DOI 10.22394/2073-2929-2020-1-72-77

Сценарное моделирование информационно-политических угроз в интернет-пространстве

Борщенко В. В.

Северо-Западный институт управления РАНХиГС, Санкт-Петербург, Российская Федерация; boss-victor@yandex.ru

РЕФЕРАТ

В статье рассматриваются информационные угрозы воздействия различных методов политической манипуляции, влияющие на социальное развитие страны.

Теория сценариев, представленная в статье, позволяет оценивать возможные альтернативные варианты их реализации в интернет-пространстве.

Обоснован метод сценарного прогнозирования информационно-политических угроз.

Ключевые слова: информационно-политические угрозы, политическая манипуляция, теория сценариев, информационно-ресурсный потенциал, безопасность

Scenario Modeling of Information and Political Threats in the Internet

Victor V. Borshchenko

North-West Institute of management — branch of RANEPA, St. Petersburg, Russian Federation; boss-victor@yandex.ru

ABSTRACT

The article deals with information threats concerning the influence of different political manipulation methods, affecting the social development of the country. The theory of scenarios presented in the article allows to evaluate possible alternatives to their implementation in the Internet space. The scenario forecasting method for information and political threats is proved.

Keywords: Information and political threats, political manipulation, scenario theory, information and resource potential, security

Развитие информационных технологий и формирование на их основе информационного общества привели к появлению принципиально новых механизмов, влияющих на развитие общественно-политических процессов в государстве. В основе этих механизмов лежит использование информации в глобальном информационном пространстве. Важнейшим элементом этого пространства является Интернет, представляющий собой глобальную сеть, объединяющую все компьютерные устройства, независимо от того, в какой точке Земли они находятся в случае их подключения к этой сети.

Информационно-ресурсный потенциал сети включает в себя множество элементов, как связанных собственно с информацией (ее накоплением, обработкой, сохранением и использованием), так и с технологическими процессами, обеспечивающими эффективность воздействия с помощью информации на общественное сознание, что порождает определенные риски.

Далее приведем определения некоторых терминов в соответствии с ГОСТ Р 51898-2002 «Аспекты безопасности. Правила включения в стандарты»:

• риск — это термин, сочетающий в себе вероятность нанесения определенного ущерба и тяжесть этого ущерба, который рассматривается как нанесение вреда здоровью людей, имуществу или окружающей среде;

- допустимый риск это риск, который в данной конкретной ситуации считается приемлемым при существующих общественных ценностях;
- остаточный риск это риск, остающийся после принятия защитных мер;
- опасность потенциальный источник возникновения ущерба;
- безопасность состояние защищенности, при котором отсутствует возможность реализации недопустимого риска.

Под оценкой риска предлагается понимать процесс анализа потенциальной опасности посредством использования информации для ее выявления и количественной оценки, а также основанную на результатах анализа процедуру проверки, устанавливающую, не превышен ли допустимый риск. На рисунке, приведенном ниже, данный процесс представлен схематически.

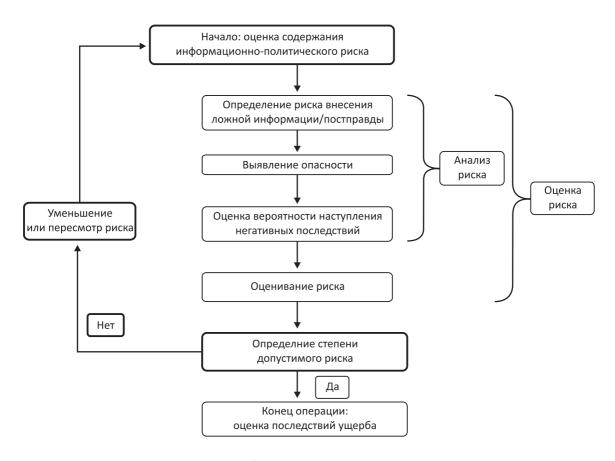


Рис. Итеративный процесс оценки риска и уменьшения риска

Источник: Составлено автором на основе ГОСТ р 51898-2002 [Электронный ресурс]. URL: https://www.lawmix.ru/gosts/4386 (дата обращения: 17.12.2019)

Основной сферой информационно-политических угроз является информационное обеспечение действий в области политики, политической жизни общества, в пределах распространения непосредственного влияния политиков и политических организаций, воздействия политических идей.

- Информационно-политическая угроза совокупность факторов и условий, создающих опасность нарушения информационно-политической безопасности.
- Информационно-политические риски сочетание вероятности реализации информационно-политических угроз и ущерба вследствие реализации этих угроз.

• Информационно-политическая безопасность — состояние защищенности информационно-политической среды.

В настоящее время эта сфера существенно расширена за счет потенциальных возможностей Интернета по созданию и тиражированию политической информации в рамках персонального контента (блоги, чаты, форумы, сайты) и рассылки ее политическим сторонникам, в адрес политических партий и органов государственной власти; участию в блогах, чатах, форумах и телеконференциях политических партий, некоммерческих организаций (в части политических вопросов), представителей государственной власти, политических лидеров, депутатов; участию в политических мероприятиях, таких как: интернет-голосования, референдумы, социологические опросы; выработка политических программ, законодательных инициатив, проектов политических решений и других; виртуальные съезды партий и проведение других политических мероприятий; организации своих сторонников для участия в реальных политических действиях (митинг протеста или поддержки, подача петиций, забастовки, политические акции и т. п.).

Определение степени допустимого риска регламентируется разработанными стандартами, технологическими нормами, социальными запросами, политической целесообразностью и т. п.

Информационно-политические угрозы представляют собой развивающийся во времени и пространстве процесс применения различных методов политической манипуляции, с целью формирования у объектов манипуляции требуемых взглядов на социально-политическое развитие страны. Среди различных видов манипулирования особую чувствительность к изменяющимся условиям распространения информации имеет политическое манипулирование. Обобщая ряд определений, которые даются энциклопедическими словарями, можно выделить следующие параметры этого воздействия: оно представляет собой систему способов (методов) воздействия, которые, как правило, не действуют непосредственно и не носят характер «директивы», однако в общественном и в индивидуальном сознании под их влиянием возникают политические установки или закрепляются паттерны политического поведения, направленные на достижение целей организаторами соответствующего воздействия. Достаточно часто манипулирование осуществляется в рамках «психологической модели», которая позволяет вызывать определенную реакцию индивида на триггеры, вызывающие предсказуемую реакцию. Данный подход носит в определенном смысле механистический характер и основывается на разработке методов психологической обработки человека с целью вызвать у него строго определенную реакцию.

В зависимости от преследуемых целей можно выделить следующие виды политической манипуляции:

- действия, которые направлены на убеждение и вовлечение групп людей и организаций в проект или цель, которая была поставлена;
- действия, которые проводятся для достижения цели.

В основе моделирования таких процессов лежит теория сценариев, на основе которой строятся гипотетические логически связанные последовательности событий.

Теория позволяет: во-первых, определять конкретные варианты будущего развития информационно-политических угроз и при необходимости наращивать множество вариантов их развития; во-вторых, количественно или качественно оценивать возможные альтернативные варианты их реализации¹. К основным видам сценариев относятся: вербальные сценарии (сценарии-эссе, аналитический сценарий)², фрейм-сценарии [5; 6], веера вариантов (решений, концепций) [1; 3], информационно-признаковые модели [2] и некоторые другие.

В качестве исходных данных для построения сценариев могут быть использованы: наличие проблемной (военной, политической, экономической или другой) ситуации, заключающей в себе объект и предмет анализа; количественные и качественные характеристики субъектов проблемной ситуации, в том числе степень их значимости; условия и факторы развития ситуации, их информационные признаки, связи между ними, их количественные и качественные характеристики; масштаб действия, вре-

² Понятие сценария в политической науке [Электронный ресурс]. URL: http://lektsii.com/2-57851.html (дата обращения: 10.12.2019).

¹ Белякова Г. Я. Методология научных исследований в менеджменте : учеб. пособие / Г. Я. Белякова, Л. Р. Батукова, С. А. Беляков. Красноярск : Сиб. федер. ун-т, 2013. С. 21–23.

менной интервал, социальное пространство, которое охватывает проблемная ситуация; особенности отражения проблемной ситуации в общественном сознании, степень ее значимости для общества; предполагаемые варианты и результаты разрешения проблемной ситуации (конечные состояния развития проблемной ситуации); конкретный и поэтапный план действий (как последовательность некоторой совокупности мероприятий), направленный на ее оперативное разрешение.

Эти исходные данные широко используются для построения типовых сценариев развития информационно-политических угроз различного вида.

Вместе с тем в известных методах сценарного моделирования слабо учитывается влияние состояния информационной среды на процесс формирования и развития этих угроз в целом, а также не рассматривается зависимость состояния акторов от информационного воздействия. Кроме того, типовые модели требуют их адаптации к конкретной общественно-политической обстановке, особенностям политических взглядов различных слоев населения, социальных групп, государственных, политических и общественных деятелей, в том числе их индивидуальных свойств (характеристик) и т. п.

Вместе с тем в известных подходах есть ряд методологических приемов, комплексное применение которых позволяет на их основе построить новую общую технологию сценарного моделирования информационно-политического воздействия (манипулирования), учитывающую информационный фактор в процессе формирования и развития угрозы. Эта технология представляет собой взаимосвязанную реализацию следующих модельных блоков: «структура информационно-политической угрозы», «политическая структура», «определение информационно-критических элементов политической структуры», «операционно-временная модель информационно-политического воздействия», «оценка текущего состояния информационно-политической безопасности».

Модельный блок «структура информационно-политической угрозы» представляет собой совокупность проявляющихся в информационном пространстве информационных признаков (фактов), характеризующих объективно сложившуюся совокупность неблагоприятных условий и факторов (форс-мажор), субъективные намерения и замыслы (желания), объективные возможности реализации субъективных намерений, наличие существующих сил и средств, а также необходимых и достаточных условий, складывающихся без участия субъекта или создаваемые субъектом. Модельный блок «политическая структура» представляет собой описание основных элементов политической структуры страны и их связи между собой и с внешней средой. Основное внимание при моделировании политической структуры должно уделяться изучению зависимости состояния каждого элемента политической структуры от воздействия различных видов информации.

Модельный блок «определение информационно-критических элементов политической структуры» представляет собой механизм определения таких элементов ее институциональной, нормативной, коммуникативной, культурно-идеологической, функциональной подсистем, а также таких элементов ее информационной инфраструктуры, акт манипуляционного воздействия в отношении которых или нарушение (или прекращение) функционирования информационных компонент которых приводит к потере государственного или политического управления, разрушению инфраструктуры, необратимому негативному изменению (или разрушению) экономики страны, субъекта Российской Федерации либо административно-территориальной единицы или существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный срок. На эти элементы информационнополитическое воздействие осуществляется в первую очередь.

Модельный блок «операционно-временная модель информационно-политического воздействия» представляет собой установление сложившейся на конкретный момент времени совокупности информационных признаков и связей между ними, характеризующей какое-либо манипуляционное воздействие в Интернете (информационно-признаковая модель на уровне элементарных информационных признаков), либо определение вариантов действий (операций) по реализации методов информационно-политического манипулирования в Интернете во времени (информационно-признаковая модель в терминах мероприятий) и возможных конечных результатов реализации угрозы.

Модельный блок «оценка текущего состояния информационно-политического воздействия» представляет собой механизм определения по выявленной совокупности информационных признаков (фактов) отдельных действий по применению методов информационно-политического воздействия и их места в одной из разработанных операционно-временных моделей. Факт проведения какого-либо мероприятия (угрозы) в этих моделях позволяет прогнозировать возможность наступления связанного с ним последующего мероприятия (угрозы). Это позволяет контролировать динамику развития угрозы и принимать обоснованные меры для ее ликвидации. Модельный блок «расчет индекса политической безопасности» представляет собой использование прогнозной вероятности реализации информационно-политических угроз для расчета численного значения индекса политической безопасности, в зависимости от применяемого метода информационно-политического манипулирования, например, по методике ПИР-Центра (российский аналитический центр, специализирующийся на научно-исследовательской, образовательной и издательской деятельности в области международной безопасности)¹.

Таким образом, предлагаемый метод сценарного прогнозирования информационно-политических угроз позволяет: во-первых, построить модели информационно-политических угроз, реализуемые на основе методов информационно-политического манипулирования в интернет-пространстве с учетом его информационно-ресурсного потенциала; во-вторых, определить основные направления информационно-политического воздействия (информационно-критические элементы политической системы) и выработать меры превентивного противодействия ожидаемым угрозам; в-третьих, получить численные значения опасности информационно-политической угрозы на различных этапах ее развития для принятия квалифицированных решений.

Литература

- 1. Де Боно Эдвард. Использование латерального мышления [Электронный ресурс]. URL: http://www.pseudology.org/webmaster/Bono_LateralnoeMyshlenie2.pdf (дата обращения: 10.12.2019).
- 2. *Левкин И. М., Микадзе С. Ю.* Добывание и обработка информации в деловой разведке. СПб: ИТМО. 2015. С. 15–18.
- 3. Метод генерации идей: веер концепций [Электронный ресурс]. URL: http://prismotrov.com/idea-generation-method-conceptual-fan/ (дата обращения: 12.12.2019).
- 4. Метод сценария: примеры и история [Электронный ресурс]. URL: http://fb.ru/article/281994/metod-stsenariya-primeryi-i-istoriya (дата обращения: 13.12.2019).
- 5. Минский М. Фреймы для представления знаний [Электронный ресурс]. URL: https://litresp.ru/chitat/ru/%D0%9C/minskij-marvin/frejmi-dlya-predstavleniya-znanij (дата обращения: 13.12.2019).
- 6. Schank R., Abelson R. Scripts Plans and Knowledge, Advance Papers of Fourth Intern. Joint Conf. On Artif. Intell., 1975, № 2. Р. 151–157. [Русский перевод: Труды IV Межд. конф. по искусств, интеллекту. Т. 6. М.: Научн. совет по компл. пробл. «Кибернетика» АН СССР, 1975. С. 208–220].

Об авторе:

Борщенко Виктор Владимирович, преподаватель факультета профессионального образования и довузовской подготовки Северо-Западного института управления РАНХиГС (Санкт-Петербург, Российская Федерация); boss-victor@yandex.ru

References

1. *De Bono Edvard.* Ispol'zovanie lateral'nogo myshleniya [Elektronnyi resurs]. URL: http://www.pseudology.org/webmaster/Bono LateralnoeMyshlenie2.pdf (data obrashcheniya: 10.12.2019).

¹ Индекс международной безопасности iSi (описание и методология расчета) [Электронный ресурс]. URL: http://www.pircenter.org/media/content/files/9/13462438640.pdf (дата обращения: 13.12.2019).

- 2. Levkin I. M., Mikadze S. Yu. Dobyvanie i obrabotka informatsii v delovoi razvedke. SPb: ITMO. 2015. S. 15–18.
- 3. Metod generatsii idei: veer kontseptsii [Elektronnyi resurs]. URL: http://prismotrov.com/idea-generation-method-conceptual-fan/ (data obrashcheniya: 12.12.2019).
- 4. Metod stsenariya: primery i istoriya [Elektronnyi resurs]. URL: http://fb.ru/article/281994/metod-stsenariya-primeryi-i-istoriya (data obrashcheniya: 13.12.2019).
- 5. *Minskii M.* Freimy dlya predstavleniya znanii [Elektronnyi resurs]. URL: https://litresp.ru/chitat/ru/%D0%9C/minskij-marvin/frejmi-dlya-predstavleniya-znanij (data obrashcheniya: 13.12.2019).
- 6. *Schank R., Abelson R.* Scripts Plans and Knowledge, Advance Papers of Fourth Intern. Joint Conf. On Artif. Intell., 1975, № 2. P. 151–157. [Russkii perevod: Trudy IV Mezhd. konf. po iskusstv, intellektu. T. 6. M.: Nauchn. sovet po kompl. probl. "Kibernetika" AN SSSR, 1975. S. 208–220].

About the author:

Victor V. Borshchenko, Lecturer of Department of Pre-University and Professional Training of North-West Institute of Management — Branch of RANEPA (Saint Petersburg, Russian Federation); boss-victor@yandex.ru