

Секция «Математическое моделирование политических процессов»

Моделирование угроз национальной безопасности Российской Федерации в информационной сфере на основе метода дерева целей

Кривельская Екатерина Петровна

Аспирант

Московский государственный лингвистический университет, Москва, Россия

E-mail: krivelskaya.ekaterina@yandex.ru

- 1) В связи со стремительно меняющейся международной обстановкой и появлением новых вызовов и угроз в международных отношениях задача обеспечения информационной безопасности, как следствие развития информационных технологий занимает значительное место в системе обеспечения национальной безопасности России. В период массовой информатизации всех сфер человеческой деятельности одной из важнейших составляющих национальной и международной безопасности становится информационная безопасность и защита информации, которая считается стратегическим национальным ресурсом.
- 2) Одним из перспективных методов анализа сложных социально-политических проблем, достаточно широко применяющимся в последнее время, является так называемый метод дерева целей, в основе которого лежит процедура декомпозиции рассматриваемой сложной проблемы на более простые составляющие ее подпроблемы, их анализ и последующий синтез решения исходной проблемы. Метод дерева целей и основанные на нем предметно-ориентированные технологии могут применяться и при исследовании проблем национальной безопасности Российской Федерации в информационной сфере.
- 3) На первом этапе был проведен анализ действующей Доктрины информационной безопасности Российской Федерации, принятой в 2000 году. Представленные в Доктрине угрозы были актуализированы, детализированы и выстроены в виде иерархической структуры. В разработке иерархии угроз учитывались новые тенденции и явления в информационной сфере, которые представляют на данном этапе развития определенную опасность для национальной безопасности России. Представленная иерархия содержит 4 уровня с 49 узлами угроз и 5 источников угроз.
- 4) На сегодняшний день можно выделить две большие группы угроз информационной безопасности России: «1. Угрозы в гуманитарной сфере» и «2. Киберугрозы», которые составляют первый уровень угроз.
- 5) В отличие от Доктрины информационной безопасности Российской Федерации от 2000 года в данной модели были выделены и детализированы угрозы в гуманитарной сфере, а именно угрозы существующей политической системе, которые включают в себя такое явление как «цветные» и «интернет революции». Кроме того, особое внимание уделено аспекту духовно-нравственного развития России и ее имиджу, которые включают в себя угрозы подмены культурных и духовно-нравственных ценностей, духовно-нравственного упадка, снижения уровня культуры и образования, дискредитации религиозных институтов и оскорбления чувств верующих, а также деградации образовательных институтов, института брака и семьи, русского языка и культуры.
- 6) Что касается источников угроз, то к ним были отнесены следующие: иностранные государства, органы государственной власти РФ, несистемная оппозиция, криминальные структуры и элементы, террористические группировки.

- 7) Формирование деревьев угроз, подобных представленному выше, является, на наш взгляд, весьма важной и перспективной задачей. Действительно, даже если не будет проводиться количественный анализ деревьев угроз и их «привязка» к возможным сценариям развития ситуации или стратегиям поведения сторон, наличие достаточно полной базы данных подобных иерархических структур обеспечит существенную поддержку в информационно-аналитической работе.
- 8) На втором этапе исследования была проведена экспертная оценка степени относительной (сравнительной) значимости угроз информационной безопасности России со стороны представленных источников угроз. Оценки угроз были выставлены на основе метода последовательного сравнения с дальнейшим нормированием их приоритетов.
- 9) В целом сравнивая основные группы угроз («1. Угрозы в гуманитарной сфере» и «2. Киберугрозы») можно видеть, что угрозы, связанные с гуманитарной сферой, представляются более значимыми (оценка значимости -0,6), нежели киберугрозы (оценка значимости - 0,4). Если рассмотреть детализацию этих угроз, т.е. перейти к рассмотрению угроз 2-го, 3-го и 4-го уровней, то данный вывод также находит свое подтверждение. Таким образом, для национальной безопасности России в информационной сфере в настоящий момент более существенными представляются угрозы в гуманитарной сфере, нежели в киберпространстве, что связано с актуальными явлениями на международной арене и уже имеющимся опытом России, когда из-за агрессивного информационно-психологического воздействия на сознание граждан, а также негативное воздействие на все остальные составляющие гуманитарного аспекта информационной безопасности, в 1990-е годы нашей стране был нанесен ущерб, ликвидация последствий которого потребовала долгих лет.
- 10) Что касается значимости и влиятельности источников угроз, то согласно построенной модели наиболее значимым источником угроз являются иностранные государства (оценка значимости - 0,473), далее идут органы государственной власти РФ (оценка значимости - 0,16) и несистемная оппозиция (оценка значимости - 0,153), далее следуют террористические группировки (оценка значимости - 0,114) и криминальные структуры и элементы (оценка значимости - 0,1).
- 11) Следует отметить, что органы государственной власти в качестве источника угроз информационной безопасности занимают второе место по своей значимости и влиянию в связи с нерешенностью ряда проблем в социальной жизни общества, таких как, например, состояние сферы образования и здравоохранения, ненадлежащим исполнением указов и распоряжений президента России, а также в связи с несбалансированной расстановкой приоритетов развития общества, ухудшающимся экономическим положением страны и падением материального благосостояния граждан.
- 12) На основе проведенного исследования и построенной модели можно констатировать, что для Российской Федерации на данном этапе приоритетным направлением обеспечения информационной безопасности страны является гуманитарная сфера, что обусловлено уже имеющимися проблемами в этой области. Что касается кибербезопасности, то данное направление только набирает свою значимость и является весьма важной областью обеспечения информационной безопасности России. Говоря о существующих источниках угроз, то на данный момент наиболее высокую степень угрозы представляют иностранные государства, затем «следуют» органы государственной власти, и несистемная оппозиция, идущая с небольшим «отставанием». Поскольку оценки значимости источников угроз имеют долю субъективности, то при тех или

иных изменениях во внешнем или внутреннем климате страны, значимость госструктур и несистемной оппозиции может колебаться. Однако следует подчеркнуть, что все же в обозримом будущем основным источником угроз будут выступать иностранные государства.

Источники и литература

- 1) Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895.
- 2) Стратегия национальной безопасности Российской Федерации до 2020 года. Утверждена Указом Президента Российской Федерации от 12 мая 2009 г. № 537
- 3) Выписка из «Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». Концепция утверждена Президентом Российской Федерации 12 декабря 2014 г. № К 1274.
- 4) Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. Утверждены Президентом Российской Федерации Д.Медведевым 3 февраля 2012 г., № 803.
- 5) Стратегия развития информационного общества в Российской Федерации. Утверждена Президентом Российской Федерации В.Путиным 7 февраля 2008 г., № Пр-212.
- 6) Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. Утверждены Президентом Российской Федерации В.Путиным 24 июля 2013 г., № Пр-175.
- 7) Т.Саати. Принятие решений. Метод анализа иерархий. Перевод с английского Р. Г. Вачнадзе. Москва: Радио и связь, 1993. 278 с.

Слова благодарности

Слова благодарности хотелось бы выразить моему научному руководителю, доктору технических наук, Абаеву Льву Черменовичу за отвагу научить гуманитария методам математического моделирования и компьютерного анализа, а так же заведующему кафедрой политологии Белозерову Василию Клавдиевичу за наставления и поддержку во всех начинаниях молодых и талантливых.

Иллюстрации

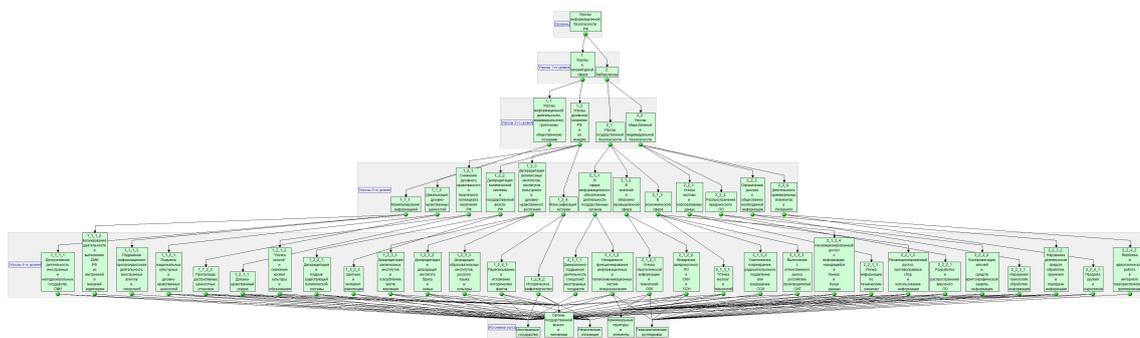


Рис. 1. Иерархия угроз информационной безопасности России

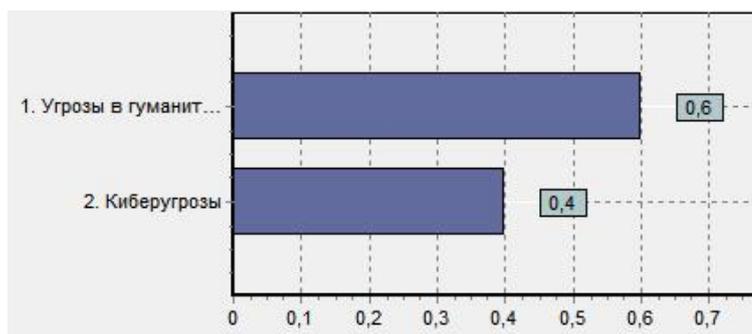


Рис. 2. Угрозы первого уровня

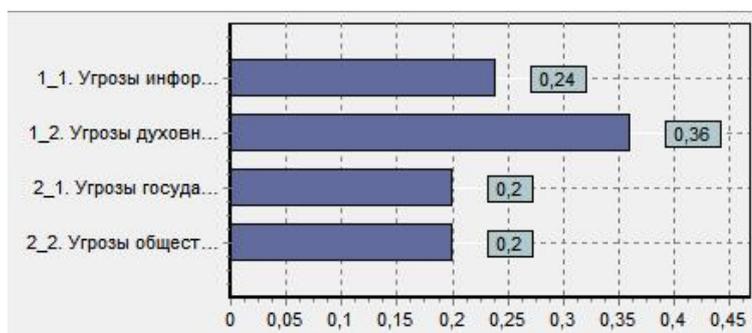


Рис. 3. Угрозы второго уровня

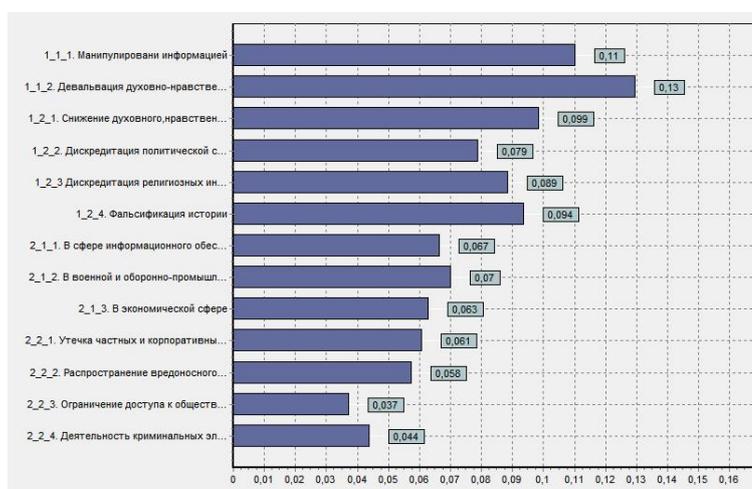


Рис. 4. Угрозы третьего уровня

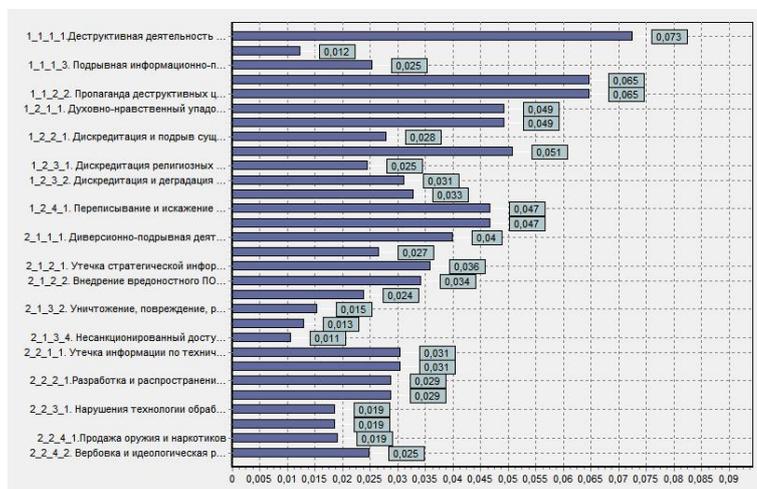


Рис. 5. Угрозы 4-го уровня

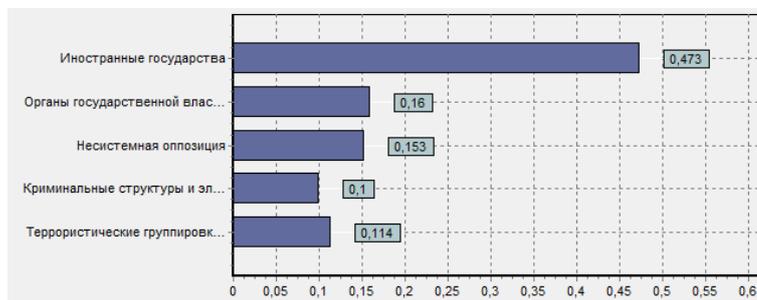


Рис. 6. Источники угроз