О ВЕРОЯТНОСТНОМ ПРОГНОЗИРОВАНИИ РИСКОВ В ИНФОРМАЦИОННОЙ ВОЙНЕ. ЧАСТЬ 1. АНАЛИЗ СТРАТЕГИЙ ОПЕРАЦИЙ И КОНТРОПЕРАЦИЙ ДЛЯ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ

Манойло А.В.[1], Костогрызов А.И.[2]

Цель 1-й части работы: *на основе анализа основных стратегий операций и контроопераций в информационной войне (ИВ) сформировать общие положения подхода к математическому моделированию с тем, чтобы во 2-й заключительной части предложить модель и методы для вероятностного прогнозирования частных и интегрального рисков и с их помощью провести системный анализ выявленных возможностей по управлению рисками в ИВ.*

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. На основе их применения разработаны примеры, иллюстрирующие работоспособность предложенного подхода. Для отдельных ретроспективных данных проведен системный анализ выявленных возможностей по управлению рисками в ИВ (во 2-й заключительной части статьи).*

Научная новизна: *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 адекватной дифференциации «истина» — «ложь». Изучению этой лицевой стороны посвящены политологические исследования. В отличии от этих исследований в настоящей работе предложена математическая основа для системного анализа развития информационных операций и возможных способов противодействия им. Результаты математического моделирования операций и контроопераций ИВ представляются на количественном уровне вероятностных прогнозов рисков в терминах вероятностей «успеха» и «неудачи» в зависимости от конкретных исходных данных, формируемых по фактам или оцениваемых гипотетически. В работе изучены возможности по востребованным способам противодействия операциям в ИВ с указанием достижимых количественных оценок для управления рисками.*

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

DOI: 10.21681/2311-3456-2023-6-2-19

1. Введение

В настоящей работе 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 складыва-

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. Москва, Россия. E-mail: Cyberhurricane@yandex.ru

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

ющийся 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.

Примечание. Несмотря на всю важность, в сферу настоящих исследований ИВ, сосредоточенных на управлении психикой человека, не вошли кибероперации, которые преимущественно направлены на технические системы[3].

Информационные операции, столь распространенные сегодня, несколько лет назад присутствовали практически исключительно в деятельности спецслужб и были элементами оперативных игр, разыгрываемых разведками. Ситуативность складывания сценария самих оперативных игр и преследуемые ими сугубо тактические цели, вызванные желанием чем-нибудь «зацепить» противника или на чем-нибудь его подловить, не давали возможности выйти информационным операциям на оперативный простор. В этом контексте сам термин «информационная война» на протяжении многих десятилетий не воспринимался серьезно: его считали ловкой находкой «газетчиков», пытающихся таким путем поднять тираж своих изданий. Похоже, серьезно к информационным операциям с самого начала отнеслись только военные США, уже в 1988 году внесшие термин «психологическая операция» в Полевой устав Армии FM 33.1-1.

Сами же информационные операции к 2014 году уже начинают складываться как самостоятельный вид деятельности, но в их планировании продолжают преобладать «ремесленный» подход. Каждая операция разрабатывается индивидуально, как уникальный образец, под нее подбирается такая же уникальная (и неповторимая, подготовленная под конкретные особенности конкретной оперативной остановки) схема организации, не похожая ни на одну из предыдущих.

Однако, в 2014 г. все существенно меняется: Крым добровольно входит в состав Российской Федерации. Для Запада это решение народа Крыма становится настоящим шоком, похоже, ни США, ни Турция такого от крымчан не ожидали. Возможность прямого военного вмешательства в форме, например, высадки десанта, в 2014 году у США и НАТО имелась, но была упущена. В этом плане у США остался только один весомый инструмент агрессивного ответа – информационные операции. Гибридизация современных войн вывела ИВ на новую ступень эволюции, в условиях разнородных факторов и неопределенностей, начинают использоваться разнообразные стратегии ведения ИВ. При этом в информационных операциях появляются новые инструменты – например, «фейки» (заведомо ложная информация провокационного и резонансного характера), сочетание которых с различными технологиями распространения информации сделало их абсолютным информационным оружием, угрожающим национальной безопасности государств [1-4]. Спайка фейков и вирусных технологий произошла в 2016 году в период президентской избирательной кампании в США [1, 5].

Сегодня создается устойчивое впечатление, что теория живет отдельно, практика (в виде «Скрипалей», «Аргентинского кокаинового дела», «Панамского досье» и др. — см. далее) – отдельно, и они не только не помогают друг другу, но и слабо пересекаются. В этом и заключается основная причина торможения развития отечественной научной школы исследования ИВ. Разрыв между теорией и практикой, в первую очередь на уровне научно обоснованных количественных прогнозов и управления рисками в условиях разнообразных неопределенностей, обусловливает актуальность настоящей работы.

В условиях разнородных неопределенностей для проведения научно-практических исследований ИВ остро востребовано математическое моделирование систем. При этом в качестве моделируемой системы предлагается рассматривать виртуальную репутацию государства, его руководства и иных представителей власти в условиях реализации разнородных угроз 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 прогнозного анализа выявленных возможностей по управлению рисками в ИВ.

Примечания. 1. Под системой понимается комбинация взаимодействующих элементов, организованная для достижения одной или нескольких поставленных целей (по ГОСТ Р 57193-2016 «Системная и программная инженерия. Процессы жизненного цикла систем»).

2. Под риском понимается 1) мера опасности с ее последствиями (по ФЗ «О техническом регулиро-

3 В концепциях национальной безопасности США и РФ нанесение внезапного кибердара может быть приравнено к объявлению войны со всеми вытекающими последствиями, т.е. кибератаки могут спровоцировать прямой вооруженный конфликт даже между ядерными державами, что делает их чрезвычайно опасными и в мирное время.

вании», ГОСТ Р 51898-2002 «Аспекты безопасности. Правила включения в стандарты», ГОСТ Р 51901.1-2002 «Менеджмент риска. Анализ риска технологических систем», ГОСТ Р 51897-2011 «Менеджмент риска. Термины и определения» и др.) или как более общее определение — 2) эффект неопределенности в целях и/или задачах (по ГОСТ Р ИСО 31000-2010 Менеджмент риска. Принципы и руководство).

Работа состоит из двух частей.

В настоящей, 1-й части, проведен анализ основных стратегий ИВ, мер противодействия операциям ИВ (контроопераций), характера стратегических операций ИВ [1-9]. 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 рассмотренных ретроспективных данных определены некоторые правдоподобные диапазоны возможных значений исходных данных применительно к математическому моделированию и извлечению аналитических знаний для изучения возможностей по прогнозированию рисков (во 2-й части статьи).

Во 2-й заключительной части «Модель, методы, примеры» предложены модель и методы для вероятностного прогнозирования частных и интегрального рисков в ИВ. С их помощью на основе отдельных ретроспективных данных на примерах проиллюстрирована работоспособность модели и методов и проведен системный анализ выявленных возможностей по управлению рисками в ИВ.

2. Анализ основных стратегий

Ситуация с внезапным вхождением Крыма в состав Российской Федерации побудила специальные службы США реагировать на ходу, «с колес», поскольку времени на раскачку, как было замечено президентом России В. В. Путиным[4], у них уже не было. В этом плане прежние подходы к ведению ИВ, отличающиеся высокой избирательностью, не годились. В 2014 г. США остро нуждались именно в массовом проведении информационных операций. Это, в свою очередь, привело разведывательное сообщество США к идее перевода процессов планирования, организации и проведения информационных операций на промышленные рельсы. «Промышленный» подход, в свою очередь, привел к унификации организационно-технологических схем информационных операций, которые в итоге свелись в одну единственную универсальную базовую схему, появившуюся у американских спецслужб ориентировочно к лету 2015 г. Эта схема впервые получила свое «боевое крещение» в печально знаменитом скандале с «Панамским досье» 2016 г. В этом деле стандартная схема информационных операций, представляющая собой итерационную последовательность вбросов и технологических пауз («периодов тишины»), присутствует в чистом, незамутненном и абсолютно незамаскированном виде, ее легко можно разглядеть даже неспециалисту. Благодаря этой схеме «Панамский скандал», как известно, имел определенный успех. С этого самого момента все информационные операции спецслужб США становятся репликой «Панамского досье».

Новые стратегии ИВ и соответствующие технологические решения, выработанные США, дали возможность не только повысить частоту проведения самих операций (то есть, поставить их производство на конвейер), но и позволили испытывать на этой платформе различные оперативные сценарии и сюжеты, сделавшие современные информационные операции похожими на телевизионные сериалы. Так, в «Деле об отравлении Скрипалей» (совместной операции британских и американских спецслужб, продолжающейся еще и в настоящее время) только в течение одного 2018 г. были отработаны два сценария – «игра с пошаговым повышением ставок» и «ловля на живца» или приманку. В скандале с т.н. аргентинским кокаином – «ловля на приманку», в роли которой выступал сам кокаин, арестованный аргентинской полицией безопасности. «Дело Марии Бутиной» — это прием «ловли на живца», причем в роли «живца» выступила сама фигурантка дела, задержанная ФБР за создание в США «российской шпионской сети». История с перехватом в Генте в 2018 г. крупной партии кокаина, промаркированной символикой, похожей на символику «Единой России», — это «наклеивание ярлыков». «Выборы в Интерпол» (ноябрь 2018), завершившиеся срывом избрания российского кандидата А. Прокоп-

4 «Времени на раскачку нет» — одна из самых знаменитых цитат В. В. Путина. Например, в 2018 году на инаугурации: «Жизнь постоянно ставит перед нами новые вызовы, новые непростые задачи, и над их решением нам ещё предстоит напряженно работать. Времени на раскачку нет». См.: «Владимир Путин вступил в должность Президента России». http:// kremlin.ru, 7 мая 2018 г. URL: http://kremlin.ru/events/president/news/57416

чука, – это сценарий «скрытой угрозы», и т.д. [5]. Благодаря этим сценариям информационные операции превратились в тонкую многоходовую психологическую игру с привязкой ко временной оси.

В настоящей работе основные стратегии ИВ проанализированы на примере информационных операций против России. Анализ проведен в интересах разработки общих положений математического моделирования операций и контроопераций ИВ для прогнозирования рисков и системного анализа возможностей по управлению рисками в ИВ. Рассмотрены три основные стратегии: последовательного «удушения», «загонной охоты» и шантажа.

2.1. Стратегия «удушения» (так называемая «Петля Анаконды»)

Это — стратегия последовательно «удушения» конкретного политического лидера (как правило, президента страны) путем организации его травли сразу по нескольким независимым друг от друга направлениям, в определенный момент сходящимся в одном фокусе и дающим кумулятивный эффект.

Таким фокусом может стать выдвинутое в адрес лидера государства какое-либо особо тяжкое обвинение – например, в терроризме (радиационном, химическом, бактериологическом) и наркоторговле, на котором в определенный момент одновременно фокусируются все линии, отрабатываемые организаторами травли. Суммарный эффект от внезапной трансформации множества различных версий в один «окончательный» и «не подлежащий обжалованию» вердикт нередко лишает жертву травли не только «воздуха» (жертва начинает «задыхаться», утратив волю к сопротивлению), но и воли к самой жизни и к ее продолжению. В этой стратегии каждый новый этап реализации любой из линий травли (каждая новая операция или оперативная комбинация) должна еще сильнее сжимать «удавку», наброшенную на «шею» лидера, сжимая его грудь и легкие «на выдохе» — в тот самый момент, когда он в очередной раз среагирует на очередную провокацию и тем самым «откроется» перед противником — подставит себя под удар. Если он в таком положении «сделает выдох», обратно «набрать воздух в легкие» ему уже не дадут – «петля анаконды» на его груди и шее сожмется ровно настолько, насколько при выдохе сократилась его грудная клетка, и через некоторое время жертва просто погибнет от удушья.

Типичным примером применения «Петли Анаконды» на оперативном уровне (в рамках одной стратегической операции ИВ) являются:

- цепочка «Литвиненко – Скрипаль — Навальный», в которой обвинения в отравлениях с каждым этапом набирают обороты и становятся все более радикальными;
- цепочка «Бутина (обвиненная в создании разведывательно-диверсионно-террористической сети на территории США) – Аверьянов (обвиненный в создании диверсионно-террористической сети на территории ЕС) – «отравители Навального» (обвиненные в создании диверсионно-террористической сети на территории РФ»);
- линия «ядов» (полоний-новичок-вакцина);
- линия создания «террористических сетей и инфраструктуры» (одиночная группа «Петров-Боширов» в Солсбери – «в/ч 29155» и сеть баз в Европе – попытка создания такой же сети в США);
- явно вырисовывающаяся «кокаиновая» цепочка (поставок): «Аргентина (2017 г., 0,4 т.) – Бельгия (2018 г., 2 т.) – Кабо-Верде (2019 г., 9,5 т.).

При этом организаторы травли придерживаются следующего технологического приёма. Так, например, если в отношении лидера государства одновременно разворачиваются три кампании по его дискредитации по трем различным «основаниям» – по обвинению в политических убийствах (кампания №1), наркоторговле (№2) и покровительстве наемникам (№3), то ошибки, допущенные жертвой при попытке отразить удар, нанесенный по первой линии, сразу же используется для того, чтобы нанести удар с другого направления – по второй линии, а при попытке жертвы отразить и этот удар новая атака на нее приходит с направления №3. Так жертву травли, изматывая, «гоняют по кругу», и она вынуждена ради своего спасения хаотично метаться от одного источника угрозы к другому, пытаясь их нейтрализовать хотя бы на время.

Как именно действует стратегия «Петли Анаконды» в ИВ против России, показано на рис. 1. Для наглядной иллюстрации на рис. 2 показана последовательность информационных атак на РФ и ее лидера, выстроенная в хронологическом порядке.

2.2. Стратегия «загонной охоты»

Суть – в приклеивании на лидера ярлыка «международного преступника (террориста)» и организация его «международного уголовного преследования»): состоит в выдвижении прямых обвинений в терроризме и подведении конкретных представителей российского руководства под действие Freedom Act USA, допускающего внесудебную ликвидацию «главарей и пособников террористических группировок», или в

Рис. 1. «Петля анаконды» в ИВ против России. ©А.В. Манойло

Рис. 2. Хронологическая шкала информационных атак на РФ и ее лидера. ©А.В. Манойло

назначении за их головы конкретного денежного вознаграждения (как за Н. Мадуро и его сторонников в 2020 г.).

В рамках данной стратегии сходящимися линиями, например, могут быть «обвинения России в убийствах американских солдат в Афганистане» или «дело Навального» (идущее в развитии общей линии, заданной «делом Скрипалей»). Все это новейшие варианты стратегии «загонной охоты» 2020 года.

2.3. Стратегия прямого шантажа

«Венесуэльский прецедент» (2019) и попытка государственного переворота в Беларуссии (2020) показали, что на определенном этапе стратегической операций ее мишени – лидеру страны – может быть задан прямой вопрос: на что ты готов пойти ради того, чтобы сохранить свои активы за рубежом (если они есть) и даже жизнь?

Причем, если лидер страны не поймет сделанного ему намека, то его можно подвести под действие Freedom Act USA и затем ликвидировать без суда и следствия (как К. Сулеймани 03.01.2020 г.), или назначить за его голову цену, объявив особо опасным международным преступником (военным преступником или даже «наркотеррористом»), как это было сделано в отношении Н. Мадуро и его соратников в 2020 году.

Типичными примерами шантажа могут служить факты:

— 13 марта 2018г. Т. Мэй 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];

— захват 32 российских граждан (и одного гражданина Республики Беларусь) в Белоруссии по обвинению в участии в т. н. «ЧВК Вагнера» и «подготовке терактов», угроза выдачи этих людей СБУ;

— ультиматум, выдвинутый США и группой стран по поводу избрания А. Прокопчука на выборах в Интерпол (2018).

При этом следует отметить, что, по мере нарастания накала информационной войны против РФ, шантаж со стороны США и их военно-политических союзников в отношениях с РФ становится все более грубым и используется все чаще.

На основе результатов проведенного анализа вышеизложенных стратегий и фактов для условий разнородных неопределенностей сделаны следующие выводы применительно к последующему математическому моделированию:

— основные стратегии ИВ формально могут быть описаны в терминах случайных событий, характеризующих возникновение и развитие во времени возможных угроз реализации операций ИВ для достижения цели дискредитации репутации государства, его руководства и иных представителей власти;

— для случая неприменения ответных мер противодействия информационным операциям или

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/

применения лишь пассивных мер, таких как отрицания или оправдания, указания на нестыковки в обвинениях и т. п. 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 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-х месяцев);
- средним временем условно приемлемого восстановления репутации (несколько месяцев, по ретроспективным данным — в среднем около полугода).

3. Анализ мер противодействия информационным операциям

В настоящее время уже накоплен определенный опыт успешного противодействия информационным операциям США и их союзников – в том числе, в форме активных мероприятий (так называемых информационных контроопераций). В целом все применяемые меры противодействия операциям ИВ можно разделить на пять основных видов контроопераций:

1) перехват информационной повестки;
2) перехват оперативной инициативы;
3) отвлечение на негодный объект;
4) информационные прививки;
5) операции «возвратного типа» (класса «бумеранг»).

1) Перехват информационной повестки

Типичным примером такого рода мер противодействия операциям ИВ являются 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.

2) Перехват оперативной инициативы
(или операции прямого действия).

Типичным примером такого рода мер противодействия операциям ИВ являются:

- т. н. «Дело Диосдадо Кабельо» (август 2019) – операция по разоблачению агента ЦРУ в ближайшем окружении президента Венесуэлы Н. Мадуро;
- «Русский информатор в ЦРУ», или оперативная игра в «поиск крота» с Р.О'Брайеном, помощником президента США по национальной безопасности (октябрь 2019);
- «Русская методичка» Сьюзан Райс (2020) – заявление Сьюзан Райс об использовании русскими специальной «методички» для политической дестабилизации США.

3) Отвлечение на негодный объект

Примером такого рода мер противодействия операциям ИВ стал т.н. «приезд Суркова и Манойло в Донецк» (в октябре 2019 г.) – наглядный пример того, как один информационный вброс может запустить информационное цунами.

4) Информационные прививки

Подобного рода меры предназначены для выработки у целевых аудиторий коллективного иммунитета на негативное информационное воздействие (ожидаемого содержания).

5) Операции «возвратного типа» (или операции класса «бумеранг»)

Это — информационные контроперации, рассчитанные на использование инерции, набранной операцией противника. Типичным примером такого рода операции может служить оперативная комбинация, разыгранная с США в марте 2020 г. – сразу после объявления Д. Трампа о начале «антинаркотеррористической операции» в Венесуэле. Данная операция получила название «Предупреждение Трампу: главное – не выйти на самого себя».

Далее с целью формирования множества правдоподобных исходных данных для последующего моделирования более подробно приведены результаты анализа первых двух мер (контроопераций).

В рамках анализа меры «Операции перехвата информационной повестки» необходимо отметить, что на данный момент «Скрипальские чтения» (рис. 3) уже довольно подробно описаны и разобраны как в публикациях СМИ[6], так и в различных научных источниках [5][7].

6 См.: Skripal Readings as an Example of a Special Operation to Intercept the Information Agenda. The Latest Practice of Modern Information Warfare and Psychological Operations. // Medium. 2020, Mar. 8. URL: https://medium.com/@andreimanoilo

7 См. в [5]: п. 5.1. «Скрипальские чтения» как пример специальной операции по перехвату информационной повестки.

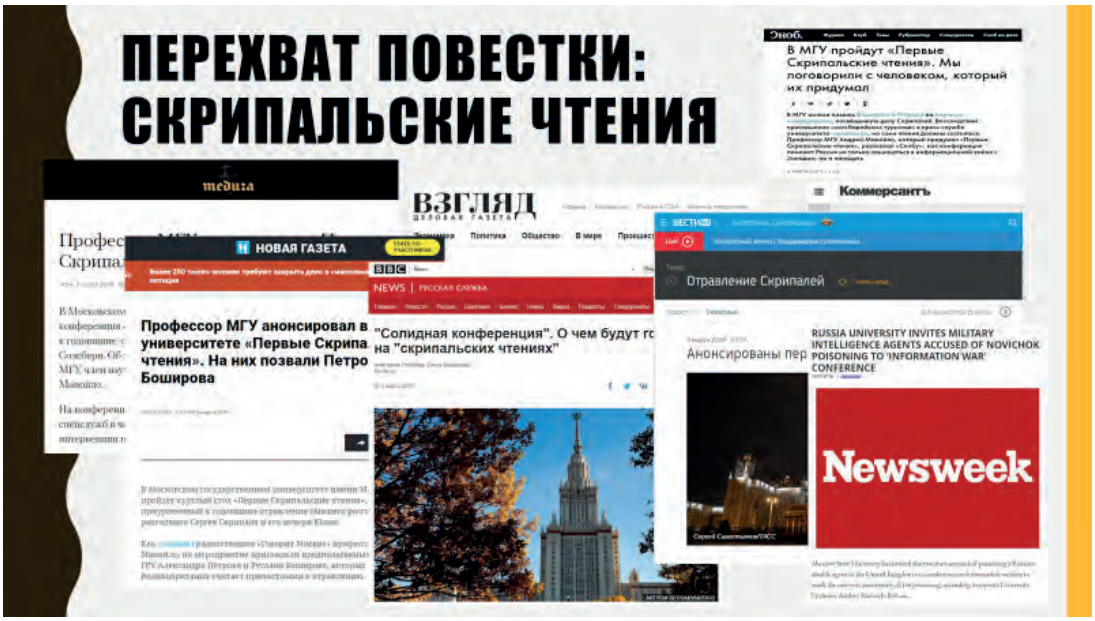

Рис. 3. «Скрипальские чтения» (3-4 марта 2019 г.): заголовки некоторых СМИ, ©А.В. Манойло

Рис. 4. «Скрипальские чтения» (3-4 марта 2019 г.): «вирусный эффект». ©А.В. Манойло

Рис. 5. «Скрипальские чтения» (3-4 марта 2019 г.): схема и результат операции. ©А.В. Манойло

Эта оперативная контроперация, проведенная 3-4 марта 2019 г. в Москве, на сегодняшний день продолжает оставаться одной из самых эффективных операций по перехвату информационной повестки – благодаря грамотно использованному тройному «вирусному эффекту» (см. рис. 4). О ее эффективности говорят статистические данные: так, за в период проведения операции (с 3 по 4 марта 2019 г.) только в одном Телеграмм-канале информационный повод захватил внимание аудитории в один миллион триста тысяч (1 304 640) человек. Совокупный же охват аудиторий в СМИ только за время проведения контроперации составил более 50 миллионов человек (опубликован 101 материал, см. рис. 5).

В рамках меры «Операция по перехвату оперативной инициативы» («операции прямого действия»), в отличие от остальных видов информационных контропераций, всегда присутствует нацеленность на нанесение противнику прямых потерь. Их результатом становятся выявленные и раскрытые тайные операции иностранных спецслужб, разоблачение их агентуры, чистки (после провалов), ведущие к потерям квалифицированных кадров, и утрата иностранными разведчиками веры в непогрешимость своего руководства и собственную неуязвимость и избранность. В то время как операции 1, 3, 4 и 5-го типов только создают условия для оказания разведывательного воздействия (перехватывают информационную повестку, отвлекают внимание противника на негодный объект и т.д.), операции прямого действия это разведывательное воздействие оказывают. Главным же итогом подобного рода операций становится перехват оперативной инициативы у противника и способность навязывать ему собственные правила игры. Но это далеко не все – как

следствие, дополнительно снижается частота возникновения разнородных угроз (т.к. необходимо время на проработку новых, еще не вскрытых идей в ведении ИВ) и растягивается среднее время развития угроз до появления целевого негативного эффекта (т.к. новые неапробированные идеи в ведении ИВ при их реализации сами наталкиваются на собственные недоработки и противодействия). Кроме того, более определенно может быть установлено реальное время восстановления на приемлемом уровне репутации государства, его руководства и иных представителей власти (которая в глазах международного сообщества может быть временно ухудшена после актов информационного воздействия со стороны противника).

Главный принцип операций прямого действия состоит в следующем: противника надо мотивировать только один раз. Все остальное он должен сделать сам, своими руками, без принуждения и лишних напоминаний, а именно: раскрыть собственную тайную операцию; выдать собственную агентуру, схемы и каналы связи; засветить кадровый состав разведчиков, участвующих в операции. И быть при этом твердо уверенным в том, что другого выхода у него нет.

В этом плане одним из важных примеров операций прямого действия является операция по разоблачению агента ЦРУ в ближайшем окружении Николаса Мадуро – так называемое «Дело Диосдадо Кабельо», проведенная в Венесуэле в августе 2019 года [7]. Эта операция, состоявшая всего из одного информационного вброса, опубликованного в венесуэльском издании «Medium» 17 августа 2019 г., вызвала настоящую панику в ЦРУ и, как следствие, привела к провалу одной из самых тщательно готовившихся и законспирированных тайных операций. Вероятно, именно из-за провала этой операции и раскрытия их агента влияния в ближайшем окружении Мадуро США временно приостановили свою работу по Венесуэле (поставили ее «на паузу» до выработки «Плана Б») вплоть до 26 марта 2020 г. – почти на семь месяцев. Схема и хронология операции подробно описана в [5][8]. Это – тот самый редкий случай, когда информационный вброс, сделанный 17 августа 2019 г., 21 августа добил до самого президента США Д. Трампа и вынудил его лично включиться в операцию по прикрытию своего агента, публично признав сам факт ведения тайных переговоров с «человеком из ближайшего окружения венесуэльского президента» (за спиной Н. Мадуро).

Другим примером операции прямого действия является оперативная игра, затеянная с новым помощником президента США по национальной безопасности Робертом О'Брайеном, сменившем в сентябре 2019 г. на этом посту Джона Болтона (уволенного 10 сентября 2019 г. президентом Д. Трампом из-за провала политики США в Венесуэле – сразу после завершения операции «Дело Диосдадо Кабельо») [5][9]. Бывший заместитель директора ЦРУ Роберт О'Брайен, придя в Белый Дом, сразу же стал выяснять, откуда «русские» узнали о контактах Д. Кабельо с ЦРУ. О'Брайен не без оснований решил, что о секретной операции русские могли узнать, только имея источник внутри разведсообщества США; значит, где-то там сидит «крот». Поиск «крота» привел людей О'Брайена к журналистам «Medium», причастным к размещению вброса о контактах Кобельо; к ним было сделано несколько разведподходов с целью выяснить, не проплатила ли эту публикацию «русская разведка».

7 октября 2019 года на сайте «Medium» появляется статья: «Andrei Manoilo: No es cierto que los rusos tengamos informantes internos en la CIA, al menos no por ahora» («Андрей Манойло: Неправда, что у русских есть свои информаторы в ЦРУ, по крайней мере, сейчас»[10], в которой Манойло, отвечая на прямой вопрос об источниках информации о связях Д. Кабельо с американской разведкой, категорически опровергает версию о том, что все материалы о Кабельо он получил от «собственного информатора в окружении директора ЦРУ или директора национальной разведки». Ответ Манойло вынесли в заголовок интервью. Когда статью увидели латиноамериканские журналисты и обозреватели, они перепечатали ее как сенсационное признание от первого лица, но тут же потеряли приставку «No»[11] (в самом начале заголовка, начинавшегося со слов «No es cierto...»). В результате категорическое отрицание превратилось в признание («у русских есть свой источник в ЦРУ»), которое, по-видимому, окончательно убедило американских разведчиков, что русский «крот» — не выдумка, он действительно существует. Опираясь на эти «сведения», Р. О'Брайен провел в структурах разведсообщества

8 См. [5]: Вирусные технологии и «эпидемии» каскадного типа на примере операции по разоблачению агента влияния ЦРУ, бывшего вице-президента Венесуэлы Диосдадо Кабельо 17-21/08/2019.

9 См. [5]: Продолжение «дела Диосдадо Кабельо»: поиск «крота».

10 См.: Andrei Manoilo (Andrey Manoylo): No es cierto que los rusos tengamos informantes internos en la CIA, al menos no por ahora. // Medium. 2019, Oct. 7 URL: https://vicentequintero.medium.com/andrei-manoilo-no-es-cierto-que-los-rusos-tengamos-informantes-internos-en-la-cia-y-la-casa-blanca-8b6c6b78bc85

11 Логический оператор «не» (логического отрицания) существует только в сознании человека; при трансляции информации из сознания в подсознание оператор «не» просто отбрасывается, и отрицание превращается в признание.

Рис. 6. «Поиск русского крота» в октябре 2019 года. ©А.В. Манойло

Рис. 7. Примеры оперативных игр (2020 г.). ©А.В. Манойло

грандиозную «чистку», в результате которой СНБ США, аппарат директора национальной разведки и оперативный директора ЦРУ покинуло несколько десятков сотрудников – в основном, специалистов по Латинской Америке и славистов (см. рис. 6). Был ли среди них русский «крот» — никто не знает.

Еще одним примером операции прямого действия является оперативная комбинация, связанная с находкой «русской методички» (по организации госпереворотов) для дестабилизации политической ситуации в США, о которой говорила Сьюзан Райс 31 мая 2020г. в эфире CNN, которую она видела своими глазами[12] (рис. 7).

В этом интервью С. Райс заявила, что «беспорядки, вызванные смертью в Миннеаполисе афроамериканца Джорджа Флойда, якобы могли быть организованы

12 См.: Экс-советник Обамы считает, что протесты в США организованы по «российской методичке». [Электронный документ] / ТАСС. Официальный сайт. 2020, 1 июня. URL: https://tass.ru/mezhdunarodnaya-panorama/8612639 (Дата обращения: 1 июня 2020 г.)

извне», подчеркнув, что уверена в российском следе в беспорядках в США: «их цель — не просто опозорить Соединенные Штаты, а разделить нас, сделать так, чтобы мы вступили в борьбу друг с другом». Свое скандальное заявление С. Райс сделала в связи с массовыми беспорядками и погромами, охватившими США в мае 2020 года.

Заявление, сделанное С. Райс, очевидно, не было случайной импровизацией. Напротив, оно было сделано намеренно, на пике роста массовых протестов в США, обеспечивших этому заявлению максимальный резонансный эффект. Теперь американцы наконец то нашли того, кто погрузил Соединенные Штаты в пучину цветной революции: этим врагом оказалась Россия. Все вместе это очень напоминало начало новой оперативной комбинации американских спецслужб, поставившей себе целью зацепить содержащимися в откровениях Райс обвинениями кого-нибудь из высокопоставленных российских чиновников (вывести их на ответную реакцию) и, тем самым, утвердить американское общество в мысли о том, что именно Россия несет главную ответственность за организацию массовых беспорядков и хаос, в который страна погрузилась после убийства Флойда. В этой комбинации вслед за первой порцией резонансных обвинений, озвученных устами С. Райс (первым информационным вбросом), обязательно должны были последовать другие, способные за несколько последовательных итераций довести российское руководство до «белого каления», заставив их «отрицать очевидное», изворачиваться или оправдываться. Заключительным этапом данной операции могло бы стать обвинение России в сознательном подрыве национальной безопасности Соединённых Штатов и в государственном терроризме. Расчет был на то, что российская сторона никогда не признает существование такой методички и будет все яростно отрицать, постепенно втягиваясь в ловушку, подготовленную для нее американской разведкой.

Однако этим планам американских разведчиков не суждено было сбыться: неожиданно для них и для самой С. Райс российские патриоты нашли ту самую «русскую методичку», которую видела Райс в свою бытность помощника президента Обамы и на которую она ссылалась в своем интервью телекомпании CNN. Этой «методичкой» оказалась монография «Color Revolutions: Techniques in Breaking Down Modern Political Regimes» (Цветные революции: техники взлома современных политических режимов), изданная А. Манойло и О. Карповичем в 2015 г. в США (рис. 7)[13]. Именно её С. Райс и видела, похоже, в Библиотеке Конгресса США (в каталоге библиотеки есть соответствующая отметка) в то самое время, когда она была помощником президента по национальной безопасности. В результате у организаторов оперативной игры произошел «разрыв программы»: они рассчитывали на совершенно иную линию поведения российской стороны. После того, как 7 июня 2020 года факт «обнаружения» «российской методички» был озвучен в открытом эфире телеканала «Звезда», операция американских спецслужб была «поставлена на паузу»; история с обвинениями России в организации цветной революции в США дальнейшего продолжения не получила.

Перечень конкретных фактов применения различных операций ИВ и мер противодействия операциям ИВ (контроопераций) можно было бы продолжить. Можно вспомнить историю с отравлением Навального, являющуюся точной копией «Дела об отравлении Скрипалей». Среди других операций специальных служб США и их союзников также можно выделить операции ИВ гибридного типа, такие, как:

— «антинаркотеррористическая операция» США против Венесуэлы, начатая 26 марта 2020 г., дополняющая сценарий информационной операции (в ходе которой за головы Мадуро и 14 его ближайших соратников объявляется награда в 10—15 млн. долл.) угрозой применения силы: угрозой морской блокады, угрозой похищения и ареста и, наконец, угрозой военного вторжения по сценарию вторжения в Панаму в 1989 году;
— операция ЦРУ по захвату (при содействии КГБ Белоруссии) 32 российских граждан, следовавших транзитом в одну из стран Ближнего Востока (в которых США подозревали сотрудников ЧВК Вагнера), и попытка переправить их на Украину для развертывания на базе этой оперативной комбинации массированной информационной кампании с перспективой реализацией стратегий «загонной охоты» и прямого шантажа.

Тем не менее для целей настоящей статьи приведенных фактов предостаточно.

На основе результатов проведенного анализа вышеизложенных контроопераций ИВ, рассматривае-

13 В аннотации к данному изданию сказано: «The monograph is devoted to the analysis of the problems associated with the dismantling of the political regimes in modern states (both authoritarian and democratic type) and with the role of technology in the process of color revolutions».

мых как активные меры противодействия угрозам, и ретроспективных фактов для условий разнородных неопределенностей сделаны следующие выводы применительно к последующему математическому моделированию:

— основные меры противодействия операциям ИВ формально могут быть описаны в терминах случайных величин, характеризующих замедление развития во времени возможных угроз (вплоть до отмены операции ИВ в ее изначальном виде) и тем самым воспрепятствование достижению цели дискредитации репутации государства, его руководства и иных представителей власти;
— меры противодействия операциям ИВ, а также диагностика наличия угроз в информационном пространстве могут быть привязаны к оси времени и конкретным реализуемым угрозам. С формальной точки зрения успешные меры противодействия операциям ИВ, в т.ч. в упреждающем режиме, ведут к снижению частоты возникновения конкретных угроз (т.к. необходимо время на проработку новых, еще не вскрытых идей в ведении ИВ – например, снижение с 6 до 4-х операций в год) и растягиванию среднего времени развития этих угроз до появления целевого негативного эффекта (т.к. новые неапробированные идеи для ведения ИВ при их реализации сами наталкиваются на собственные недоработки и противодействия – например, с 3-х до 7 месяцев и более), а также в случае состоявшихся актов информационного воздействия — к более адекватному пониманию того времени, которое потребуется для восстановления на приемлемом уровне репутации государства, его руководства и иных представителей власти (которая в глазах международного сообщества может быть временно ухудшена после актов информационного воздействия – например, восстановление репутации за 1 месяц в сравнении с 6 месяцами для пассивных мер противодействия угрозам).

Отдельные операции ИВ и контроперации могут оказаться составными элементами в проведении стратегических операций, анализ характера которых проведен ниже.

4. Анализ характера стратегических операций

В отличие от оперативных игр, стратегические операции в ИВ, как правило, имеют и генеральный план, и четко обозначенные цели на ближнесрочную, среднесрочную и долгосрочную перспективы. Главным критерием их эффективности является гарантированное достижение стратегически значимого результата, причем не вообще (как в оперативных играх), а именно того, ради которого эта операция разработана. Классическим примером операций такого типа является так называемое «Дело об отравлении Скрипалей» (начавшаяся в 2018 году, см. рис. 8).

Операция американских и британских спецслужб в Солсбери (Великобритания), более известная как «Дело об отравлении Сергея и Юлии Скрипалей», на сегодняшний день остается самой успешной стратегической операцией, проведенной противником. В основе всех ее каскадных реакций лежит один единственный резонансный инцидент: попытка отравления бывшего агента МИ-6 Сергея Скрипаля (являвшегося, одновременно, бывшим офицером ГРУ) и его дочери Юлии. Как бы мы не относиться с нравственной стороны дела к этой операции, приходится признать, что первые два этапа этой операции (весна и осень 2018 года) были выполнены совершенно; все цели, поставленные организаторами этой операции, были достигнуты; все ловушки сработали; все «приманки» и «крючки» были «проглочены» противником, которые большую часть работы сделал за британских разведчиков, даже не подозревая об этом. Наконец, в скандальное дело был вовлечен президент РФ, фактически лично поручившийся за Петрова и Боширова (на Восточном экономическом форуме), что стало для МИ-6 полной неожиданностью. Подробный разбор схемы и хода данной операции представлен в [8].

При рассмотрении данной операции может сложиться впечатление, что сама операция началась и полностью завершилась в 2018 году; при этом сами Скрипали исчезли (по некоторым сведениям, в 2020 году их переправили в Новую Зеландию). Однако это впечатление обманчиво: операция ЦРУ и МИ-6 не прекращалась ни на минуту. Только в одном 2019 г. в рамках этой операции британской и американской разведками (в тесном содружестве с Der Spiegel) было отработано пять эпизодов:

— восьмого февраля 2019 г. британские таблоиды Daily Mail и Daily Telegraph одновременно сообщили, что в Лондон Петров и Боширов прилетали не одни; тем же рейсом с ними прилетел третий член «солсберецкой группировки» — Федотов (он же, по данным британских журналистов, Сергеев), кадровый сотрудник ГРУ и, возможно, начальник Петрова и Боширова.

Рис. 8. «Дело Скрипалей» (2018-н.вр.) как классический пример стратегической операции. © А.В. Манойло

После «осечки» с устранением Скрипалей, Федотов остался в Солсбери – наблюдать за тем, как будут развиваться события (хотя должен был улететь тем же рейсом Аэрофлота, что и его подчиненные). При этом свидетельства источников Daily Mail и Daily Telegraph о дальнейшей судьбе Федотова (Сергеева) в финальной части статей расходятся: Daily Mail, опираясь на источники в британской криминальной полиции, утверждает, что Федотов, убедившись, что Скрипали выжили и их теперь не достать, покинул Великобританию; Daily Telegraph, опираясь на показания источников из национальной разведки (МИ-6), напротив, отметила, что у разведки Великобритании нет достоверных доказательств того, что Федотов вообще покидал территорию Соединенного Королевства. Тем самым два печатных издания создали «вилку», опубликовав две почти идентичные версии, диаметрально расходящиеся на финальной стадии, и, тем самым, дали понять, что Федотов, возможно, и есть тот самый «крот» в руководстве ГРУ (ставший перебежчиком), от которого МИ-6 и получила упреждающую информацию о готовящемся визите Петрова и Боширова в Солсбери (для проведения задушевной беседы)[14];

— восьмого ноября 2019 г. The New York Times, ссылаясь на источники в спецслужбах четырех различных западных стран, публикует информацию о существовании в структуре российской военной разведки (которую они по привычке продолжают называть ГРУ) сверхсекретной воинской части №29155, специализирующейся на организации государственных переворотов и «внесудебных ликвидациях»; в статье указывается, что это та самая воинская часть, в которой служат Петров и Боширов; раскрывается имя генерала ГРУ, руководящего данной частью[15]. Им оказывается генерал-майор Аверьянов, в отношении которого «информационный партнер» МИ-6 Der Spiegel публикует полные установочные данные, полученные, предположительно, кадровыми разведчиками ЦРУ/МИ-6 и их агентурой в ходе оперативной установки личности «подозреваемого»; попутно выдвигается версия о том, что в Европе действует целая сеть «ликвидаторов», управляемых из единого центра и функционирующая по такому же принципу, что и террористические сети ИГИЛ и Аль-Кайды, запрещенных в РФ)[16];

14 См.: Britain will take ‘every possible step’ to extradite Novichok trio from Russia, warns Priti Patel after Scotland Yard named third GRU spy wanted over Salisbury attack on double-agent Sergei Skripal and daughter Yulia. // Daily Mail. 2019, Feb 8. URL: https://www.dailymail.co.uk/news/article-10012043/THIRD-Russian-spy-wanted-Salisbury-poisoning.html (Дата обращения: 10 февраля 2021)

15 См.: Schwirtz, Michael. Top Secret Russian Unit Seeks to Destabilize Europe, Security Officials Say. [Электронный документ] // New York Times. 2019, 8 oct. URL: https://www.nytimes.com/2019/10/08/world/europe/unit-29155-russia-gru.html (Дата обращения: 15 ноября 2020)

16 См.: Рассекречено подразделение, которое отвечает за дестабилизацию Европы. // Экспресс-Газета. 2019, 18 ноя. URL: https://www.eg.ru/politics/806825-rassekrecheno-podrazdelenie-kotoroe-otvechaet-za-destabilizaciyu-evropy-079957/

— 23 ноября 2019 г. сразу два издания Der Spiegel и The Insider – публикуют личные (установочные) данные восьми сотрудников той самой «сверхсекретной» воинской части ГРУ №29155, о которой немецкая газета писала 8 ноября; личные данные на каждого подобраны в виде развернутой анкеты и напоминают результаты оперативной установки, осуществленной британской и американской разведками (на журналистское расследование это вообще не похоже) и легализованные через их агентуру в окружении главреда Der Spiegel (а, может быть, благодаря прямой договоренности с немецкой разведкой, сделавшей нужный звонок в редакцию немецкого издания)[17]; при этом Der Spiegel и The Insider прозрачно намекают, что располагают подробной установочной информацией на всех (или почти всех) военнослужащих указанной воинской части, а публикация всего лишь восьми анкет связана исключительно с тем, что «газета не резиновая» и большее число разоблачений просто бы не поместилось на газетной странице; тем самым британская (и, возможно, американская) разведка наглядно продемонстрировала, что она может персонально установить личность каждого сотрудника секретного подразделения ГРУ №29155, вплоть до последнего клерка;
— 24 августа 2019 г. в Берлине неизвестным был убит Зелимхан Хангошвили, бывший чеченский боевик, воевавший против федеральных войск и участвовавший в организации терактов; западные издания Bellingcat, The Insider, Dossier Center и Der Spiegel, заявляют, что убийство – политическое и организовано российской военной разведкой[18]. Немецкая криминальная полиция и контрразведка первоначально занимают осторожную позицию, но к концу ноября 2019 года (почти синхронно с сенсационным «разоблачением» в/ч №29155 журналистами-расследователями Der Spiegel) их тон меняется на обвинительный и, в результате разразившегося дипломатического скандала, 4 декабря 2019 г. два российских дипломата признаются персонами нон-грата и вынуждены покинуть страну[19];
— 5 декабря 2019 г. французская газета Le Monde публикует статью о том, что на территории Франции, во французских Альпах, обнаружена «секретная база диверсантов ГРУ»[20]; отмечается, что эта база служила местом сбора и отдыха для диверсионных групп, забрасываемых в различные точки Европы; что на этой базе «восстанавливали силы» (после удачно проведенных операций) Петров, Боширов и многие из тех восьми сотрудников в/ч №29155, личные данные которых опубликовали расследователи Der Spiegel. Завершается статья французских журналистов выводом о том, что в Европе у «террористов» ГРУ, похоже, есть опорные базы и лагеря, и база в Альпах, скорее всего, не единственная.

Все пять эпизодов готовились самостоятельно, внешне – независимо друг от друга; так, чтобы создавалось впечатление того, что журналисты-расследователи из разных изданий практически одновременно вышли на след диверсантов из ГРУ и отработали этот «след» на отлично, документально подтвердив предположения, которые западные разведки очень осторожно высказывали в 2018 и начале 2019 г. После того, как все пять эпизодов были отработаны в СМИ, стало ясно, что эти сюжеты имеют много точек пересечения, и остается только сделать последний шаг – связать их все вместе в одну историю, в которой ГРУ потребуют признать террористической организацией, такой же, как ИГИЛ[21].

Такой «точкой сборки» в самом конце июня 2020 года должна была стать «сенсационная новость», опубликованная The New York Nimes: 26 июня её обозреватели, опираясь на сведения собственных источ-

17 См.: Bulgarien — Geheimdienstanschlag in Sofia: GRU-Killerteam aus Russland. [Электронный документ] // Der Spiegel. 2019, 23 ноября. URL: https://www.spiegel.de/politik/ausland/bulgarien-geheimdienstanschlag-in-sofia-gru-killerteam-aus-russland-a-1297753.html (Дата обращения 4 января 2020 г.)

18 См.: Russischer Geheimdienst womöglich in Mord an Exil-Georgier verwickelt. [Электронный документ] // Der Spiegel. 2019, 30 авг. URL: https://www.spiegel.de/politik/ausland/berlin-mord-in-moabit-hinweis-auf-russischen-geheimdienst-a-1284400.html (Дата обращения 4 января 2020 г.)

19 См.: Германия высылает двух сотрудников посольства РФ из-за убийства в Берлине. [Электронный документ] //DW. 2019, 4 дек. URL:

https://www.dw.com/ru/germanija-vysylaet-dvuh-diplomatov-rf-iz-za-ubijstva-v-parke-tirgarten/a-60133996 (Дата обращения 4 января 2020 г.)

20 См.: La Haute-Savoie, camp de base d'espions russes spécialisés dans les assassinats ciblés. [Электронный документ] // Le Mond. 2019, 5 дек. URL: https://www.lemonde.fr/international/article/2019/12/04/la-haute-savoie-camp-de-base-d-espions-russes_6021648_3210.html; Russian spies used French Alps as 'base camp' for hits on Britain and other countries. [Электронный документ] // The Telegraph. 2019, 5 дек. URL: https://www.telegraph.co.uk/news/2019/12/05/russian-spies-used-french-alps-base-camp-hits-britain-countries/ (Дата обращения 04 января 2020 г.)

21 Запрещена в РФ.

ников из разведки США, сообщили, что российская военная разведка платила талибам и их пособникам (в Афганистане) за убийства американских солдат. В статье «Russia Secretly Offered Afghan Militants Bounties to Kill U.S. Troops, Intelligence Says» («[Американская] разведка сообщает, что Россия тайно платила афганским боевикам за убийства американских солдат [в Афганистане]») утверждалось, что ради убийства американских солдат в контакт с талибами вступили военнослужащие той самой воинской части 29155, в которой проходят службу Петров и Боширов; те, в свою очередь, исправно уничтожали американских военнослужащих «за деньги, передаваемые им агентами ГРУ»[22]. В качестве мотива совершения преступления было названо желание отомстить американцам за преследование сотрудников ГРУ за инцидент в Солсбери[23].

Трудно сказать, почему этот план, весьма реальный и очень хорошо просчитанный, так и не был реализован: в самый последний момент его «поставили на паузу», решив, что еще не время. Возможно, на реализацию этого плана повлияла набиравшая обороты президентская избирательная кампания, переключившая внимание Трампа на борьбу с внутренними противниками и не оставившая ему времени для интриг против России. Не случайно источники NYT из разведсообщества США отмечали, что информация об операциях ГРУ в Афганистане была получена еще в начале февраля 2020 года, но, однако, все это время она оставалась «без движения», поскольку президент США Дональд Трамп «не знал, что с ней делать»[24].

На основе результатов проведенного анализа характера стратегических операций для условий разнородных неопределенностей сделаны следующие выводы применительно к последующему математическому моделированию:

— стратегические операции в ИВ формально могут быть 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 (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. Математически выполнение плана стратегической операции может быть описано в терминах случайных событий, характеризующих развитие во времени возможных угроз для элементов этой структуры, связь элементов характеризуется логическими условиями «И», «ИЛИ» для достижения целей в ИВ;
— по каждому составному элементу меры противодействия операциям ИВ, а также диагностика наличия угроз в информационном пространстве могут быть привязаны к оси времени и конкретным реализуемым угрозам. С формальной точки зрения успешность мер противодействия операциям ИВ полностью аналогична успешности, определенной выше.

С точки зрения влияния на репутацию государства, его руководства и иных представителей власти все вышеизложенное характеризуется множеством факторов, доступное воздействие на которые позволит управлять возникающими частными и интегральным рисками (для каждого из факторов учитываются принципиальная возможность, целесообразность и осуществимость воздействия на них). Каковы пределы достигаемой эффективности от управления рисками? – На этот вопрос возможно ответить только в результате математического моделирования операций и контроопераций в условиях реализации разнородных угроз при ведении ИВ.

5. Общие положения предлагаемого подхода к математическому моделированию

За основу предлагаемого подхода к математическому моделированию принят подход, изложенный в разные годы в приложении к различным системам [10-15] 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

22 Russia Secretly Offered Afghan Militants Bounties to Kill U.S. Troops, Intelligence Says. By Charlie Savage, Eric Schmitt and Michael Schwirtz. [Электронный документ] // The New York Times. 2020. June 26. URL: https://www.nytimes.com/2020/06/26/us/politics/russia-afghanistan-bounties.html

23 Russia Secretly Offered Afghan Militants Bounties to Kill U.S. Troops, Intelligence Says. By Charlie Savage, Eric Schmitt and Michael Schwirtz. [Электронный документ] // The New York Times. 2020. June 26. URL: https://www.nytimes.com/2020/06/26/us/politics/russia-afghanistan-bounties.html

24 «The Trump administration has been deliberating for months about what to do about a stunning intelligence assessment». См.: Russia Secretly Offered Afghan Militants Bounties to Kill U.S. Troops, Intelligence Says. By Charlie Savage, Eric Schmitt and Michael Schwirtz. [Электронный документ] // The New York Times. 2020. June 26. URL: https://www.nytimes.com/2020/06/26/us/politics/russia-afghanistan-bounties.html

системы». 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. В качестве исходной системы выступает оцениваемая реальная репутация государства, его руководства и иных представителей власти в условиях ИВ.

Под моделируемой системой понимается система, для которой решение задач системного анализа осуществляется с использованием ее формализованной модели и, при необходимости, формализованных моделей учитываемых сущностей, объединенных целевым назначением в задаваемых условиях (по ГОСТ Р 59341). В свою очередь под целостностью моделируемой системы понимается такое ее состояние, которое отвечает целевому назначению модели системы.

В качестве моделируемой системы, используемой для вероятностного прогноза расчетных показателей рисков на задаваемый период времени, выступает моделируемая система в элементарном состоянии «целостность моделируемой системы обеспечена». Элементарные состояния, формально определенные как «целостность моделируемой системы обеспечена» и «целостность моделируемой системы нарушена», при проведении исследований должны быть конкретизированы с учетом специфики реальной системы, целей и требований к сохранению ее функциональности и эффективности. Например, если в качестве моделируемой системы выступает репутация государства, под состоянием «целостность моделируемой системы нарушена» может пониматься достижение целей противником при проведении тех или иных операций ИВ, направленных против руководства страны, против которого направлены информационные операции, под состоянием «целостность моделируемой системы нарушена» может пониматься неспособность руководства этой страны принимать адекватные решения и осуществлять их эффективную реализацию (по мнению общественности, на которую нацелены операции ИВ, например, по мнению электората).

Соответственно на определенном выше пространстве элементарных событий предлагаемая (в части 2 статьи) модель позволяет рассчитать показатели вероятности обеспечения целостности и вероятности нарушения целостности моделируемой системы в течение задаваемого периода прогноза. С учетом последствий последний показатель может быть интерпретирован как риск нарушения целостности моделируемой системы в течение задаваемого периода прогноза.

Моделируемая система простой структуры представляет собой систему из единственного элемента или множества элементов, логически объединенных для системного анализа как один элемент. Анализ моделируемой системы простой структуры осуществляют по принципу «черного ящика», когда известны входы и выходы, но неизвестны внутренние детали функционирования системы.

В качестве исходных данных для моделирования «черного ящика» выступают:

- частота возникновения источников угроз;
- среднее время развития возникшей угрозы до ее реализации в виде нарушения целостности моделируемой системы;
- время между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы;
- длительность диагностики моделируемой системы;
- среднее время восстановления нарушенной целостности моделируемой системы;
- длительность периода прогноза.

Моделируемая система сложной структуры представляется как совокупность взаимодействующих элементов, каждый из которых представляется в виде «черного ящика», функционирующего в условиях неопределенности. Причем элементы связаны логическими условиями «И», «ИЛИ» для достижения целей моделируемой системы.

Выводы

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. Сформулированы общие положения и определены исходные данные для математического моделирования.

2. На основе результатов анализа сделаны следующие обобщенные выводы применительно к последующему математическому моделированию (в следующей публикации 2-й части статьи):

— 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 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 (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. Математически выполнение плана стратегической операции может быть описано в терминах случайных событий, характеризующих развитие во времени возможных угроз для элементов этой структуры, связь элементов характеризуется логическими условиями «И», «ИЛИ» для достижения целей в ИВ.

(Продолжение следует)

Литература

1. 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.
2. Трубецкой А. Ю. Психология репутации. — М.: Наука, 2005. — 291 с.
3. Устинова Н. В. Политическая репутация: сущность, особенности, технологии формирования: дис. канд. полит. наук. — Екатеринбург: УГУ, 2005. — 166 с.
4. Шишканова А. Ю. Репутация политического лидера: особенности и технологии формирования // Огарёв-Online. 2016. №7(72). С. 2.
5. 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.
6. 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/
7. Манойло А.В. Дело Скрипалей как операция информационной войны // Вестник Московского государственного областного университета. — 2019. — № 1.
8. Манойло А.В. Цепные реакции каскадного типа в современных технологиях вирусного распространения фейковых новостей // Вестник Московского государственного областного университета (Электронный журнал). — 2020. — № 3.
9. 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.
10. 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, с. 220–229.
11. 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
12. 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
13. 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
14. 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
15. Костогрызов А. И., Нистратов А.А. Анализ угроз злоумышленной модификации модели машинного обучения для систем с искусственным интеллектом // Вопросы кибербезопасности. 2023, №5. DOI:1021681/2311-3456-2023-5-9-24, с. 9–24.

ON PROBABILISTIC FORECASTING OF RISKS IN INFORMATION WARFARE. PART 1. ANALYSIS OF OPERATIONS AND COUNTEROPERATIONS STRATEGIES FOR MATHEMATICAL MODELING

Manoilo A.V.[25], Kostogryzov A.I.[26]

The purpose of the 1st *part of the work: on the basis of the analysis of the main strategies of operations and counteroperations in information warfare (IW), to form general provisions of the approach to mathematical modeling in order to propose a model and methods for probabilistic forecasting of particular and integral risks in the 2nd and final part, and with their help to conduct a systematic analysis of the identified opportunities for risk management in IW.*

Result of research: *based on the results of the analysis of strategies of operations and counteroperations (in the 1st part of the article), a model and methods for probabilistic forecasting of particular and integral risks in IW are proposed. Based on their application, examples have been developed to illustrate the efficiency of the proposed approach. For some retrospective data, a systematic analysis of the identified opportunities for risk management in IW was carried out (in the 2nd final part) articles).*

Scientific novelty: *today the impact of heterogeneous threats in the conduct of IW in the international public media space is expressed in purposeful compromising fabrications of a resonant nature (false facts, false intentions) that contribute to the discrediting and discrediting of the reputation of the state, its leadership and other representatives of the authorities. This front side of IoT is visible to all consumers of information, but without an adequate differentiation between "true" and "false". The study of this on the front side, political science studies are devoted. In contrast to these studies, this paper proposes a mathematical basis for a system analysis of the development of information operations and possible ways to counteract them depending on specific initial data, formed on the basis of facts or estimated hypothetically. The paper examines the possibilities for popular methods of countering operations in IoT with the indication of achievable quantitative estimates for risk management.*

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

References

1. Manojlo A.V. Fejkovye novosti kak ugroza nacional'noj bezopasnosti i instrument informacionnogo upravlenija // Vestnik Moskovskogo universiteta. Serija 12: Politicheskie nauki. — 2019. — № 2. — S. 41–42.
2. Trubeckoj A. Ju. Psihologija reputacii. — M.: Nauka, 2005. — 291 s.
3. Ustinova N. V. Politicheskaja reputacija: sushhnost', osobennosti, tehnologii formirovanija: dis. kand. polit. nauk. — Ekaterinburg: UGU, 2005. — 166 s.
4. Shishkanova A. Ju. Reputacija politicheskogo lidera: osobennosti i tehnologii formirovanija // Ogarjov-Online. 2016. №7(72). S. 2.
5. Manojlo A. V., Petrenko A. I., Frolov D. B. Gosudarstvennaja informacionnaja politika v uslovijah informacionno-psihologicheskoj vojny. 4-e izd., pererab. i dop. — Gorjachaja linija-Telekom Moskva, 2020. — 636 s.
6. Manojlo A.V. Sovremennaja praktika informacionnyh vojn i psihologicheskih operacij. Virusnye tehnologii i «jepidemii» kaskadnogo tipa na primere operacii po razoblacheniju agenta vlijanija CRU, byvshego vice-prezidenta Venesujely Diosdado Kabel'o 17-21/08/2019. // Nacionalna sigurnost (Nacionalna sigurnost). 2019. Vypusk №3. S. 3-8. URL: https://nacionalna-sigurnost.bg/broi-3/
7. Manojlo A.V. Delo Skripalej kak operacija informacionnoj vojny // Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta. — 2019. — № 1.

25 Andrey V. Manoilo, Dr.Sc. (Political Science), Ph.D. (Physics & Mathematics), Professor of Lomonosov Moscow State University, Professor of the Faculty of Political Science of Lomonosov Moscow State University. Moscow, Russia. E-mail: Cyberhurricane@yandex.ru

26 Andrey I. Kostogryzov, Dr.Sc. (Technology), Professor, Federal Research Center "Informatics and Control" of the Russian Academy of Sciences. Moscow, Russia. E-mail: Akostogr@gmail.com

8. Manojlo A.V. Cepnye reakcii kaskadnogo tipa v sovremennyh tehnologijah virusnogo rasprostranenija fejkovyh novostej // Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta (Jelektronnyj zhurnal). — 2020. — № 3.
9. Klimov S. M. Modeli analiza i ocenki ugroz informacionno-psihologicheskih vozdejstvij s jelementami iskusstvennogo intellekta. / Sbornik dokladov i vystuplenij nauchno-delovoj programmy Mezhdunarodnogo voenno-tehnicheskogo foruma «Armija-2018». 2018. S. 273-277.
10. Kostogryzov A. I. Prognozirovanie riskov po dannym monitoringa dlja sistem iskusstvennogo intellekta / BIT. Sbornik trudov Desjatoj mezhdunarodnoj nauchno-tehnicheskoj konferencii – M.: MGTU im. N.Je. Baumana, 2019, ss. 220-229
11. 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
12. 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
13. Kostogryzov A.I. Podhod k verojatnostnomu prognozirovaniju zashhishhennosti reputacii politicheskih dejatelej ot «fejkovyh» ugroz v publichnom informacionnom prostranstve // Voprosy kiberbezopasnosti. 2023, №3. S. 114–133. DOI:1021681/2311-3456-2023-3-114-133
14. Kostogryzov A., Makhutov N., Nistratov A., Reznikov G. Probabilistic predictive modeling for complex system risk assessments (Verojatnostnoe uprezhdajushhee modelirovanie dlja ocenok riskov v slozhnyh sistemah). 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
15. Kostogryzov A.I.. Nistratov A.A. Analiz ugroz zloumyshlennoj modifikacii modeli mashinnogo obuchenija dlja sistem s iskusstvennym intellektom // Voprosy kiberbezopasnosti. 2023, №5. DOI:1021681/2311-3456-2023-5-9-24, s. 9–24.