Сангалов Виктор Александрович

УГРОЗЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИИ В ИНФОРМАЦИОННОЙ СФЕРЕ

В статье рассматривается влияние международных отношений на кибербезопасность Российской Федерации, приобретающую в современных условиях всё большую актуальность. Определяются наиболее вероятные виды киберугроз, выявляются центры и методы противоправного воздействия. Прогнозируются некоторые направления кибервоздействия на отечественную информационную инфраструктуру. Основное внимание автор акцентирует на взаимосвязи политических явлений и информационного противоборства, выявленной в ходе изложенного анализа.

Адрес статьи: www.gramota.net/materials/3/2015/8-3/44.html

Источник

Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики

Тамбов: Грамота, 2015. № 8 (58): в 3-х ч. Ч. III. С. 161-167. ISSN 1997-292X.

Адрес журнала: www.gramota.net/editions/3.html

Содержание данного номера журнала: www.gramota.net/materials/3/2015/8-3/

12. Ahlquist A. Die Kulturwörter der westfinnischen Sprachen: ein Beitrag zu der älteren Kulturgeschichte der Finnen. Helsingfors, 1875. 323 S.
13. Ahlquist A. Om Ungerska sprakets förvandtskap med Finskan (A magyar és a finn nyelvek rokon-ságáról). Helsingfors, 1863. 280 S.
14. Ahlquist A. Wotisk grammatik jemte språkprof och ordförteckning. Helsingfors, 1855. 115 S.
15. Castrén M. A. Vorlesungen uber die Finnische Mythologie. Uebersezt von. A. Schifner. St.- Petersb., 1853. 349 S.
16. Thomsen V. Beriginger mellem de finske og de baltiske (litauisk-lettiske) Sprog. Kobenhavn, 1891. 192 S.
17. Thomsen V. Den gotiske sprogklasses inflydelse pe den finske. Kobenhavn, 1869. 244 S.
18. Walton G. M., Cohen G. L. A Question of Belonging: Race, Social Fit, and Achievement // Journal of Personality and Social Psychology. 2007. Vol. 92. No. 1. P. 82-96.

FAMILY RELATIONS AND SOCIAL STRUCTURE OF THE WESTERN FINNISH PEOPLE OF THE PERIOD OF THE EARLY MIDDLE AGES BY THE MATERIALS OF FINNISH LANGUAGE

Popova Mariya Sergeevna
Voronezh State University
middle_ages@inbox.ru

The article provides an analysis of the institution of the family relations and social structure of the Western Finnish people of the period of the early Middle Ages on the basis of linguistic data. The author examines the lexical units of Finnish language and the related languages**,** which allow better understanding the system of the blood relations and social relations of the Western Finnish people of the period of the early Middle Ages. The paper also studies the traces of the influence of other people and cultures on the objects under research.

Key words and phrases: social structure; family relations; blood relationships; the Western Finnish people; the early Middle Ages.

УДК 327.84
Политология

В статье рассматривается влияние международных отношений на кибербезопасность Российской Федерации, приобретающую в современных условиях всё большую актуальность. Определяются наиболее вероятные виды киберугроз, выявляются центры и методы противоправного воздействия. Прогнозируются некоторые направления кибервоздействия на отечественную информационную инфраструктуру. Основное внимание автор акцентирует на взаимосвязи политических явлений и информационного противоборства, выявленной в ходе изложенного анализа.

Ключевые слова и фразы: национальная безопасность; информационная безопасность; кибербезопасность России; киберугрозы; кибервойна; информационная война; международные отношения; политика; спецслужбы; кибершпионаж.

Сангалов Виктор Александрович
Нижегородский государственный университет имени Н. И. Лобачевского
vsangalov@gmail.com

УГРОЗЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИИ В ИНФОРМАЦИОННОЙ СФЕРЕ©

Актуальность рассматриваемых проблем определяется возрастающей ролью информационных технологий в современных международных отношениях, прежде всего в политическом противоборстве между государствами. Анализируются примеры практического применения кибернетического и информационного воздействия с целью оказания влияния на руководителей государств во время принятия внешнеполитических решений, сделана попытка спрогнозировать развитие ситуации и сформулировать ряд мер, необходимых для локализации возможных негативных последствий.

Угрозы безопасности России в киберпространстве

Согласно «Стратегии национальной безопасности Российской Федерации до 2020 года» [6] (далее – «Стратегия»), на обеспечение национальных интересов Российской Федерации (РФ) негативное влияние будут оказывать (наряду с другими факторами) силовые подходы в международных отношениях, а также совершенствование форм противоправной деятельности в кибернетической области и сфере высоких технологий. Прогнозируется увеличение глобального информационного противоборства, рост угрозы стабильности индустриальных и развивающихся стран мира, их социально-экономическому развитию и демократическим институтам. Получат развитие националистические настроения, ксенофобия, сепаратизм и насильственный экстремизм, в том числе под лозунгами религиозного радикализма.

Одной из основных угроз безопасности государства «Стратегия» определяет информационные средства ведения борьбы, в т.ч. способные привести к новому витку гонки вооружений в военной, политической и социальной плоскостях. Негативное воздействие на обеспечение национальной безопасности в сфере высоких технологий (IT-сфере) оказывают зависимость информационной инфраструктуры органов государственной

власти и управления, стратегических и критически важных объектов промышленного комплекса, средств массовой информации (СМИ) и т.д. от импортной компонентной базы, необоснованные односторонние санкции в отношении научных организаций России, недостаточное развитие нормативной правовой базы.

Для противостояния угрозам в области информационных технологий «Стратегия» предполагает: проведение перспективной военно-технической политики, разработку системы основополагающих концептуальных, программных документов, снижение зависимости от иностранной технологической базы за счёт инновационного развития национальной экономики, фундаментальной и прикладной науки. Также на обеспечение безопасности России в данном контексте оказывает влияние проведение рациональной и прагматичной внешней политики. В сложившейся в настоящее время внешнеполитической ситуации, в соответствии с положениями «Стратегии», Россия будет наращивать взаимодействие, в т.ч. и в области информационного противоборства, в первую очередь со странами РИК (Россия, Индия и Китай) и БРИК (Бразилия, Россия, Индия и Китай).

В целях определения сферы кибербезопасности, классификации угроз, декларирования методов информационного противоборства, способов защиты интересов личности, общества, государства, а также IT-инфраструктуры органов власти и управления, объектов промышленного комплекса, СМИ Указом Президента РФ от 9 сентября 2000 года № Пр-1895 утверждена «Доктрина информационной безопасности Российской Федерации» [3].

В последние несколько лет информационное противоборство на международной арене нарастает в нелинейной прогрессии. Секретарь Совета Безопасности России Н. П. Патрушев приводил данные о 90 миллионах кибератак на российские информационные ресурсы с 2010 года. За первое полугодие 2014 года количество подобных воздействий превысило 57 миллионов. С учётом данного факта органы власти на законодательном уровне стараются своевременно реагировать на вновь выявляемые направления и методы кибервоздействия. Например, в соответствии с положениями «Стратегии», с целью повышения эффективности противодействия киберугрозам и актуализации государственной политики, Советом Безопасности России 8 августа 2012 года определены «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов (КВО) инфраструктуры Российской Федерации» [7].

Кроме того, заинтересованными ведомствами периодически проводятся заседания, посвящённые острым вопросам информационной безопасности. Так, 29 ноября 2013 года в Совете Федерации состоялось парламентское обсуждение проекта Концепции стратегии кибербезопасности России, 1 октября 2014 года Президент РФ Владимир Путин на заседании Совета Безопасности РФ выступил по вопросу противодействия угрозам в информационной сфере и др.

Метод анализа реальных угроз кибербезопасности РФ в контексте международных политических событий

По информации, опубликованной в немецком журнале «Der Spiegel» на основании документов, предоставленных источниками из зарубежных спецслужб, Агентство национальной безопасности США (АНБ) готовится к новым этапам войны в киберпространстве. Отмечается подготовка к крупному конфликту с другими государствами именно в киберпространстве. На указанные цели АНБ в 2013 году получило бюджет в $1 млрд. Также для обеспечения превосходства США и их союзников (Великобритании, Канады, Австралии и Новой Зеландии) над потенциальными противниками хакеры из специальных военизированных киберподразделений должны будут сфокусировать свое внимание на уязвимых местах в их компьютерных системах. Речь идет, прежде всего, о жизненно важных системах электро- и водоснабжения, заводах, аэропортах и системах денежных потоков потенциального противника. Планируется проникновение хакеров АНБ в эти системы для внедрения вредоносного программного обеспечения. Приведено описание нескольких секретных программ по созданию подобного оружия в США.

По данным Национальной ассоциации инноваций и развития информационных технологий (НАИРИТ), количество DDOS-атак в 2013 году выросло на 178%, тогда как в предыдущие годы отмечалось ежегодное увеличение указанного показателя не более 15%.

На этом фоне и в связи с рядом негативных событий на мировой арене (обострение обстановки в странах Ближнего Востока, украинский кризис) в печатных и электронных СМИ возросло число публикаций об угрозах кибербезопасности России. Так, среднее число публикаций о событиях в информационной сфере в 2013 году составило 756 новостей, а в 2014 году – 768.

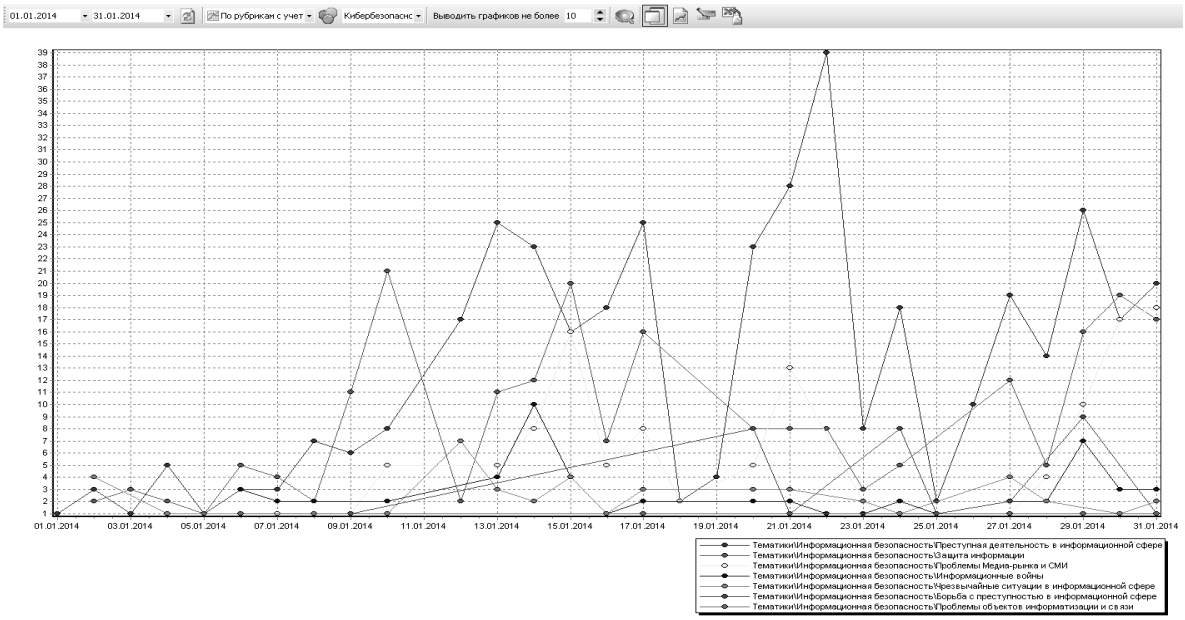
декабрь 13	598	декабрь 14	752
ноябрь 13	733	ноябрь 14	505
октябрь 13	1077	октябрь 14	1361
сентябрь 13	627	сентябрь 14	371
август 13	1029	август 14	631
июль 13	1031	июль 14	825
июнь 13	351	июнь 14	535
май 13	615	май 14	628
апрель 13	749	апрель 14	711
		март 14	1297
		февраль 14	933
		январь 14	664
среднее за месяц	**756**	**среднее за месяц**	**768**

Изложенные факты и упомянутое выше заявление Н. П. Патрушева подтверждает положение «Стратегии» о нарастании противоборства в информационной сфере.

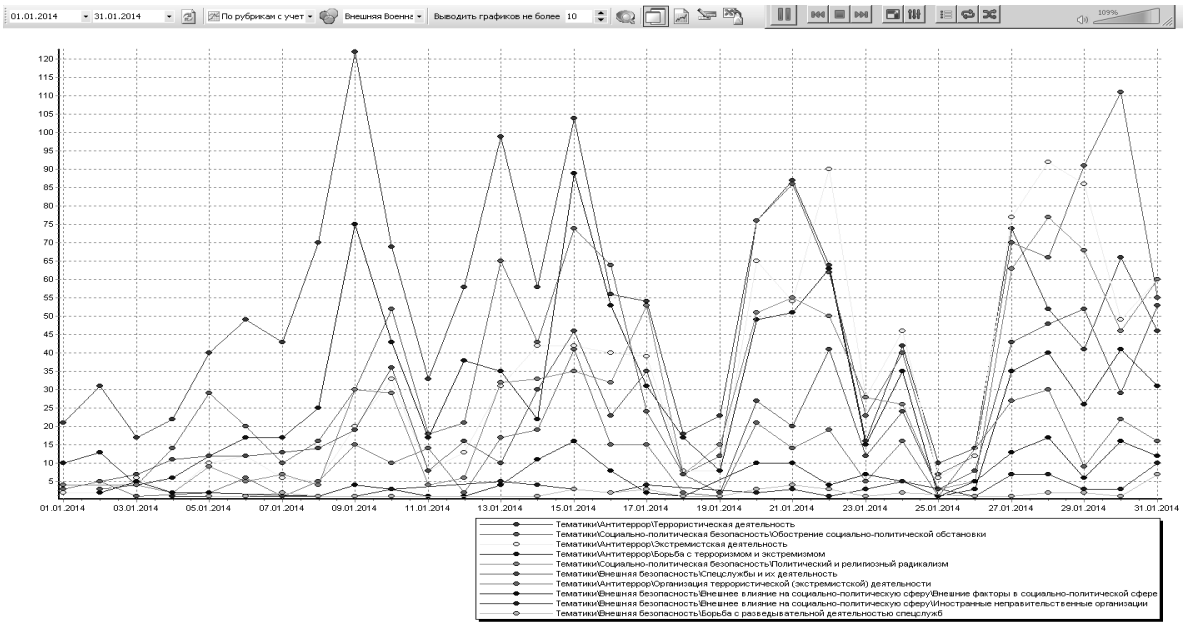
С целью определения реальных угроз кибербезопасности России со стороны зарубежных государств, направлений кибервоздействия, некоторых элементов тактики иностранных структур в этом направлении можно провести анализ влияния международных процессов на IT-безопасность. На основании полученных данных также представляется возможным оценить степень готовности России к подобного рода противостоянию, соответствие действующих направлений внешней и внутренней политики выявленным угрозам.

В ходе анализа оценивалось количество новостей (для удобства по месяцам) в военно- и внешнеполитической сферах, а также реакция в информационной области на наиболее резонансные мировые события. В качестве аналитического материала использовались публикации с 1 января 2014 года по 28 февраля 2015 года в ведущих отечественных СМИ (Российская газета, Российское информационное агентство «Новый регион», Эхо Москвы, Коммерсант и др.), электронных порталах (Утро.ru, Слон.ru, Деловые новости и др.) региональных и федеральных органов власти, различных политических течений, экспертных изданий, а также популярных блогах. Новости отбирались в различные тематики по направлениям «Информационная безопасность», «События в политической, оборонной и социальной сферах», а также «Внешняя безопасность». Для наглядности представим полученные результаты в графической форме.

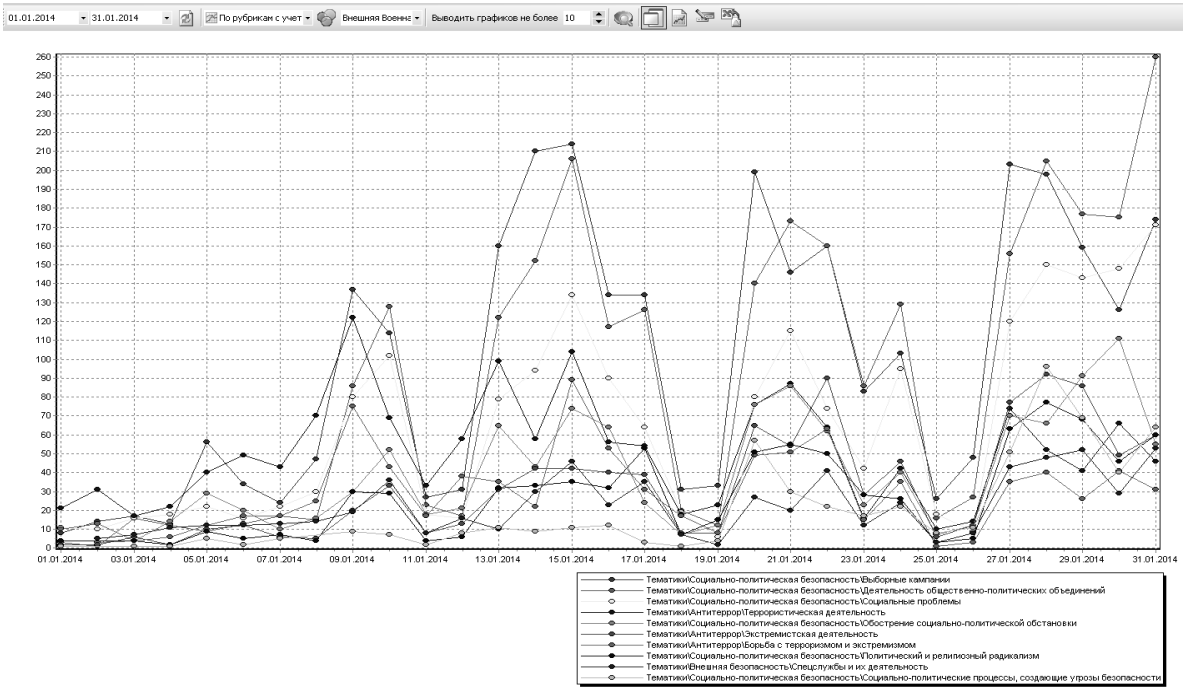
Пример графического представления новостей за январь 2014 года по указанным категориям (авторское исполнение)



«Новости в информационной сфере в январе 2014 года» (авторское исполнение)



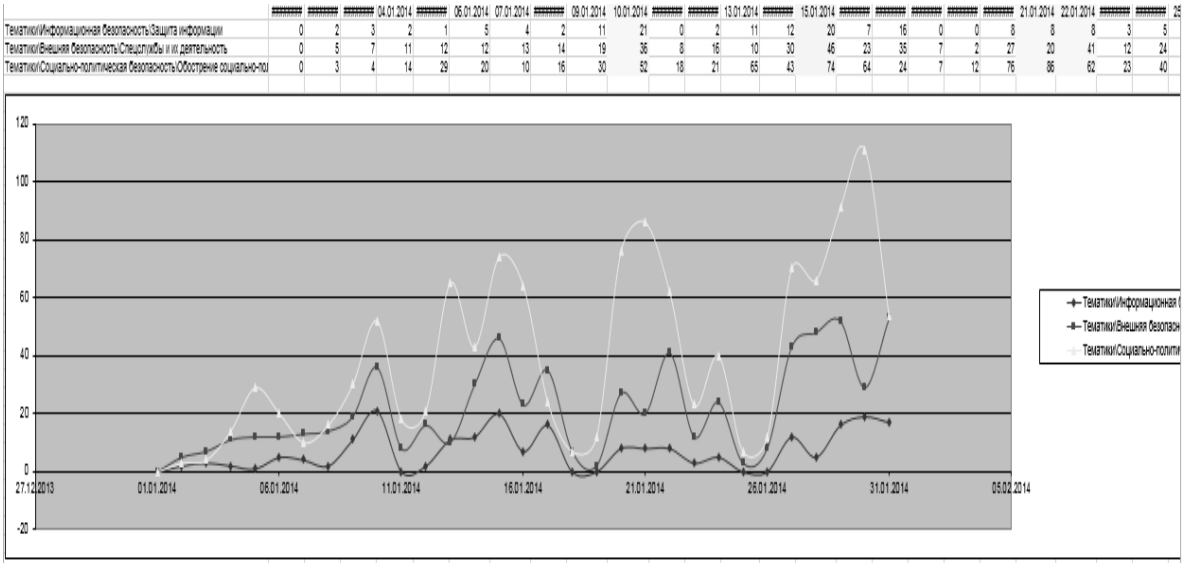
«Новости в политической и социальной сферах в январе 2014 года» (авторское исполнение)



Из оценки вида графиков можно сделать вывод о том, что существуют максимумы и минимумы, т.е. наблюдается реакция на мировые события, которая находит своё отражение и в информационной сфере. Ширина максимумов в среднем 3-4 дня, что может свидетельствовать о «подготовке информационного поля», самом событии, публикации подробной информации о его итогах. Следует отметить, что интерес к событию быстро спадает (1-2) дня. Графики новостей для различных тем из одного направления имеют похожий характер.

Для простоты анализа возьмём темы «Защита информации», «Спецслужбы и их деятельность» (предполагая, что кибервойны относятся к деятельности спецслужб) и «Обострение социально-политической обстановки» (в эту же тему попадали сообщения о внешнеполитических и военных событиях).

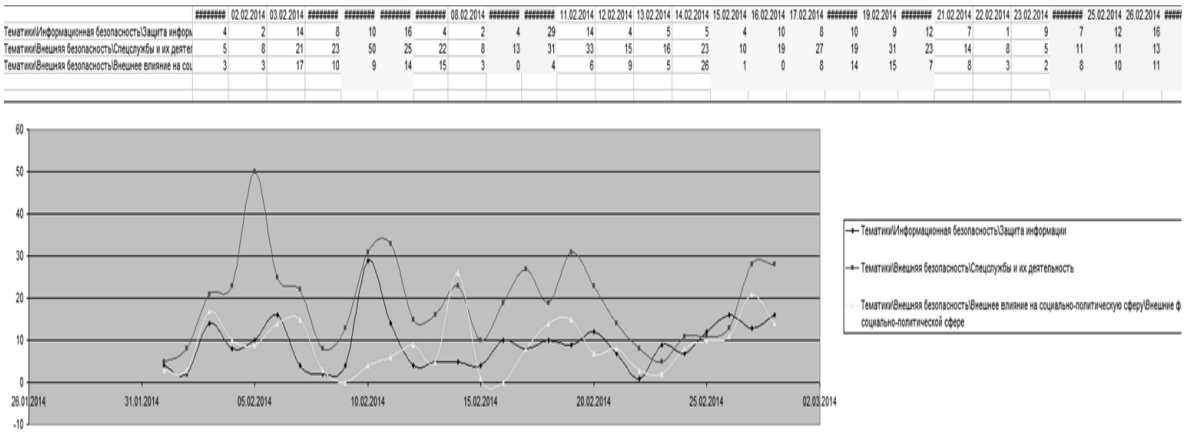
Пример указанных графиков за январь 2014 года (авторское исполнение)



Так, максимумы графиков «Спецслужбы и их деятельность» и «Обострение социально-политической обстановки» 10 января 2014 года обусловлены большим количеством новостей о крупнейшей утечке данных из Пентагона в связи с деятельностью Эдварда Сноудена. Существенный вклад в максимум графика «Защита информации» в этих же датах вносят новости об обсуждении «Концепции стратегии кибербезопасности РФ». В этой связи можно сделать вывод о получении российской стороной от Э. Сноудена информации о киберугрозах безопасности РФ со стороны США и соответственно ускорении процесса выработки предложений по их нейтрализации.

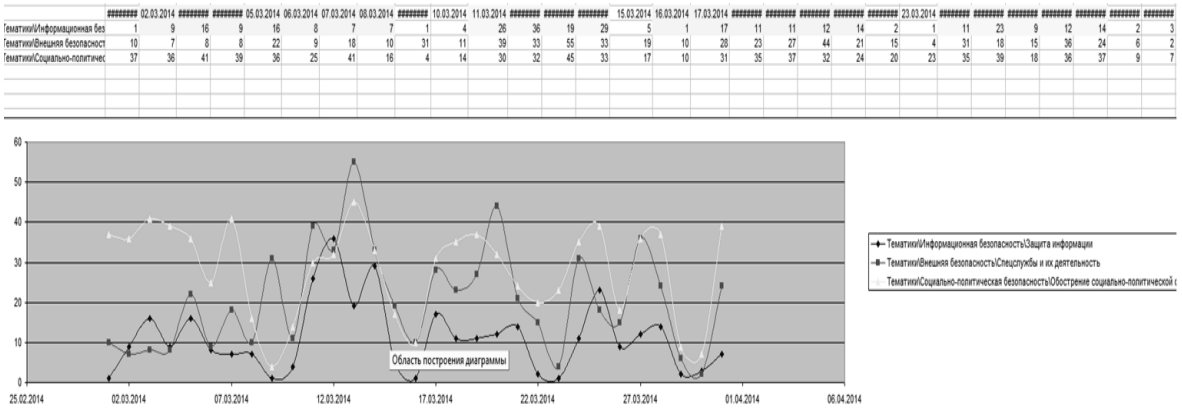
Максимумы 21 января 2014 года объясняются новостями о проведении встречи «Женева-2». В то же время в области информационной безопасности появилось большое количество сообщений о слежках спецслужб США за телефонными переговорами лидеров Европейского союза.

Графики новостей за февраль 2014 года (авторское исполнение)



Аналогичный анализ февральских новостей показывает рост числа публикаций о биткоинах. После заявлений некоторых важных политических игроков (Япония, Россия) о планах по интеграции биткоинов в финансовые и платёжные системы появились сообщения об атаках на биржу биткоинов. Исходя из этого, можно предположить, что ЕС и США увидели угрозу утраты части контроля над распределением финансовых потоков и организовали крах, а впоследствии запрещение биткоинов в некоторых странах.

Графики новостей за март 2014 года (авторское исполнение)



Пики графиков в марте 2014 года соответствуют DDOS-атакам на сайты ведущих российских СМИ, кредитно-финансовых учреждений накануне референдума в Крыму. Воздействие было оказано с территории Украины. В это же время на территории данной страны присутствовали специалисты в информационной сфере стран НАТО. Несмотря на потенциальную возможность спецслужб США организовать атаку на информационную инфраструктуру критически важных объектов (наподобие атаки вируса Stuxnet на ядерные объекты Ирана), ограничились лишь DDOS на популярные официальные сайты, что больше соответствует пропагандистскому воздействию нежели какой-либо деструктивной деятельности.

Из оценки графического представления видно, что в периоды отсутствия каких-либо международных крупных событий также отсутствовали и новости о кибератаках, имеющих какой-либо международный политический резонанс. Максимумы графика «Защита информации» во время отсутствия резонансных событий объясняются сообщениями о краже частной информации.

Выявленные реальные угрозы кибербезопасности России

Подобный анализ новостей, опубликованных в 2014 и начале 2015 гг., показал, что рост сообщений о хакерских атаках на официальные сайты новостных изданий, органов государственной власти, сайты кредитно-финансовых учреждений происходит в большинстве случаев во временных рамках важных политических событий (например, Олимпиада в г. Сочи). При этом зачастую атаки ограничиваются лишь блокированием доступа к сайтам, без каких-либо политических заявлений. Наиболее распространенными в настоящее время являются DDOS-атаки, проводимые перед важными событиями (референдум в Крыму), т.е. носящие характер «упреждающего удара».

Кроме атак на информационные ресурсы, в начале марта 2014 года с территории Украины (во время предполагаемого нахождения там экспертов по кибербезопасности стран НАТО) зафиксированы попытки несанкционированного доступа к космическим спутникам РФ, а 24 марта того же года вышел на орбиту российский спутник ГЛОНАСС.

На протяжении всего анализируемого периода отмечались сообщения о скандалах, связанных с просушкой политических деятелей, обвинением представителей какой-либо страны в крупных кражах пользовательских данных, банковской информации, выдачей третьими странами лиц, подозреваемых в противоправной деятельности в сфере информационной безопасности. События такого рода происходили во временных рамках политически важных встреч на высшем уровне.

Так, 11 июля 2014 года перед визитом В. В. Путина на Кубу, в США в прессе широко обсуждался арест по подозрению в киберпреступлениях российского гражданина. После визита российского лидера «Российская газета» неоднократно писала о попытках США дискредитировать политический строй на Кубе, отказываясь от традиционных форм и методов тайных операций Вашингтона в пользу приёмов кибервойны.

3 февраля 2015 года Голландия выдала США очередного российского хакера, подозреваемого в краже данных 160 млн кредиток, 5 февраля 2015 года Российских хакеров заподозрили в создании вируса-шпиона для *iPhone.* В то же время 5 февраля 2015 года пик новостных событий в политической сфере связан с проведением переговоров Ангелы Меркель и Франсуа Олланда в Москве.

Данные события можно считать частью информационного противоборства между руководством государств, в т.ч. и союзных (слежка США за Германией). Возможной целью указанного воздействия может являться стремление получить дополнительные аргументы на переговорах.

Рост сообщений о массовом заражении пользователей компьютерными вирусами в основном отмечался в период проведения крупных международных мероприятий (Чемпионат мира по футболу 2014 года, Олимиада в г. Сочи) и не носил политического либо военного характера. Однако имели место отдельные публикации об уникальных вредоносных программах (вирус *Stuxnet* на Иранских ядерных объектах, программная закладка в жёстких дисках, выявленная «Лабораторией Касперского» в феврале 2015 года). Характер используемых при этом технологий говорит о причастности к появлению данных вирусов экспертов иностранных спецслужб и о невозможности создания таких программ третьими лицами.

Ещё один вид киберугрозы – несанкционированный доступ к мобильным платформам зарубежных производителей (*iPhone*, смартфоны на базе *Android*), подтверждаемый периодическими новостями о появлении вирусов под данное оборудование, новостями о слежке за телефонными переговорами политиков, периодическими обвинениями ведущих государств в адрес компаний-производителей IT-техники. Например, 11 июня 2014 года китайцы сочли *iPhone* угрозой национальной безопасности, в феврале 2015 года появились новости о краже из облачного хранилища Д. А. Медведева нескольких гигабайт персональных и рабочих данных.

Необходимо отметить, что кроме описанных типов противоправного воздействия на информационные ресурсы в анализируемом периоде публиковались новости о китайских, северокорейских, исламских хакерах, однако их деятельность не была направлена против интересов нашей страны.

Таким образом, на сегодняшний день основными реальными угрозами кибербезопасности России в контексте политических процессов можно считать атаки на официальные Интернет-ресурсы различного рода организаций, а также провоцирование международных скандалов, основанием для которых служат обвинения граждан России в хакерской деятельности, с целью дискредитации международной политики, проводимой руководством РФ. Также фиксируются отдельные хорошо подготовленные целенаправленные атаки на важные объекты оборонной и промышленной инфраструктуры.

Достаточность законодательных, технологических и внешнеполитических мер, принимаемых руководством России для противодействия киберугрозам

Проведённый анализ позволяет сделать следующие выводы:

- «Стратегией национальной безопасности Российской Федерации до 2020 года» и «Доктриной информационной безопасности Российской Федерации» учтены практически все существующие на сегодняшнее время угрозы кибербезопасности России со стороны иностранных государств. С целью реализации политики противостояния такого рода воздействиям, руководствуясь указанной нормативно-правовой базой, руководством РФ принимаются меры по защите интересов нашей страны. Например, 29 ноября 2013 года в Совете Федерации состоялись парламентские слушания, посвященные проекту «Концепции стратегии кибербезопасности Российской Федерации», целью которой является определение целенаправленной и системной государственной политики развития национального сектора применения информационных технологий. Изложенный анализ подтвердил реальность угроз, указанных в Концепции.
- На базе спецслужб ведётся работа по созданию и совершенствованию «государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы России», состоящей из сети специальных центров по обеспечению кибербезопасности в регионах и главного центра. Задача комплекса – выявление, противодействие и ликвидация инцидентов, угрожающих безопасности «защищаемых информационных ресурсов». С помощью Системы анализируются поступающие из центров данные для «оценки степени защищенности информационных ресурсов» и предотвращения готовящихся кибератак. Так, 12 мая 2014 года в России созданы кибервойска. Стоит отметить, что в странах – мировых лидерах кибервойска уже существуют в течении нескольких лет.

- Государством на регулярной основе выделяются средства на снижение зависимости от иностранной программно-компонентной базы. Однако в условиях значительного технологического разрыва отечественная IT-инфраструктура (в т.ч. критически важных объектов ядерной, энергетической, оборонной промышленности, науки, систем связи, государственных органов) строится с высокой степенью использования импортных программно-аппаратных комплексов.
- В данных документах недостаточно отражён такой важный аспект, как воздействие на социально-политическую сферу посредством *web*-технологий. США активно используют этот метод ведения кибервойн.
- Переориентация российской политики в части, качающейся взаимодействия глобальной информационной безопасности, на выстраивание отношений с азиатскими партнёрами и сокращение взаимодействия с ЕС также соответствует мерам, определённым «Стратегией национальной безопасности РФ до 2020 года». В условиях напряжённых отношений между Россией и Западом такой шаг выглядит наиболее целесообразным. Также, как следует из оценки новостей в 2014 – начале 2015 годов, действия азиатских стран в киберпространстве не были направлены против российских интересов. Одновременно США предпринимают попытки по дискредитации на международной арене российско-китайского партнёрства. Об этом можно судить по заявлению 21 октября 2014 года представителей США о причастности властей Китая к похищению данных пользователей *iCloud*, в то время как накануне – 20 октября 2014 года – объявлено о намерении России и Китая подписать соглашение по кибербезопасности.
- Ещё одним шагом для обеспечения информационной безопасности РФ может стать инициатива по созданию международной нормативно-правовой базы, регулирующей отношения в киберпространстве, т.к. кибероружие в настоящий момент не попадает под международный контроль: оно не ограничено никакими конвенциями или надзорными органами.

Из приведённых пунктов видно, что меры, принимаемые российским руководством на законодательном (п. 1), внешнеполитическом (п. 5) и технологическом (п. 2, п. 3) уровнях в целом соответствуют существующим на сегодняшний момент угрозам национальной безопасности в информационной сфере и направлены на локализацию, а также упреждение негативного воздействия. Вместе с тем существуют области (п. 4, п. 6), которым стоит уделить больше внимания и сосредоточить работу на развитии предложенных направлений.

Список литературы

1. **Булавин А. В.** О подходах США и Китая к обеспечению кибербезопасности // Общество: политика, экономика, право. 2014. № 1. С. 27-31.
2. **Демидов О.** Киберкомандование США: уроки для России // Индекс безопасности. 2013. Т. 19. № 3 (106). С. 119-125.
3. **Доктрина информационной безопасности Российской Федерации**: утверждена Президентом РФ от 9 сентября 2000 года № Пр-1895 // Российская газета. 2000. 28 сентября.
4. **Казаковцев А. В.** НАТО и кибербезопасность // Вестник Волгоград. гос. университета. Сер. 4: История. Регионоведение. Междунар. отношения. 2012. № 2 (22). С. 110-113.
5. **Карпова Д. Н.** Киберпреступность: глобальная проблема и её решение // Власть. 2014. № 8. С. 46-50.
6. **О Стратегии национальной безопасности Российской Федерации до 2020 года**: Указ Президента РФ от 12 мая 2009 года № 537 // Собрание законодательства Российской Федерации. 2009. № 2. Ст. 2444.
7. **Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации** [Электронный ресурс]: утверждены Президентом РФ 3 февраля 2012 года № 803. URL: http://www.scrf.gov.ru/documents/6/113.html (дата обращения: 02.04.2015).
8. **Поскребышева Е. С., Старкин С. В.** Внешнеполитическая стратегия «Союза правых сил» и прогнозы национального разведывательного совета США: сравнительный анализ // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. Тамбов: Грамота, 2011. № 2 (8): в 3-х ч. Ч. 3. С. 144-148.
9. **Старкин С. В.** Проблемы типологизации разведывательной информации в американском теоретическом дискурсе // Вестник Нижегородского университета им. Н. И. Лобачевского. 2011. № 1. С. 329-335.

RISKS TO NATIONAL SECURITY OF RUSSIA IN INFORMATIONAL SPHERE

Sangalov Viktor Aleksandrovich
Lobachevsky State University of Nizhni Novgorod – National Research University
vsangalov@gmail.com

The article examines the influence of international relations on the cyber-security of the Russian Federation, which becomes even more relevant under modern conditions. The author mentions the most probable types of cyber-dangers, identifies the centers and methods of illegal influence, predicts certain trends of cyber-influence on domestic informational infrastructure. Special attention is paid to the interrelation of political phenomena and informational confrontation identified in the course of the analysis.

Key words and phrases: national security; informational security; cyber-security of Russia; cyber-dangers; cyber-war; informational war; international relations; policy; special services; cyber-espionage.