УДК 343.34

ВАЖНОСТЬ СОВЕРШЕНСТВОВАНИЯ МЕХАНИЗМОВ ОРГАНИЗАЦИИ КИБЕРБЕЗОПАСНОСТИ В СОВРЕМЕННЫХ УСЛОВИЯХ

К.Ф. Джаббарова

Исследуется важность совершенствования механизмов организации кибербезопасности в современных условиях. Рассматриваются вопросы усиления системы кибербезопасности и киберпространства.

Ключевые слова: кибербезопасность; кибербезопасность в мире; киберпреступления; хакерские атаки; злоумышленники в киберпространстве.

THE IMPORTANCE OF IMPROVING CYBERSECURITY ARRANGEMENTS UNDER CURRENT CONDITIONS

K.F. Jabbarova

The importance of improving the mechanisms for organizing cybersecurity in the current environment is explored. The issues of strengthening the system of cybersecurity and cyberspace are considered.

Keywords: cybersecurity; cybersecurity in the world; cybercrime; hacker attacks; attackers in cyberspace.

В последние десятилетия в мире изменилось многое, прежде всего карта мира и границы суверенных государств, образовались новые государства, новые региональные объединения и организации, международные структуры. Все это обусловливает рассмотрение и координацию множества проблем. Проявились серьезные проблемы для всех стран мира и мирового сообщества в целом, такие как: влияние глобальных тенденций, политических и экономических процессов, новых конфликтов, войны, расхождение и противоречие международных и политических отношений, обеспечение национальной и международной безопасности, разработка и осуществление более эффективных механизмов, правил, порядка и инструментария для укрепления государственности, государственного строя, государственных институтов, структур и прочие.

Еще в феврале 2014 г., на Всемирном экономическом форуме в Давосе, одной из главных была обозначена глобальная проблема обеспечения кибербезопасности. Кроме того, возрастание бесконечных кибератак и киберугроз в мировом киберпространстве привело к осознанию масштабности глобальных угроз киберпреступлений и опасного объема ущерба, наносимого этим мировой экономике и мировому сообществу в целом. М. Клименский справедливо пишет, что "в условиях глобализации современных международных отношений, а также в связи со все возрастающей ролью информационно-коммуникационных систем в жизни современного общества, скорейшее решение проблем кибербезопасности, а также адекватный ответ на угрозы международной и национальной кибербезопасности представляется делом чрезвычайной важности, во многом требующим совместных действий мирового сообщества" [1].

Во многих странах мира нуждаются в ускорении развития важных индикаторов в области кибербезопасности, повышении эффективности киберпространства, особенно в повышении надежности программных продукций по обезвреживанию вредоносных элементов киберпространства, активизированию работы международных антивирусных компаний и научных заведений, коммерческих структур в сфере кибербезопасности.

Все эти факторы требуют внедрения комплекса организационно-технических мер и процедур в системе мирового киберпространства с учетом негативных факторов уязвимости механизмов безопасности, скомпрометированных паролей и идентифицируемых кодов, зараженных съемных носителей в мобильных устройствах, "подозрительных" обновлений, раскрытия технологической

конфигурации, внешнего управления по разделению сетей и защиты от публичных сетей и прочего. Статистика многолетней скрытой активности вредоносных программ продемонстрировала необходимость совершенствования подходов в области информационной безопасности. В частности, рекомендуются комплексные решения, сочетающие развитие нормативной базы, внедрение лучших практик менеджмента информационной безопасности. С точки зрения кибербезопасности первостепенные шаги следует сделать в направлении развития методологии, методов и средств тестирования на проникновение и аудит безопасности программного кода в мировом киберпространстве [2, с. 28–37].

Одной из современных проблем и трудностей в сфере кибербезопасности является необходимость защиты данных в киберпространстве и их неприкосновенности. Генеральный директор службы внутренней разведки Федеративной Республики Германия Ханс-Георг Масен отмечает, что страны, которые имеют общую демократическую ценность, должны сотрудничать для нейтрализации киберугроз. Самый важный аспект внутренней безопасности – защита секретной информации и важнейших объектов инфраструктуры, поскольку именно они обеспечивают условия для жизнедеятельности современного общества [3, с. 7–13].

Проблемы кибернападений и кибератак, как мы отметили, постоянно растут, и способы подобных нападений меняются, совершенствуются, особенно увеличиваются кибердудары по Интернету, в результате чего происходит сбой в системе киберпространства и интернет-сети. Участились случаи нанесения кибератак с целью ослабления внешней политики и политики безопасности отдельных государств, инфраструктурных и социальных систем, банковских и финансовых структур. Такие киберугрозы требуют объединения усилий всех государств для координации сотрудничества, обмена важной информацией с зарубежными партнерами в сфере кибербезопасности. Проблемы обеспечения кибербезопасности в контексте глобальных угроз обусловливают создание новых механизмов по решению глобальных проблем киберпространства и по противодействию кибератакам, преступным деяниям злоумышленников, устойчивости системы кибербезопасности и информационной безопасности в целом.

Глобальные угрозы кибербезопасности обусловливают активизацию сотрудничества ведущих страни мира по обеспечению кибербезопасности. В том числе, по мнению специалистов Нью-Йоркской корпорации Карнеги, необходима модернизация и формирование более гибких и надежных механизмов сотрудничества между США, Российской Федерацией и другими быстро развивающимися странами, такими как Китай и Индия, что отражено в отчетном докладе по проекту “Второй симпозиум”, который проходил в Берлине 27–29 июня 2015 г. Отмечается, что появляющиеся технологии в системе киберпространства предлагают огромные возможности для развития человека, но при этом они сами представляют новые угрозы и вызовы.

Вопросы кибербезопасности способны также осложнить международные отношения, привести к кибервойне, поэтому требуется усиление взаимодействия между странами мира по недопущению нарастания напряженности в мировом киберпространстве [4]. Еще в апреле 2011 г. Институтом Восток – Запад Глобальной инициативы кибербезопасности (США) и Институтом проблем информационной безопасности Московского государственного университета (Россия) был подготовлен двусторонний проект Россия – США по выработке основ критически важной терминологии в области кибербезопасности. Целью данного документа является начало реального диалога экспертов и уполномоченных лиц обеих сторон в сфере кибербезопасности, выработка более глубокого понимания точек зрений в области данной глобальной проблемы [5].

Необходимость усиления тенденции сближения международной политики и выработке механизмов по противодействию киберпреступлений объясняется ростом числа кибератак, причем стремительным ростом, передовые компании и ведущие транснациональные компании мира понесут многомиллиардные убытки. Только расходы на обеспечение информационной безопасности и кибербезопасности подобных компаний выросли до уровня 14 % в год. С каждым годом усиливаются негативные последствия проблемы эскалации угроз кибербезопасности, исходящих от организованных преступных групп и хакерских группировок [6].

Наряду с существующими проблемами в международном пространстве ИКТ и интернет-сети, имеются множественные расхождения по формированию и осуществлению международной политики в области кибербезопасности с участием основных кибердержав и участников киберпространства. Вместо того, чтобы объединить усилия государств по пресечению и предотвращению кибератак, преступных деяний злоумышленников в киберпространстве, отдельно взятые крупные страны концентрируют огромные ресурсы

и силы по противодействию хакерских вмешательств страны-противника. В современном мире существуют тандемы, которые демонстрируют масштабность международного противостояния и противоречий в сфере обеспечения кибербезопасности. США – Китай, США – Израиль и Иран, США – Россия и прочие постоянно обвиняют друг друга в кибершпионаже и хакерских атаках. На наш взгляд, продолжение такой международной политики и мировых процессов в сфере кибербезопасности ничего хорошего не принесет этим странам. Необходимо более глубоко изучить проблемы взаимоотношений стран в сфере кибербезопасности и разработать механизмы повышения надежности системы кибербезопасности как в отдельно взятой в стране, так и мире в целом.

Следует отметить, что проблемы обеспечения кибербезопасности глобального масштаба требуют больше разума и политической воли со стороны руководителей крупных кибердержав. Более того, подобный подход должен основываться на осознании серьезности последствий несогласованной политики в сфере кибербезопасности. Необходимы скоординированные действия и сбалансированная международная политика в сфере кибербезопасности. Кроме того, применение современных цифровых технологий создает новые угрозы, в том числе глобальные угрозы надежности и эффективности инфраструктуры, в том числе инфраструктуры киберпространства и интернет-сети. Наряду с развитием IT-технологий приходится создавать надежные меры защиты, объединяя усилия, поскольку в глобальном мире в одиночку решить эти вопросы невозможно. Генеральный секретарь Международного телекоммуникационного союза Хамадун Туре на конференции "Сотрудничество в глобальной кибербезопасности: проблемы и перспективы", проходящей в рамках международной выставки Bakutel-2013, заявил, что вопрос обеспечения кибербезопасности является глобальным и потому должен решаться на мировом уровне, на базе международного сотрудничества [7].

Информационное оружие супердержав, инициированные ими кибервойны, кибератаки и "управляемые кризисы" создают глобальные угрозы для всего мирового сообщества. Дело в том, что с развитием инфраструктуры ИКТ, информатизация всей системы отраслей национальной экономики, военных структур и прочих объединений военно-оборонного назначения возросла в масштабе глобальных угроз не только для "других" стран мира, но и для тех стран, которые владеют самым мощным арсеналом киберсредств, киберсистем, кибероружий, кибертехникой и киберинфраструктуры. Например, в США поддержание лидерства в области развития информационных и телекоммуникационных технологий рассматривается американским военно-политическим руководством в качестве важнейшего компонента глобального информационного превосходства [8]. Однако, как мы отметили ранее, этого недостаточно для обеспечения полноценной защиты информационной безопасности США и предотвращения кибератак на их компании, коммерческие банки, государственные и военные структуры.

На наш взгляд, прежде всего, необходимо решение этих глобальных вопросов политическим регулированием, сближением национальных интересов в сфере кибербезопасности в рамках международного сотрудничества и обеспечением международной информационной безопасности в целом, которая является одной из главных критериев эффективности системы международной безопасности. Так считает и исследователь И. Сафронова, по ее мнению, одной из важнейших особенностей современного общества, государства и международных отношений является стремительное развитие, а также повсеместное внедрение и использование новейших информационно-коммуникационных технологий. Проникновение ИКТ во все сферы жизнедеятельности оказало весьма значительное влияние на всю систему современных международных отношений. В политической сфере все большее значение приобретают не силовые, а информационные факторы [9], которые обусловливают все аспекты обеспечения надежности системной функции и механизмы киберпространства, его инфраструктурный потенциал, иначе решить вопросы глобальных проблем кибербезопасности и геополитические разногласия будет очень сложно.

Рассматривая масштабы и последствия глобальных проблем в международной системе кибербезопасности, отметим, что актуальность вопросов расширения международного сотрудничества и совершенствования международной политики в сфере киберпространства, активизации усилий ведущих стран мира по смягчению предельно напряженной ситуации и вопиющего разгула киберпреступлений и кибератак в мировом киберпространстве обусловлена важностью стабилизации ситуации и повышения эффективности в глобальной информационной сфере и мировом киберпространстве. А. Смирнов отмечает, что феномен информационной глобализации оказывает преобразующие действия на все сферы жизнедеятельности – экономику, политику, безопасность, социальную сферу, культуру, образование и досуг; взаимодействие различных стран

и регионов в процессе совершенствования и применения результатов ИКТ становится одной из самых динамичных и многообещающих сфер международного сотрудничества [10].

Обеспечение международной безопасности в информационной сфере и в мировом киберпространстве требует не только усилий отдельных стран мира, но и разработку и осуществление максимально эффективных международных инструментов. Поэтому все экономические и политические ресурсы по противодействию угрозам международной информационной и кибербезопасности должны рассматриваться на самом высоком мировом уровне с участием основных кибердержав.

Обеспечение кибербезопасности в контексте глобальных угроз, наряду с совместными усилиями международного сообщества, диктует важность разработки и осуществления превентивных действенных мер против кибератак и киберпреступлений в мировом киберпространстве, что обусловлено следующими факторами:

- в современном мире все глобальные вопросы и проблемы международных отношений, экономического сотрудничества, повышения имиджа страны, укрепления ее места на международном арене, в основном, реализуются при активном и рациональном обмене информации, развитии инфраструктуры ИКТ и интернет-сети, системы информатизации, обеспечении информационной безопасности, устойчивости системы защиты киберпространства;
- в мировом киберпространстве появились опасные тенденции, растет количество киберпреступлений, кибератак, кибершпионажа и прочих преступных деяний злоумышленников;
- нарастает напряженность между странами, особенно ведущими странами мира в сфере киберпространства, налицо все компоненты кибервойны;
- странам мира необходимо разработать адекватные модели государственной политики и национальную концепцию по кибербезопасности, отвечающие требованиям национальной безопасности страны в контексте глобальных вызовов и других тенденций современности;
- необходимо усовершенствовать международные механизмы и общую международную политику по разработке и осуществлению действенных и эффективных инструментов обеспечения кибербезопасности во всем мире, развивать международное сотрудничество, мобилизовать усилия ведущих стран мира по повышению эффективности международной системы кибербезопасности.

Литература

1. *Клименский М.М.* Кибербезопасность: существующие угрозы и проблемы ее обеспечения на современном этапе / М.М. Клименский. URL: http://www.pglu.ru.1
2. *Марков А.С.* Организационно-технические проблемы защиты от целевых вредоносных программ типа Stuxnet / А.С. Марков, А.А Фадин. // Вопр. кибербезопасности. 2013. № 1 (1).
3. Эффективность кибероборонь // Concordian: журнал по проблемам безопасности обороны Европы. 2014. Т. 5, № 2 “Защита киберпространства”.
4. Проект “Новые механизмы решения глобальных проблем, связанных с международной финансовой системой, энергетической безопасностью и изменением климата: “Сотрудничество между США, Российской Федерацией, Китаем и Индией”. Нью-Йоркская корпорация Карнеги, 2015 год. URL: http://www.fsvc.org
5. Двусторонний проект Россия – США по кибербезопасности. Основы критически важной терминологии / Институт Восток – Запад Глобальной инициативы кибербезопасности (США) и Институт проблем информационной безопасности Московского государственного университета (Россия). URL: http://www.iisi.msu.ru
6. *Клау Тим.* Основные результаты Глобального исследования тенденций информационной безопасности на 2016 год: спроса компаний финансового сектора. PricewaterhouseCoopers International Limited. URL: http://www.pwc.ru
7. *Мустафаева К.* Вместе против глобальных угроз / К. Мустафаева // Азербайджанские известия. 04.12.13. URL: http://www.azerizv.az
8. *Корсаков Г.* Информационное оружие супердержавы: кибервойна и “управляемые кризисы” / Г. Корсаков. URL: http://www.hvylya.net
9. *Сафронова И.Л.* Политические проблемы обеспечения международной информационной безопасности / И.Л. Сафронова. М., 2006. 211 с.
10. *Смирнов А.И.* Информационная глобализация и Россия: вызовы и возможности / А.И. Смирнов. М.: Парад, 2005. 43 с.