О.В. Казарин, В.Ю. Скиба, Р.А. Шаряпов

НОВЫЕ РАЗНОВИДНОСТИ УГРОЗ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Решение задач по противодействию угрозам международной информационной безопасности необходимо выполнять как в рамках национальных систем предупреждения и нейтрализации угроз информационной безопасности, так и в рамках системы международной информационной безопасности.

Создаваемая система международной информационной безопасности должна быть способна решать большой круг задач классификации и типологии угроз на различных направлениях: политическом, дипломатическом, технологическом, экономическом, организационном. Предложения по противодействию рассматриваемым угрозам в рамках создания и развития такой системы также рассматриваются в настоящей работе.

Ключевые слова: глобальное информационной пространство, кибервойны, кибертерроризм, киберпреступность, информационно-коммуникационные технологии, международная информационная безопасность, угрозы международной информационной безопасности.

Введение

Актуальность проблемы обеспечения международной информационной безопасности (МИБ) обусловлена повышением роли и значения глобального информационного пространства (ГИП) в решении стратегических задач развития современного общества.

Глобальное информационное пространство (и его основная составляющая – сеть Интернет), с одной стороны, используется и в обозримой перспективе будет использоваться для обеспечения работоспособности объектов критических инфраструктур, расширения доступа граждан к информации, а с другой – может быть использована криминальными структурами, международными террористическими организациями и враждебными государствами

для нарушения работоспособности этих объектов, создания очагов социальной напряженности.

Именно указанные факторы и современные тенденции их изменения и должны стать основой при определении составных частей и облика *системы международной информационной безопасности*. При формировании и, в дальнейшем, при функционировании системы МИБ необходимо проводить перманентный развернутый анализ текущей ситуации в ГИП, в первую очередь анализ количества и качества угроз со стороны государств, преступников и террористов, использующих информационно-коммуникационных технологий (ИКТ) в деструктивных целях. Необходимо постоянно уточнять и классифицировать угрозы МИБ, делать подробную оценку этих угроз, уточнять планы и формат деятельности по противодействиям угрозам МИБ на перспективу.

1. Угрозы международной информационной безопасности, их классификация и типология

Среди основных базовых понятий необходимо определить понятие «*международная информационная безопасность*» и сопутствующие ему понятия.

Международная информационная безопасность – состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве[1].

Обеспечение международной информационной безопасности состоит в необходимости расширения связей между государствами с целью выработки общих усилий по борьбе с использованием ИКТ:

- для осуществления враждебных действий и актов агрессии;
- в террористических и экстремистских целях;
- в преступных целях;
- в качестве инструмента вмешательства во внутренние дела суверенных государств.

Эти усилия должны быть направлены сегодня:

- на определение состава, содержания и характеристик возникающих угроз МИБ и достижение общего понимания смысла этих угроз;
- на обмен на постоянной основе результатами анализа сложившейся ситуации и информацией о потенциальных нарушителях и инцидентах, связанных с работоспособностью информационных инфраструктур, с целью выработки адекватных

мер противодействия потенциальным угрозам, в том числе международного характера;
- на разработку механизмов и мер по обнаружению угроз МИБ и атак на информационные инфраструктуры и выявлению их источников и, в случае обнаружения, применение той или иной формы принуждения для устранения угрозы и прекращения атаки.

Решение проблемы обеспечения МИБ сводится к осознанию и реализации следующей очевидной парадигмы. Сегодня ни одно государство не способно в одиночку успешно противостоять современным угрозам, исходящим из ГИП. Поэтому особую значимость в современных условиях приобретает согласованная (коллективная) деятельность заинтересованных стран в области МИБ, превращение *системы МИБ* в одно из средств разрешения межгосударственных противоречий.

Угроза – совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства.

Угроза в информационном пространстве (*угроза информационной безопасности*) – совокупность условий и факторов, создающих опасность для личности, общества, государства и их интересов в информационном пространстве.

Угроза международной информационной безопасности (*угроза МИБ*) – угроза в глобальном информационном пространстве, *приводящая к нарушению международного мира и безопасности*.

Угрозы МИБ имеют, как правило, объективный характер и возникают в результате появления противоречий между индивидами, общественными группами, государствами при их взаимодействии в ГИП.

Классификацию угроз МИБ можно проводить по следующим классифицирующим признакам:
- местонахождение источника угрозы (внешняя, внутренняя);
- степень сформированности угрозы (потенциальная, реальная);
- степень субъективного восприятия (завышенная, заниженная, адекватная, мнимая, неосознанная);
- характер (природная, антропогенная, техногенная, комбинированная (конвергентная));
- среда для осуществления угрозы (технологическая, социальная);
- сфера жизнедеятельности, для которой опасна угроза (экономическая, социальная, политическая, оборонная, международная).

Классификация угроз МИБ имеет существенное значение при создании и функционировании системы обеспечения информационной безопасности как отдельной страны, так и групп государств, а также системы МИБ. Классификация в данном случае предназначена для постоянного использования в практической деятельности в области МИБ. Обычно в качестве оснований деления в классификации выбирают признаки, существенные для данной предметной области. В этом случае классификация выявляет существенные сходства и различия между угрозами МИБ. В другом случае, когда цель классификации состоит лишь в систематизации предметов, в качестве основания выбираются признаки, удобные для этой цели, но, возможно, несущественные для самих предметов. Такая классификация называется искусственной. Наиболее ценной является классификация, основанная на познании законов связи между видами, перехода от одного вида к другому в процессе развития.

Классификация по существенным признакам называется *типологией*. Она основывается на понятии типа как единицы расчленения изучаемой реальности, конкретной идеальной модели развивающихся угроз МИБ. Типология является обычно результатом некоторого огрубления действительных граней между типами угроз. С развитием знаний об угрозах происходит уточнение и изменение типологии.

При таком подходе в соответствии с документами в области МИБ[2] в настоящее время можно выделить следующие основные классы угроз МИБ, а именно использование ИКТ:

а) в качестве информационного оружия в военно-политических целях, противоречащих международному праву, для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;

б) в террористических целях, в том числе для оказания деструктивного воздействия на элементы критической информационной инфраструктуры, а также для пропаганды терроризма и привлечения к террористической деятельности новых сторонников;

в) для вмешательства во внутренние дела суверенных государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей или теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию;

г) для совершения преступлений, в том числе связанных с неправомерным доступом к компьютерной информации, с созданием,

использованием и распространением вредоносных компьютерных программ.

Можно выделить следующую типологию, связанную с угрозами МИБ. Последние могут осуществляться путем *информационно-технического и/или информационно-гуманитарного воздействия на объекты воздействия*. *Информационно-техническое воздействие* предполагает использование ИКТ для осуществления враждебных действий и актов агрессии, при этом ИКТ превращаются в информационное оружие, которое может быть использовано в военно-политических и иных целях. *Информационно-гуманитарное воздействие* предполагает использование специально подготовленного контента, распространяемого с помощью глобальной информационной инфраструктуры, в том числе, для вмешательства во внутренние дела суверенных государств и других враждебных действий.

Таким образом, помимо классов, видов и подвидов угроз МИБ, можно выделить механизмы (или каналы) их реализации: информационно-техническое и/или информационно-гуманитарное воздействие и именно противодействие этим механизмам и, соответственно, новым угрозам МИБ[3] должно стать одним из основных направлений деятельности формирующейся системы МИБ[4].

2. Проблемы и новые разновидности угроз международной информационной безопасности

Особую политическую актуальность в последнее время приобретают следующие проблемы МИБ.

1. Одна из самых серьезных проблем обозначена в Форталезской декларации государств – членов БРИКС (Бразилия, Россия, Индия, Китай, Южная Африка) 15 июня 2014 г.[5] В ней отмечено, что «необходимо сохранять ИКТ, и в частности Интернет, как инструмент мира и развития и не допускать их использования в качестве оружия». В Уфимской декларации VII саммита БРИКС (принята 9 июля 2015 г. в г. Уфе, Российская Федерация) в ст. 34, посвященной вопросам использования и развития ИКТ, также была выражена общая озабоченность государств – членов БРИКС «в связи с использованием ИКТ для целей транснациональной организованной преступности, разработки оружия и осуществления террористических актов»[6]. В итоговом докладе от 22 июля 2015 г. (A/70/174) Группы правительственных экспертов ООН по международной информационной безопасности 4-го созыва (2014–

2015 гг.)[7] ситуация охарактеризована так: «Ряд государств занимаются наращиванием потенциала в сфере ИКТ для военных целей. Использование ИКТ в будущих конфликтах между государствами становится более вероятным». Сейчас уже понятно, что проведение кибероперации против объектов транспортной инфраструктуры, электросетей, плотин, химических заводов, атомных электростанций и других критических инфраструктур технически возможно. Такие операции могут повлечь за собой обширные последствия, приводя к большому числу жертв среди гражданского населения и нанося значительный ущерб. Именно поэтому в разных странах проводится большое число исследований и дискуссий о возможности применения существующих норм международного права и, в первую очередь, права применения силы для противодействия злонамеренному использованию ИКТ.

Принципиальный ответ на этот вопрос был дан еще в 2013 г. в докладе от 24 июня 2013 г. (A/68/150) Группы правительственных экспертов ООН по МИБ 3-го созыва (2012–2013 гг.)[8], содержащем следующий вывод экспертов: «Международное право, и в частности Устав Организации Объединенных Наций, применимо и имеет важное значение для поддержания мира и стабильности и создания открытой, безопасной, мирной и доступной ИКТ-среды».

Проблема только в том, как именно применять действующие нормы международного права в киберпространстве, как сформировать необходимые правовые механизмы регулирования международных отношений в данной области, как адаптировать понятийный аппарат международного права конфликтов к киберпространству.

Примерно такая же ситуация и с другой отраслью международного права – международным гуманитарным правом. Нормы международного гуманитарного права, регулирующие ведение военных действий, в принципе применимы в ходе вооруженного конфликта с использованием ИКТ, однако не совсем понятно, как их применять, и то, окажутся ли они достаточно эффективными в подобной ситуации. Следовательно, важно обсуждать проблемы, которые кибервойна создает для толкования и применения международного гуманитарного права, а также возможные гуманитарные последствия кибервойны.

2. В упомянутом выше докладе Группы правительственных экспертов ООН по МИБ от 22 июля 2015 г. (A/70/174) говорится: «Существует все более реальная опасность использования ИКТ для террористических целей, в том числе для совершения террористических нападений на объекты ИКТ или связанную с ИКТ инфраструктуру, а не только для вербовки сторонников, финанси-

рования, обучения и подстрекательства, причем если не принять соответствующих мер, то это может поставить под угрозу международный мир и безопасность».

Феномен ИГИЛ продемонстрировал, что в условиях отсутствия международных согласованных мер и механизмов противодействия указанному в докладе Группы правительственных экспертов ООН использованию Интернета вполне реально создать мощную и эффективную службу Интернет-пропаганды и Интернет-рекрутирования. Именно поэтому задача разработки таких мер и механизмов должна рассматриваться как одна из первоочередных для научного и экспертного сообщества.

3. Главы государств – членов Шанхайской организации сотрудничества (Россия, Китай, Казахстан, Киргизия, Таджикистан и Узбекистан) в своей Душанбинской декларации 12 сентября 2014 г.[9] заявили: «Государства – члены ШОС активизируют совместные усилия по созданию мирного, безопасного, справедливого и открытого информационного пространства, основываясь на принципах уважения государственного суверенитета и невмешательства во внутренние дела других стран. Они будут сотрудничать в сфере предотвращения использования ИКТ в целях подрыва политической, экономической и общественной безопасности и стабильности государств-членов, а также общечеловеческих моральных основ социальной жизни, пресекать пропаганду идей терроризма, экстремизма, сепаратизма, радикализма, фашизма и шовинизма с использованием сети Интернет».

За последние три десятилетия появилось такое количество угроз информационной безопасности, что, казалось бы, новым уже нет места. Поэтому авторы не перестают удивляться изобретательности и находчивости производителей и разработчиков новых средств проведения кибератак и враждебного использования контента (новых механизмов информационно-технического и/или информационно-гуманитарного воздействия) и, соответственно, появлению новых угроз.

Вот только несколько наиболее характерных[10] фактов (читай: новых разновидностей угроз МИБ), появившихся (или ставших известными, обнародованных) буквально за последний год.

1. *Кибершпионаж АНБ, осуществляемый «через жесткие диски»*. В «Лаборатории Касперского» не исключают причастности Агентства национальной безопасности (АНБ) США к кибершпионажу через жесткие диски, выпускаемые фирмами Western Digital, Seagate, Toshiba и другими производителями. «Прямых доказательств нет, однако исходя из связи группы Equation Group со вредоносными программами Stuxnet и Flame (программы 2010 года,

целью которых являлись Иран и другие страны Ближнего Востока и Северной Африки), можно предположить причастность АНБ», – пояснили в «Лаборатории Касперского»[11].

Предположительно, шпионское программное обеспечение способно было перепрограммировать прошивку жестких дисков и благодаря этому оставалось невидимыми для антивирусов. Эта вредоносная программа также получала незаконный доступ к данным пользователей «зараженных» жестких дисков. Зараженные компьютеры были обнаружены в 30 странах мира, большинство из них находилось в Иране, России, Пакистане, Афганистане, Китае, Мали, Сирии, Йемене и Алжире. Наибольший интерес вызывали правительственные и военные организации, банки, а также телекоммуникационные и энергетические компании.

2. *Хищение информации у производителя SIM-карт спецслужбами США и Великобритании.* Крупнейшая в Европе телекоммуникационная компания Deutsche Telekom, которая использует SIM-карты компании Gemalto, базирующейся в Нидерландах, не исключает возможности того, что их механизм защиты был взломан спецслужбами США и Великобритании. Интернет-издание Intercept[12] со ссылкой на данные, предоставленные экссотрудником американских спецслужб Эдвардом Сноуденом (Edward Snowden), сообщило, что АНБ США и Управление правительственной связи (УПС) Великобритании похитили шифровальные ключи крупнейшего мирового производителя SIM-карт Gemalto.

3. *Смурф-технологии в мобильных устройствах.* В интервью программе «Панорама» британской телерадиокомпании BBC Э. Сноуден рассказал, что УПС способно взламывать смартфоны без ведома их пользователей[13]. Это происходит посредством отправки на мобильное устройство сообщения с зашифрованным текстом, о котором не догадывается пользователь. После этого спецслужба получает доступ ко всем личным сообщениям, фотографиям пользователя и истории его браузера. Кроме того, посредством удаленного доступа можно включать микрофон владельца телефона для его прослушивания и даже сфотографировать этого человека.

Для прослушки и слежки за пользователями используется так называемый «комплект смурфов», который назван в честь синих существ, придуманных и нарисованных бельгийским художником Пьером Кюллифором. «Так, “мечтательный смурф” представляет собой инструмент управления питанием, что означает: ваш телефон можно включать и выключать без вашего ведома», – заявил Э. Сноуден. «“Любопытный смурф” – это механизм, управляющий

микрофоном. Например, если (телефон) у вас в кармане, то можно включить микрофон и слушать все, что происходит вокруг вас – даже если ваш телефон выключен. “Смурф-следопыт” – механизм геолокации, который позволяет УПС отслеживать вас с большей точностью», – отметил Э. Сноуден.

По его словам, «пользователи смартфонов практически ничего не могут сделать для того, чтобы не дать спецслужбам получить “полный контроль” над своим телефоном». Полученными данными британской УПС центр делится со своими коллегами из АНБ, действуя по принципу «технологии в обмен на информацию».

4. *Мнимые и настоящие угрозы с точки зрения американских государственных структур и спецслужб.* В марте 2015 г. директор Национальной разведки США Джеймс Клеппер (James Clapper) заявил, что Россия является наиболее искусным противником США в киберпространстве. Он считает, что по сложности и скрытости кибератак Россия превзошла Китай[14]. В ходе презентации доклада «Международная оценка угроз разведывательному ведомству США» на собрании комитета сената США по вооруженным силам директор национальной разведки США отметил, что киберугрозы, исходящие со стороны России, являются более серьезными, чем ранее были оценены.

В докладе обращается внимание на то, что Россия выделилась в международном киберпространстве как один из самых «сложных» государственных акторов, а Министерство обороны Российской Федерации ведет активную работу по укреплению своего киберкомандования.

По данным Национальной разведки США, российский киберпотенциал включает в себя не только схожие с американскими технологии нападения на вражеские системы управления войсками и ведения киберпропагандистских операций, но и технологии воздействия на системы промышленного контроля, электросети, системы управления воздушным движением, а также на нефте- и газораспределительные сети.

Эксперты сходятся во мнении, что США совершенно не имеют представления о реальных кибервозможностях России, поскольку долгое время игнорировали необходимость отслеживать развитие в России этого направления.

Все эти факты также говорят о своеобразной угрозе, «исходящей» от спецслужб США и их европейских коллег, руководители которых, обвиняя таким образом Россию (или Китай, или кого-то еще), не приводят никаких доказательств. И тем не менее на подобные заявления (читай: угрозы) наша страна должна определенным образом реагировать. Надо все время пытаться понять, что стоит

за такими заявлениями. Это всего лишь выбивание бюджетных средств, демонстрация необходимости реформирования ведомства в каких-то корпоративных интересах или что-то другое? И как нашей стране на все это необходимо (и нужно ли на это) реагировать?

5. *Террористическое интернет-рекрутирование и интернет-пропаганда*. Общепризнано, что глобальные социальные сети становятся новыми формами информационного противоборства и удобным плацдармом для деятельности международных террористических организаций и в первую очередь для осуществления соответствующей пропаганды, рекрутирования новых сторонников и распространения вируса страха перед террористическими угрозами. В ноябре 2014 г. директор УПС Великобритании Роберт Ханниган (Robert Hannigan) в статье «The web is a terrorist's command-and-control network of choice» (Террористы используют Интернет как сеть оперативного управления), газета «The Financial Times»[15], отмечал, что террористы ИГИЛ использовали возможности Интернета для создания глобальной международной террористической сети, а мессенджеры и социальные сети (Twitter, Facebook и WhatsApp) используются экстремистами для пропаганды своих идей и вербовки новых членов.

В феврале 2015 г. в интервью СМИ министр национальной безопасности США Джей Джонсон (Jeh Johnson) сообщил, что по сравнению с планированием и организацией терактов 11 сентября современные террористические организации более эффективно используют Интернет, социальные сети и другие средства для провокации индивидуальных терактов[16].

18–19 февраля 2015 г. в Вашингтоне Государственный департамент США организовал и провел под эгидой Президента США Барака Обамы Саммит по борьбе с насильственным экстремизмом (Summit on Countering Violent Extremism), где собрались высокопоставленные представители органов государственной власти из более чем 60 стран мира. Одним из основных вопросов было противодействие распространению идей терроризма и привлечению его новых сторонников в Интернете и социальных сетях. Б. Обама в своем выступлении отметил, что террористические группы (Аль-Каида), ИГИЛ сознательно ведут пропаганду для достижения своих целей среди молодых мусульман, используя в ГИП высококачественное видео, онлайн-СМИ, социальные медиа, свои аккаунты в Twitter[17]. По словам Генерального секретаря ООН Пан Ги Муна, выступившего на Саммите, лидеры экстремистов зачастую завлекают в ряды террористов недовольных безработных молодых людей, используя социальные медиа для расширения своих рядов и распространения вируса страха[18]. По мнению Верховного

представителя ЕС Федерики Могерини (Federica Mogherini), принявшей участие в Саммите в Вашингтоне, «Интернет стал основным средством для радикализации и вербовки»[19].

Наиболее известным («прогремевшим») случаем в последнее время, связанным с этими противоправными действиями, стала история студентки философского факультета МГУ Варвары Карауловой, которой в ноябре 2015 г. на заседании Мосгорсуда предъявлено официальное обвинение в попытке присоединиться к боевикам запрещенной в России террористической группировки «Исламское государство» в Сирии[20].

Таким образом, следует признать: в лице ИГИЛ мир столкнулся с гораздо более коварным и изощренным противником, нежели Аль-Каида. В том числе и тогда, когда вопрос касается пропаганды и рекрутирования «волонтеров» в свои ряды.

По данным на весну 2015 г.[21], более 20 тысяч иностранных граждан из 90 стран мира влились в ряды ИГИЛ в Ираке и Сирии. Как считают в Национальном антитеррористическом центре США, не менее 3400 бойцов рекрутированы в странах Запада. Подчас это люди, получившие хорошее светское образование[22].

Это результат, в том числе, весьма умелой пропаганды ИГИЛ, развернутой в соцсетях, в отличие от той же Аль-Каиды, которая делала акцент на «контактную агитацию» в медресе и мечетях. В частности, по данным Госдепартамента США, только в «Твиттере» ИГИЛ делает в сутки около 90 тысяч публикаций! Исламисты обращаются к своей аудитории в каждой стране на ее языке. Их ролики скроены по всем законам рекламы. Пропаганда специально нацелена на молодежь.

По данным Генпрокуратуры РФ, почти все террористические организации имеют свои интернет-ресурсы, информация на которых размещена на нескольких языках. Количество таких сайтов исчисляется тысячами, и среди них значительное количество русскоязычных[23].

В том числе, действует отдельная программа привлечения в ИГИЛ молодых женщин, которых призывают не только становиться бойцами ИГИЛ, но и женами «героических исламистов». В такой пропаганде на стороне исламистов задействованы и женщины, которые агитируют приезжать в Сирию и Ирак в поисках «преданных и надежных воинов джихада» в роли будущих мужей. Интересно, что Аль-Каида, например, никогда женщин к своей агитации не привлекала.

По некоторым данным в настоящее время во Всемирной сети существует уже несколько сотен экстремистски настроенных информационных ресурсов. Сегодня в Сети представлены абсолютно

все известные своими радикальными взглядами группы. Причем материалы они переводят не менее чем на 40 различных языков.

На «остроту» этой проблемы, в том числе и на факты, связанные с хорошо известными осенними (2015 г.) терактами, оперативно отреагировали наши законодатели. Парламентарии считают, что «бить» нужно не только по тем, кто изготавливает взрывные устройства, но и по тем, кто занимается финансированием и пропагандой терроризма. Любое пособничество (вербовка, агитация в социальных сетях и пр.) будет в нашей стране сурово караться. Нужно перекрыть любые лазейки воспроизводства терроризма внутри страны, рекрутирования «пушечного мяса».

6. *Массовая киберкража у банков*. Киберкража продолжалась два года и затронула около 100 банков, платежных систем и других финансовых организаций из почти 30 стран, в частности из России, США, Германии, Китая, Украины, Канады, Гонконга, Тайваня, Румынии, Франции, Испании, Норвегии, Индии, Великобритании, Польши, Пакистана, Непала, Марокко, Исландии, Ирландии, Чехии, Швейцарии, Бразилии, Болгарии и Австралии. Эксперты полагают, что за этим громким инцидентом стоит международная группировка киберпреступников из России, Украины, ряда других европейских стран, а также Китая.

Криминальная группировка, получившая название Carbanak, использовала методы, характерные для целевых атак. Однако в отличие от многих других инцидентов это ограбление *знаменует собой новый этап*: теперь киберпреступники могут красть деньги напрямую из банков, а не у их клиентов[24].

7. *Угрозы информационной безопасности в международной экономической деятельности*. Существует целый пул угроз МИБ, возникающих в рамках деятельности международных (региональных) экономических организаций. Так, в схеме обмена электронными документами при трансграничном взаимодействии органов государственной власти государств – членов Евразийского экономического союза между собой и с Евразийской экономической комиссией с участием доверенной третьей стороны возникают коллизии, которые связаны с возникновением ситуации, при которой субъект взаимодействия (юридическое или физическое лицо) потенциально может подать в государственный орган электронный документ, который он получил от другого субъекта, находящегося в юрисдикции, отличающейся от государственного органа подачи. В этом случае государственный орган не сможет корректно проверить такой электронный документ. Такая угроза может возникнуть, например, при обеспечении государственных закупок в электронной форме в рамках ЕАЭС.

Другой разновидностью угроз МИБ при нарушении трансграничной передачи электронных документов может быть «ситуация», которая порождается конструкцией типа «электронный документ с неопределенной юридической силой», – это документ, который поступил в юрисдикцию получателя, но его юридическая сила еще не подтверждена с помощью квитанций доверенной третьей стороны. Например, возможен случай, когда электронный документ был подписан электронной подписью и отправлен получателю, но до инициации получателем процедуры формирования квитанций сертификат открытого ключа проверки подписи был скомпрометирован. Очевидно, что в юрисдикции получателя такой электронный документ юридической силы иметь не будет. При этом на момент формирования электронного документа и в процессе его передачи от отправителя к получателю документ обладал всеми свойствами, позволяющими считать его юридически значимым.

В целом прогнозные исследования в области потенциальных угроз информационной безопасности, в том числе угроз МИБ, говорят об увеличении рисков, связанных, например, с атаками с использованием связи между устройствами (Machine-to-Machine, M2M). В 2016–2017 гг. ожидается дальнейшее развитие вредоносных программ, использующих протоколы связи между подобными устройствами. Используя их, киберпреступники получат новые средства доступа к корпоративным сетям. Распространяются специально созданные вредоносные программы, «нацеленные» на Интернет вещей. Их разрушительный потенциал заключается в возможности атаковать миллионы устройств, подключенных к сети. Диапазон новых целей для атак очень широк: от все более популярных «умных» часов до подключенного к Интернету медицинского оборудования[25].

Совершенствуются методы и средства проведения атак в облачных и виртуальных средах. Обнаруженная в 2015 г. уязвимость Venom продемонстрировала способность вредоносных программ обойти гипервизор и получить доступ к хосту операционной системы в виртуальной среде. Растущая зависимость от виртуализации, а также от частных и гибридных облаков делает эти атаки еще более привлекательными с точки зрения киберпреступников. В то же время мобильные устройства будут использоваться для удаленных атак на государственные и частные облачные технологии и системы.

Все это говорит не только о чрезвычайно высоком уровне злонамеренности «будущих угроз», но и о высоком разнообразии сред для их осуществления, сфер жизнедеятельности, для которых эти угрозы опасны, враждебном характере и уровне подготовленности акторов, потенциально способных осуществлять эти угрозы.

3. Противодействие новым разновидностям угроз международной информационной безопасности

Угрозы МИБ, в том числе и рассмотренные выше, беспокоят сейчас многих, поскольку в последние годы в некоторых государствах отрабатываются технологии использования Интернета, социальных сетей, мобильной связи для влияния извне на общественное сознание, организации массовых волнений и государственных переворотов. Сложность противодействия таким деструктивным действиям состоит в том, что данная проблема еще только становится предметом исследования специалистов. В процессе ее решения необходимо найти общественно признанный баланс между правом граждан на доступ к информационно-телекоммуникационным сетям и обеспечением национальной безопасности. Этот баланс каждая страна находит самостоятельно, исходя из своих социально-культурных традиций и национальных приоритетов.

В результате исследований предстоит разработать правовые механизмы, позволяющие предотвратить использование ИКТ для вмешательства во внутренние дела суверенных государств. Возможно, *надо включить такие деструктивные действия в число признаков агрессии*, закрепленных в Резолюции Генеральной Ассамблеи ООН 1974 г. № 3314[26], со всеми вытекающими из этого международно-правовыми последствиями.

В особом ряду стоят сегодня противоправные действия, связанные с использованием ИКТ в террористических целях, для пропаганды идей терроризма и рекрутирования через социальные сети и друге электронные медиа в свои ряды новых сторонников. Исследования в этой области являются в явном виде мультидисциплинарными, междисцилинарными и в технических науках (информационные технологии, информационная безопасность, телекоммуникации и т. д.), и в гуманитарных (социальные науки, психология, правоведение, криминалистика, религиоведение, международные отношения и т. д.).

Так, в декабре 2015 г. состоялось заседание секции научного совета при Совете Безопасности Российской Федерации, где были рассмотрены подходы противодействия идеологии терроризма. Представители научного сообщества подчеркнули, что распространение радикальных идеологий международными террористическими организациями, в том числе так называемым «Исламским государством», проводится с применением современных технологий информационно-психологического воздействия. В связи с этим отмечена необходимость выявления применяемых террористами технологий и выработки действенных ответных мер, обсуждены

методы предотвращения вербовки граждан в ряды международных террористических организаций, в частности способы контрпропаганды с участием религиозных организаций, объединяющих представителей традиционного мусульманского духовенства, общественных организаций, средств массовой информации, социальных сетей[27].

Сейчас наша страна, как никогда раньше, предпринимает активные усилия по противодействию этой угрозе: блокируются сайты террористической направленности, принимаются законодательные инициативы в этой области, ведется серьезная борьба правоохранительных органов против (кибер-)террористических организаций и конкретных персон и т. д. (10 ноября 2015 г. Генеральный прокурор Российской Федерации Ю. Чайка на открытии в Сочи VII региональной конференции Международной ассоциации прокуроров (МАП) для государств Центральной и Восточной Европы, Центральной Азии сообщил, что по требованию Генпрокуратуры России были блокированы 800 интернет-сайтов террористической и экстремистской направленности, с 4,5 тыс. страниц была удалена незаконная информация[28].) В то же время такое противодействие должно *носить комплексный, системный характер*. Для чего необходимо опираться и на систему МИБ при изучении деятельности международных (кибер-)террористических организаций и их действий в отношении нашей и других стран.

В рамках противодействия угрозам МИБ при международном экономическом взаимодействии в рамках Евразийского экономического союза сейчас ведутся работы по созданию Интегрированной информационной системы Союза[29], где существующая система МИБ с ее региональными подсистемами может быть привлечена для организации такой деятельности.

Таким образом, следует констатировать, что в современном компьютерном и коммуникационном мире постоянно возникают все новые и новые разновидности угроз в ГИП, в том числе угроз МИБ. *Некоторые из них даже невозможно спрогнозировать*. Это объясняется *постоянным и стремительным развитием ИКТ* и, в целом, науки и технологий, смена поколений которых осуществляется примерно каждые 6–8 месяцев. Нельзя не учитывать и интеллект злоумышленника. Это понятно, когда речь идет о государственных организациях, осуществляющих враждебные действия и имеющих в своем распоряжении самые последние достижения науки и техники, лучших специалистов в различных ИТ- и социальных областях. Но речь идет и о «рядовом хакере» и группах хакеров, кибертеррористах и киберпреступниках, которые зачастую хорошо образованы и технически оснащены, а часто и достаточно

(финансово, политически, идеологически) мотивированы для выполнения злоумышленных действий. Это объясняется еще и геополитической, геостратегической и геоинформационной ситуацией в современном мире, в том числе в ГИП. Эта *ситуация стремительно меняется, меняются действия, политическая и экономическая мотивация различных акторов на международной арене, появляются новые акторы ГИП*. Все это необходимо учитывать при противодействии угрозам МИБ и их прогнозированию.

Таким образом, следует считать, что компьютерные атаки и воздействия с использованием специально подготовленного контента (информационно-технические и информационно-гуманитарные воздействия) будут постоянно эволюционировать и «разрастаться». Поэтому необходимо систематически обновлять существующие перечни угроз информационной безопасности и, более того, необходимо проводить прогнозные исследования в этой области, чтобы, по возможности, им противостоять, хотя бы в ближайшей и среднесрочной перспективе.

Несмотря на все сложности создавшейся геополитической ситуации в мире, в настоящее время становится все более актуальным вопрос об *определении направлений совместной деятельности по налаживанию взаимодействия между странами в области МИБ*. Основой для такого взаимодействия должно стать сближение позиций по содержанию проблемы, *пониманию опасности угроз МИБ*[30].

Резюмируя сказанное, можно сделать вывод о том, что противодействие угрозам МИБ является предметом заботы прежде всего национальных органов государственной власти. В то же время по мере развития ГИП становится все более ясным, что успех каждой страны по защите его национальных секторов в определенной степени будет зависеть от успехов в этой области других стран. Жизнь международного сообщества в целом и каждой страны в отдельности будет более защищенной от угроз МИБ, исходящих из ГИП, тогда, когда будут разработаны и внедрены методы противодействия угрозам МИБ, средства выявления, пресечения и ликвидации последствий этих угроз.

Заключение

Масштаб угроз МИБ сегодня многократно возрос под воздействием такого сложного и противоречивого явления, как глобализация. С одной стороны, в условиях глобализации резко усилилась взаимозависимость государств и конфликты в ГИП начали всерьез угрожать всеобщей безопасности и стабильности. С другой стороны,

углубляя неравномерность экономического развития государств, глобализация создает питательную среду для накопления кризисного потенциала во многих странах мира. Именно на этой основе возникают и разрастаются новые разновидности угроз МИБ, появляются различного рода новые акторы ГИП, сделавшие своим орудием насилие и беззаконие в нем[31].

Перспективная система МИБ, ее эффективное и своевременное формирование и укрепление позволит всем участникам процессов, протекающим в ГИП, в первую очередь государствам и их правительствам, создать надежную и защищенную среду, которая будет способствовать поддержанию международного мира и безопасности, включая мирное урегулирование споров и конфликтов, неприменение силы, невмешательство во внутренние дела, соблюдение основных прав и свобод человека.

Примечания

[1] Конвенция об обеспечении международной информационной безопасности (концепция) // Совет Безопасности Российской Федерации [Электронный ресурс]. URL: http://www.scrf.gov.ru/documents/6/112.html (дата обращения: 07.12.2015).

[2] Там же; Основы государственной политики Российской Федерации в области международной информационной безопасности, утв. Президентом Российской Федерации 24 июля 2013 года, № Пр-1753.

[3] Следуя целям данной работы, дальнейший анализ новых разновидностей угроз МИБ будет исходить именно из этой классификационной схемы и типологии угроз.

[4] В рамках цикла работ, посвященных современным угрозам МИБ, авторы предполагают в следующей статье привести классификатор угроз МИБ и процедуру систематического (периодического) обновления его содержания. Задачу классификации угроз МИБ предполагается рассматриваться как задачу многокритериальной номинальной экспертной классификации с выделением генеральных классов угроз, их видов и подвидов и распределении (экспертными методами) имеющихся угроз по этим классам, видам и подвидам с получением финального классификатора (перечня) угроз МИБ.

[5] Форталезская декларация (принята по итогам шестого саммита БРИКС), г. Форталеза, Бразилия, 15 июня 2014 года // Президент России [Электронный ресурс]. URL: http://static.kremlin.ru/media/events/files/41d4f1dd6741763252a8.pdf (дата обращения: 07.12.2015).

[6] VII саммит БРИКС. Уфимская декларация (Уфа, Российская Федерация, 9 июля 2015 года). С. 21 // Там же [Электронный ресурс]. URL: http://static.kremlin.ru/media/events/files/ru/YukPLgicg4mqAQIy7JRB1HgePZrMP2w5.pdf (дата обращения: 07.12.2015).

[7] Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности от 22 июля 2015 г. A/70/174 // Организация Объединенных Наций [Электронный ресурс]. URL: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N15/228/37/PDF/N1522837.pdf?OpenElement (дата обращения: 07.12.2015).

[8] Об итогах заключительного заседания группы правительственных экспертов ООН по обеспечению международной информационной безопасности // Министерство иностранных дел Российской Федерации [Электронный ресурс]. URL: http://www.mid.ru/foreign_policy/un/-/asset_publisher/U1StPbE8y3al/content/id/105050 (дата обращения: 07.12.2015).

[9] Душанбинская декларация глав государств – членов Шанхайской организации сотрудничества, 12 сентября 2014 года // Президент России [Электронный ресурс]. URL: http://www.kremlin.ru/supplement/4750 (дата обращения: 07.12.2015).

[10] С точки зрения рассматриваемой в данной статье исследовательской проблемы.

[11] Исследовательский проект «Вредоносные программы нового поколения: источники разработки, цели, характер, особенности и последствия их применения» (III этап, итоговый) // Институт проблем информационной безопасности МГУ им. М.В. Ломоносова [Электронный ресурс]. URL: http://www.iisi.msu.ru/UserFiles/File/publications/Project_2015.pdf (дата обращения: 07.12.2015); Работа студентов // Российский государственный гуманитарный университет [Электронный ресурс]. URL: http://www.rsuh.ru/iintb/science/work-studentov2/ (дата обращения: 07.12.2015).

[12] *Васильков А.* Время менять SIM-карты // Компьютерра [Электронный ресурс]. URL: http://www.computerra.ru/116338/sim-card-kis/ (дата обращения: 07.12.2015).

[13] *Васильев А.* Сноуден рассказал о слежке западных спецслужб за смартфонами // Росс. газ. 2015. 8 окт.

[14] *Gady F.-S.* Russia tops China as principal cyber threat to US // The Diplomat [Электронный ресурс]. URL: http://thediplomat.com/2015/03/russia-tops-china-as-principal-cyber-threat-to-us/ (дата обращения: 07.12.2015).

[15] *Hannigan R.* The web is a terrorist's command-and-control network of choice // The Financial Times [Электронный ресурс]. URL: http://www.ft.com/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html#axzz3I2F0l6FM (дата обращения: 07.12.2015).

[16] Терроризм принимает форму «одиночных» действий // Газета «Жэнминь жибао» он-лайн [Электронный ресурс]. URL: http://russian.people.com.cn/n/2015/0224/c31520-8853085.html (дата обращения: 07.12.2015).

[17] Remarks by the President in Closing of the Summit on Countering Violent Extremism // The White House [Электронный ресурс]. URL: https://www.whitehouse.gov/the-press-office/2015/02/18/remarks-president-closing-summit-countering-violent-extremism (дата обращения: 07.12.2015).

[18] Preventing violent extremism, promoting human rights go hand-in-hand, Ban tells Washington summit // United Nations News Centre [Электронный ресурс]. URL: http://www.un.org/apps/news/story.asp?NewsID=50123#.VSwVPvCLXIY (дата обращения: 07.12.2015).

[19] Washington Summit on Countering Violent Extremism // European Union. European External Action Service [Электронный ресурс]. URL: http://eeas.europa.eu/top_stories/2015/200215_white_house_summit_on_countering_violent_extremism_en.htm (дата обращения: 07.12.2015).

[20] Сама В. Караулова полностью признала свою вину в попытке участия в ИГИЛ.

[21] *Бовт Г.* Вместо бородачей – мачо. Такая реклама Аль-Каиде и не снилась // Комсомольская правда [Электронный ресурс]. URL: http://www.kp.ru/daily/26391.5/3268488/ (дата обращения: 07.12.2015).

[22] Та же В. Караулова, студентка философского факультета МГУ, по словам ее отца, многие годы прожила на Западе.

[23] Генпрокуратура: ИГ вербует боевиков через кампанию в духе современной «попкультуры» // ТАСС – информационное агентство России [Электронный ресурс]. URL: http://tass.ru/politika/2425470 (дата обращения: 07.12.2015).

[24] Великое банковское ограбление: Carbanak APT // Kaspersky Lab [Электронный ресурс]. URL: https://business.kaspersky.ru/velikoe-bankovskoe-ograblenie-carbanak-apt/2678/ (дата обращения: 07.12.2015).

[25] Какие угрозы подстерегают в 2016 году? // Международный компьютерный журнал «Computerworld Россия» [Электронный ресурс]. URL: http://www.computerworld.ru/news/Kakie-ugrozy-podsteregayut-v-2016-godu (дата обращения: 07.12.2015).

[26] Резолюция Генеральной Ассамблеи ООН 3314 (XXIX) «Определение агрессии» от 14 декабря 1974 года // Организация Объединенных Наций [Электронный ресурс]. URL: http://www.un.org/ru/documents/decl_conv/conventions/aggression.shtml (дата обращения: 07.12.2015).

[27] Научные подходы противодействия идеологии терроризма рассмотрены на заседании секции научного совета при Совете Безопасности Российской Федерации: Совет Безопасности Российской Федерации [Электронный ресурс]. URL: http://www.scrf.gov.ru/news/991.html (дата обращения: 07.12.2015).

[28] Генпрокуратура: ИГ вербует боевиков через кампанию в духе современной «попкультуры» [Электронный ресурс].

[29] Решение Коллегии Евразийской экономической комиссии от 14 апреля 2015 года № 29 // Электронный фонд правовой и нормативно-технической документации [Электронный ресурс]. URL: http://docs.cntd.ru/document/420268983 (дата обращения: 07.12.2015).

[30] Резолюция «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» (A/RES/69/28), принята без голосования 2 декабря 2014 г. // Организация Объединенных Наций [Электронный ресурс]. URL: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N14/662/43/PDF/N1466243.pdf?OpenElement (дата обращения: 07.12.2015).

[31] *Казарин О.В., Шаряпов Р.А.* Вредоносные программы нового поколения – одна из существенных угроз международной информационной безопасности // Вестн. РГГУ. 2015. № 12 (155). Сер. «Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность». С. 9–23.