О ВЕРОЯТНОСТНОМ ПРОГНОЗИРОВАНИИ РИСКОВ В ИНФОРМАЦИОННОЙ ВОЙНЕ. Часть 2. МОДЕЛЬ, МЕТОДЫ, ПРИМЕРЫ

Манойло А. В.[1], Костогрызов А. И.[2]

DOI: 10.21681/2311-3456-2024-1-45-60

Настоящая 2-я часть работы является окончанием статьи, опубликованной в №6(58) 2023 г.

Цель 2-й части работы: *предложить модель и методы для вероятностного прогнозирования частных и интегрального рисков в информационной войне (ИВ), с их помощью на основе отдельных ретроспективных данных на примерах подтвердить работоспособность модели и методов и провести системный анализ выявленных возможностей по управлению рисками в ИВ.*

Методы исследования включают *методы теории вероятностей, методы системного анализа. В качестве моделируемой системы формально могут выступать виртуальная репутация государства, его руководства и иных представителей власти в условиях реализации разнородных угроз в ИВ. Получаемые результаты математического моделирования операций и контроопераций ИВ используются в интерпретации к исходной системе, в интересах которой проводятся соответствующие расчеты.*

Результат работы: *на основе результатов анализа стратегий операций и контроопераций (в 1-й части статьи) предложены модель и методы для вероятностного прогнозирования частных и интегрального рисков в ИВ. Результаты математического моделирования операций и контроопераций ИВ представлены на количественном уровне прогнозов в терминах вероятностей «успеха» и «неудачи» в зависимости от конкретных исходных данных, формируемых по фактам или оцениваемых гипотетически. Тем самым создана математическая основа для анализа развития информационных операций и возможных способов противодействия им на уровне получаемой в результате моделирования более адекватной функции распределения времени между соседними нарушениями системной целостности.*

В работе изучены возможности по востребованным способам противодействия операциям противника в ИВ с указанием достижимых количественных оценок и рациональных способов эффективного управления рисками. На основе их применения проанализированы примеры, иллюстрирующие работоспособность предложенного подхода.

Научная новизна: *впервые предложены количественные методы прогнозирования рисков, связанных с целенаправленными усилиями противника по дискредитацией репутации государства, его руководства и иных представителей власти в глазах мирового сообщества. Для условий неопределенности формализованы способы противодействия угрозам в квазиреальном масштабе времени. Выявлены достижимые границы в превентивном управлении рисками при ведении ИВ.*

Ключевые слова: *вероятность, репутация, прогнозирование, риск, системный анализ, угроза.*

ON PROBABILISTIC FORECASTING OF RISKS IN INFORMATION WARFARE. Part 2. MODEL, METHODS, EXAMPLES

Manoilo A. V.[3], Kostogryzov A. I.[4]

This 2nd part of the work is the end of an article published in No6_2023.

The purpose of the 2nd part *of the work is to propose a model and methods for probabilistic forecasting of particular and integral risks in information warfare (IW), with their help to confirm their usability and to conduct a systematic analysis of the identified opportunities for risk management in IW on the basis of individual retrospective data on examples.*

1 Манойло Андрей Викторович., доктор политических наук, кандидат физико-математических наук, профессор МГУ им. М. В. Ломоносова, профессор факультета политологии МГУ им. М. В. Ломоносова. E mail: Cyberhurricane@yandex.ru

2 Костогрызов Андрей Иванович, доктор технических наук, профессор, Федеральный исследовательский центр «Информатика и управление» Российской академии наук. E mail: Akostogr@gmail.com

3 Andrey V. Manoilo, Dr. Sc. of Political Sciences, Ph. D. of Physical and Mathematical Sciences, Professor of Lomonosov Moscow State University, Professor of the Faculty of Political Science of Lomonosov Moscow State University. E-mail: Cyberhurricane@yandex.ru

4 Andrey I. Kostogryzov, Dr.Sc. of Technical Sciences, Professor, Federal Research Center «Informatics and Control» of the Russian Academy of Sciences. E-mail: Akostogr@gmail.com

Research methods include *methods of probability theory, methods of system analysis. Formally, the virtual reputation of the state, its leadership and other representatives of the authorities in the context of the implementationof heterogeneous threats in the IW can act as a simulated system. The obtained results of mathematical modeling of IW operations and counteroperations are used in the interpretation of the initial system, in the interests of which the corresponding calculations are carried out.*

Results: *based on the results of the analysis of operations and counteroperations strategies (in the 1st part of the article), a model and methods for probabilistic forecasting of particular and integral risks in IW are proposed. The results of mathematical modeling of operations and counter-operations are presented at the quantitative level of forecasts in terms of the probabilities of «success» and «failure» depending on specific initial data generated by facts or estimated hypothetically. Thus, a mathematical basis has been created for analyzing the development of information operations and possible ways to counteract them at the level of a more adequate time distribution function between neighboring violations of system integrity obtained as a result of modeling.*

The paper examines the possibilities for popular ways to counter operations in the IW, indicating achievable quantitative estimates and rational ways to effectively manage risks. Based on their application, examples illustrating the efficiency of the proposed approach are analyzed.

Scientific novelty: *for the first time, quantitative methods of forecasting risks associated with the purposeful enemy efforts to discredit the reputation of the state, its leadership and other representatives of the authorities in the eyes of the world community are proposed. For conditions of uncertainty, methods of countering threats on a quasi-real time scale have been formalized. Some achievable boundaries in preventive risk management in IW have been identified.*

Keywords: *probability, reputation, forecasting, risk, system analysis, threat.*

1. Введение

Сегодня воздействие разнородных угроз при ведении ИВ в международном публичном медиапространстве выражается в целенаправленных компрометирующих выдумках резонансного характера (лжефактах, лженамерениях), способствующих опорочиванию и дискредитации репутации государства, его руководства и иных представителей власти. Эта лицевая сторона ИВ видна всем потребителям информации, но без адекватного отделения «истины» от «лжи». Изучению этой лицевой стороны интерпретации событий посвящены многие политологические исследования. В отличии от этих исследований в настоящей работе представлена математическая основа для анализа развития информационных операций и возможных способов противодействия им на уровне получаемой в результате математического моделирования более адекватной функции распределения времени между соседними нарушениями системной целостности. При этом для условий реализации разнородных угроз в качестве моделируемой системы в работе выступают виртуальная репутация государства, его руководства и иных представителей власти.

В статье под информационной войной (ИВ) понимается особый вид гибридной войны, осуществляемый с применением информационных операций со стороны противника и мер противодействия (контроопераций) со стороны защищающейся стороны. ИВ охватывает управление психикой человека (его сознанием и подсознанием), и через это операции в ИВ направлены в итоге на дискредитацию репутации государства, его руководства и иных представителей власти в глазах мирового сообщества с последующим принуждением к подчинению неким «правилам» в интересах тех сторон, которые развязывают ИВ. Репутация государства, его руководства и иных представителей власти рассматривается как стихийно складывающийся в массовом общественном сознании образ государства, его руководства и иных представителей власти, отражающий характер ожидаемых от них действий или поведения внутри государства и на международной политической арене. По сути репутация — это некий ценный виртуальный актив, используемый для поддержания конкурентоспособности и эффективного развития государства и подлежащий особому хранению и защите, в т. ч. в условиях ИВ.

Цель настоящей работы состоит в предложении востребованных модели и методов для вероятностного прогнозирования частных и интегрального рисков в ИВ и с их помощью на основе отдельных ретроспективных данных – в проведении системного анализа выявленных возможностей по управлению рисками в ИВ.

В 1-й части статьи «Анализ стратегий операций и контроопераций для математического моделирования» проведен анализ основных стратегий ИВ, мер противодействия операциям ИВ (контроопераций), характера стратегических операций ИВ [1–10]. По результатам этого анализа разработаны общие положения математического моделирования для прогнозирования рисков и системного анализа выявленных возможностей по управлению рисками в ИВ. Развитие операций и контроопераций ИВ формализовано с использованием понятия моделируемой системы. Получаемые результаты математического моделирования операций и контроопераций ИВ

для моделируемой системы используются в интерпретации к исходной системе, в интересах которой проводятся соответствующие расчеты.

На основе результатов анализа, проведенного в 1-й части для условий разнородных неопределенностей, сделаны следующие обобщенные выводы применительно к математическому моделированию, проводимому в настоящей заключительной части работы:

- основные стратегии ИВ формально могут быть описаны в терминах случайных событий, характеризующих возникновение и развитие во времени возможных угроз реализации операций и контроопераций в ИВ;
- для случаев применения активных и пассивных мер противодействия угрозам. Возникновение и развитие угроз может быть привязано к оси времени и охарактеризовано:
  - возможной частотой возникновения конкретных угроз (несколько операций в год, по ретроспективным данным в среднем около 4–6 операций в год);
  - средним временем развития этих угроз до появления целевого негативного эффекта от реализации этих угроз (несколько месяцев, по ретроспективным данным в среднем около 3–7 месяцев);
  - средним временем условно приемлемого восстановления репутации (по ретроспективным данным в среднем от одного месяца до полугода);
- стратегические операции в ИВ формально могут быть описаны в виде сложной структуры генерального плана с обозначением целей на ближнесрочную, среднесрочную и долгосрочную перспективы во времени. Каждый из составных формализованных элементов этой структуры (реально разнесенных в пространстве и времени) связан с другими элементами логическими условиями и реализует конкретный фрагмент стратегии и набор операций ИВ для достижения интегральной цели дискредитации репутации государства, его руководства и иных представителей власти. Формально выполнение плана стратегической операции может быть описано в терминах случайных событий, характеризующих развитие во времени возможных угроз для элементов этой структуры, и связано для элементов логическими условиями «И», «ИЛИ» для достижения целей в ИВ.

Ниже предлагаются модель и методы для вероятностного прогнозирования частных и интегрального рисков, с их помощью на основе отдельных ретроспективных данных на примерах иллюстрируется работоспособность модели и методов и проводится системный анализ выявленных возможностей по управлению рисками в ИВ.

2. Вероятностная модель

За основу предлагаемого подхода к математическому моделированию принят подход, изложенный в разные годы в приложении к различным системам [11–20] и доведенный до реализации на уровне ГОСТ Р 59341-2021 «Системная инженерия. Защита информации в процессе управления информацией системы», ГОСТ Р 59991 «Системная инженерия. Системный анализ процесса управления рисками для системы».

С учетом неопределенностей расчет вероятностных показателей делается при условии или в предположении реальной или гипотетической повторяемости возможных событий и их независимости. Для математической формализации приняты следующие допущения:

- к началу периода прогноза целостность моделируемой системы полагается обеспеченной;
- для различных вариантов развития угроз существуют технологии и меры для выявления признаков возникновения источников угроз и воспрепятствования реализации угрозам (например, с использованием контроопераций), а также следов реализации угроз.

Кроме того, делается предположение о наличии возможностей по определению предпосылок к реализации угроз, а также возможностей по приемлемому восстановлению нарушаемых условий для моделируемой системы (с точки зрения противодействия операциям ИВ). Обоснованное использование выбранных мер противодействия операциям ИВ является предупреждающими контрмерами (контроперациями).

За основу формализации принят следующий поэтапный алгоритм возникновения и реализации угроз для моделируемой системы: сначала возникает источник угрозы и начинает инициироваться. Например, выполняется одно или несколько действий или вбрасывается информация, прямо или косвенно влияющие на репутацию государства или его руководства – практическим примером могут служить первые действия по «Делу об отравлении Скрипалей» и соответствующие вбросы в СМИ по стратегии «Игры с пошаговым повышением ставок» с 4 по 15 марта 2018 г., включая выступление Т. Мэй 13 марта 2018 г., когда она предъявила России ультиматум, согласно которому Россия в течение 24 часов должна «правдоподобно объясниться» по поводу инцидента в Солсбери (т. е. публично признать свою вину в отравлении С. и Ю. Скрипалей), иначе Великобритания будет рассматривать «химическую атаку в Солсбери» как акт военной агрессии[5], интервью

5 «Тереза Мэй выдвинула Москве ультиматум, согласно которому в течение 24 часов российская сторона должна правдоподобно объясниться по поводу инцидента. Срок ультиматума истек в 03:00 мск 14 марта 2018 г.». См.: Лондон официально обвинил Россию в отравлении Скрипаля. // Lenta.ru/ 2018, 13 мар. URL: https://lenta.ru/news/2018/03/14/skripal/

Ю. Скрипаль 23 мая 2018 г., вбросы по стратегии «Загонной охоты» с 5 сентября по 8 октября 2018 г., тем самым началось развитие угрозы, выражающееся в разрастающемся воздействии на массовое общественное сознание, определяющее понятие репутации. По прошествии какого-то времени, свойственного менталитету массового общественного сознания (т. е. времени, в течение которого без опровержения вброшенной информации или иных ментальных контрдействий начинает признаваться ее достоверность с соответствующим восприятием относительно репутации государства или его руководства).

Развитие угрозы осуществляется до нарушения целостности моделируемой системы, это означает реализацию возникшей угрозы (в реальности это может означать ухудшение репутации государства или его руководства до того целевого уровня, который ставился при начале соответствующих операций ИВ). Под целостностью моделируемой системы, характеризующей «успех» в ИВ, понимается такое ее состояние, которое отвечает целевому назначению модели системы. Целостность формально считается нарушенной («неудача» в результате реализации угроз за период прогноза) лишь после перехода из элементарного состояния «целостность моделируемой системы обеспечена» в элементарное состояние «целостность моделируемой системы нарушена» (т. е. на практике какая-то существенная часть субъектов, на которые осуществляется информационно-психологическое воздействие, поверит или сделает вид, что поверит в достоверность вброшенной информации. Практическим примером в «Деле об отравлении Скрипалей» нарушением целостности моделируемой системы можно считать введенные администрацией США 22 августа 2018 г. санкции в отношении России из-за приписываемой ей причастности к отравлению 4 марта 2018 г. экс-полковника ГРУ Сергея Скрипаля и его дочери Юлии в Солсбери – со ссылкой на нарушение Россией американского закона о контроле над химическим и биологическим оружием и запрете его военного применения от 1991 года). Нарушение целостности моделируемой системы характеризует состояние «неудачи» в ИВ.

Если инициировавшийся источник угрозы был выявлен до наступления элементарного состояния «целостность моделируемой системы нарушена» и приняты адекватные контрмеры, то считается, что целостность моделируемой системы не нарушена (примером такого рода мер противодействия операциям ИВ могут служить так называемые «Скрипальские чтения», перехватившие на 48 часов информационную повестку у западных (в основном, британских, американских и немецких) и российских СМИ с 3 по 4 марта 2019 г. – в первую годовщину инцидента в Солсбери). Результатом применения очередной диагностики является восстановление нарушенной целостности моделируемой системы до условно приемлемого уровня или подтверждение целостности при отсутствии ее нарушения – см. описание на рис. 1 (например, удержание политической и экономической стабильности в России после введения тысяч санкций против нее и начальных резких падений курсов рубля может рассматриваться как восстановление нарушенной целостности моделируемой системы до приемлемого уровня в условиях сложившихся реалий).

Таким образом, сформулированная модель является ничем иным, как адаптированным случаем типовой модели опасного воздействия на защищаемую систему, описанной в [11–20] и рекомендуемой ГОСТ Р 59341, ГОСТ Р 59991.

3. Базовая модель (периодический контроль состояния целостности)

Предлагаемые модель и методы позволяют оценить вероятности сохранения целостности (слева на рис. 1) и нарушения целостности моделируемой системы (справа на рис. 1) на протяжении заданного периода прогноза. Именно эта последняя вероятность с учетом негативных последствий определяется как риск нарушения целостности моделируемой системы на протяжении заданного периода прогноза. Для моделируемой системы непревышение допустимого уровня риска является следствием достаточно частого диагностирования и применения эффективных средств диагностики и восстановления приемлемой целостности при существующих ограничениях.

Для описания процессов возникновения, развития и противодействия операциям ИВ в моделируемой системе введены обозначения исходных данных моделирования:

σ – частота возникновения источников угроз;

β – среднее время развития возникшей угрозы до ее реализации в виде нарушения целостности моделируемой системы (т. е. до перехода в элементарное состояние «целостность моделируемой системы нарушена» для этого источника угроз);

$T_{меж}$ – время между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы;

$T_{диаг}$ – длительность диагностики моделируемой системы (в случае неиспользования способа повышения адекватности модели по ГОСТ Р 59341-2021, приложению В 2.4 длительность диагностики $T_{диаг}$ включает в себя среднее время восстановления нарушенной целостности моделируемой системы $T_{восст}$);

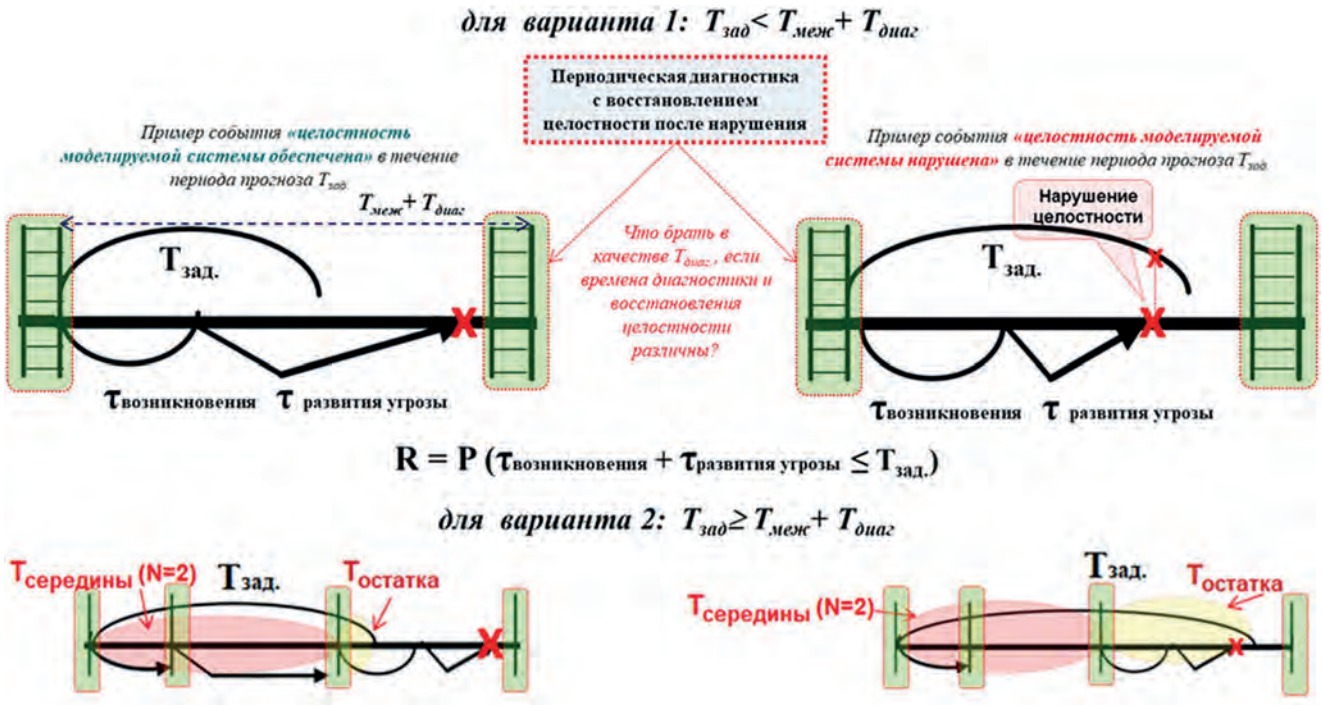

Рис. 1. Формальные случаи сохранения и нарушения целостности

$T_{восст}$ – среднее время восстановления нарушенной целостности моделируемой системы (применяется при использовании способа повышения адекватности модели по ГОСТ Р 59341-2021, приложению В 2.4);

$T_{зад}$ – длительность периода прогноза.

Для оценки вероятности нарушения целостности моделируемой системы (справа на рис. 1) $R_{наруш.}$ на протяжении заданного периода прогноза $T_{зад}$ используется выражение:

$$R_{наруш.} = 1 - P_{возд.}, \quad (1)$$

где $P_{возд.}$ – это вероятность обеспечения целостности моделируемой системы (слева на рис. 1) на протяжении заданного периода прогноза $T_{зад}$.

Возможны два варианта:

1. заданный оцениваемый период $T_{зад}$ меньше периода между окончаниями соседних диагностик ($T_{зад} < T_{меж} + T_{диаг}$);
2. заданный оцениваемый период $T_{зад}$ больше или равен периоду между окончаниями соседних диагностик ($T_{зад} \ge T_{меж} + T_{диаг}$), т.е. за это время заведомо произойдет одна или более диагностик.

Для варианта 1 вероятность $P_{возд(1)}(\sigma, \beta, T_{меж}, T_{диаг}, T_{зад})$ обеспечения целостности моделируемой системы на протяжении заданного периода прогноза $T_{зад}$ вычисляется как распределение от суммы времен возникновения и активизации опасности на момент завершения периода прогноза $T_{зад}$ – см. рис. 1:

$$P_{возд(1)} = \begin{cases} (\sigma - \beta^{-1})^{-1} \left\{ \sigma e^{-T_{зад}/\beta} - \beta^{-1} e^{-\sigma T_{зад}} \right\}, & если\ \sigma \ne \beta^{-1}, \\ e^{-\sigma T_{зад}} \left[1 + \sigma T_{зад} \right], & если\ \sigma = \beta^{-1}. \end{cases} \quad (2)$$

Эту же формулу используют для оценки вероятности обеспечения целостности моделируемой системы без какой-либо диагностики.

Для варианта 2 вероятность $P_{возд(2)}$ обеспечения целостности моделируемой системы на протяжении заданного периода прогноза $T_{зад}$. Предлагается определять по формуле (полагая, что нарушения могут произойти на срединном участке или в конце после последней диагностики до истечения длительности прогноза):

$$P_{возд(2)} = P_{серед} + P_{кон}, \quad (3)$$

где $P_{серед}$ – вероятность отсутствия нарушений целостности моделируемой системы в течение всех периодов между диагностиками, целиком вошедшими в $T_{зад}$. С учетом доли этих периодов $\frac{N(T_{меж} + T_{диаг})}{T_{зад}}$ в общем оцениваемом периоде $T_{зад}$, расчет осуществляется по формуле

$$P_{серед} = \frac{N(T_{меж} + T_{диаг})}{T_{зад}} \cdot P^{N}_{возд(1)}(\sigma, \beta, T_{меж}, T_{диаг}, T_{меж} + T_{диаг}), \quad (4)$$

N – число периодов между диагностиками, которые целиком вошли в пределы времени $T_{зад}$, $N = [T_{зад} / (T_{меж} + T_{диаг})]$ (в общем случае здесь при моделировании N – может быть действительным числом, т.е. не обязательно целым);

$P_{возд(1)}(\sigma, \beta, T_{меж}, T_{диаг}, T_{меж} + T_{диаг})$ – вероятность отсутствия нарушений целостности за один период между диагностиками, целиком вошедший в пределы времени $T_{зад}$, вычисляют по формуле (2);

$P_{кон}$ – вероятность обеспечения целостности после последней диагностики (в конце $T_{зад}$). С учетом доли

остатка $T_{ост} = T_{зад} - N (T_{меж} + T_{диаг})$ в общем периоде прогноза $T_{зад}$ расчет осуществляется по формуле

$$P_{кон} = \frac{T_{ост}}{T_{зад}} \cdot P_{возд(1)}(\sigma, \beta, T_{меж}, T_{диаг}, T_{ост}) \quad (5)$$

Значение $P_{возд(1)}(\sigma, \beta, T_{меж}, T_{диаг}, T_{ост})$ для остатка от задаваемого прогнозного периода вычисляют по формуле (2) с тем отличием, что вместо $T_{зад}$ стоит остаток $T_{ост}$.

Использование дополнительно стандартного способа повышения адекватности модели по ГОСТ Р 59341-2021, приложению В 2.4 позволяет учитывать не только среднее время системной диагностики $T_{диаг}$, но и среднее время восстановления целостности моделируемой системы $T_{восст}$.

Предложенная модель пригодна для проведения оценок системы, представимой в виде отдельного «черного ящика», причем для случая, когда времена диагностики и восстановления нарушенной целостности совпадают. Для случая, когда времена диагностики и восстановления нарушенной целостности не совпадают, предлагается использовать способ повышения адекватности, предложенный в кандидатской диссертации Нистратова А. А.[6] и доведенный до реализации в ГОСТ Р 59341, см. также рекомендации по моделированию в ГОСТ Р 59991.

Для комплексной оценки в приложении к моделируемым системам сколь угодно сложной параллельно-последовательной структуры предлагается использовать следующий алгоритм генерации новых моделей.

Рассмотрим простейшую структуру из двух независимых элементов, соединенных последовательно, что означает логическое соединение «И» (рис. 2), или параллельно, что означает логическое соединение «ИЛИ» (рис. 3). Предположение независимости имеет место быть.

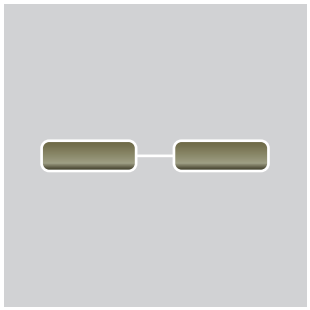

Рис. 2. Система из последовательно соединенных элементов

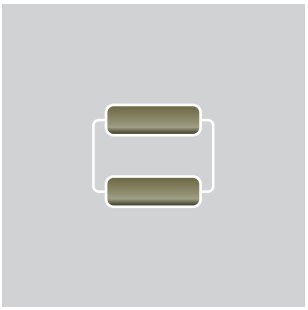

Рис. 3. Система из параллельно соединенных элементов

Обозначив для i-го элемента функцию распределения (ФР) времени наработки на нарушение целостности через $Bi(t) = P(\tau i \le t)$, получим:

1) для последовательно соединенных независимых элементов время до нарушения целостности равно минимуму из двух времен τi: выхода из строя 1-го или 2-го элементов (т. е. система переходит в состояние нарушенной целостности, когда откажет либо 1-й, либо 2-й элемент). В этом случае для системы в целом ФР времени наработки $B(t)$ на нарушение целостности определяется выражением

$$B(t) = P(\min(\tau 1, \tau 2) \le t) = 1 - P(\min(\tau 1, \tau 2) > t) = \\ = 1 - P(\tau 1 > t)\, P(\tau 2 > t) = 1 - [1 - B1(t)]\, [1 - B2(t)], \quad (6)$$

2) для параллельно соединенных независимых элементов (когда оба элемента находятся в функциональном состоянии и при выходе из строя одного из них другой продолжает функционировать) время до нарушения целостности равно максимуму из двух времен τi: выхода из строя 1-го и 2-го элементов, т.е. система переходит в состояние нарушенной целостности, когда выйдут из строя оба – и 1-й и 2-й элементы. В этом случае ФР времени наработки на нарушение целостности для системы в целом

$$B(t) = P(\max(\tau 1, \tau 2) \le t) = \\ = P(\tau 1 \le t)\, P(\tau 2 \le t) = B1(t)\, B2(t). \quad (7)$$

Применяя приведенные рекуррентные соотношения (6) – (7), можно получать соответствующие оценки для сколь угодно сложной логической структуры с параллельно-последовательным соединением элементов. На выходе моделирования системы – вероятность обеспечения целостности в течение заданного периода времени. Если для каждого элемента просчитать эту вероятность для всех точек $T_{зад}$. от нуля до бесконечности, то получится траектория ФР времени обеспечения целостности по каждому из элементов (или траектория, не являющаяся ФР, но близко ее аппроксимирующая) в зависимости от расчетных параметров – см. подробнее ГОСТ Р 59341-2021, приложение В.

4. Об извлечении скрытых аналитических знаний

Чтобы провести системный анализ для ответа на условный вопрос «Что будет, если...» в терминах элементарных событий за период прогноза, при формировании сценариев возможных нарушений статистика реальных событий по желанию исследователя может быть дополнена гипотетическими событиями, характеризующими ожидаемые и/или прогнозируемые условия для моделируемой системы. Применительно к анализируемому сценарию модели

6 Нистратов А. А. Методика прогнозирования техногенных рисков и ее реализация с использованием Интернет-технологии. Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.17 «Теоретические основы информатики». Федеральное государственное бюджетное учреждение науки Институт проблем информатики Российской академии наук (ИПИ РАН), 2013. 150 с.

ориентированы на расчет вероятности определенного элементарного состояния в течение задаваемого периода прогноза. Для негативных последствий при оценке рисков этой расчетной вероятности сопоставляют возможный материальный, моральный или репутационный ущерб. Тогда риск нарушения целостности моделируемой системы на протяжении заданного периода прогноза определен как дополнение до единицы вероятности обеспечения целостности моделируемой системы в сопоставлении с возможными последствиями относительно тех угроз, которые могут оказаться реализованными.

Согласно модели развитие критичных ситуаций в моделируемой системе считается не нарушающим ее целостности в течение заданного периода прогноза (т.е. в течение всего периода прогноза система пребывает в элементарном состоянии «целостность моделируемой системы обеспечена»), если в течение всего периода прогноза либо источники опасности не инициируются, либо после активизации происходит их оперативное выявление и принятие адекватных мер противодействия операциям ИВ. При этом, согласно допущениям, к началу прогноза моделируемая система пребывает в элементарном состоянии «целостность моделируемой системы обеспечена». Предполагается, что существуют не только средства диагностики целостности моделируемой системы, но и способы поддержания и/или ее восстановления при выявлении источников опасности или следов их активизации (см. допущения в разделе 2).

Какие скрытые знания позволяет извлечь вероятностное прогнозирование рисков?

На рис. 4 проиллюстрированы ограничения к допустимым рискам, экспоненциальная и некая более адекватная ФР времени между соседними нарушениями системной целостности с одинаковой частотой нарушений λ .

Ориентируясь на простейшую, весьма грубую, аппроксимацию экспоненциальной ФР (с одним параметром – частотой нарушений), можно легко констатировать выполнение или невыполнение задаваемых требований к уровню допустимых рисков. Ниже «пограничной полосы» – требование выполнено, выше – не выполнено. Однако это – все извлекаемые знания... Из «плюсов» – лишь удобство сравнения. И все...

Ориентируясь на более адекватную ФР или аппроксимирующую ФР функцию (например – с помощью предложенных модели и методов), если при ее создании для каждого критичного составного элемента задавались характеристики угроз и предпринимаемые меры противодействия операциям ИВ, возможно извлечение следующих знаний – см. рис. 4, 5:

- рассчитать реальную зависимость вероятности нарушения целостности системы и составных подсистем от характеристик разнородных угроз и предпринимаемых мер противодействия операциям ИВ;
- оценить точность прогнозирования по сравнению с экспоненциальной аппроксимацией ФР;
- определить период эффективного функционирования, в течение которого нарушений не ожидается (по критерию непревышения допустимых рисков) – для определения упреждающих противодействий угрозам за время, не превосходящее данного периода;
- выделить зоны прогнозных периодов времени, когда возможны нарушения требований к допустимому риску – для определения упреждающих противодействий угрозам или обоснованного управления рисками для этих зон (в т. ч. избегание рисков или смягчение требований из-за неизбежного резкого возрастания рисков в пределах, признанных приемлемыми);
- сравнить периоды эффективности, в течение которого нарушений не ожидается (по критерию непревышения допустимых рисков) с соответствующими периодами при экспоненциальной аппроксимации ФР.

Кроме этого, зафиксировав уровни «допустимых рисков» для системы и составных подсистем, а также считая неизменными все параметры, за исключением одного, возможно решение различных

Рис. 4. Фрагменты ФР, демонстрирующие экспоненциальную и более адекватную аппроксимацию

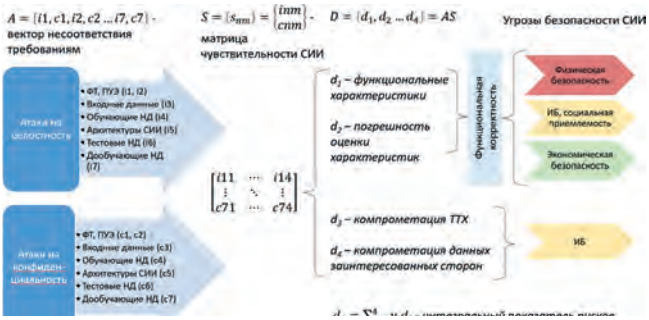

Рис. 5. Фрагменты прогнозной зависимости риска, иллюстрирующий обоснование аналитических выводов (не является ФР), см. также рис. 12

оптимизационных задач, связанных с обоснованием эффективных упреждающих мер обеспечения целостности моделируемой системы в условиях разнородных угроз.

Тем самым для условий неопределенности способы противодействия угрозам могут быть формализованы в квазиреальном масштабе времени (т.е. в масштабе времени, близком к реальному для моделируемой системы в принятых допущениях и ограничениях).

5. Примеры

Первые два примера приводятся ниже для понимания достижимого уровня рисков «фейковой» дискредитации положительной репутации виртуального политического деятеля государства в условиях, учитывающих действующее законодательство РФ. В качестве моделируемой системы в примерах выступает репутация политического деятеля. Результаты этих примеров, полученных с применением модели, аналогичной предложенной выше [18], используются далее для сравнения с другими условиями ведения ИВ по примерам 3–5.

В отличие от внутренних норм, закрепляемых в законодательствах различных государств, на международном уровне зачастую отсутствуют событийные ограничения, связанные с целями операций в ИВ и возможностями по противоборству. Цели могут оказаться долговременными, ожидаемое информационное воздействие на людей может измеряться месяцами и годами. Более того, неопределенными остаются временные характеристики развития разнородных угроз на психику человека в разных странах. В примерах 3–5 в качестве моделируемой системы выступает репутация виртуального государства и его руководства. Исходные данные сценариев ИВ сформированы с учетом ретроспективных данных в международном информационном пространстве в период с конца 2015 г. по настоящее время.

В примере 3 речь идет о виртуальном не суверенном государстве (готовом не противодействовать операциям ИВ против него или имитировать такое противодействие) и о некоем виртуальном суверенном государстве, реализующем лишь пассивные меры противодействия операциям ИВ (отрицания или оправдания, указания на нестыковки в обвинениях и т. п.), но без учета активных контрдействий. В примере 4 проводится анализ ведения ИВ виртуальным суверенным государством, реализующим не только пассивные меры противодействия операциям ИВ, но осуществляющим активные контроперации. В примере 5 проводится анализ применения длительных стратегических информационных операций в ИВ и противоборствующих контроопераций.

Пример 1 [18]. В примере осуществлен прогноз защищенности репутации виртуальных кандидатов на выборные должности от «фейков» с момента их выдвижения за 60 дней до выборов согласно законодательству РФ. Для проведения математического моделирования сформированы следующие исходные данные, учитывающие современные взгляды на характеристики «фейковых» угроз в эпоху информационно-психологического противоборства [1–5, 18] – см. табл. 1.

Результаты прогноза показали [18]: вероятностный риск дискредитации положительной репутации политика составит 0.56 в течение 1 месяца с увеличением до 0.81 в течение 2-х месяцев. Анализ показал, что сохранить изначально положительную репутацию политика в течение 2-х месяцев практически не удастся с вероятностью от 0.5 до 0.9, поскольку ожидается превалирование быстродействующих «фейков», для которых среднее время развития возникшей «фейковой» угрозы до ее реализации не будет превышать 1 месяца. При сокращении длительности судебной реакции до 2-х недель риск дискредитации изначально положительной репутации политика не будет снижаться ниже 0.6. В практической интерпретации обоснован закономерный вывод: совершенствование российского правосудия с целью сокращения до двух недель среднего времени восстановления положительной репутации добропорядочного и законопослушного политика не принесет им ожидаемой защищенности от «фейков». Вероятность дискредитации репутации политического деятеля в публичном информационном пространстве России будет соизмерима с вероятностью сохранения изначальной положительной репутации.

Таблица 1

Исходные данные для примера 1

Моделируемая система	Частота возникновения угроз, σ	Среднее время развития угроз, β	Период между диагностиками, $T_{меж}$	Длительност диагностики, $T_{диаг}$	Среднее время восстановления целостности системы, $T_{восст}$
Репутация политического деятеля	1 раз в неделю	20 суток	1 сутки	8 часов	2 недели

Таблица 2

Исходные данные для моделирования системы по примеру 2

Моделируемая система	Частота возникновения угроз, σ	Среднее время развития угроз, β	Период между диагностиками, $T_{меж}$	Длительност диагностики, $T_{диаг}$	Среднее время восстановления целостности системы, $T_{восст}$
Репутация политического деятеля	5 раз в месяц (что соизмеримо с примером 1)	20 суток (то же, что в примере 1)	1 час (вместо 1 суток для примера 1)	2 часа (вместо 8 часов для примера 1)	1 неделя (вместо 2-х недель в примере 1)

Пример 2 [18]. В примере осуществлен прогноз защищенности репутации кандидатов на выборные должности от «фейков» в период агитации за 28 дней до выборов согласно законодательству РФ. Для проведения математического моделирования сформированы следующие исходные данные – см. табл. 2.

Результаты прогноза показали: вероятностный риск дискредитации положительной репутации политика составит 0.24 в течение задаваемых 14 суток с увеличением до 0.42 в течение 28 суток (сравните с неутешительными результатами примера 1). Анализ показал, что сохранить изначально положительную репутацию политика в течение 28 суток выборной агитации сложно, но не невозможно – вероятность «успеха» может составить 0.6–0.7 против риска неудачи 0.3–0.4, т. е. вероятность «успеха» в 1.5–2 раза выше, чем риск неудачи. При сокращении сроков судебной реакции с 2-х недель до нескольких дней (от 3 до 7) риск дискредитации изначально положительной репутации политика составит в диапазоне 0.15–0.24. Эти цифры дают некоторую надежду на успешное противодействие «фейковым» угрозам.

По результатам рассмотрения примеров 1 и 2 обосновано, что наиболее эффективными на сегодня способами повышения защищенности репутации политических деятелей в РФ от «фейков» являются комплексные меры, включающие в первую очередь:

- мониторинг и выявление угроз с проведением каждый час диагностики публичного информационного пространства на предмет появления «фейков» при длительности самой диагностики не более 2-х часов;
- развитие системы правосудия и защиты репутации политического деятеля таким образом, чтобы имели место реальные возможности оперативной подачи соответствующего иска в суд при выявлении «фейка» (подача иска – за минуты) и приоритетного рассмотрения иска с тем, чтобы окончательный судейский вердикт был сформирован за несколько дней (в срок, не превышающий 7 суток) до истечения законодательных сроков агитации за политика.

На практике это достижимо с созданием и внедрением систем искусственного интеллекта, поддерживающего противодействие «фейковым» угрозам, что требует специальной научно-технической проработки. Но на международном уровне эти рекомендации не применимы. Более детально примеры по «фейковым» угрозам см. в [18].

Из результатов моделирования в примерах 1 и 2 следует, что риск на уровне 0.3 вполне может рассматриваться в качестве условно допустимого для угроз, свойственных ИВ. Справедливости ради следует отметить, что для автоматизированных систем требования к допустимым рискам гораздо более жесткие. Так, допустимая вероятность нарушения надежности предоставления информации и интегральный риск нарушения реализации процесса управления информацией системы с учетом требований по защите информации задаются на уровне 0.01–0.05, допустимая вероятность нарушения конфиденциальности информации – на уровне 0.001–0.005, а допустимая вероятность нарушения своевременности обработки запросов в системе – на уровне 0.1–0.3 (последнее – соизмеримо с полученными в примерах 1, 2 результатами прогнозов). При этом период прогноза для расчетных показателей подбирают таким образом, чтобы вероятностные значения рисков не превышали допустимые (см. ГОСТ Р 59341).

Пример 3. В примере осуществлен прогноз целостности моделируемой системы, в качестве каковой выступает репутация виртуального государства и его руководства в условиях угроз ИВ без использования каких-либо противодействующих контроопераций. В качестве аналога моделируемого сценария угроз рассмотрены, например, действия против РФ по стратегии «удушения» («Петли Анаконды») с 9 ноября 2015 г. по настоящее время с учетом пассивных мер противодействия (отрицания или оправдания, указания на нестыковки в обвинениях и т.п.), но без учета активных контрдействий со стороны РФ (каковые начали осуществляться с 3 марта 2019 г – см. 1-ю часть статьи). Учитывая разноплановость и неравномерную повторяемость разнородных угроз ИВ, исходные данные для моделирования сформированы по статистике ретроспективных данных, приведенных в 1-й части и во введении настоящей статьи.

Таблица 3

Исходные данные для примера 3

Моделируемая система	Частота возникновения угроз, σ	Среднее время развития угроз, β	Период между диагностиками, $T_{меж}$	Длительност диагностики, $T_{диаг}$	Среднее время восстановления целостности системы, $T_{восст}$
Репутация государства и его руководства	6 операций в год	3 месяца	1 сутки	8 часов	6 месяцев

Реализация угроз завершается некоторым нарушением приемлемой целостности моделируемой системы (т. е. ухудшением состояния государства, связанного с его репутацией) с полным или частичным достижением целей, которые ставились противником при начале соответствующих операций ИВ – например, до введения действительно чувствительных экономических санкций или политических воздействий. В качестве некоторых из таковых способов «удушения» в реальности были санкции, введенные в рассматриваемый период времени против РФ и ее союзников. Правдоподобные исходные данные для моделирования отражены в табл. 3.

Прежде, чем учесть все исходные данные из табл. 3, рассмотрим гипотетичный случай отсутствия какой-либо диагностики информационного пространства, пассивных и активных мер противодействия угрозам. Этот случай свойственен не суверенным государствам, готовым не противодействовать операциям ИВ против него или имитировать такое противодействие. Результаты прогноза с использованием предложенной выше модели показали: вероятностный риск нарушения целостности моделируемой системы в случае отсутствия какой-либо диагностики информационного пространства, пассивных и активных мер противодействия угрозам составит 0.69 при прогнозе на полгода с увеличением до 0.999 в течение двух лет – см. рис. 6. В практической интерпретации это означает, что в реальности первая же реализованная угроза приведет к достижению поставленных противником целей информационной операции против не суверенного государства. Поражение такого государства в ИВ неизбежно, оно будет заключаться в разрушении репутации государства и его руководителей внутри страны и на международной арене, и в полном подчинении победителю.

Суверенное государство осуществляет регулярный контроль информационного пространства и, как минимум, пассивные меры противодействия – таковыми могут быть отрицания или оправдания в информационном пространстве, указания на нестыковки в обвинениях и т. п. Кроме того, предпринимаются усилия по восстановлению нарушаемой репутации – см. рассматриваемые усредненные сценарные условия в табл. 3.

Результаты прогноза показали: вероятностный риск нарушения целостности моделируемой системы при регулярном контроле информационного пространства и пассивных мерах противодействия угрозам составит 0.26 при прогнозе на полгода с увеличением до 0.80 в течение двух лет – см. рис. 7. Пилообразность зависимости объясняется тем, что перед диагностикой с возрастанием времени риск возрастает, после диагностики – ненамного снижается с учетом возможностей восстановления после потенциальных нарушений целостности. Математически это определяется выражениями (3)–(5), а также способами повышения адекватности модели по ГОСТ Р 59341-2021, приложению В 2.4.

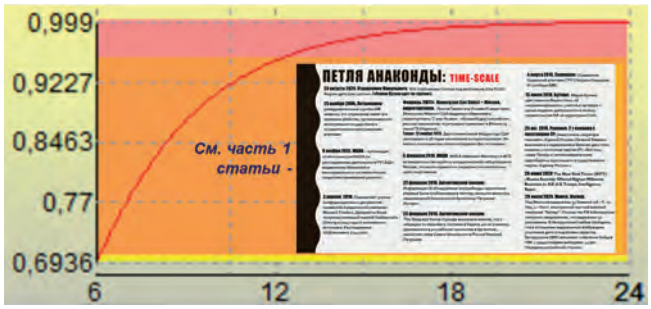

Рис. 6. Зависимость риска нарушения целостности моделируемой системы от периода прогноза (в месяцах) в случае отсутствия какого-либо контроля, пассивных и активных мер противодействия угрозам

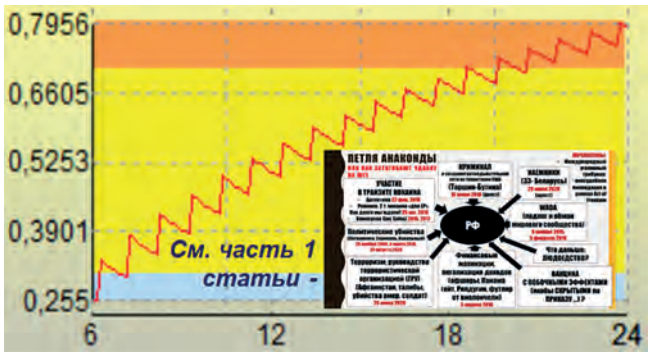

Рис. 7. Зависимость риска нарушения целостности моделируемой системы от периода прогноза (в месяцах) при регулярном контроле и пассивных мерах противодействия угрозам

В практической интерпретации приведенные на рис. 7 результаты расчетов означают, что в реальности при прогнозировании на полгода вероятность «успеха» в 3 раза больше вероятности «неудачи» (поскольку за этот сравнительно короткий срок реально может быть реализована угроза в рамках одной операции противника). При прогнозировании на год шансы «успеха» и «неудачи» оцениваются где-то «50 на 50», т.е. приблизительно равны. При прогнозировании на два года вероятность «неудачи» в 4 раза превышает вероятность «успеха» в сохранении приемлемой репутации в сценариях угроз из табл. 3. Таким образом, результаты расчетов по примеру 3 подтверждают: применение лишь пассивных мер противодействия угрозам при средне- и долгосрочных прогнозах малоперспективно, для рассмотренного сценария (см. табл. 3) в течение срока двух лет и более неизбежно последуют «неудачи» в ИВ.

Пример 4. В примере осуществлен прогноз целостности моделируемой системы, в качестве каковой выступает репутация виртуального государства и его руководства в условиях угроз ИВ с учетом пассивных и активных мер противодействия угрозам. Активные меры противодействия угрозам в ИВ заключаются в проведении контроопераций, характеристика которых приведена в 1-й части статьи.

Моделируется параллельная структура системы, представленная на рис. 3. С точки зрения защищающейся стороны формализация противодействия выглядит следующим образом: целостность моделируемой системы сохраняется, если «ИЛИ» применение пассивных мер противодействия угрозам обеспечивает «успех» (это – верхний моделируемый элемент со сценарием угроз из табл. 3 примера 3), «ИЛИ» применение активных мер противодействия угрозам с использованием контроопераций обеспечивает «успех» в ИВ (это – нижний элемент, исходные данные для него характеризуются сценарием угроз из табл. 4). На практике нарушение целостности моделируемой системы из двух логически параллельных элементов наступает только тогда, когда оба они в условиях информационных угроз, свойственных каждому элементу (а эти условия в общем случае различны), оказываются в состоянии «неудачи», т.е. в элементарном состоянии «целостность моделируемой системы нарушена» (т.е. на практике, невзирая на активные и пассивные меры противодействия какая-то существенная часть субъектов, на которые осуществляется информационно-психологическое воздействие, поверит или сделает вид, что поверит в достоверность вбрасываемой при реализации угроз информации).

Комментарии к табл. 4: в результате контроопераций согласно результатам системного анализа их ретроспективного влияния на ход ИВ (из 1-й части статьи и введения) среднее время развития угроз для нижнего элемента увеличено с 3-х до 7 месяцев, в то же время сделано предположение, что среднее время восстановления целостности снизится с полугода до 1 месяца, что является вполне правдоподобным за счет заранее предусмотренных смягчающих мер противодействия угрозам. Остальные учитываемые параметры остались неизменными по сравнению с примером 3.

Результаты прогноза показали (см. рис. 8): вероятностный риск нарушения целостности моделируемой системы при регулярном контроле информационного пространства, пассивных и активных мерах противодействия угрозам в ИВ составит 0.085 при прогнозе на полгода с увеличением до 0.45 в течение двух лет – см. рис. 8. Пилообразность зависимости объясняется так же, как и для примера 3. Несколько усиленный рост рисков при прогнозе в районе 13 и 19 месяцев по сравнению с рис. 7 объясняется тем, что среднее время развития угроз изменилось с 3-х месяцев до 7.

В практической интерпретации приведенные на рис. 8 результаты расчетов означают, что в реальности при прогнозировании на полгода вероятность «успеха» на порядок больше вероятности «неудачи»

Таблица 4

Исходные данные для нижнего элемента (см. рис. 3) по примеру 4

Моделируемый элемент системы, реализующий активные меры противодействия	Частота возникновения угроз, σ	Среднее время развития угроз, β	Период между диагностиками, $T_{меж}$	Длительност диагностики, $T_{диаг}$	Среднее время восстановления целостности системы, $T_{восст}$
Репутация государства и его руководства	6 операций в год (то же, что для верхней подсистемы)	7 месяцев (в сравнении с 3 месяцами для верхней подсистемы)	1 сутки (то же, что для верхней подсистемы)	8 часов (то же, что для верхней подсистемы)	1 месяц (в сравнении с 6 месяцами для верхней подсистемы)

Рис. 8. Зависимость риска нарушения целостности моделируемой системы от периода прогноза (в месяцах) при регулярном контроле, пассивных и активных мерах противодействия угрозам

Рис. 9. Зависимость риска нарушения целостности моделируемой системы от периода прогноза (в месяцах) для гипотетически идеального варианта

([1–0.085] / 0.085~10.8), поскольку за этот сравнительно короткий срок скорее всего не может быть реализовано ни одной угрозы, т.к. время развития угроз до их реализации в результате контроопераций увеличилось до 7 месяцев. При прогнозировании на 12–16 месяцев вероятность «успеха» в противодействии угрозам составит от 0.177 до условно допустимого уровня 0.30, что в 2.3–4.6 раза больше вероятности «неудачи». При прогнозировании на два года в сценариях угроз из таблиц 3 и 4 вероятности «успеха» и «неудачи» приблизительно одинаковы (0.55 против 0.45). Таким образом, результаты расчетов по примеру 4 показали: применение активных мер противодействия угрозам (т. е. использование контроопераций) в дополнение к пассивным мерам противодействия угрозам перспективно при кратко- и среднесрочном прогнозе ведения ИВ (до 16 месяцев). Вместе с тем, при ведении ИВ в течение двух лет и более по сценарию, приведенному в таблицах 3 и 4, «успехи» и «неудачи» приблизительно равновероятны.

При этом возникает чисто гипотетичный, но важный практический вопрос: «Какой эффективности можно добиться, если в пассивном и активном противоборстве ориентироваться на результаты, свойственные только активным мерам противодействия угрозам?», т.е. каковы могут быть самые оптимистические результаты контроопераций? На практике это означает полное информирование защищающейся стороны о планах противника (что с реальным противником не достижимо никогда). С математической точки зрения анализ этого гипотетически идеального варианта означает, что исходные данные для моделирования верхней и нижней подсистем (в структуре рис. 3) одинаковы и принимают значения из табл. 4.

Результаты прогноза для этого гипотетически идеального варианта показали (см. рис. 9): вероятностный риск нарушения целостности моделируемой системы составит 0.053 при прогнозе на полгода (что вполне сравнимо с 0.085 для вполне реального варианта из рис. 8) с увеличением до 0.41 в течение двух лет (что также вполне сравнимо с 0.45 из рис. 8). В практической интерпретации приведенные на рис. 9 результаты расчетов означают, что в идеале вероятность «неудачи» в противодействии угрозам не превысит условно допустимого уровня 0.30 при прогнозировании на срок до 20 месяцев (что вполне сравнимо с 16 месяцами из рис. 8), это как минимум в 2.3 раза меньше вероятности «неудачи» ([1 – 0.30] / 0.30 ~ 2.3).

Таким образом, результаты расчетов по примеру 4 показали: при кратко- и среднесрочном планировании даже при полном информировании о планах противника гипотетически идеальный вариант применения активных мер противодействия угрозам несущественно повышает эффективность контроопераций в ИВ. Для управления рисками правомерна рекомендация: при планировании контроопераций целесообразно ориентироваться на активные и пассивные меры противодействия угрозам с расчетом удержания эффекта от контрвоздействий в ИВ до 16 месяцев.

Пример 5. В примере осуществлен прогноз целостности сложной моделируемой системы (см. рис. 10), в качестве каковой выступает репутация виртуального государства и его руководства, подвергающихся длительным стратегическим информационным операциям ИВ и осуществляющих противоборствующие контроперации.

Рис. 10. Моделируемая система для примера 5

Подсистема 1 характеризует проведение стратегических операций в заданный период времени. Как частный случай период времени может быть равен одному году. Структура подсистемы 1 аналогична структуре, рассмотренной в примере 4. Элемент 11 ассоциируется с пассивными мерами противодействия угрозам (как в примерах 3, 4), элемент 12 ассоциируется с активными мерами противодействия угрозам (как в примере 4).

Подсистемы 2 и 3 также характеризуют проведение стратегических операций в заданный период времени. Как частный случай период времени может быть равен одному году (как и для подсистемы 1). Структура подсистем 2 и 3 аналогична структуре подсистемы 1, а также структуре, рассмотренной в примере 4. Аналогично элементы 21 и 31 также ассоциируются с пассивными мерами противодействия угрозам (как в примерах 3, 4), элементы 22 и 32 ассоциируются с активными мерами противодействия угрозам (как в примере 4). Разница между подсистемами 2 и 3 лишь в том, что за счет последствий контроопераций в период функционирования подсистемы 1 в подсистеме 2 возникает уже не 6, а 5 информационных операций со стороны противника, а в подсистеме 3 возникает уже не 6 или 5, а 4 операции со стороны противника.

Исходные данные для моделирования сформированной системы по примеру 5 отражены в табл. 5.

Важно заметить, что, единый период прогноза для всех трех подсистем при применении предложенной модели интерпретируется так: с точки зрения защищающейся стороны целостность моделируемой системы сохраняется, если за задаваемый период прогноза «И» для первой, «И» для второй, «И» для третьей подсистем их целостность не будет нарушена – то есть на практике нарушение целостности моделируемой системы из трех логически последовательных подсистем наступает тогда, когда состояние одной из них в условиях информационных угроз, свойственных каждой из подсистем и ее элементов (эти условия в общем случае различны), оказалась в элементарном состоянии «целостность подсистемы нарушена». В свою очередь, это состояние будет тогда, когда в период прогноза одновременно оба элемента окажутся в элементарном состоянии «целостность элемента нарушена» (что на практике означает достижение целей операции противником).

Это вовсе не означает, что подсистемы физически действуют в одно и то же время. Логически это могут быть разные по содержанию, но единые по длительности периоды, объединенные единым комплексом стратегических операций в ИВ – например, подсистема 1 ассоциируется с 2018 годом из «Дела Скрипалей», подсистема 2 – с 2019 годом, а подсистема 3 – с 2020 годом (см. в 1-й части статьи рис. 8). Тогда с помощью предложенной модели в примере может быть оценена возможность противодействия трехгодичному комплексу стратегических операции ИВ со стороны противника.

Результаты прогноза для защищающейся стороны показали (см. рис. 11, 12):

Таблица 5

Исходные данные для моделирования сложной системы по примеру 5

Моделируемая подсистема	Частота возникновения угроз, σ	Среднее время развития угроз, β	Период между диагностиками, $T_{меж}$	Длительност диагностики, $T_{диаг}$	Среднее время восстановления целостности системы, $T_{восст}$
Подсистема 1, состоящая из элементов 11 / 12	6/6 операций в год (как в таблице 3)	3/7 месяцев (как в таблицах 3 и 4)	1/1 сутки (как в таблицах 3 и 4)	8/8 часов (как в таблицах 3 и 4)	6/1 месяц (как в таблицах 3 и 4)
Подсистема 2, состоящая из элементов 21 / 22	5/5 операций в год (меньше, чем в подсистеме 1 за счет последствий контроопераций)	3/7 месяцев (как в таблицах 3 и 4)	1/1 сутки (как в таблицах 3 и 4)	8/8 часов (как в таблицах 3 и 4)	6/1 месяц (как в таблицах 3 и 4)
Подсистема 3, состоящая из элементов 31 / 32	4/4 операций в год (меньше, чем в подсистеме 2 за счет последствий контроопераций)	3/7 месяцев (как в таблицах 3 и 4)	1/1 сутки (как в таблицах 3 и 4)	8/8 часов (как в таблицах 3 и 4)	6/1 месяц (как в таблицах 3 и 4)

- вероятностный риск нарушения целостности подсистемы 1 за год (например, за 2018 год из «Дела Скрипалей» при 6 операциях в год) составит 0.19, подсистемы 2 – 0.15 (например, за 2019 год при 5 операциях в год), подсистемы 3 – 0.12 (например, за 2020 год при 4 операциях в год), а моделируемой системы в целом (например, за все 3 года) – 0.39. Если для каждого отдельного года результаты могут быть расценены как успешные (риски от 0.12 до 0.19 в год), то для комплекса стратегических операций за 3 года результат неутешительный (риск = 0.39), для управления рисками необходимо изыскивать политические, экономические, социальные и иные контрмеры по уменьшению частоты возникновения угроз (желательно не более 4-х операций в год), увеличению времени развития угроз до их реализации (желательно не менее 7 месяцев), а также по дальнейшему снижению времени восстановления целостности системы (в среднем для восстановления репутации за время не более 1 месяца);
- если при планировании контроопераций рассматривать периоды прогноза по полгода для каждой из подсистем, то риск нарушения целостности всей моделируемой системы составит 0.192, риск нарушения целостности моделируемой системы не превысит условно допустимого уровня 0.30, если период прогноза не превысит 9.8 месяцев. Это внушает умеренный оптимизм и уверенность в рациональности планируемых пассивных и активных мер противодействия угрозам, проявляемых в течение полугода (со значениями параметров из табл. 5). Из этих результатов для управления рисками вытекает рекомендация: при планировании контроопераций против комплекса стратегических операций противника в ИВ целесообразно ориентироваться на контроперации, применимые в течение периода до 9 месяцев, а также на иные меры противодействия угрозам с расчетом удержания эффекта от контрвоздействия в ИВ до 16 месяцев (последнее – с учетом результатов исследований в примере 4);
- если рассматривать периоды прогноза от 10 до 19 месяцев для каждой из подсистем, то риск нарушения целостности моделируемой системы составит от 0.3 до 0.7, это может быть интерпретировано как существенная неопределенность в шансах на «успех» или «неудачу» (при этом сумма всех трех периодов комплекса стратегических операций составит от 30 до 57 месяцев). Если рассматривать периоды прогноза свыше 19 месяцев для каждой из подсистем, то риск нарушения целостности моделируемой системы составит уже свыше 0.7, что может быть интерпретировано как однозначная «неудача» для защищающейся стороны. Для управления рисками правомерна рекомендация: в условиях неопределенности не планировать контроперации, ощутимый эффект от которых ожидается после 19 месяцев после их реализации (конечно, возможны исключения, связанные с заведомо определенными для государства и мира датами – такими, как годовщина важного памятного события, Олимпийские игры и т. п.).

Рис. 11. Риски нарушения целостности за год для подсистем 1–3 и моделируемой системы в целом

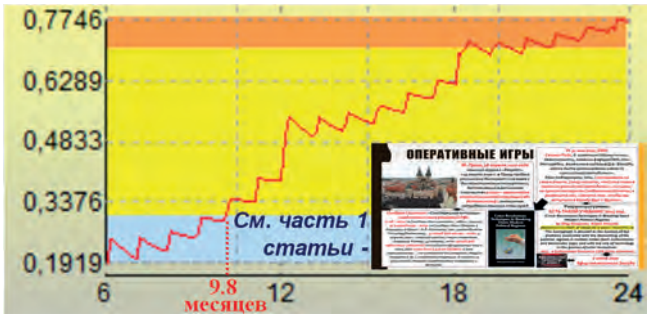

Рис. 12. Зависимость риска нарушения целостности моделируемой системы от периода прогноза (в месяцах)

Таким образом, приведенные примеры 1–5 демонстрируют работоспособность предложенных методов математического моделирования для вероятностного прогнозирования рисков. Полученные результаты моделирования и сформулированные рекомендации представляют собой аналитическую аргументацию для количественного обоснования упреждающего управления рисками в ИВ.

Заключение

1. Для математического моделирования различных способов ведения ИВ проведен анализ основных стратегий операций «удушения», «загонной охоты», прямого шантажа. В интересах аналитических исследований рассмотрены такие меры противодействия информационным операциям (меры контроопераций), как перехват информационной повестки и оперативной инициативы, отвлечение

на негодный объект, информационные прививки и контроперации возвратного типа. Проведен анализ характера стратегических операций в современной ИВ.

2. Предложены модель и методы для вероятностного прогнозирования частных и интегрального рисков в ИВ, связанных с дискредитацией репутации государства, его руководства и иных представителей власти. Для условий неопределенности способы противодействия угрозам формализованы в квазиреальном масштабе времени. Основные стратегии ИВ формально описаны в терминах случайных событий, характеризующих возникновение и развитие во времени возможных угроз реализации операций и контроперации в ИВ. Стратегические операции в ИВ формализованы в виде сложной структуры с привязкой к генеральному плану и обозначением целей на ближнесрочную, среднесрочную и долгосрочную перспективы во времени. Каждый из составных формализованных элементов этой структуры связан с другими элементами логическими условиями и реализует конкретный фрагмент стратегии и набор операций ИВ для достижения интегральной цели противника и контроперации как меры противодействия защищающейся стороны.
3. В качестве исходных данных для математического моделирования операций и контроперации ИВ выступают: частота возникновения источников угроз; среднее время развития возникшей угрозы до ее реализации; время между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы; длительность диагностики; среднее время восстановления нарушенной целостности; длительность периода прогноза. Получаемые результаты моделирования используются в интерпретации к исходной системе, в интересах которой проводятся соответствующие расчеты.
4. Работоспособность предложенных модели и методов подтверждена на разобранных примерах, охватывающих:
   - «фейковые» воздействия на положительную репутацию виртуального политического деятеля государства в условиях, учитывающих действующее законодательство РФ, а также меры противодействия «фейкам» для удержания рисков в допустимых пределах;
   - реализацию информационных операций против виртуального несуверенного государства (готового не противодействовать операциям ИВ против него или имитировать такое противодействие) и некоего виртуального суверенного государства, реализующего лишь пассивные меры противодействия операциям ИВ (отрицания или оправдания, указания на нестыковки в обвинениях и т. п.), но без учета активных контрдействий;
   - реализацию информационных операций против виртуального суверенного государства, применяющего не только пассивные меры противодействия операциям ИВ, но и осуществляющего активные контроперации;
   - реализацию длительных стратегических информационных операций в ИВ и противоборствующих контроперации.

   На изученных практических примерах определены достижимые границы рисков, которые могут быть использованы в поиске эффективных контрмер при ведении ИВ.
5. Математическое моделирование на примерах ведения ИВ и проведенный системный анализ зависимостей прогнозируемых рисков от исходных данных позволили выявить скрытые возможности по управлению рисками в ИВ и обосновать практические меры по удержанию рисков в допустимых пределах.

Литература

.1. *Манойло А. В., Костогрызов А. И. О вероятностном прогнозировании рисков в информационной войне. Часть 1. Анализ стратегий операций и контроперации для математического моделирования // Вопросы кибербезопасности. 2023, №6. С. 2–19. DOI: 10.21681/2311-3456-2023-6-2-19*
2. *Манойло А. В. Фейковые новости как угроза национальной безопасности и инструмент информационного управления // Вестник Московского университета. Серия 12: Политические науки. — 2019. — № 2. — С. 41–42.*
3. *Трубецкой А. Ю. Психология репутации. – М.: Наука, 2005. – 291 с.*
4. *Устинова Н. В. Политическая репутация: сущность, особенности, технологии формирования: дис. канд. полит. наук. – Екатеринбург: УГУ, 2005. – 166 с.*
5. *Шишканова А. Ю. Репутация политического лидера: особенности и технологии формирования // Огарёв-Online. 2016. №7(72). С. 2.*
6. *Манойло А. В., Петренко А. И., Фролов Д. Б. Государственная информационная политика в условиях информационно-психологической войны. 4-е изд., перераб. и доп. — Горячая линия-Телеком Москва, 2020. — 636 с.*
7. *Манойло А. В. Современная практика информационных войн и психологических операций. Вирусные технологии и «эпидемии» каскадного типа на примере операции по разоблачению агента влияния ЦРУ, бывшего вице-президента Венесуэлы Диосдадо Кабельо 17-21/08/2019. // Национална сигурност (Nacionalna sigurnost). 2019. Выпуск №3. С. 3–8. URL: https://nacionalna-sigurnost.bg/broi-3/*

8. *Манойло А. В. Дело Скрипалей как операция информационной войны // Вестник Московского государственного областного университета. — 2019. — № 1.*
9. *Манойло А. В. Цепные реакции каскадного типа в современных технологиях вирусного распространения фейковых новостей // Вестник Московского государственного областного университета (Электронный журнал). — 2020. — № 3.*
10. *Климов С. М. Модели анализа и оценки угроз информационно-психологических воздействий с элементами искусственного интеллекта. / Сборник докладов и выступлений научно-деловой программы Международного военно-технического форума «Армия-2018». 2018. С. 273–277.*
11. *Костогрызов А. И., Степанов П. В. Инновационное управление качеством и рисками в жизненном цикле систем – М.: Изд. «Вооружение, политика, конверсия», 2008. – 404с.*
12. *Andrey Kostogryzov, Andrey Nistratov, George Nistratov Some Applicable Methods to Analyze and Optimize System Processes in Quality Management // InTech. 2012. P. 127–196. URL = http://www.intechopen.com/books/total-quality-management-and-six-sigma/some-applicable-methods-to-analyze-and-optimize-system-processes-in-quality-management*
13. *Grigoriev L., Kostogryzov A., Krylov V., Nistratov A., Nistra- tov G. Prediction and optimization of system quality and risks on the base of modelling processes // American Journal of Operation Researches. Special Issue. 2013. V. 1. P. 217–244. http://www.scirp.org/journal/ajor/*
14. *Andrey Kostogryzov, Pavel Stepanov, Andrey Nistratov, George Nistratov, Oleg Atakishchev and Vladimir Kiselev Risks Prediction and Processes Optimization for Complex Systems on the Base of Probabilistic Modeling // Proceedings of the 2016 International Conference on Applied Mathematics, Simulation and Modelling (AMSM2016), May 28-29, 2016, Beijing, China, pp. 186–192. www.dropbox.com/s/a4zw1yds8f4ecc5/AMSM2016%20Full%20Proceedings.pdf?dl=0*
15. *Костогрызов А. И. Прогнозирование рисков по данным мониторинга для систем искусственного интеллекта / БИТ. Сборник трудов Десятой международной научно-технической конференции – М.: МГТУ им. Н.Э. Баумана, 2019, сс. 220–229*
16. *Kostogryzov A., Nistratov A., Nistratov G. (2020) Analytical Risks Prediction. Rationale of System Preventive Measures for Solving Quality and Safety Problems. In: Sukhomlin V., Zubareva E. (eds) Modern Information Technology and IT Education. SITITO 2018. Communications in Computer and Information Science, vol 1201. Springer, pp.352–364. https://www.springer.com/gp/book/9783030468941*
17. *Kostogryzov A, Nistratov A. Probabilistic methods of risk predictions and their pragmatic applications in life cycle of complex systems. In «Safety and Reliability of Systems and Processes», Gdynia Maritime University, 2020. pp. 153–174. DOI: 10.26408/srsp-2020*
18. *Костогрызов А. И. Подход к вероятностному прогнозированию защищенности репутации политических деятелей от «фейковых» угроз в публичном информационном пространстве // Вопросы кибербезопасности. 2023, №3. С. 114–133. DOI:1021681/2311-3456-2023-3-114-133*
19. *Kostogryzov A., Makhutov N., Nistratov A., Reznikov G. Probabilistic predictive modeling for complex system risk assessments (Вероятностное упреждающее моделирование для оценок рисков в сложных системах). Time Series Analysis – New Insights. IntechOpen, 2023, pp. 73–105. http://mts.intechopen.com/articles/show/title/probabilistic-predictive-modelling-for-complex-system-risk-assessments*
20. *Костогрызов А. И.. Нистратов А. А. Анализ угроз злоумышленной модификации модели машинного обучения для систем с искусственным интеллектом // Вопросы кибербезопасности. 2023, №5. С.*