

МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В УСЛОВИЯХ КОНФЛИКТОВ

Евневич Е.Л.¹, Фаткиева Р.Р.²

Аннотация

Цель: разработка модели конфликта в условиях информационного воздействия при ограничении расходов на мероприятия противодействия.

Метод: математическое моделирование осуществляется с использованием марковской модели развития ситуации в условиях конфликта противоборствующих сторон. Оценка вероятности нахождения системы в том или ином состоянии в заданное время позволяет произвести анализ состояния системы при наличии и отсутствии информационных воздействий, их распознавание и применение защитных мер, а также анализ переходов между этими состояниями.

Результат: разработана модель, которая может быть применена для формализации и оценки защищенности социально-важных объектов. Разработанный метод учитывает изменяющиеся условия функционирования защищаемой информационной системы и заключается в определении текущего состояния системы, прогнозировании её поведения с помощью марковской модели при различных конфигурациях системы защиты и в выборе конфигурации, позволяющей достичь максимальной эффективности функционирования системы.

Ключевые слова: информационное воздействие, марковская модель, конфронтация, противодействие, прогнозирование.

DOI:10.21681/2311-3456-2020-2-42-49

Введение

Массовые «информационные вбросы» в обществе могут привести к потере баланса в социально-экономических системах и резкому переходу к новому равновесию. Такие события могут быть неблагоприятными для их участников, хотя каждый участник может потерять еще больше, не подчиняясь всеобщей активности. Адаптивная массовая активность людей в указанных условиях может привести к социальным и экономическим потерям. Эти потери могут быть сокращены информационным противодействием, самоорганизацией посредством целенаправленных действий, требующих дополнительных ресурсов. Для изучения факторов неблагоприятных массовых событий могут быть использованы нелинейные модели с одновременным усилением, отслеживанием и ограничением влияния информационных процессов на массовые элементы системы. Однако такое ограничение требует привлечения дополнительных ресурсов. Массовые события, связанные с поведением независимых субъектов (физических и юридических лиц) могут оказать значительное влияние на социально-экономические процессы и системы. При моделировании сильных и нежелательных воздействий на систему возникают ситуации со следующими типичными особенностями:

- субъекты могут инициировать однотипные по смыслу информационные сообщения, приводя-

щие к массовым событиям, последствия которых затрагивают каждого субъекта, в то же время последствия зависят от общего числа участников действий;

- если количество участников, выполняющих информационные воздействия, достигает некоторого заданного значения, субъекты, не участвующие в действиях, сталкиваются с ущербом (нежелательными последствиями) или ожидают возникновения ущерба (нежелательных последствий в будущем) и фактический или ожидаемый ущерб увеличиваются с отсрочкой принятия решения о присоединении к действиям;
- все участники терпят ущерб в результате массовых событий, вызванных деструктивной информацией;
- интенсивность массовых событий может быть снижена в результате привлечения дополнительных информационных ресурсов.

Исследование различных сценариев поведения показало, что синергетический эффект от влияния информационного воздействия друг на друга двух подсистем проявляется либо в достижении неустойчивого равновесия, либо в хаотическом поведении с влиянием случайных факторов на утрату равновесия. Анализ результатов поведения позволил установить возмож-

1 Евневич Елена Людвиговна, кандидат физико-математических наук, старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, Санкт-Петербург, Россия. E-mail: eva@iiias.spb.su (ORCID ID 0000-0002-8203-0814)

2 Фаткиева Роза Равильевна, кандидат технических наук, доцент, старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, Санкт-Петербург, Россия. E-mail: rikki2@yandex.ru (ORCID ID 0000-0003-4065-9611)

ные причины неожиданного катастрофического роста интенсивности массовых событий, которые могут иметь место при воздействии деструктивных сообщений. Временные задержки влияния отдельных групп субъектов друг на друга и случайные факторы могут привести к неустойчивому режиму функционирования системы. При этом после этого уход от катастрофической траектории требует гораздо больше ресурсов, чем предотвращение утраты равновесия. Все это демонстрирует, что в современном обществе увеличивается зависимость поведения населения от содержания информационного потока. Такой поток на различных уровнях несет в себе как позитивную, так и деструктивную составляющую, где в качестве деструктивной составляющей могут выступать [1]:

- ложные сообщения об авариях на предприятиях промышленности (атомных электростанциях, химических заводах и других), о заминированных домах, поездах, самолетах, о финансовых крахах компаний, провокации и слухи в политической сфере;
- различного вида информация, вызывающая страх, агрессию, недовольство, раздражительность, порождающая сомнения, призывающая к деструктивным действиям;
- информационные сигналы, изменяющие психофизическое состояние людей, повышающие их утомляемость, вызывающие головные боли, повышающие давление и другие;
- деструктивные программы как отрицательно влияющие на людей, так и дезорганизирующие различные системы управления, вычислительные сети и технические средства и так далее.

Известны публикации, связанные с общими вопросами мониторинга и прогнозирования событий. В [2] речь идет об источниках и простейших способах количественного прогнозирования угроз терроризма и экстремизма. На примере статистики МВД РФ показана возможность прогнозирования таких угроз регрессионно-корреляционным методом. Дан пример прогнозирования путём построения интеллектуальной экспертной системы на базе нечёткой логики с применением алгоритмов Мамдани и Цукамото. В [3] раскрываются аспекты мониторинга рисков техногенных нарушений и аварийных ситуаций в рамках одноуровневой модели. Вопросы автоматического синтеза моделей наблюдаемых событий для их прогнозирования не ставятся. В [4] отражены особенности проявления современного терроризма. В [5-7] раскрываются возможности применения традиционных методов анализа временных рядов и модельного прогнозирования криминалистических угроз с уклоном активного участия в процессе такого прогнозирования человека. Аспекты автоматического многоуровневого связывания наблюдаемых событий и алгоритмы построения соответствующих многоуровневых моделей для их прогнозирования машинами не обсуждаются. Предложенные модели защищаемой информационной системы, основанные на использовании аппарата марковских процессов, отличаются от известных решений новыми совокупностями выде-

ленных состояний и связями между ними. Среди релевантных работ по подобным моделям следует отметить [8-11], однако они имеют более частный характер и не учитывают возможность прогнозной оценки защиты информационной системы от комплексных деструктивных воздействий. В какой-то мере вопросы поиска адаптивных мер защиты рассматривались и другими российскими учеными в [12-14].

Важным требованием к построению модели информационных процессов в условиях конфликтов служит оценка процесса управляемости, поэтому задача мониторинга и прогнозирования информационных систем является актуальной.

Постановка задачи

Рассмотрим суть предлагаемого метода, исходя из следующей постановки задачи. Известны причины развития конфликтной ситуации, в частности, возникновение различных по содержанию и природе конфликтов между отдельными лицами (от рядовых граждан до политиков), группами, партиями и слоями населения, которые могут разрешаться не правовыми путями, а с применением средств информационного воздействия. Считается, что по результатам социологических исследований и имеющейся статистики могут быть определены виды таких конфликтов, оценены количественные и отдельные временные характеристики, характерные для процессов назревания этих противоречий, перерастания их в стадию деструктивных воздействий. Исходя из уровня обеспеченности агрессивных групп информационными средствами и их численности установлены предельные значения последствий возможного разрешения конфликтов деструктивными способами и средствами. Определены возможные способы и средства противодействия им.

Однако в общем случае неясно, какие мероприятия и как часто нужно производить для достижения наибольшего эффекта противодействия информационным воздействиям при ограниченных материальных ресурсах.

Необходимо разработать метод, позволяющий прогнозировать опасность информационного воздействия для общества на требуемый момент времени в зависимости от предпринимаемых мер противодействия.

Многоуровневая модель развития конфликта

В обобщенном виде конфликт можно представить в виде способа разрешения противоречий в интересах, целях, взглядах, возникающих в процессе социального взаимодействия, и заключающийся в противодействии участников этого взаимодействия.

Для разработки методов прогнозирования формализуем процесс развития конфликта на каждом из уровней, представленных на рисунке 1, в виде иерархической модели, где каждый из уровней представлен своей моделью развития i -го конфликта. Как показывает практика, развитию конфликтной ситуации предшествуют различного вида информационные воздействия социального и экономического характера, которые провоцируют конфликт. В острой фазе конфликта из-за наличия информационного воздействия у субъекта от-

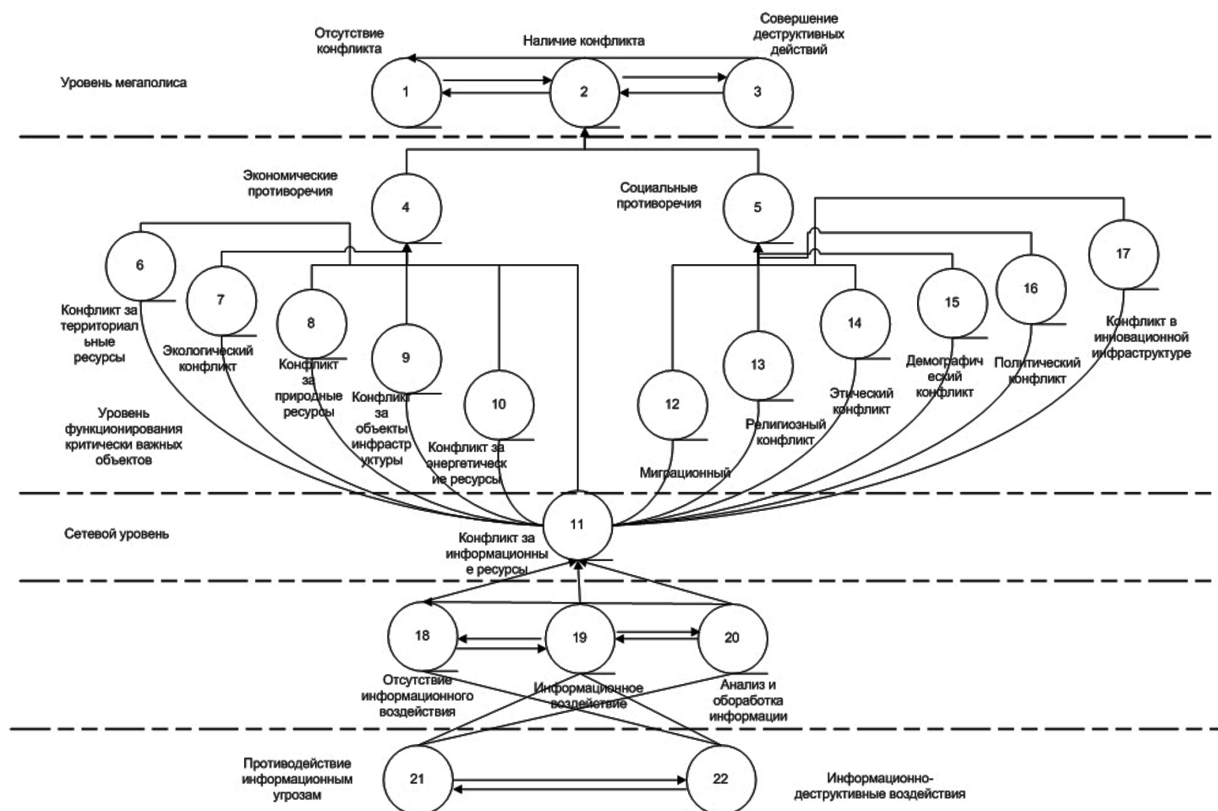


Рис.1. Многоуровневая модель мегаполиса в условиях конфликта

ношений возникает необходимость поиска информационных ресурсов для оценки и анализа полученного информационного воздействия. Возникает борьба за информационные ресурсы. В зависимости от уровня развития конфликтной ситуации сценарий может варьироваться от утаивания информации до умышленного внедрения ложной информации для формирования необходимого комплекса деструктивных воздействий на уровне отдельно взятых групп населения или возникновения так называемых информационных войн, в которые включены достаточно широкие слои населения.

Использование ограничений на влияние информационных ресурсов позволяет поддерживать и развивать конфликт в нужном для сторон развитии, провоцируя участников на выявление тех или иных социальных или экономических противоречий с формированием необходимости совершения тех или иных, в том числе и деструктивных действий, для лиц, вовлеченных в развитие ситуации.

Представленные на рисунке 1 причины развития конфликта между отдельными лицами, группами и слоями населения и их структурами позволяют сформировать процесс развития конфликтной ситуации на основе количественных и временных характеристик. Это дает возможность в зависимости от уровня развития конфликтной ситуации оценить необходимые мероприятия по противодействию.

Однако в условиях мегаполиса социальные и экономические противоречия могут усиливаться друг другом

до достижения синергетического эффекта, что не всегда может быть отражено в количественных оценках и, соответственно, затрудняет формирование допустимого перечня мер противодействия.

Возникает необходимость разработки метода, позволяющего прогнозировать развитие конфликта на требуемый момент времени при ограниченных материальных ресурсах.

Модель противодействия конфликтному состоянию

Для построения простейшей модели формализуем процесс развития и предотвращения конфликта марковской моделью [15], представленной на рис. 2. Этому процессу можно поставить в соответствие следующие состояния: 1-отсутствие конфликта; 2-наличие конфликта; 3-информационное воздействие; 4-совершение деструктивных действий.

Интенсивности перехода между состояниями λ_{ij} ; $i, j = 1, \dots, 4$ определяются с использованием статистических методов или на основе экспертного оценивания.

В этом случае процесс перехода из состояния в состояние возможно описать системой дифференциальных уравнений [16], позволяющей учитывать не только вероятности наступления того или иного события, но влияние мероприятий по противодействию развитию конфликта. Переходы из одного состояния в другое, отраженные на графе дугами, позволяют сформировать множество $P_i(t)$ вероятностей нахождения процесса

в том или ином состоянии. Например, переход из состояния 1 в состояние 2 на момент времени t возможен под воздействием информационных сообщений для определенной социальной группы. Обратный переход возможен при мирном урегулировании имеющихся противоречий. В случае, если этого добиться не удалось, возникает нарастание конфликта с переходом в противостояние, которое может закончиться противоправными действиями конфликтующих сторон. Возникает необходимость разрешения конфликтной ситуации за счет изменения управляющих параметров согласно целевой функции противодействия [17]. В этом случае возможны два варианта выполнения целевой функции противодействия W_0 за счет:

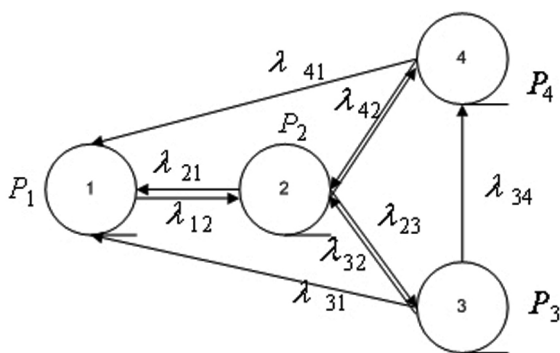


Рис. 2. Модель развития конфликта

1. Минимизации возможных допустимых последствий:

$$W_0 = \min_i \sum_{i=1}^n P_i(t) R_i(t), \quad (1)$$

где n - число рассматриваемых состояний конфликтной ситуации, $P_i(t)$ - вероятность нахождения конфликта в i -ом состоянии на момент времени t , $R_i(t)$ - возможные предельно допустимые негативные последствия от деструктивных воздействий при разрешении конфликта, выраженные в стоимостном отношении.

2. Максимизации эффекта осуществленных мероприятий по противодействию развитию конфликтной ситуации:

$$W_0 = \max_j \sum_{j=1}^l M_j, \quad (2)$$

где M_j - возможные допустимые мероприятия по противодействию конфликтной ситуации, l - число мероприятий, при условии минимизации стоимостных затрат на их проведение.

Условия ограничения возможных стоимостных затрат можно представить в виде:

$$\sum_{i=1}^m C_{ij}(\lambda_{ij}, t) \leq C_{дон}, \quad (3)$$

где $C_{ij}(\lambda_{ij}, t)$ - стоимостные затраты на разрешение i -го конфликта при j -ом мероприятии; $C_{дон}$ - допустимые суммарные затраты на разрешение всех конфликтов на заданном интервале времени.

Алгоритм поиска целесообразных мероприятий по противодействию развитию конфликта

Для нахождения целевой функции W_0 определим алгоритм решения сформулированной задачи в виде последовательности шагов:

Ш1. Формирование перечня n возможных конфликтных ситуаций различной направленности, развитие которых может носить деструктивный характер на каждом из уровней рассматриваемого объекта.

Ш2. Определение состояний, происходящих в системе, с определением интенсивностей перехода из состояния в состояние на основе анализа статистических данных или с использованием аппарата экспертных оценок.

Ш3. Оценка возможных вероятностей $P_i(t)$ нахождения i -го конфликта в k -ом состоянии на момент времени t и предельно допустимых последствий R_i от деструктивных воздействий при разрешении i -го конфликта на момент времени t .

Ш4. Формирование перечня M_j - возможных допустимых мероприятий по противодействию конфликтной ситуации.

Ш5. Выбор варианта выполнения целевой функции противодействия развитию конфликта (1) или (2), а также условий ограничения возможных стоимостных затрат при достижении целевой функции W_0 (3).

Ш6. Оценка параметров перехода из выделенных состояний и интенсивностей перехода в заданный путь развития конфликтной ситуации при проведении мероприятий из данного согласно целевой функции (1)-(2) перечня.

Ш7. Принятие в качестве искоемых мероприятий тех, которые соответствуют наибольшему значению целевой функции, полученной на Ш.6.

Результаты моделирования

В качестве исходных данных выступали интенсивности переходов анализируемых процессов из одного состояния в другое. Полагалось, что имеет место конфликт, способный перерасти в деструктивные воздействия с одной из сторон. Для оценки влияния комплекса мероприятий по противодействию конфликтной ситуации была построена модель развития конфликта (рис. 2).

Рассмотрим этапы формирования конфликта: при информационном воздействии, формируемым в состоянии 3, устранение конфликтной ситуации возможно за счет перехода из состояния 3 в состояние 1 или формированием конфликтной ситуации в состоянии 2 с дальнейшим переходом в состояние 1. В первом случае воздействовать на процесс возможно за счет увеличения интенсивности перехода λ_{31} путем максимизации мероприятий по урегулированию информационных воздействий согласно варианту (2). Во втором случае целесообразно воздействовать на интенсивности переходов $\lambda_{32} - \lambda_{21}$ за счет минимизации возможных допустимых последствий согласно варианту (1).

Результаты прогнозирования для случая развития конфликта без осуществления мероприятий по урегулированию конфликта, первого и второго случаев представлены на рис 3-5, где $P_j(t)$ - вероятность нахождения

Моделирование информационных процессов в условиях конфликтов

ния процесса в j -ом состоянии; t -время, на которое осуществляется прогноз; кривые вероятности нахождения процесса в состояниях 1-4.

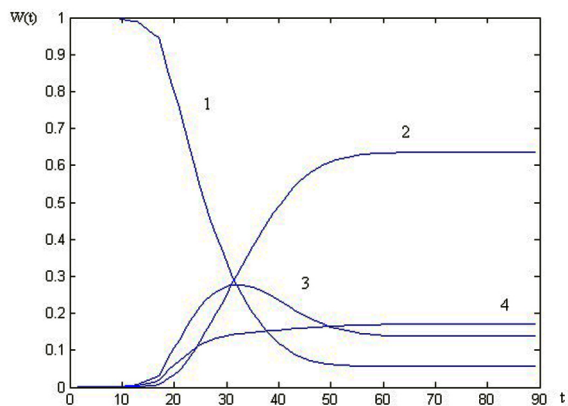


Рис. 3 Результаты прогнозирования конфликта без мероприятий по урегулированию конфликта

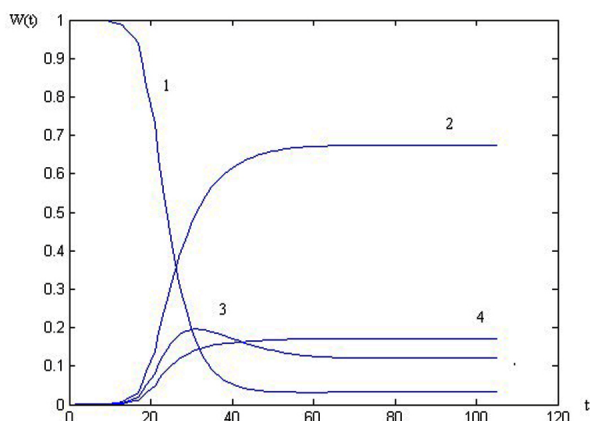


Рис. 4 Результаты прогнозирования конфликта в условиях максимизации мероприятий по урегулированию информационных воздействий

Анализируя полученные результаты можно сделать выводы о целесообразности применения того или иного комплекса мероприятий при воздействии на развитие конфликтной ситуации.

Вариант воздействия на процесс за счет увеличения интенсивности перехода λ_{31} путем максимизации мероприятий по урегулированию информационных воздействий (рис. 4, кривая 2) показывает снижение вероятности нахождения в конфликтной ситуации ($P_1 = 0,01$; $P_2 = 0,14$; $P_3 = 0,65$; $P_4 = 0,2$) по сравнению с развитием конфликта без осуществления мероприятий ($P_1 = 0,02$; $P_2 = 0,1$; $P_3 = 0,6$; $P_4 = 0,28$), а также

сдвиг по времени между информационным воздействием, развитием конфликта и совершением деструктивных воздействий (кривые 1, 3, 4), что дает выигрыш во времени по сравнению с развитием без формирования комплекса мероприятий.

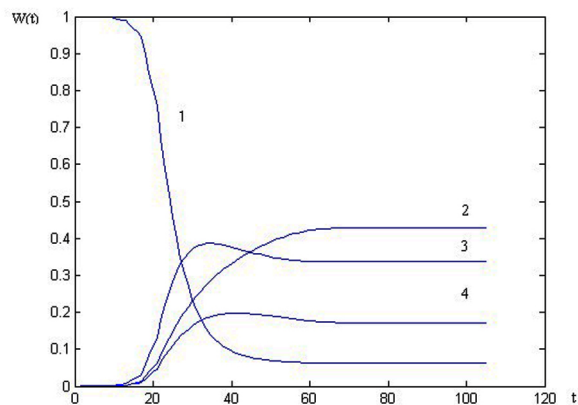


Рис. 5 Результаты прогнозирования конфликта в условиях минимизации возможных допустимых последствий

Вариант воздействия на интенсивности переходов $\lambda_{32} - \lambda_{21}$ за счет формирования комплекса мероприятий по минимизации возможных допустимых последствий (1) является нецелесообразным вариантом. Согласно траекториям изменения кривых на рис. 5 имеет место сдвиг времени пика конфликта в меньшую сторону, что не всегда позволяет должным образом отреагировать адекватно на сложившуюся ситуацию. Наибольшую оценку из представленных ранее (рис. 5, кривая 4) имеет вероятность совершения деструктивных действий ($P_1 = 0,09$; $P_2 = 0,18$; $P_3 = 0,41$; $P_4 = 0,32$), что также может усугубить ситуацию.

Заключение

Использование предлагаемого подхода как для анализа многоуровневой совокупности сложившихся противоречий, так и для отдельных конфликтных ситуаций позволяет оценить динамику развития конфликтной ситуации и выявить необходимые мероприятия по стабилизации ситуации и снижению риска деструктивных воздействий. Применение метода с надлежащей исходной статистикой позволяет осуществить прогнозирование развития ситуации с необходимой заданной точностью и осуществить оперативное построение адекватных текущим ситуациям моделей.

Дальнейшее направление исследований целесообразно посвятить построению моделей, предусматривающих многомерное связывание наблюдаемых событий в пространстве и времени с применением синтезируемых моделей для автоматизированного поиска целесообразных вариантов синтеза структурно-сложных мероприятий по противодействию. Многоуровневые модели наблюдаемых событий, связанных с информационными сетевыми угрозами, предлагается строить в

виде многоуровневых относительно конечных операционных автоматов. В качестве основных показателей эффективности автоматического построения таких автоматов (моделей наблюдаемых событий) целесообразно использовать показатели полноты и время, затрачиваемое на построение. Для расширения марковских моделей защищаемых систем предложено использовать

подход от общего к частному, позволяющий постепенно уточнять пространство возможных событий моделируемых систем. В качестве показателей эффективности их защиты от комплексных деструктивных воздействий рекомендовано использовать интегральные показатели как по времени, так и по событиям с учетом значимости самых событий.

Рецензент: Ловцов Дмитрий Анатольевич, Заслуженный деятель науки Российской Федерации, доктор технических наук, профессор, заведующий кафедрой информационного права, информатики и математики Российского государственного университета правосудия. Москва, Россия. E-mail: dal-1206@mail.ru

Литература

1. Осипов В.Ю., Юсупов Р.М. Информационный вандализм, криминал и терроризм как современные угрозы обществу // Труды СПИИРАН. 2009. № 8. С. 34–45.
2. Молотникова А.А., Звонкова Д.В. Об источниках и простейших способах количественного прогнозирования угроз терроризма и экстремизма // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. 2017. № 12. С. 119–123.
3. Андреева О.Н. Метод мониторинга рисков техногенных нарушений и аварийных ситуаций // Научные технологии. 2017. № 18 (3). С. 85–91.
4. Петров А.В. Антитеррористическая безопасность: сущность и содержание // Вестник ТвГУ. Серия «Философия». 2018. № 1. С. 113–122.
5. Прогнозирование развития криминальной ситуации в Республике Казахстан: Монография / Коллектив авторов. – Астана: Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан. 2017. 172 с.
6. Fatkiewa R.R., Vorobiev V.I., Levonevskiy D.K. Approach to Information Security Control of Complex Computer Networks. In Proceedings of the 19th IEEE International Conference on Soft Computing and Measurements (Saint Petersburg, Russian Federation, May 25-27, 2016). SCM 2016. IEEE Xplore, 2016. pp. 71-72. DOI: 10.1109/SCM.2016.7519687.
7. Levonevskiy D.K., Fatkiewa R.R., Ryzhkov S.R. Network AttackS Detection Using Fuzzy Logic. In Proceedings of the 18th IEEE International Conference on Soft Computing and Measurements (Saint Petersburg, Russian Federation, May 19-21, 2015). SCM 2015. IEEE Xplore, 2015. pp. 243-244. DOI: 10.1109/SCM.2015.7190470.
8. Пермякова М.А., Пермякова О.В. Вероятностный подход к проектированию СЗИ с применением марковских процессов // Актуальные проблемы современной науки, техники и образования. 2017. № 1. С. 214 – 217.
9. Магазев А.А., Цырульник В.Ф. Исследование одной марковской модели угроз безопасности компьютерных систем // Моделирование и анализ информационных систем. 2017. № 24 (4). С. 445-458. DOI: 10.18255/1818-1015-2017-4-445-458.
10. Евлевская Н.В., Привалов А.А., Скуднева Е.В. Марковская модель конфликта автоматизированных систем обработки информации и управления с системой деструктивных воздействий нарушителя // Известия Петербургского университета путей сообщения. 2015. № 1 (42). С. 78-84.
11. Абрамов П.Б. Модель информационного конфликта на основе марковских форм с внешними потоками событий. В сборнике: Охрана, безопасность, связь – 2014. Материалы международной научно-практической конференции. Воронежский институт МВД России (Воронеж, Россия, 27 ноября 2014). 2015. С. 7-12.
12. Андреещев И.А. Оптимизация технических параметров системы защиты информации на основе полумарковской модели функционирования информационной системы // Информация и безопасность. 2017. № 20 (1). С. 49 -56.
13. Маричев А.В., Щетникова Д.А. Анализ существующих технологий адаптивной передачи потоковых данных // Вестник Воронежского института высоких технологий. 2018. № 1 (24). С. 47-49.
14. Воробьев В.И., Фаткиева Р.Р., Евневич Е.Л., Марков В.С. Приведение результатов сетевых измерений информационной безопасности в соответствии с рекомендациями ФСТЭК на основе процедуры гармонизации // Управление экономическими системами: электронный научный журнал. 2015. № 12 (84). С. 22.
15. Тихонов В.И. Марковские процессы / М.: Сов.радио, 1977. 488 с.
16. Колмогоров А.Н. Об аналитических методах в теории вероятностей // Успехи математических наук. 1938. № 5. С. 5–41.
17. Х. Майн, С. Осаки. Марковские процессы принятия решений / Главная редакция физико-математической литературы. М. Наука, 1977. 176 с.

MODELING OF INFORMATION PROCESSES IN CONFLICT SITUATIONS

Evnevich E.³, Fatkueva R.⁴

Purpose: development of a model of conflict in the context of information impact under limitations for counteraction measures costs.

Method: mathematical modeling is based on the Markov chains apparatus and model of the situation development under conflict of the parts of confrontation. Assessing the probability of a system being in a particular state at a given time moment enables the analysis of a system state under or without information impacts, detection of the latter and counteraction to them, as well as the analysis of the transitions between the system states.

Result: the model developed can be applied to formalization and assessment of the security of socially important objects. The method obtained takes into account the changing conditions of functioning of information system under protection and consists in determination of the system current state, in forecasting its behavior using the Markov model for various configurations of the protection system and in configuration selection in order to achieve maximum system performance.

Keywords: information impact, Markov model, confrontation, counteraction, forecasting.

References

1. Osipov V.Yu., Yusupov R.M. Informacionnyi vandalizm, kriminal i terrorizm kak sovremennye ugrozy obshchestvu // Trudy SPIIRAN [SPIIRAS Proceedings]. 2009. № 8. pp. 34–45.
2. Molotnikova A.A., Zvonkova D.V. Ob istochnikakh i prostejshikh sposobakh kolichestvennogo prognozirovaniya ugroz terrorizma i ekstremizma // Nauka i obrazovanie: khozyajstvo i ekonomika; predprinimatel'stvo; pravo i upravlenie [Science and Education; State Economy; Business; Law and Management]. 2017. № 12. pp. 119–123.
3. Andreeva O.N. Metod monitoringa riskov tekhnogennykh narushenii i avarijnykh situacii // Naukoemkie tekhnologii [Journal Science Intensive Technologies]. 2017. № 18 (3). pp. 85–91.
4. Petrov A.V. Antiterroristicheskaya bezopasnost': sushchnost' i sodержanie // Vestnik TvGU. Seriya "Filosofiya" [Herald of TvGU. Series: Philophy]. 2018. № 1. pp. 113–122.
5. Prognozirovanie razvitiya kriminal'noi situacii v Respublike Kazakhstan: Monografiya / Kollektiv avtorov. Astana: Akademiya pravoohranitel'nykh organov pri General'noj prokurature Respubliki Kazakhstan. 2017. 172 p.
6. Fatkueva R.R., Vorobiev V.I., Levonevskiy D.K. Approach to Information Security Control of Complex Computer Networks // In Proceedings of the 19th IEEE International Conference on Soft Computing and Measurements (Saint Petersburg, Russian Federation, May 25-27, 2016). SCM 2016. IEEE Xplore, 2016. pp. 71-72. DOI: 10.1109/SCM.2016.7519687.
7. Levonevskiy D.K., Fatkueva R.R., Ryzhkov S.R. Network AttackS Detection Using Fuzzy Logic // In Proceedings of the 18th IEEE International Conference on Soft Computing and Measurements (Saint Petersburg, Russian Federation, May 19-21, 2015). SCM 2015. IEEE Xplore, 2015. pp. 243-244. DOI: 10.1109/SCM.2015.7190470.
8. Permyakova M.A., Permyakova O.V. Veroyatnostnyi podkhod k proektirovaniyu SZI s primeneniem markovskikh processov // Aktual'nye problemy sovremennoi nauki, tekhniki i obrazovaniya [Actual Problems of Science, Technology and Education]. 2017. № 1. pp. 214 – 217.
9. Magazev A.A., Cyrul'nik V.F. Issledovanie odnoi markovskoi modeli ugroz bezopasnosti komp'yuternykh sistem // Modelirovanie i analiz informacionnykh sistem [Modeling and Analysis of Information Systems]. 2017. № 24(4). pp 445-458. DOI: 10.18255/1818-1015-2017-4-445-458.
10. Evglevskaya N.V., Privalov A.A., Skudneva E.V. Markovskaya model' konflikta avtomatizirovannykh sistem obrabotki informacii i upravleniya s sistemoi destruktivnykh vozdeystvii narushitelya // Izvestiya Peterburgskogo universiteta putei soobshcheniya [Proceedings of Petersburg Transport University]. 2015. № 1 (42). pp. 78-84
11. Abramov P.B. Model' informacionnogo konflikta na osnove markovskikh form s vneshnimi potokami sobytii. V sbornike: Okhrana, bezopasnost', svyaz' – 2014. Materialy mezhdunarodnoi nauchno-prakticheskoi konferencii. Voronezhskii institut MVD Rossii (Voronezh, Rossiya, 27 noyabrya 2014). 2015. pp. 7-12.
12. Andreevskiy I.A. Optimizaciya tekhnicheskikh parametrov sistemy zashchity informacii na osnove polumarkovskoi modeli funkcionirovaniya informacionnoi sistemy // Informaciya i bezopasnost' [Information and Security]. 2017. № 20 (1), pp. 49 -56.
13. Marichev A.V., Shchetnikova D.A. Analiz sushchestvuyushchikh tekhnologii adaptivnoi peredachi potokovykh dannykh // Vestnik Voronezhskogo instituta vysokikh tekhnologii [Vestnik of Voronezh Institute of High Technologies]. 2018. № 1 (24). pp. 47-49.

3 Elena Evnevich, Ph.D., St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, St. Petersburg, Russia. E-mail: eva@iias.spb.su (ORCID ID 0000-0002-8203-0814)

4 Rosa Fatkueva, Ph.D., Associate Professor, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, St. Petersburg, Russia. E-mail: rikki2@yandex.ru (ORCID ID 0000-0003-4065-9611)

14. Vorob'ev V.I., Fatkueva R.R., Evnevich E.L., Markov V.S. Privedenie rezul'tatov setevykh izmerenii informacionnoi bezopasnosti v sootvetstvii s rekomendatsiyami FSTEK na osnove procedury garmo-nizatsii // Upravlenie ekonomicheskimi sistemami: elektronnyi nauchnyi zhurnal [Management of Economic systems. Scientific Electronic Journal]. 2015. № 12 (84). pp. 22.
15. Tikhonov V.I. Markovskie processy / M.: Sov.radio. 1977. 488 p.
16. Kolmogorov A.N. Ob analiticheskikh metodakh v teorii veroyatnoei // Uspekhi matematicheskikh nauk [Russian Mathematical Surveys]. 1938. № 5. pp. 5–41.
17. H.Majn, S. Osaki. Markovskie processy prinyatiya reshenii / Glavnaya redakciya fiziko-matematicheskoi literatury. M. Nauka. 1977. 176 p.

