Секция «Информационное обеспечение внешней политики»

Новые аспекты политики России в сфере информационной безопасности

Научный руководитель – Баринова Екатерина Александровна

Ляпкина Ольга Александровна
Студент (бакалавр)
Московский государственный университет имени М.В.Ломоносова, Факультет мировой политики, Москва, Россия
E-mail: olyapkina@yandex.ru

За последние несколько десятилетий к традиционным пространствам взаимодействия между государствами добавилась информационная среда. И на сегодняшний день мы являемся свидетелями стремительной интенсификации противостояния в ней. Нетрудно заметить, что перманентным хакерским атакам подвергается критическая инфраструктура всех центральных игроков на международной арене.

В связи с существенными изменениями, произошедшими в сфере информационных технологий, назрела потребность в трансформации Доктрины информационной безопасности РФ от 9 сентября 2000 года. 5 декабря 2016 года Указом Президента РФ была утверждена новая Доктрина ИБ. Относительно устаревшей версии, состояние ИБ и направления обеспечения ИБ рассматриваются в новой Доктрине в разрезе стратегических национальных приоритетов, что делает документ более структурированным и последовательным. Доктрина 2016 года логически продолжает Стратегию национальной безопасности в качестве «документа стратегического планирования»[1]. Это порождает перспективу создания иерархии документов в сфере ИБ с учётом стратегических национальных интересов.

Доктрина 2016 года обозначает «глобальный трансграничный характер информационной сферы», где информационные технологии «стали неотъемлемой частью всех сфер деятельности личности, общества и государства»[2]. Благодаря масштабным работам, проведённым по разработке правового регулирования сферы информационных технологий и ИБ, в новом документе исчез пункт о неразвитости данного направления. Также в принятом документе отсутствуют разделы, связанные с обеспечением ИБ в духовной сфере, в общегосударственных информационных и телекоммуникационных системах, в правоохранительной и судебной сферах, а также раздел, описывающий положения государственной политики обеспечения ИБ РФ. Раздел о международном сотрудничестве РФ в сфере обеспечения ИБ трансформировался в отдельные пункты раздела «Стратегические цели и основные направления обеспечения ИБ». Важно отметить отсутствие угроз, связанных с негативной деятельностью государственных органов власти, однако при этом заметно увеличилось количество внешних угроз.

Главная угроза - «отдельные государства»[3], которые разными способами стремятся дестабилизировать обстановку внутри РФ. Пользуясь отсталостью российских ИТ, они осуществляют политику доминирования в киберпространстве, которая выражается в заметном росте компьютерной преступности, разведывательной деятельности со стороны иностранных государств.

Поэтому одним из приоритетных направлений является курс на импортозамещение, который не изменился с 2000 года. Проблема заключается в следующем: социально-экономическое развитие России зависит от геополитических интересов зарубежных стран, поэтому нам необходим суверенитет в данной сфере. С одной стороны дан импульс на скорейшее развитие отечественных кибертехнологий, научно-исследовательских программ, а

с другой стороны, в трехлетнем бюджете 2017-19 года заметно сокращена финансовая поддержка развития научно-технологического комплекса.

Особое внимание уделено росту воздействия со стороны террористических и экстремистских организаций, деятельность которых направлена на разжигание этнических, религиозных конфликтов, расшатывание стабильности общества. Данные субъекты используют метод воздействия на сознание населения. За последние годы предельно участились случаи вербовки граждан РФ посредством социальных сетей, рекламы, личного контакта и т п.

В современных условиях военно-политическое руководство ведущих иностранных государств имеет тенденцию к расширению масштабов применения информационных технологий, направленных на подрыв внутриполитической и социальной стабильности РФ. Российскими правоохранительными структурами фиксируется существенное увеличение количества компьютерных преступлений, атак на "объекты критической инфраструктуры, усиление разведывательной деятельности иностранных государств в отношении РФ"[4]. По данным ФСБ, за 2010 зафиксировано 3 млн. кибератак на все виды ресурсов, в 2014 - 57 млн., а в 2016 цифра достигла 70 млн. Связано это с ростом напряжённости международно-политической ситуации (Причины вспышки кибершпионажа 2014 - Сочинская Олимпиада, присоединение Крыма, ситуация в Донбассе. В 2016 - Сирийский конфликт, Украинский конфликт, Президентские выборы в США, Летняя олимпиада в Бразилии). Поэтому возникает необходимость создания системы защиты от хакерских угроз.

Отдельным пунктом отмечено усиление кибербомбежек в кредитно-финансовой сфере. По сообщениям СМИ, в ноябре 2016 произошла массовая кибератака на 5 крупнейших российских банков. А в декабре службам ФСБ удалось предотвратить повторное масштабное нападение на отечественную банковскую систему. Недавно ЦБ потребовал усилить защиту внутри банковских операций от хакерских атак. Ввиду этого стоит ожидать изменение финансирования в области защиты информации.

В Доктрине обозначена конкретная "угроза применения ИТ в целях нанесения ущерба суверенитету, территориальной целостности, политической и социальной стабильности РФ"[5]. Зарубежные страны наращивают информационно-технический потенциал для воздействия в военных целях. Специальные службы "оказывают информационно-психологическое воздействие"[6] с целью размывания духовно-нравственных ценностей и манипуляций сознанием населения (основная группа риска - молодёжь). Для этого поддерживается сотрудничество с этническими, религиозными, правозащитными организациями.

Отмечается тенденция к росту предвзятых оценок в отношении государственной политики России за рубежом, откровенной дискриминации отечественных СМИ, росту попыток помешать осуществлению профессиональной деятельности журналистов. 23 ноября 2016 Европарламент принял резолюцию о противодействии российской пропаганде. В связи с этим, депутаты ЕС приравняли информационные агентства "Russia Today" и "Спутник" к ИГИЛ, террористической организации, запрещённой в России. Авторов многих отечественных изданий депортируют, отказывают в аккредитации, угрожают закрытием редакций за рубежом. Все это порождает рост антироссийских настроений за рубежом и угрожает ИБ России.

Основные направления обеспечения ИБ в области обороны Доктрина предлагает рассматривать в соответствии с военной политикой.

Поэтому, основной целью доктрины ИБ является предотвращение военных конфликтов в результате применения информационных технологий и противодействие попыткам манипуляции со стороны иностранных служб специального назначения. Основными методами обеспечения ИБ значатся следующие: мониторинг и анализ информационного пространства с целью обнаружения компьютерных угроз, нейтрализация выявленных вредонос-

ных программ, прогнозирование возможных рисков и планирование мер по обеспечению ИБ. В настоящий момент, разрабатывается и принимается Российское законодательство в области ИБ. 24 января 2017 года в 1 чтении комитет по безопасности ГД рассмотрел законопроект о "критической информационной инфраструктуре" РФ. Это законопроект был разработан ФСБ ещё в 2013 году. В предварительном тексте определяются понятия "критической информационной инфраструктуре", вводится государственный контроль за обеспечением ИБ, определяется порядок финансирования ИБ, вводится практика тестирования, проведения учений, плановых и внеплановых проверок для специалистов-ИТ. Также за разработку вирусной программы, нацеленной на причинение вреда "критической информационной инфраструктуре", за незаконный доступ к информации, за нарушения правил эксплуатации и за соучастие в организованной кибератаки можно будет получить срок от 5 - 10 лет (В настоящее время преступление в информационной сфере наказывают со сроком до 7 лет).

Однако Microsoft и Cisco раскритиковали данный проект, заявив о нежелании следовать законам, учитывая тот факт, что аналогичное законодательство есть в США, Германии, Австрии, где эти компании его исполняют.

Это естественно, что государство стремиться контролировать распространение информации, однако в современных условиях цензура - это большая проблема, потому что лю бой человек может быть источником распространения информации.

Обобщая вышесказанное, Доктрина ИБ 2016 года носит явно милитаризованный характер. А значит, подчиняется военным целям и способствует наращиванию военной мощи государства. Политолог Алексей Мухин обосновывает необходимость принципиального изменения доктринальных документов тем, что "изменение внешнеполитической ситуации несёт информационное и военное воздействие со стороны стран НАТО или стран, которые аффилированные с НАТО.

В настоящее время ведётся глобальная кибервойна. Уровень развития информационных технологий и инструментов уже позволяет разделить потенциал в киберсфере на оборонительный и наступательный. Опасность ведения информационных войн порождает «гонку вооружений» в информационном пространстве. После вступления в должность 45-ого президента США Дональда Трампа на сайте Белого дома была опубликована программа новой администрации, где сказано, что США будут развивать оборонные и наступательные возможности в киберпространстве. Между тем 22 февраля 2017 Министр обороны России Сергей Шойгу заявил в Госдуме о том, что в стране созданы войска информационных операций, которые смогут решать проблемы кибератак. По имеющимся данным, во всех армиях ведущих государств созданы информационные войска. Самые многочисленные информационные войска в Китае (около 20 000 чел.), а в РФ около 1000. Наблюдается тенденция к их увеличению. В связи глобальной информатизацией общества не только Россия, но и остальные страны, подверженные угрозам ИБ, нуждаются в международном сотрудничестве в вопросах регулирования информационного взаимодействия и создания нормативно-правовой базы. Ещё в 2011 году группой правительственных экспертов ООН по международной ИБ началась выработка глобального пакта об электронном ненападении. Документ будет содержать обязательства о соблюдении принципов и правил поведения в киберпространстве, основное внимание в нём будет уделено запретам на кибератаки в отношении критически важных информационных ресурсах государства. Важным условием пакта является недопущение милитаризации информационного пространства. Вполне вероятно что, если акторы международных отношений всерьёз хотят создать безопасное и управляемое инфопространство, то необходимо определить информационный инструментарий, который уже разделяется на наступательный и оборонительный. Например, кибершпионаж и хакерские атаки относятся к наступательной составляющей, тогда

как криптографические ключи нового поколения - к оборонительной. Однако на пути принятия пакта существуют следующие трудности: добровольный характер подписания и контроль над исполнением его положений в инфопростанстве.

На сегодняшний день борьба ведётся не только в физических сферах (космос, атмосфера, вода), но и в информационной среде. Причём в физических сферах предполагается ведение военных действий в военное время, то в информационном пространстве борьба ведётся сегодня и приобретает всё большее значение. Можно сказать, что результат борьбы в киберпространстве определит исход военных действий. Кто победит в кибервойне, тот обеспечит себе победу на поле боя.

[1] Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 5.12.2016 г. N 646)
[2] Там же
[3] Там же
[4] Там же
[5] Там же
[6] Там же

Источники и литература

1) Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 N Пр-1895)
2) Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 5.12.2016 г. N 646)
3) http://www.atlas-nsk.ru/news/186 (Министерство связи и массовых коммуникаций Российской Федерации «Научно-технический центр «Атлас» федеральное государственное унитарное предприятие Новосибирский филиал)
4) Законопроект № 47571-7 «О безопасности критической информационной инфраструктуры Российской Федерации» (находится на рассмотрении), [Электронный ресурс], http://asozd2.duma.gov.ru/main.nsf/(SpravkaNew)?OpenAgent&RN=47571-7&02
5) Иванова, В. Европарламент принял резолюцию о противодействии российским СМИ [Электронный ресурс], https://ria.ru/mediawars_freedom_of_speech/20161123/1482000699.html - статья в Интернете
6) http://www.fsb.ru/ (Федеральная служба безопасности Российской Федерации)
7) http://www.un.org/ru/index.html (Организация Объединённых Наций)
8) ФСБ обвинила Microsoft и Cisco в противодействии закону о кибератаках [Электронный ресурс], http://www.interfax.ru/russia/546770 - статья в Интернете