотальной защиты при осуществлении всех возможных сценариев реализации угроз, тем не менее сами сценарии должны разрабатываться максимально подробно, поскольку от этого зависит подготовленность к принятию в критической ситуации соответствующих практических решений.

Упомянутые процессы сложны и требуют длительного процесса планирования с участием заинтересованной общественности, а уполномоченные правительством лица должны действовать в качестве интеллектуального центра, в котором осуществляется сбор, анализ и сопоставление информации, а также формирование общей картины системных рисков и угроз кибербезопасности. Только через эффективное сотрудничество с независимыми экспертами и коммерческими структурами можно находить ответы на перманентные изменения в развитии технологий и функционировании киберпространства, вырабатывать стратегии противодействия и активной защиты.

2.3. Управление ресурсами

Вопросы, связанные с сетью и обеспечением безопасности данных и каналов передачи цифрового контента, а также обеспечением деятельности структур кибербезопасности являются относительно новым явлением и это важно учитывать при осуществлении стратегического планирования. На политическом уровне проблема не столь однозначна как может показаться, поскольку обеспечение информационной безопасности неизбежно приводит к необходимости перераспределения ограниченных ресурсов, что в свою очередь сопровождается многочисленными конфликтами с акторами ответственными за проблематику традиционных сфер обеспечения безопасности.

Сегодня в политическую терминологию вошла дефиниция «кибервойна» и этот факт нельзя забывать при осуществлении информационной защиты Олимпиады. В некоторых странах в последние годы активно создаются кибервойска для ведения боевых действий в интернете. В октябре 2010 года в полную силу заработало киберкомандование США (US Cyber Command) со штатом более 1 тыс. человек. Специальные киберподразделения есть у Великобритании, Китая, Израиля и Индии. Россия же, как рассказывал журналистам в июле 2011 года глава департамента МИД РФ по вопросам новых вызовов и угроз Илья Рогачев, по уровню инвестиций в технологии и кадры для борьбы в киберпространстве заметно отстает от зарубежных игроков[7]. Хорошо сказано, но факты свидетельствуют, что сказано дипломатически деликатно.

Ограниченность ресурсов направляемых на обеспечение кибербезопасности является одной из дисфункциональных детерминант любых крупных международных

[7] Цит. по: Черненко Е., Габуев А. Россия указала выход для интернета. Совбез и МИД придумали, как установить мир и порядок в киберпространстве // Коммерсантъ, 2011,№178 (4719), 23.09.

соревнований. Один из уроков проведения в 1996 году Олимпиады в Атланте состоит в том, что даже крупные инвестиции в сферу безопасности не могут гарантировать тотальную защищенность.

Важно учитывать, что противостояние осуществляется не на уровне финансовых ресурсов, направляемых на защиту или же террористами на создание угроз безопасности, но прежде всего на уровне интеллектов, поскольку угрозы носят ассиметричный характер. Тем более что за годы подготовки к Олимпиаде у террористов и иных делинквентно ориентированных акторов есть время продумать новые схемы нападений и обеспечить соответствующую логистику.

Огромные логистические преимущества акторов, кто заинтересован в планировании террористических актов во время проведения Олимпиады, позволяют создать соответствующую инфраструктуру за несколько лет до начала соревнований, осуществить наблюдения за действиями служб безопасности и установить контакты с лицами, обладающими инсайдерской информацией.

Будучи не в состоянии обратить внимание на новые тенденции в хакерских сообществах, бюрократия тем самым создает проблему обеспечения национальной безопасности. При этом речь должна идти не только о менеджменте непосредственно международных соревнований, но и о структурах обеспечения функционирования государства в целом.

3. Проблемные аспекты российской нормативной базы обеспечения кибербезопасности зимних Олимпийских игр в Сочи

«Где мудрость, которую мы потеряли в знании?
Где знания, которые мы потеряли в информации?»
Томас Стернз Элиот[8]

На взгляд автора настоящей статьи и с учетом международного опыта каждый стратегический документ в сфере кибербезопасности должен учитывать существование пяти уровней, на которых возможны угрозы компьютерным системам:

1. Уровень индивидуальных пользователей, малого бизнеса, локальных масс-медиа и муниципальных органов управления.
2. Уровень крупных и средних предприятий, а также общенациональных масс-медиа.
3. Уровень критической инфраструктуры государства.
4. Уровень государственных структур.
5. Уровень коммуникации с глобальными телекоммуникационными сетями.

Поскольку защищенность любой системы определяется степенью защиты наиболее слабого из ее элементов, то государство должно реализовывать киберстратегию не только и не столько с позиций защиты своих объектов, но исходя из системного принципа и в интересах общества в целом. Как далее по тексту будет нами показано, в стране явно недостаточно уделяется вопросам кибербезопасности.

Реализуемая сегодня политическая линия по обеспечению кибербезопасности страны не способна не только способствовать уменьшению числа атак на компьютерные системы, но и на практике в процессе появления в национальной инфраструктуре все большего числа уязвимостей де-факто стимулирует такие атаки. Важнейшим документом в сфере безопасности является «Доктрина информационной безопасности», утвержденная Президентом Российской Федерации В.В. Путиным 9 сентября 2000 г., № Пр-1895. За прошедшее десятилетие, в части нейтрализации киберугроз этот документ однозначно устарел, однако его пересмотр даже не ставится в общественную повестку дня.

---

[8] Thomas Stearns Eliot, 1888 —1965, американо-английский поэт, драматург и литературный критик, лауреат Нобелевской премии по литературе 1948 года.

Зарубежные эксперты утверждают, что в Интернете «год» идентичен трем календарным месяцам – настолько быстро развиваются телекоммуникационные технологии. Поэтому только перманентный процесс выявления и нейтрализации новых угроз и рисков позволит хоть в какой-то мере соответствовать реалиям развития технологий.

Вести речь о реальных достижениях в вопросах международного сотрудничества в сфере кибербезопасности также не приходится. Россия не стала присоединяться к Будапештской конвенции Совета Европы 2001 года по борьбе с киберпреступностью, ратифицированной 31 страной (еще 16 подписали, но пока не ратифицировали этот основополагающий документ). Правящую элиту не устраивает записанное в документе право спецслужб одних стран проникать в киберпространство других стран и проводить там операции, не ставя местные власти в известность. Не случайно отсутствует информация о международном сотрудничестве нашей страны по обеспечению кибербезопасности предстоящей в Сочи Олимпиады.

Отсутствие системы обеспечения коллективной кибербезопасности однозначно является системной дисфункцией и выход необходимо искать максимально оперативно. В этом отношении в связи с напряженными отношениями между Россией и Великобританией маловероятно, что достоянием российских спецслужб станет опыт британских коллег, накопленный при подготовке летних Олимпийских игр в Лондоне в 2012 году.

Указанный дискурс когнитивной самоизоляции не может соответствовать национальным интересам. Достаточно показательно, что при подготовке к Олимпийским играм в Пекине американское правительство сотрудничало с китайскими властями в вопросах обучения персонала навыкам безопасности, предоставляло консультационные услуги и оборудование»[9]. Общепризнано, что борьба с терроризмом является международной, поэтому ориентация на «квасной патриотизм» однозначно должна быть признана одной из угроз стратегии обеспечения безопасности Олимпиады.

Стратегия эта вызывает, на наш взгляд, больше вопросов, чем дает гарантии в вопросах обеспечения кибербезопасности. Но, может существуют официальные документы в развитии Стратегии? По идее, таким документом должен был бы стать Указ Президента РФ от 14.05.2010 N 594 "Об обеспечении безопасности при проведении XXII Олимпийских зимних игр и XI Паралимпийских зимних игр 2014 года в г. Сочи" (вместе с "Положением об оперативном штабе по обеспечению безопасности при проведении XXII Олимпийских зимних игр и XI Паралимпийских зимних игр 2014 года в г. Сочи").

Почему мы говорим «должен был бы стать», ответ на этот тезис содержится в пунктах 5 и 6 Указа. Цитируем пункт 5. «Оперативному штабу приступить к выполнению возложенных на него задач с 1 января 2012 г.» и только через год(!) как то указано в пункте 6. «Оперативному штабу до 1 января 2013 г.: а) определить конкретные границы территории и акватории, в пределах которых вводятся усиленные меры безопасности, а также, при необходимости, категории граждан, в отношении которых такие меры не применяются; б) представить в Правительство Российской Федерации предложения о порядке финансирования и материально-технического обеспечения усиленных мер безопасности».

Мало того что в важнейшем для обеспечении безопасности документе речь не идет о киберугрозах, так и некоторые пункты вообще не выполнимы, в частности где говорится о границах действия «усиленных мер безопасности», поскольку до настоящего времени не определены границы национального сегмента киберпространства(!), что само по себе является в условиях принятия нормативных актов юридическим нонсенсом. Министерства и ведомства, указанные в Положении об оперативном штабе и в которые обратился автор настоящей статьи, так и не смогли что-либо конкретно сообщить о своих практических

[9] Kay D.J. Engaging the ‘New China’ // National Security Watch, 2008, September 2. PP. 1-26. P. 8.

действиях, предпринимаемых уже сегодня в вопросах обеспечения информационной защиты Олимпийских игр.

А ведь кроме организационных мер необходимо сформировать инфраструктуру обеспечения кибербезопасности Олимпиады. Может в практических действиях все учтено? За ответом на этот вопрос обратимся к «Постановлению Правительства РФ от 29 декабря 2007 г. N 991 "О Программе строительства олимпийских объектов и развития города Сочи как горноклиматического курорта" (с изменениями от 11 июня, 6, 7 ноября, 31 декабря 2008 г., 26 февраля, 27 июля 2009 г., 19 января, 5 февраля, 4, 25 марта, 22 апреля, 1, 10 июня, 28 июля, 18 августа, 8 сентября 2010 г.). В многостраничном документе Федеральное агентство связи определено ответственным исполнителем по строительству следующих олимпийских объектов инфраструктуры связи:

№№ поз.	Наименование объекта	Срок начала строительства объекта	Срок окончания строительства объекта
110	Сеть радиосвязи стандарта «Тетра», включая абонентское оборудование	июнь 2010	октябрь 2012
112	Волоконно-оптические линии передачи от г.Анапы до пос. Джубга, от пос. Джубга до г.Сочи с ответвлением от пос. Джубга до г.Краснодара	июнь 2010	декабрь 2011
113	Центр оперативного управления по обеспечению безопасности и правопорядка	октябрь 2010	октябрь 2012
114	Почтовое отделение в пос. Красная Поляна	июнь 2010	август 2011

Рассмотрим подробнее, о чем идет речь в вопросах кибербезопасности Олимпиады. Сеть профессиональной подвижной радиосвязи стандарта «ТЕТРА» рассматривается как составная часть региональной и городской инфраструктуры безопасности и управления службами. Ее назначение - обслуживания олимпийских объектов и олимпийских команд, обеспечение взаимодействия силовых структур при выполнении задач обеспечения безопасности и поддержания правопорядка, обеспечения управления движением, управления коммунальными службами и многое другое. Планируемая абонентская база сети составляет 25 000 абонентов, 10 000 из которых зарезервированы за Международным олимпийским комитетом. Финансирование мероприятия: средства федерального бюджета в размере 2 197, 515 млн. рублей.

Центр оперативного управления по обеспечению безопасности и правопорядка является точкой, куда будет стекаться вся информация, необходимая для обеспечения безопасного проведения Олимпийских игр. Финансирование мероприятия: средства федерального бюджета в размере 2 496,93 млн. рублей.

Согласно плану, на территории города и олимпийских объектах будут установлены видеокамеры наблюдения, датчики, реагирующие на пожары и аварии на газопроводах или теплосетях. На транспортных средствах государственных и муниципальных служб будут установлены датчики системы ГЛОНАСС, которые позволят унифицировать сбор данных о месте нахождения любого транспортного средства, обеспечат централизованное управление логистикой перевозок грузов и гражданского населения, станут составной частью системы управления дорожным движением и многое другое.

Транспортной средой для сбора и передачи данных соответствующим оперативным службам станет магистральная ВОЛП и сеть «ТЕТРА». В послеолимпийский период объект планируется использовать в рамках программы обеспечение комплексной безопасности г. Сочи «Безопасный город». Очевидно, что почтовое отделение как сеть волоконно-оптической связи к кибербезопасности имеют далекое отношение, а иные инфраструктурные объекты только фрагментарно решают вопросы обеспечения информационной безопасности предстоящих Олимпийских игр.

Ни в полпредстве президента на Юге России, ни в других уважаемых государственных структурах ничего не смогли конкретного сказать о мерах по подготовке информационной защиты Олимпиады в Сочи. Все кивали на ФСБ. О том, что ФСБ не единственное ведомство, отвечающее за кибербезопасность, чиновники предусмотрительно умалчивали, зная, что в регионах ФСБ обеспечивает информационную безопасность всего лишь нескольких объектов. Необходимо признать, что в силу ограниченности ресурсов (в том числе и кадровых), это ведомство не в состоянии решить стратегическую задачу защиты Олимпийских игр в Сочи от кибератак и нейтрализации их последствий.

В своей ставшей популярной книге «Логика политического выживания» (The Logic of Political Survival) Брюс Буэно де Мескита и его соавторы утверждают: «Хорошая политика с точки зрения страны может быть плохой политикой с точки зрения властей, и наоборот»[10]. В полной мере вышеуказанное может быть применено к рассматриваемой нами проблематике, поскольку в вопросах кибербезопасности бюрократия не желает ориентироваться на примат меритократического дискурса, сделав ставку на патрон-клиентские сети, базирующиеся на личном доверии. Такой подход вынуждает правящую элиту использовать «ручное управление», которое в случае долгосрочных проектов перманентно дает сбои.

Сегодня в России нет такого ведомства, которое бы обладало точной или хотя бы неточной, но всеобъемлющей информацией о характере киберугроз, не говоря уже об отсутствии парадигмы управления рисками в информационной сфере. Далее мы рассмотрим основные проблемы, которые требуется решить для обеспечения кибербезопасности Олимпиады.

4. Требующие решения стратегические проблемы в сфере обеспечения кибербезопасности Олимпиады в Сочи

«Нет ничего более трудного
что можно было бы взять в руки,
более рискованного, чтобы реализовать на практике
или более сомнительного в достижении успеха,
чем взять на себя инициативу по введению
нового порядка вещей»
Николо Макиавелли

4.1. Онтологические проблемы обеспечения кибербезопасности

Приведенные автором политические факты неизбежно приводят к постановке концептуального вопроса: насколько эффективной является российская политика в сфере информационной защиты проведения Олимпийский игр и развертывания государственных инфраструктурных проектов в сфере телекоммуникаций, к примеру, таких как «электронное правительство»? Однозначный ответ – существующая политика не отвечает не только требованиям развития технологий, но и создает угрозы национальной безопасности.

Разрозненные мероприятия отдельных ведомств не могут изменить ситуацию в силу причин, о которых далее пойдет речь. Основная детерминанта дисфункциональности заключается в том, что уполномоченные государством должностные лица не считают проблему кибербезопасности заслуживающей особого внимания. Такой дискурс хотя и противоречит упомянутому нами выше зарубежному опыту обеспечения безопасности крупных международных соревнований, тем не менее, отражает общее отношение чиновников разного уровня к формированию в стране «общества знаний».

[10] Bueno de Mesquita B., Smith A., Siverson R.M., Morrow J.D. The Logic of Political Survival. Cambridge: The MIT Press, 2003.

Проблема, о которой идет речь, заслуживает отдельного исследования, сейчас же упомянем ее важнейшие аспекты. К ним относятся:

1. Упущенные сроки развертывания систем киберзащиты и осуществления научно-практического анализа путей обеспечения информационной безопасности зимних Олимпийских игр в Сочи.

2. Отсутствие навыков анализа стратегических угроз и рисков связанных с развитием инновационных технологий и их использованием террористами в противодействии государству и его гражданам.

3. Низкий уровень информационной культуры и широкое распространение функциональной неграмотности, негативно сказывающейся как на восприятии новых технологий, так и возможностей их использования в процессе осуществления модернизации.

4. Отсутствие практически на всех уровнях управления механизмов экспертного анализа тенденций в сфере осуществления противоправных действий в области телекоммуникаций и выработке мер проактивной защиты.

5. Отсутствие понимания, каким образом можно создать систему стимулов и мотиваций, как для коммерческих организаций, так и для структур гражданского общества, а также отдельных граждан участвовать в обеспечении информационной безопасности страны.

Результатом упомянутых системных дисфункций стало отсутствие полноценной стратегии государства в обеспечении кибербезопасности предстоящей Олимпиады в частности и непонимание возможных угроз при развертывании иных масштабных государственных проектов в сфере телекоммуникаций. Достаточно показательно, что ни на одном уровне представительной власти - от муниципального до федерального, не обсуждаются вопросы обеспечения кибербезопасности. Отсутствие понимания создает ложное чувство отсутствия проблем.

Широко распространено заблуждение: поскольку до настоящего времени не было кибератак с масштабными последствиями, то отсутствует и необходимость противостоять этой форме терроризма. Достаточно показательно, что еще в 2001 году чеченские террористы под руководством Хаттаба пытались путем засылки «троянских» компьютерных программ похитить средства у десяти европейских банков. Нет сомнения, что аналогичные действия будут совершаться и во время проведения международных спортивных соревнований.

Применительно к предстоящей Олимпиаде необходимо вспомнить и заявления руководства Грузии с угрозами сорвать международный спортивный форум. Достаточно вспомнить события августа 2008 года и мощное информационное воздействие Грузии на медиаресурсы Южной Осетии, а также максимальное использование созданных заблаговременно для освещения военных действий информационных центров на территории Грузии, в частности специального медиацентра для иностранных журналистов в городе Гори. Результаты той информационной войны до сих пор не учтены в практике российской политической элиты.

Очевидно, что в случае кибернападений, к примеру, на олимпийские объекты, масс-медиа по всему миру начнут генерировать интерпретации и осуществлять борьбу за их смыслы. При этом террористы могут скорректировать свою тактику в целях удовлетворения потребностей средств массовой информации.

Тот факт, что сегодня большинство хакеров, которые эксплуатируют уязвимости компьютерных систем, ощущают нехватку политической мотивации для своих противоправных действий, а также в дефицит ресурсного обеспечения, необходимых знаний и инструментов для кибератак, не означает отсутствия государственных и иных акторов способных обеспечить решение вышеупомянутых проблем в интересах подрыва имиджа России во время проведения зимних Олимпийских игр в Сочи.

4.2. Возможные политические последствия кибератак на олимпийские объекты

Сегодня иррациональная потребность бюрократии в безопасности и стабильности проявляется лишь в офлайне, в то время как неосязаемые угрозы из киберпространства подавляющим большинством чиновников игнорируются на ментальном уровне. Пока не произойдет системного сбоя в национальной безопасности, никто не станет воспринимать политические риски, связанные с кибератаками на объекты зимней Олимпиады в Сочи.

Очевидно, что в складывающихся условиях дабы отсрочить ответственность, отечественная бюрократия для высшего руководства страны на разных уровнях будет плодить связанные с обеспечением кибербезопасности мифологические нарративы. Как известно и как автор доказал опираясь на факты, огромные средства, закачанные в подготовку Олимпиады в Сочи могут обернуться крупным имиджевым провалом. И это неизбежно, если уже в ближайшее время не будут предприняты решения и практические действия по созданию современной системы информационной безопасности.

Другой вопрос, что отсутствуют политические и бизнес акторы способные не только озвучить проблему, но и предложить не частные, а действительно всеобъемлющие планы противодействия существующим и потенциально возможным угрозам. Речь должна не только и не столько об Олимпиаде. Непринятие мер по нейтрализации возможных угроз приводит к увеличивающейся уязвимости компьютерных систем, обеспечивающих на инфраструктурном уровне экономику и национальную безопасность, при этом последствия для имиджа отвечающих за Олимпиаду высших руководителей страны не волнуют чиновников, которым за это еще предстоит нести личную ответственность.

Вместо заключения. Виртуальный подарок для отечественной бюрократии

«С чем борешься, на то и повязан будешь»
Сева Новгородцев

На одном из последних заседаний организационного штаба незадолго до открытия летних 1996 года Олимпийских игр в Атланте, вице-президент США Альберт Гор прервал выступление представлявшего ФБР докладчика простым вопросом: «Кто несет ответственность?» Когда никто из присутствующих не озвучил ответ, тогда Гор снова задал вопрос и участники совещания мудро решили, что «все зависит от ситуации»[11]. Россия не Америка?..

Выходные данные публикации в печатном виде:
Бондаренко С.В. Риски и угрозы кибербезопасности зимних Олимпийских игр в Сочи / Зимние Олимпийские игры 2014 в Сочи в фокусе информационных атак. Сборник научных статей /Отв. Ред. В.В. Черноус / Южно-Российское обозрение Центра системных региональных исследований и прогнозирования ИППК ЮФУ и ИСПИ РАН. Вып. 69. Москва-Ростов-на-Дону: Социально-гуманитарные знания, 2011. С. 125-145.

[11] Цит. по: Bellavita C. Changing Homeland Security: A Strategic Logic of Special Event Security // Homeland Security Affairs, 2007, vol. 3, № 3. P. 11.

КИБЕРБЕЗОПАСНОСТЬ ОЛИМПИАДЫ. ПРОДОЛЖЕНИЕ

Бондаренко С.В.,
доктор социологических наук,
Ростов-на-Дону

Вместо введения.

Штирлиц: «Нас всех губит отсутствие дерзости
в перспективном видении проблем».
Юлиан Семенов,
«Семнадцать мгновений весны»

Уже была написана, но еще не вышла в журнале предыдущая статья «Риски и угрозы кибербезопасности зимних Олимпийских игр в Сочи», а ее текст начал свою собственную жизнь. Читая рукопись эксперты, включая работающих в очень серьезных государственных структурах, недоумевали: как могло вообще произойти, что важнейшее мероприятие глобального уровня фактически оказалось без системной киберзащиты? Факты многократно перепроверялись и… находили подтверждение, тем не менее, непонимание причин феномена оставалось, что и послужило социальным запросом на написание второй статьи, которую вы читаете.

Любого, кроме разве что ортодоксальных консерваторов отрицающих необходимость непредвзятого восприятия объективного мира, поражает насколько не изучена, а также не воспринимается людьми облеченными принимать решения сама ситуация защищенности России от киберпреступности и кибертерроризма. И в этой статье в силу объективных ограничений на ее объем невозможно дать обстоятельные ответы на извечные русские вопросы: кто виноват и, что делать? Поверьте, список фамилий виноватых займет не один десяток страниц мелким шрифтом (что в России однозначно, хотя и спорно трактуется как - виновных нет вообще, при этом, все знают, что в случае чего стрелочник всегда найдется).

Трактат, в котором будет представлен ответ на второй вопрос - «что делать», по нашему мнению, должен носить скромное название, типа «Стратегия кибербезопасности России на период до…». Пока же, в отличие от многих других стран, у нас такой стратегии нет, а что есть вместо нее - об этом и пойдет речь. При этом автор не отрицает существование множества отдельных мероприятий в сфере криптозащиты и прочей-прочей деятельности, которой заняты госструктуры, включая противодействия хакерам, а также иным злоумышленникам. Речь не об отдельных фактах, а о СИСТЕМЕ кибербезопасности страны, составной частью которой является безопасность предстоящей Олимпиады.

Полезно время от времени задавать вопросы о состоянии той или иной сферы общественных интересов, чтобы помочь лицам, принимающим решение осмыслить объективные реалии с целью принятия соответствующих политических и инфраструктурных решений в быстро изменяющейся глобальной окружающей среде. Может предыдущее предложение кому-то покажется банальным, для разъяснения его мы начнем выявлять причинно-следственные связи с типичного информационного хаоса, когда отдельные факты, связанные с развитием информационных технологий не складываются в сознании ответственных лиц в непротиворечивую картину мира.

1. Информационный хаос или отражение дисфункций системы информационной безопасности страны

«В разговоре с женщиной есть один болезненный момент.
Ты приводишь факты, доводы, аргументы.
Ты взываешь к логике и здравому смыслу.
И неожиданно обнаруживаешь, что ей
противен сам звук твоего голоса...».
С.Д. Довлатов

Итак, его Величество факты. Ниже мы представим разного масштаба эмпирические данные, а в следующих параграфах мы объясним, как они между собой связаны и, причем здесь кибербезопасность страны в целом и зимней Олимпиады в Сочи, в частности. Подчеркнем: кибербезопасность должна рассматриваться гораздо шире, чем проблема отрасли ИКТ, чего в России, увы не понимают. Итак:

- Третье десятилетие, несмотря на огромные финансовые затраты никак не может быть запущена в повседневные практики миллионов граждан страны система геопозиционирования ГЛОНАСС. Американцы начали позже нас, но их GPS давно работает в мобильных телефонах россиян и спутниковых автомобильных навигаторах, а технологии геопозиционирования широко используются не только государственными структурами, но и некоммерческими организациями. В России же сегодня акцент в большей мере делается на системы мониторинга транспорта (при этом как для чиновников, так и для граждан самое непонятное – кем, когда и зачем будет аккумулироваться, анализироваться и использоваться информация которая будет идти через эту систему, не говоря уже о кибербезопасности). В частности, предлагается установить приемники ГЛОНАСС на железнодорожные локомотивы, якобы чтобы знать, где они находятся в каждый момент времени. Однако аналогичная технология геопозиционирования на железных дорогах успешно применяется более 50(!) лет и где находятся поезда диспетчерам отлично известно и без ГЛОНАСС.

- В сфере компьютеризации за последние десятилетия ни один общенациональный государственный инфраструктурный проект не был реализован как то необходимо для модернизации страны. Достаточно вспомнить неоднократные перезапуски Единой государственной автоматизированной информационной системы (ЕГАИС), которая по замыслу должна обеспечить прозрачность производства, импорта и реализации спиртного в России. Одним из разработчиков этой системы в свое время была структура ФСБ, что не явилось гарантией качества программного продукта.

- Второе десятилетие в России официально создается «электронное правительство» и делается это без какой-либо фундаментальной научной базы. Медлительность чиновников вызывает справедливое возмущение высшего руководства, тем не менее, несмотря на многочисленные хвалебные рапорты должностных лиц, по уровню развития этой технологии мы существенно отстаем даже от стран с более низким технологическим потенциалом. В этом отставании закодировано сегодняшнее и будущее отставание в области ИТ-технологий, в том числе и в сфере кибербезопасности.

- Как упомянуто в предыдущем абзаце, существует проект создания «электронного правительства», но при этом нет концепции «электронных муниципалитетов» (которая разрабатывается энтузиастами без всякой надежды, что Родина востребует этот труд). Обратим внимание, что на уровне Конституции страны государственная и муниципальная власть в России формально разделены, а зарубежный опыт свидетельствует, что 50% доходов муниципалитеты получают от использования информационных технологий. В России же большинство муниципалитетов нищие, а компьютеры используются, в лучшем случае, в качестве пишущих машинок и для получения электронной почты (а также для

просмотра, скажем так, не служебной информации из Интернета, вместе с которой в системы попадают вирусы и трояны).

- Политические лидеры государства на регулярной основе артикулируют свою позицию по самым актуальным проблемам формирования основ информационного общества, однако на региональном и муниципальном уровнях идет сопротивление выполнению соответствующих решений. К примеру, раз в три года государственные и муниципальные гражданские служащие должны проходить аттестацию, однако ни о каком знании современных информационных технологий во время аттестации речь не идет (в Ростовской области считается, что достаточно познаний основ школьного и институтского курса «Информатики»). В соответствии с существующей системой рейтингования развития «электронного правительства», субъект Федерации может занимать высокие места, даже если подавляющее большинство чиновников не имеют представления не то что об «электронном правительстве» и кибербезопасности, а и о применении компьютерных технологий для развития территорий (не говоря уже о «формировании основ информационного общества»).

Такого рода факты можно приводить достаточно долго. Эффект может быть один: читатель перестанет удивляться тому, что предстоящая Олимпиада практически не защищена от исходящих из киберпространства угроз. Но, остается вопрос: почему же такое возможно, несмотря на существование множества уполномоченных государством ведомств. И так, кто за что отвечает…

2. Кто отвечает за кибербезопасность страны и ее граждан

«Разгадывая, как работают телеграфные столбы
и провода, мы ничего не поймем в сути сообщений».
Сергий Булгаков

Перед тем как найти ответ на самый важный вопрос, еще раз подчеркнем, что речь не идет об оценке деятельности организаций, о которых пойдет речь ниже. Для автора важнее понимание системных аспектов кибербезопасности и имеется ли в России координирующий орган, способный решать вопросы информационной безопасности государства. Но для начала определимся со смыслом понятия «системный подход».

«Системный подход означает, что деятельность отдельных предприятий (подсистем) должна изучаться как часть системы более высокого иерархического уровня с учетом внутренних и внешних связей. При этом оценивать деятельность изучаемого объекта следует не только с точки зрения достижения его локальных целей, но и обязательно с позиций того, насколько эти цели согласуются с целями системы более высокого иерархического уровня и интересами общества в целом. При системном подходе возможна суперпозия (наложение) технологических процессов подсистем, возможно упрощение системы, а иногда и отпадает необходимость в некоторых элементах.

Можно выделить несколько иерархических уровней: объект (здание), предприятие, населенный пункт, регион. Особенно велика значимость системного подхода на самом высоком уровне – уровне государства. Если говорить о масштабах всей страны, то здесь необходима системность и более высокого уровня»[12]. Именно о системности такого уровня мы и будем вести речь.

Позволим сформулировать гипотезу, в соответствии с которой направляемая руководителям информация страны о состоянии кибербезопасности проходит через многочисленные чиновничьи фильтры и потому складывается мнение о благополучии, на основе которого и принимаются стратегические решения, в том числе в вопросах оценки характера угроз и возможностей их нейтрализации. На самом же деле…

[12] Лелюшкин Н.В. Запрограммированная бессистемность // Независимая газета, 2011, 11 октября.

2.1. Федеральная служба безопасности России и проблема кибербезопасности

«Мне жена говорит: «Витя, заткнись.
На тебя рано или поздно наедет самосвал».
Виктор Геращенко,
экс-глава Центрального банка РФ

Когда речь заходит о ФСБ, даже у самых разговорчивых соотечественников просыпается генетический страх, смешанный с мистическо-патерналистским отношением к могущественной спецслужбе, о деятельности которой мы так мало знаем (несмотря на появление сайтов, а также редких пресс-релизов о задержаниях шпионов). Какое отношение это ведомство имеет к кибербезопасности? Самое прямое, ибо его сотрудники осуществляют киберзащиту госструктур.

Как мы писали в первой статье, в соответствии с Указом Президента РФ от 14.05.2010 N 594 "Об обеспечении безопасности при проведении XXII Олимпийских зимних игр и XI Паралимпийских зимних игр 2014 года в г. Сочи" (вместе с "Положением об оперативном штабе по обеспечению безопасности при проведении XXII Олимпийских зимних игр и XI Паралимпийских зимних игр 2014 года в г. Сочи") руководителем оперативного штаба должен быть именно представитель ФСБ. Жаль, что в указе Президента ничего не сказано о кибербезопасности, может соответствующие мероприятия проходят в рамках обобщенно сформулированных задач?

Хотелось бы в это верить, но в состав штаба не включены представители министерств и ведомств, имеющих непосредственное отношение к сфере связи. Странно это, так и шевелится подозрение, что в сфере информационной защиты нечто важно не учтено. Но не привыкла ФСБ обсуждать такие вопросы с общественностью, а жаль, поскольку только через мобилизацию бдительности всех участвующих в подготовке и проведении Олимпиады можно снизить уровень угроз. Для этого, к примеру, уже сегодня нужно проводить компьютерный ликбез с гражданами и чиновниками. Но такая просветительская работа не входит в сферу деятельности ФСБ. И это не единственное слабое звено в киберзащите предстоящих игр, как, впрочем, и государственных информационных систем.

Может автор уже и надоел читателю с периодическим подчеркиванием того, что речь не идет об оценке оперативной и иной деятельности ведомств, а только о системных проблемах в сфере, прежде всего, национальной кибербезопасности. Но, соблюдение техники безопасности дело всегда актуальное. Что-то же делается в вопросах защиты компьютерных систем.

Так, ФСБ осуществляет лицензирование в сфере к некоторым объектам связи, противодействует кибернападениям, однако концептуальный вопрос в ином: отвечает ли осуществляемая деятельность современным реалиям. К примеру, в сфере криптозащиты у нас со времен СССР много достижений, при этом упускается из внимания, что технологии шифрования используются сегодня даже в мобильных телефонах, не говоря уже о компьютерах. Времена изменились и необходимо защищать не только отдельные государственные структуры, но и граждан, а также коммерческие тайны бизнеса. Реальность же такова, что силовые структуры сейчас являются реципиентом передовых технологий разработанных за рубежом, а не их донором, хотя при этих структурах существуют научно-исследовательские организации прикладного профиля. В той же ФСБ имеется научно-техническая служба, а также специализированные исследовательские институции.

Наверняка действуют эти структуры в соответствии с поставленными задачами, на которые из бюджета им выделяются определенные средства, которыми они (в соответствии с неписанными законами бюрократической системы), ни с кем из смежных

ведомств не делятся. Периодически в прессе появляются сообщения о миллионах кибернападений, которые удалось отбить сотрудникам ФСБ. При этом ничего не сообщается о том, удалось ли злоумышленникам, преодолев многочисленные барьеры проникнуть в государственные системы. А без таких сведений сложно судить, насколько качественна киберзащита и что нужно сделать для повышения ее эффективности.

Зарубежный же опыт свидетельствует, что преодолеть можно все и не спасает от утечек и кибернападений даже отрезанный от компьютерных сетей бункер. По данным немецких экспертов каждые две секунды в интернете появляется новая вредоносная программа, каждый день совершается 4-5 попыток внедрения троянов в правительственную сеть. Раз в неделю в Германии подобная атака - обычно из-за рубежа - оказывается успешной[13]. В России же даже в профессиональном сообществе не узнаешь о подобных фактах, хотя ситуация в сфере кибербезопасности далеко не благостная.

Показательно, что в регионах ФСБ обеспечивает киберзащиту всего нескольких государственных объектов. Даже если допустить, что эта защита эффективна (что как мы видим по зарубежному опыту далеко не всегда так), уровень защиты всей системы государственных структур определяется защищенностью самого слабого звена и этот уровень не выдерживает критики. Три четверти государственных структур не имеют в своем штате специалиста по программному обеспечению, не говоря уже о профессионалах в сфере кибербезопасности. У вас есть еще сомнения в защищенности государственных систем?..

Независимый ИТ-аналитик Максим Букин в одном из интервью заявил, что в России правительственные структуры ощущают на себе постоянный гнет кибератак. Эксперт не стал приводить примеры атак и методов, используемых хакерами против российских сайтов. Но отметил, что наши сети пробуют на прочность китайцы, американцы, индийцы...[14] При этом, к примеру, те же индийцы сами становятся объектами кибератак. Так, группа хакеров из Китая в течение восьми месяцев воровала секретные данные с компьютеров министерства обороны Индии. В ходе расследования удалось установить, что помимо сетей, расположенных на территории Индии, взлому подверглись компьютеры индийского дипломатического представительства и в Москве[15]. Вы уверены, что у нас невозможен свой WikiLeaks?..

Если уверены, то тогда Агентство национальной безопасности США (с бюджетом $15 млрд. в 2009 году) идет к вам и к нашим общим государственным и муниципальным структурам! У этого ведомства для перехвата на территории России информации существует специальный центр разведки (крупнейший из всех существующих у АНБ), расположенный недалеко от Аугсбурга (Германия). Если как гласит народная молва у нас в информационной сфере нечего красть, то на что тратятся деньги американских налогоплательщиков? Уж в этом отношении, Россия точно не Америка! Или, может мы не хотим понимать ценность информации, не только там где она официально признанна секретной?

Подведем итоги. ФСБ самое главное ведомство в вопросах кибербезопасности, но оно не отвечает в соответствии с действующим законодательством за безопасность страны в целом. Страна это не только госструктуры, но и бизнес, граждане и некоммерческие организации, без которых в современном мире невозможно обеспечить информационную защиту. Так-то оно так, но теплится надежда: может иные министерства и ведомства обеспечивают безопасность государства…

---

[13] Sagatz K. Bund rüstet gegen digitalen Angriff // Tagesspiegel, 2011, 24.02.

[14] Цит. по: Терехов А. Хакеры добрались до российско-индийских секретов // Независимая газета, 2010, 04.07.

[15] Markoff J., Barboza D. Researchers Trace Data Theft to Intruders in China // The New York Times, 2010, 05.04.

2.2. Министерства и ведомства как акторы системы киберзащиты

«Всему готовому, совершенному поклоняются,
все становящееся недооценивается».
Фридрих Ницше

Государство декларирует: расходы на оборону и безопасность являются высшим приоритетом, при этом на практике вопросы информационной безопасности остаются на обочине проводимой политической линии. Забывается, что речь идет об *уязвимостях*, использование которых позволяет потенциальному противнику нейтрализовать любые системы защиты. Сегодня в России даже защита гражданской телекоммуникационной инфраструктуры является проблематичным вопросом для правительства, хотя государственные и муниципальные структуры широко используют коммерческие каналы связи.

Логично было бы узнать, что же делают в вопросах обеспечения информационной безопасности министерства и ведомства, имеющие прямое отношение к телекоммуникациям, куда автор статьи и обратился. В Министерстве связи и массовых коммуникаций РФ автору прямо сказали, что данным вопросом они не занимаются и при этом посоветовали сделать запрос в Федеральное агентство связи (Россвязь). Заместитель руководителя упомянутого агентства А.В. Костиков в частности, в ответе автору сообщил: «…в соответствии с Положением о Федеральном агентстве связи, утвержденным постановление Правительства РФ от 30.06.2004 № 320, *вопросы информационной безопасности не входят в полномочия Россвязи*» (выделено нами *С.Б.*).

Как такое может быть? В упомянутом Положении говорится: «Федеральное агентство связи (Россвязь) является федеральным органом исполнительной власти, осуществляющим функции по управлению государственным имуществом и оказанию государственных услуг в сфере электросвязи и почтовой связи, в том числе в области создания, развития и использования сетей связи, спутниковых систем связи, систем телевизионного вещания и радиовещания». И все вышеуказанное оказывается в информационном отношении не защищено!!!

В настоящее время во всем мире право на тайну связи считается составной частью прав человека. В России право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений гарантировано 23 статьей Конституции.

Всем операторам связи в России предъявляются требования согласования плана мероприятий по внедрению «СОРМ» (система оперативных мероприятий спецслужб)[16], в противном случае их лицензия может быть аннулирована. Теперь читатель понимает, в чем разница между отдельными мероприятиями ведомств и сферой кибербезопасности страны и Олимпийских игр в Сочи, в частности.

Действующая власть не одно десятилетие находится в процессе укрепления партнерских отношений с бизнесом, однако в вопросах обеспечения безопасности киберсреды не продвигаясь при этом ни на шаг. Российская элита не обладает, по всей видимости, потенциалом необходимым для решения системной проблемы кибербезопасности. В условиях тотальной взаимосвязи сетей, де-факто отсутствует актор, заинтересованный в комплексном развитии систем безопасности, при этом способный преодолевать широко распространенные межведомственные и межотраслевые разногласия.

Если, к примеру, в США согласно метафоре, которую приписывают Рональду Рейгану, правительство не решает проблемы, но оно их финансирует, то в России вопросы кибербезопасности отнесены к прерогативе силовых ведомств и фактически выведены из

[16] Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность». Постановление Правительства РФ от 27 августа 2005 г. N 538.

под общественного контроля, а финансирование их весьма и весьма скромное. Соответственно, для чиновников из остальных ведомств рациональным и прагматичным является не вмешательство в проблематику, за которую они непосредственно не отвечают. В этом онтологическая проблема, без понимания которой все разговоры об информационной безопасности не приводят и не приведут к кардинальным изменениям.

Достаточно показательно, что за прошедшие десятилетия российское государство не определило, где в киберпространстве находится граница его институциональных возможностей и интересов. К примеру, до сих пор нормативные акты, касающиеся сети Интернет, принимаются без определения даже точных границ национального сегмента киберпространства, что является юридическим нонсенсом, на который правоведы предпочитают закрывать глаза. Соответственно, применительно к рассматриваемой нами проблематике нет точного представления о национальных границах обеспечения кибербезопасности – на практике все сводится, в лучшем случае, исключительно к защите периметра локальных объектов.

Общеизвестно, что в инфраструктурные проекты, связанные с компьютеризацией различных сторон функционирования общества закачиваются огромные средства, однако увеличивающаяся сложность развития систем не подкрепляется системными мерами по профилактике возможных угроз. В стране нет ясной системы целей развития системы кибербезопасности и путей их достижения, а бюрократия чаще всего оказывается не способной к конструктивному диалогу с представителями экспертного сообщества.

Подчеркнем, что речь мы ведем не об отдельных нормативных актах и политических действиях, а о необходимости создания перманентно обновляемой системы стратегического планирования и реализации мер по обеспечению информационной безопасности на всех(!) уровнях ее функционирования. Такая ситуация на фоне регулярно появляющихся в прессе сообщений о разработке соответствующих программных документов и организационных мер в США, Великобритании, Франции и других странах вызывает, по меньшей мере, удивление.

В России нет такого ведомства, которое бы обладало точной или хотя бы неточной, но всеобъемлющей информацией о характере киберугроз, не говоря уже об отсутствии парадигмы управления рисками в информационной сфере. Межведомственные барьеры лишь усугубляют ситуацию.

Но, может просвещенное научное знание и система образования могут стать фундаментом обеспечения единства политики государства в вопросах информационной защиты…

2.3. Наука и образование в контексте кибербезопасности

Мюллер в разговоре с сыщиком крипо:
- Всё настолько глупо и непрофессионально,
что работать практически совершенно невозможно.
Невозможно понять логику непрофессионала.
- А может, он хитрый профессионал?
Юлиан Семенов,
«Семнадцать мгновений весны»

Автор еще будет вести речь о мифах, связанных с обеспечением кибербезопасности. Сейчас же отметим, что в обществе существует на уровне коллективного бессознательного убежденность: мол, мы не можем всего знать, тем более в сакральных вопросах, связанных с обеспечением безопасности. Есть на то специальные люди! И готовят тех людей в специальных учебных заведениях.

Да, действительно, есть в стране один институт, где готовят шифровальщиков и о нем пресса неоднократно писала. И при чем же шифровальщики? Как же –

информационная безопасность и секретность! Да… Нескоро до граждан и руководителей разного уровня дойдет актуальность проблемы кибербезопасности, хотя как отмечалось нами ранее каждый компьютер и мобильный артефакт использует алгоритмы криптозащиты, не говоря уже о получающей распространение электронной цифровой подписи, которая и есть шифровальный алгоритм.

В XVII веке в комедии Жан-Батиста Мольера "Мещанин во дворянстве" главный герой с великим удивлением узнал, что вот уже сорок лет говорит прозой. Мольер сравнивал своего героя с вороной в павлиньих перьях. Интересно с кем наши потомки сравнят современников, которые с удивлением могут в любой момент узнать, что они много лет пользуются системами криптозащиты, не имея при этом ни малейшего представления, как о самих системах, так и об основах кибербезопасности…

Четыре столетия разделяют упомянутые общие модели поведения. Может сегодня вопрос не в компьютерных артефактах, а в системных дисфункциях образования? Соответствующие устойчивые знания и навыки должны формироваться в школе, но у нас этого не делается не только там, но и в подавляющем большинстве университетов. К примеру, на Юге России два федеральных университета, которые практически не готовят специалистов способных решить проблемы кибербезопасности. Соответственно, о каком влиянии этих центров знаний на информационную защищенность Олимпийских игр можно вести речь?!

Если за рубежом половина специальностей по тематике ИКТ носят гуманитарный характер, то в России практически на эмбриональном уровне не то что преподавание, но даже научные исследования, имеющие прямое отношение к рассматриваемой нами проблематике. И это в то время когда технологии информационных, управляющих, навигационных систем относятся к числу критически важных для страны (в соответствии с Указом Президента РФ от 7 июля 2011 г. N 899).

Отсутствие внимания к знаниеемким отраслям со стороны государства само по себе препятствие в формировании «информационного общества». Россия давно утратила технологическую независимость в сфере эффективных средств киберзащиты. Такому положению способствует де-факто отсутствие научной базы реализации масштабных проектов в сфере ИКТ, приводящее к перманентному отставанию не только от экономически развитых, но и в ряде случаев и от развивающихся государств.

Утечки документов будут происходить до тех пор, пока в стране используемые ИКТ технологии бездумно используются в качестве приставок к чужим глобальным системам, телекоммуникационным, финансовым и научным. В таких условиях о системной кибербезопасности нельзя вести речь, поскольку на самых разных уровнях существует функциональная неграмотность, в рамках которой компьютер воспринимается исключительно как своеобразная пишущая машинка.

Вспомните факты, которые автор приводил в начале статьи – общее у них как раз функциональная неграмотность исполнителей и пользователей систем. И о какой кибербезопасности можно вести речь, когда нет понимания, что технологии имеют гуманитарную компоненту, без учета которой все делается «на живую нитку».

Не удивительно, что создаваемые в России социально-технологические новации, несмотря на все разговоры о необходимости модернизации, тем не менее, реализуются в других странах. Разве это не угроза национальной безопасности?..

Кроме того, в обществе есть серьезные разрушительные силы, которые уже сегодня используют новейшие телекоммуникационные технологии во вред развитию. Обладают ли политические акторы способностями, позволяющими просеивать технические смыслы, ради корректного социального и политического действия или все сводится к воспроизводству мифов?

3. К чему приводят мифы в сфере кибербезопасности

"Как это ни парадоксально, миф - это
наилучший критерий успеха истории".
Анкерсмит Франклин Рудольф

Один знакомый руководитель банка убежден, что проблем в сфере кибербезопасности не может быть: системы защиты у нас прочны, поскольку развиваются быстрее систем нападения. Аналогичной логики придерживаются и многие чиновники, даже не вникающие как на практике обеспечивается кибербезопасность. В стране есть соответствующие секретные ведомства, которые в случае чего примут меры – такова логика мифологизированного мышления.

Этим людям не имеет смысла приводить факты – для себя они давно опровергли постулаты диалектики развития, в соответствии с которыми в любых сферах защита развивается как ответ на появляющиеся новые угрозы, в противном случае нет стимулов для совершенствования. Такая безалаберность это до поры до времени, пока гром не грянул.

К примеру, в той же банковской сфере каждое финансовое учреждение проводит свою политику в вопросах информационной защиты. И никто не задумывается, а что будет, если эта политика ошибочна и способствует появлению уязвимостей. Забывается, что уже существуют полулегальные рынки, на которых продаются сведения о выявленных брешах в информационной защите и продаются инструменты изощренных кибератак.

Поразительно, но многолетнее замалчивание проблемы кибербезопасности, а также сообщения масс-медиа о фактах киберпреступности способствовали некой когнитивной «прививке» от этой проблемы в сознании даже компьютерного сообщества. В этом контексте не вызывает удивление отсутствие на метауровне понятийного аппарата, позволяющего донести сущность угроз до высших представителей власти. И никакой критической рефлексии, без чего невозможно поступательное развитие.

О мифах связанных со спецслужбами мы уже упоминали, тем не менее, для иллюстрации приведенного тезиса приведем еще один факт. В последние годы западные политики и журналисты на регулярной основе ведут речь о русских кибершпионах.

Так, в докладе американского национального управления контрразведки «Иностранные шпионы, похищающие экономические секреты США в киберпространстве», который был опубликован 3 ноября 2011 года, говорится, что главная опасность исходит от Китая и России, кибершпионы которых похищают секреты Запада. Касательно Китая это, по нашему экспертному заключению, вполне реальная ситуация. В отношении же России вопрос, по меньшей мере, спорный. Мы не станем обращаться в Службу внешней разведки РФ, тем более что там ничего конкретного не скажут, хотя с высокой вероятностью работают там специалисты соответствующего профиля.

Зададимся вопросом, на который вполне можем найти ответ и сами. Допустим, что-то кибершпионы и похитили в сфере технологических секретов. В Китае мощная промышленность и она использует добытую информацию. Спрашивается, а у нас, что делать с такими сведениями? Общеизвестно - промышленность (за редким исключением) отвергает любые инновации и как в таких экономических условиях распорядиться с добытыми сведениями? Правильно, отчеты составлять и не более того!

Миф об успешных русских кибершпионах тешит самолюбие отечественных чиновников, но он никак не согласуется с реалиями кибербезопасности России, в которой не может быть мощной киберразведки без эффективных систем киберзащиты собственных систем. В стране уровень культуры информационной безопасности негативно сказывается на функционировании критической инфраструктуры государства и бизнеса.

Реальный кардинал Ришелье, чей образ описан Александром Дюма в «Трех мушкетерах», на вопрос современников как он добился могущества, якобы ответил: «Я никогда ничего не подписывал!». Во всем мире основную часть разведывательной информации спецслужбы добывают из открытых источников. Общеизвестно, что и для террористов информация является одним из важнейших ресурсов. У нас же эти банальные истины не воспринимаются. Может потому, что у российской элиты в силу причин, рассмотрение которых выходит за рамки настоящей статьи, утрачен инстинкт самосохранения?

А гром периодически гремит, и молнии высвечивают устаревшие ментальные установки. Достаточно вспомнить ситуацию с информационной безопасностью во время конфликта с Грузией в 2008 году. Вы думаете что с тех пор ситуация кардинально изменилась? Или грузины передумали выполнять свое обещание добиться отмены Олимпиады в Сочи или испортить этот праздник с нанесением ущерба имиджу России?

Во всех странах, где проводились или будут проводиться Олимпийские игры, вопрос кибербезопасности находился и находится на одном из первых мест, наряду с графиком строительства спортивных объектов. Нужно убеждать кого-то, что в современном мире это не прихоть, а реалии «общества риска»?

Вопрос риторический. Вспомним: в начале текста автор говорил, что он, руководствуясь благими устремлениями, довел черновик предыдущей статьи до экспертов высокого уровня. Спрашивается: и что после этого изменилось? Ответ прост – ничего! Кто-либо отрицал приведенные факты и выводы статьи? Нет! А в чем тогда дело? Как Вам объяснить по-простому? Сделаем это в рамках диалога.

Вы ученые, думаете, что есть такой чиновник - потенциальный самоубийца, который поставит перед высшим руководством страны проблему безопасности, решение которой обойдется в десятки миллиардов долларов США? Ответ очевиден! Вы сами и ответили на свой вопрос!

Или Вы хотите совершить самое опасное в современной России преступление – перенаправить часть финансовых потоков в другую сторону, то есть на обеспечение кибербезопасности, лишив тем самым уважаемых потенциальных получателей возможной выгоды? Так вы тогда потенциальный государственный преступник! Впрочем, не производит ученый впечатления человека, который способен перераспределять денежные ресурсы, тем не менее… Какие тогда претензии к хорошим людям, работающим на госслужбе, которые все понимают, но ничего реально поделать не могут?!

Но, можно же начать что-то делать и в рамках имеющихся сегодня ресурсных возможностей! Слушайте, оно Вам надо?! Гром грянет, вот тогда…

Вместо заключения. Фантазия на тему телефонного разговора

«Алло, это Москва? Александр Дмитриевич Жуков — заместитель Председателя Правительства Российской Федерации, Председатель Наблюдательного совета по подготовке игр 2014 года и Дмитрий Николаевич Козак — заместитель Председателя Правительства Российской Федерации, ответственный за организацию игр-2014 в Сочи? Это Вас беспокоит доктор социологических наук Бондаренко, я насчет необходимости скорейшего принятия мер по обеспечению кибербезопасности предстоящей Олимпиады.

- Сергей Васильевич мы познакомились с Вашими материалами по этой проблеме. Сценарии возможных кибератак с анализом их последствий уже разрабатываются, межведомственные разногласия устранены, уполномоченные должностные лица работают и осознают свою персональную ответственность. Спасибо Вам и в Вашем лице всему профессиональному сообществу за своевременное обращение внимания руководства страны к важной проблеме, затрагивающей не только Олимпиаду, но и сферу инфраструктуры развития информационного общества!»…

На самом деле не было такого разговора. Увы…

Не в разговоре дело! Как там речь идет в нарративе, отработанном в народной мудрости: «Сказка – ложь, да в ней намек – добрым молодцам урок!». Касательно же использованного автором популярного стиля изложения серьезных проблем, то процитируем выдающегося отечественного генетика Николая Тимофеева-Ресовского: «Наука – баба веселая… К науке нельзя относиться со звериной серьезностью». А к проблеме кибербезопасности национальных информационных систем как нужно относиться?

Выходные данные публикации в печатном виде:
Бондаренко С.В. Кибербезопасность Олимпиады. Продолжение / Зимние Олимпийские игры 2014 в Сочи в фокусе информационных атак. Сборник научных статей /Отв. Ред. В.В. Черноус / Южно-Российское обозрение Центра системных региональных исследований и прогнозирования ИППК ЮФУ и ИСПИ РАН. Вып. 69. Москва-Ростов-на-Дону: Социально-гуманитарные знания, 2011. С. 146-165.