DOI:

СЦЕНАРНЫЙ АНАЛИЗ ПРОБЛЕМ ОБЕСПЕЧЕНИЯ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Кульба В.В., Шелков А.Б., Чернов И.В., Богатырева Л.В.
Институт проблем управления им. В.А. Трапезникова РАН,
Россия, г. Москва , ул. Профсоюзная д. 65
kulba@ipu.ru, abshelkov@gmail.com, ichernov@gmail.com, lbogat@mail.ru

Аннотация: Работа посвящена исследованию проблем повышения эффективности процессов управления обеспечением общественной безопасности и трансформацией систем законодательного регулирования и правоприменения в условиях развитого информационного общества. Представлены результаты сценарного анализа целесообразности создания единого следственного органа, полученные на основе исследования разработанной мультиграфовой модели.

Ключевые слова: цифровизация, общественная безопасность, киберпреступность, правоохранительная система, сценарный анализ.

Введение

К началу XXI в развитие процессов глобализации и проникновение новых информационных, телекоммуникационных и компьютерных технологий во все без исключения сферы жизни фактически привели к информационной революции, охватившей практически все стороны социальной действительности. Уже сегодня информационные и коммуникационные технологии являются самостоятельной и стратегически важной отраслью, непосредственно влияющей, а во многом – и определяющей потенциал, реальные возможности и пути развития любого современного общества и государства. Более того, информационные технологии стали неотъемлемой частью соответствующих и более широких социальных процессов и производственных технологий, в рамках которых они сегодня реализуют наиболее важные, ключевые «интеллектуальные» их функции.

Одновременно с этим масштабная цифровизация практически всех сторон жизнедеятельности человека, общества и государственных институтов неизбежно приводит к целому ряду носящих фундаментальный характер изменений, причем обусловленных не только и не столько ростом объемов циркулирующей информации, сколько появлением новых проблем в области национальной, общественной и информационной безопасности. Соответственно возрастает и уровень использования инфокоммуникационных технологий внутренними и международными преступными сообществами. Фактически развитие процессов цифровизации в мире и, как неизбежное следствие, смещение процессов противоправной деятельности в виртуальную среду порождает целый ряд принципиально новых как внешних, так и внутренних угроз безопасности личности, общества и государства, что неизбежно ставит новые задачи перед правоохранительной системой [1].

Работа выполнена при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16151мк.

1 Анализ проблем противодействия киберпреступности

В настоящее время большую опасность для стабильного развития государства и общества представляет киберпреступность. Несмотря на то, что сегодня единого и общепринятого юридического определения киберпреступности пока не существует, ее сущность можно достаточно объективно определить как противозаконные уголовно наказуемые действия в сфере современных информационных технологий или в реальном мире с использованием данных технологий. Таким образом, абсолютное большинство представляющих общественную опасность противозаконных и совершаемых при помощи инфокоммуникационных технологий деяний с определенной степенью условности можно подразделить на две группы: деяния, связанные с взаимодействием человека и техники, и деяния, связанные с организованным при помощи технических средств взаимодействием человека с человеком (группой людей). Причем сегодня, именно вторая группа преступлений представляет наибольшую угрозу для безопасности личности, общества и государства.

Поскольку киберпреступления включают крайне широкий спектр различных правонарушений, их типологический и классификационный анализ крайне затруднены. Один из подходов к типологизации киберпреступлений приводится в Конвенции Совета Европы о киберпреступности (*англ.:* Council of Europe Convention on Cybercrime) и включает четыре типа правонарушений: (1) преступления против конфиденциальности и сохранности компьютерных данных, доступности интернет-сервисов и работоспособности информационных систем; (2) преступления, связанные с применением

компьютеров; (3) преступления, связанные с контентом; (4) преступления, связанные с правами собственности. Приведенная типология не является исчерпывающей, поскольку и современные технологии, и способы их использования в противоправных целях непрерывно и в последние годы очень интенсивно развиваются. Одновременно с этим данная типология может служить определенной базой для структурного анализа правонарушений в информационной сфере, тем более, что основу киберпреступности составляет все же в определенной мере ограниченное число противоправных деяний.

С точки зрения объекта противоправного воздействия с использованием цифровых технологий можно выделить [2]: (1) преступления против личности; (2) преступления в финансово-экономической сфере, (3) преступления в области общественной безопасности, общественного порядка и общественной нравственности; (4) преступления в сфере государственной безопасности.

В последнее время существенно возросло количество противоправных деяний в банковско-финансовой сфере с использованием интернет-технологий, и, в частности, совершаемых путем получения доступа к средствам физических лиц – клиентов банковских учреждений. Значительный ущерб наносят преступления в цифровой среде и бизнесу, т.е. юридическим лицам, для которых уже стали критичными потери от кибератак на финансы компаний.

Основные особенности киберпреступлений, такие, как скрытность, нестандартность, технологичность и т.д. (рис.1) существенно затрудняют работу правоохранительных органов по их раскрытию, предупреждению и профилактике [3, 4].

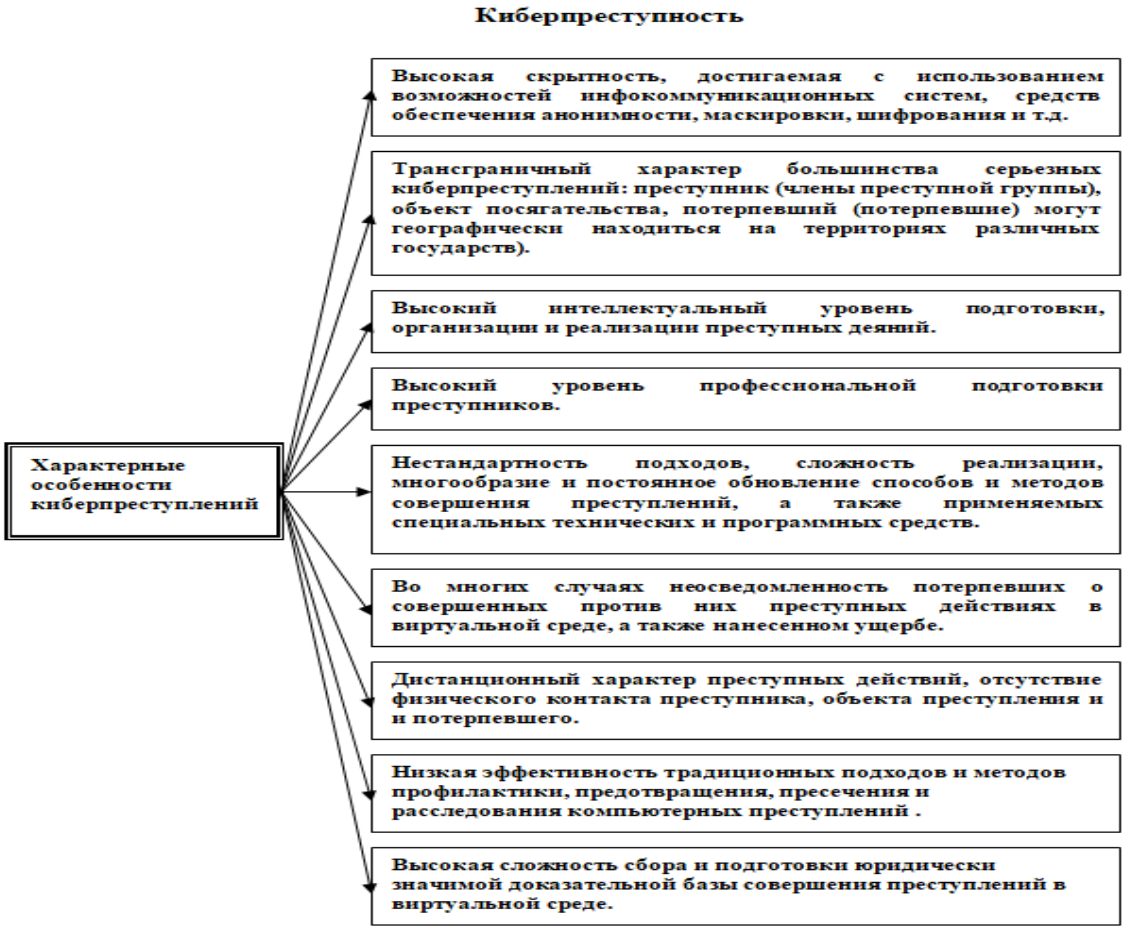

Рис.1. Характерные особенности киберпреступлений

Сегодня Россия находится в общем международном тренде развития киберпреступности, в рамках которого можно выделить следующие базовые тенденции ее развития [5]:

- высокие темпы роста количества преступлений и разнообразия форм противоправной деятельности в цифровой сфере;
- корыстная мотивация абсолютного большинства совершаемых киберпреступлений;
- усложнение методов, способов и приемов совершения киберпреступлений;
- рост криминального профессионализма осуществляющих киберпреступления лиц;

- снижение возраста киберпреступников и рост доли лиц, ранее не привлекавшихся к уголовной ответственности;
- возрастание как масштабов, так и относительной доли объема материального ущерба от киберпреступлений в суммарном ущербе от прочих видов противоправной деятельности;
- преимущественный рост киберпреступлений с использованием глобальных сетей;
- постепенный переход киберпреступности в разряд транснациональных, совершаемых международными организованными группами;
- высокий уровень латентности преступлений в виртуальной среде.

Сложившаяся ситуация и явно прослеживающиеся негативные тенденции ее возможного (а по некоторым направлениям – весьма вероятного) развития требует разработки комплексных мер и механизмов системного характера по обеспечению социальной стабильности и противодействия различным внешним и внутренним угрозам общественной безопасности.

В целом происходящие в стране и обществе процессы цифровизации, существенным образом преобразующей весь комплекс исторически сложившихся общественных отношений и механизмов **социального взаимодействия субъектов этих отношений, а также рост** мобильности социальных связей предъявляют новые высокие требования к эффективности работы правоохранительной системы. В условиях бурного развития цифровых технологий борьба с киберпреступлениями должна стать одной из приоритетных функций правоохранительной системы. Одновременно с этим необходимо подчеркнуть, что задачи раскрытия и расследования преступлений как в сфере цифровых технологий и информационной безопасности, так и в реальном мире с использованием высоких технологий являются крайне сложной задачей, решение которой требует концентрации технических и человеческих ресурсов, а также создания эффективной системы управления их использованием.

2 Сценарный анализ в управлении обеспечением общественной безопасности

Как уже отмечалось выше, в настоящее время повышение эффективности противодействия киберпреступности становится одной из важнейших составляющих процессов обеспечения общественной безопасности, причем актуальность данной задачи непрерывно возрастает. Растут и масштабы использования современных информационных технологий для организации традиционных преступлений, что также усложняет решение проблем обеспечения общественной безопасности и социальной стабильности в России.

В соответствии с Концепцией общественной безопасности Российской Федерации (утв. Президентом Российской Федерации 14.11.2013 (№ Пр-2685)) общественная безопасность определяется как «состояние защищенности человека и гражданина, материальных и духовных ценностей общества от преступных и иных противоправных посягательств, социальных и межнациональных конфликтов, а также от чрезвычайных ситуаций природного и техногенного характера», а приоритетная задача ее обеспечения определена как «защита жизни, здоровья, конституционных прав и свобод человека и гражданина».

Упомянутая выше Концепция определяет процесс обеспечения общественной безопасности как «реализацию определяемой государством системы политических, организационных, социально-экономических, информационных, правовых и иных мер, направленных на противодействие преступным и иным противоправным посягательствам, а также на предупреждение, ликвидацию и (или) минимизацию последствий чрезвычайных ситуаций природного и техногенного характера». В соответствии с действующим законодательством процесс обеспечения законности, правопорядка, общественной безопасности имеет многоуровневый характер и относится к предмету совместного ведения Российской Федерации и ее субъектов, а также в определенной мере и к ведению органов местного самоуправления. На рис. 2 отражены наиболее важные направления работы органов государственного управления, правоохранительной системы и иных уполномоченных государственных институтов в области обеспечения общественной безопасности.

Рис. 2. Основные направления обеспечения общественной безопасности

Сложность решения проблем повышения эффективности работы правоохранительной системы по обеспечению общественной безопасности в условиях интенсивного развития информационного общества заключается в том, что результаты ее деятельности существенно влияют на характер и тенденции развития социально-экономической системы (СЭС) страны в целом, а также уровень обеспечения различных составляющих национальной безопасности государства на среднесрочном и особенно на долгосрочном временном горизонте. Здесь в соответствии с целями данного исследования под СЭС понимается целостная совокупность взаимосвязанных и взаимодействующих политических, правовых, социальных, экономических и иных государственных и общественных институтов и управляемых ими процессов.

Одной из основных и критически важных задач, которые необходимо решать в процессе подготовки и принятия решений в рассматриваемой предметной области (в особенности касающихся структурных преобразований правоохранительной системы), является комплексная (в том числе прогнозная) оценка эффективности ожидаемых результатов реализации принимаемых решений и их возможного влияния (как позитивного, так и негативного) на наиболее важные сегменты СЭС.

Одновременно с этим серьезными проблемами управления процессами трансформации права и системы правоприменения особенно в условиях интенсивного развития цифровых технологий являются: (1) отсутствие полной информации об исследуемой сложной СЭС, ее окружении и взаимодействии с внешней средой; (2) отсутствие точных значений большинства факторов исследуемой системы; (3) наличие различных аспектов, влияющих на принятие решения (политические, правовые, экономические, социальные, технические и т.п.); (4) сложность объединения знаний экспертов в различных предметных областях об исследуемой системе в единую картину; (5) невозможность построения точной численной модели объекта управления.

В этой связи наиболее эффективным методом решения поставленной задачи является методология сценарного анализа, принципиально позволяющая в условиях неполной информации и неопределенности использовать в качестве исходных данные как качественного, так и количественного типа [1, 6].

Процессы управления обеспечением общественной безопасности в своей основе базируются на результатах комплексного анализа и оценки широкого спектра социально-экономических, политических и др. показателей (индикаторов), позволяющих оценивать сложившуюся ситуацию в государстве и обществе, а также риски ее дестабилизации. При этом необходимо особо отметить, что, поскольку высокий уровень общественной безопасности является во многом определяющим условием успешного социально-экономического развития государства и общества, то при оценке эффективности принимаемых в рассматриваемой предметной области управленческих решений и особенно их последствий необходимо принимать во внимание значительное количество разнообразных по своей природе и назначению факторов.

Необходимо отметить, что, при определении параметров оценки уровня общественной безопасности и особенно тенденций развития ситуации в рассматриваемой предметной области наиболее существенным, как правило, оказываются не только абсолютные значения выбранных факторов, но и устойчивые тенденции их изменения. При этом необходима предварительная оценка валидности предстоящих измерений, то есть соответствия того, что измеряется, тем понятиям, которые измерения собственно и представляют. Также крайне важно, чтобы измерения позволяли прогнозировать альтернативные варианты развития проблемной ситуации в будущем (т.е. обладали упомянутой выше прогностической валидностью), что должно позволять повысить обоснованность планирования и результативность реализации управленческих решений по обеспечению общественной безопасности, социальной стабильности и устойчивости поступательного общественного и государственного развития.

Основная трудность использования приведенных групп факторов в процессе аналитического исследования проблем обеспечения общественной безопасности заключается в их причинно-следственной взаимозависимости, многоплановости, нелинейности и динамичности развития взаимосвязей.

Предпринимавшиеся и предпринимающиеся попытки разработки точных методов решения задач рассматриваемого класса сталкиваются со значительными трудностями, что, с одной стороны, связано с необходимостью формирования ограниченного (обозримого) множества обобщенных показателей общественной безопасности, с другой – весьма сложными являются и сами процедуры обобщения, свертки, агрегирования и т.п. значительного числа динамично изменяющихся наборов разнородных факторов, в общем случае представляющих собой достаточно сложные иерархические (многоуровневые) системы различных показателей и экспертных оценок.

Кроме того, традиционно используемые подходы и методы математического и имитационного моделирования исследуемых общественных и социально-экономических процессов в рассматриваемой предметной области в своем большинстве основаны на наличии полной информации о сложной социально-экономической системе, ее окружении и взаимодействии ее сегментов (подсистем). Однако реально данные необходимой степени полноты и точности собрать практически невозможно, особенно в условиях быстро изменяющейся обстановки и скрытного характера многих угроз и сопряженных с ними рисков.

В силу сказанного выше, эффективное решение рассматриваемой задачи возможно на базе методологии сценарного анализа, базирующейся на формировании и исследовании имитационных моделей развития ситуации, формируемых на основе выделенного множества факторов (индикаторов), а также структуры и характеристик причинно-следственных связей между ними. Сценарный подход предполагает формальное построение сценариев в форме гипотетических траекторий движения моделируемой системы в фазовом пространстве ее состояний, описываемых множеством переменных (факторов и индикаторов) на основе информации о ее структуре и желательных программах развития.

Функционально-технологическая схема применения методологии сценарного анализа в процессах управления обеспечением общественной безопасности приведена на рис.3.

Проведенный анализ различных математических моделей применительно к моделированию и генерации возможных сценариев развития сложных систем показал, что для этих целей достаточно удобно использовать аппарат знаковых, взвешенных знаковых, функциональных и модифицированных знаковых графов [6]. Аппарат позволяет работать с данными как качественного, так и количественного типа, причем степень использования количественных данных может увеличиваться в зависимости от возможностей количественной оценки взаимодействующих факторов в итерационном цикле моделирования.

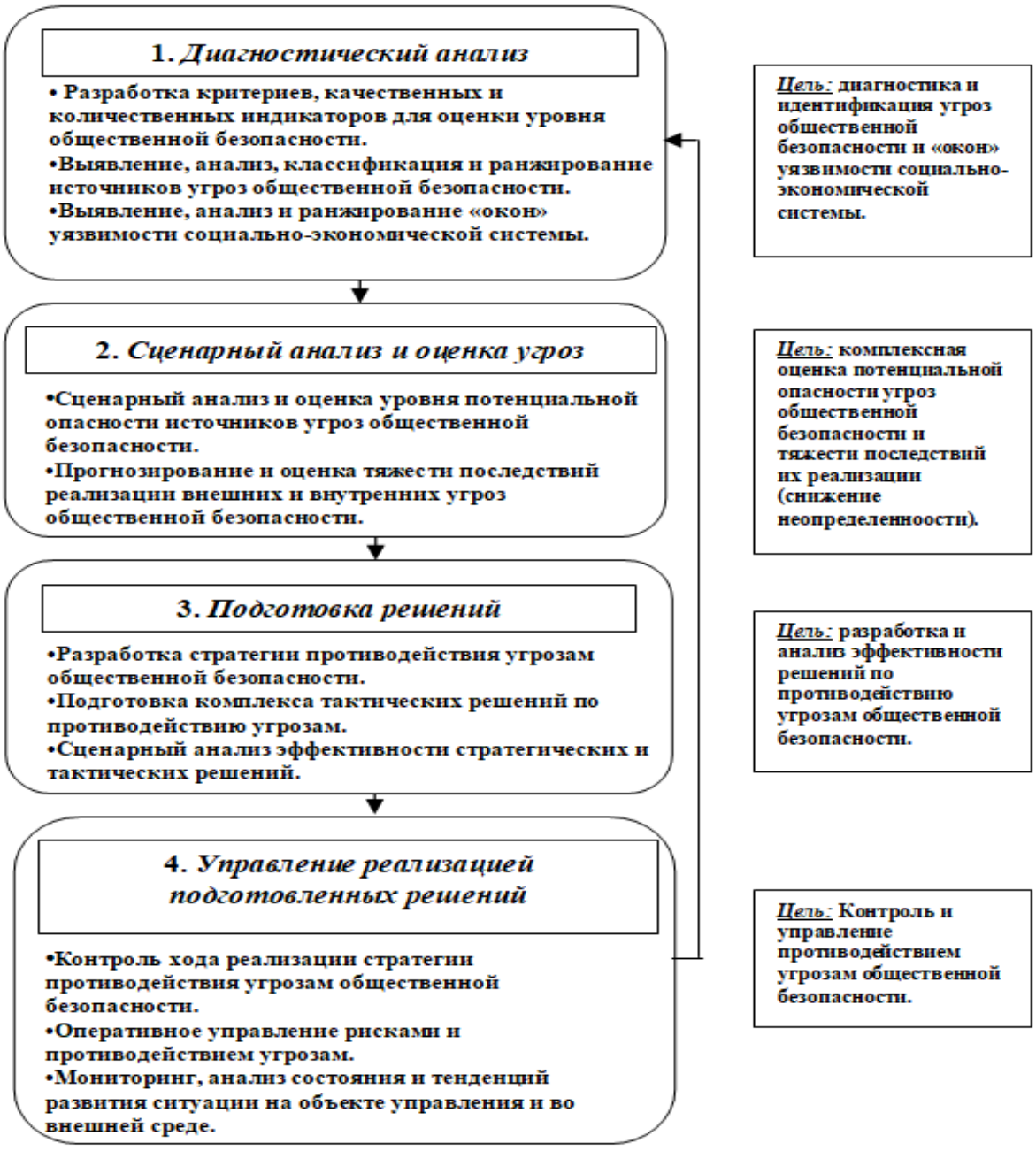

Рис. 3. Сценарный анализ процессов управления противодействием угрозам общественной безопасности

При моделировании процессов управления развитием и трансформацией правоохранительной системы на содержательном уровне параметрами вершин графовой модели являются ключевые показатели (факторы), описывающие состояние и динамику развития ситуации в политико-правовой, социально-политической или социально-экономической сферах, структура знакового графа отражает причинно-следственные взаимосвязи между ними. Совокупность значений параметров вершин в графовой модели описывает конкретное состояние исследуемой ситуации в определенный момент времени. Изменение значений параметров вершин графа порождает импульс и интерпретируется как переход исследуемой системы из одного состояния в другое. Управление развитием системы моделируется изменением структуры и подаваемыми импульсами в определенные вершины графа.

3 Сценарный анализ проблем совершенствования структуры правоохранительной системы

Изложенные выше проблемы повышения эффективности процессов обеспечения общественной безопасности в целом и расследования киберпреступлений – в частности, а также имеющиеся недостатки в организации предварительного следствия и объективные бюджетные ограничения на

содержание и развитие правоохранительной системы вновь ставят более широкий вопрос о целесообразности создания в России единого следственного органа (комитета, бюро, службы и т.д. – здесь дело не в названии), который с различной степенью интенсивности обсуждается общественностью, научным и экспертным сообществом с 90-х годов прошлого века.

Безусловно, цели создания единого следственного органа существенно шире проблем повышения эффективности борьбы с преступлениями в цифровой среде или с использованием современных инфокоммуникационных технологий. В более широком плане здесь речь должна идти о повышении качества предварительного следствия в целом, хотя сегодня вполне очевидно, что тенденции развития информационного общества будут все активней способствовать росту актуальности проблем борьбы с киберпреступлениями. Одновременно с этим создание подобного следственного органа (впрочем, как и любые структурные изменения правоохранительной системы) имеет как очевидные преимущества, так и определенные риски, состав и содержание которых в настоящее время активно обсуждается в научной среде.

Не вдаваясь в детали данных дискуссий, подчеркнем, что они имеют объективную основу, поскольку задачи проведения любых и особенно носящих принципиальный, системообразующий характер структурных преобразований системы правоохранительных органов характеризуются крайне высоким уровнем сложности, которая заключается в том, что полученные результаты существенно влияют на характер и тенденции социального, политического и экономического развития страны в целом, а также уровень обеспечения различных составляющих национальной безопасности государства на среднесрочном и особенно на долгосрочном временном горизонте.

Сложность решения рассматриваемых проблем заключается еще и в том, что любые ошибки, допущенные в процессе подготовки, принятия и реализации управленческих решений в области совершенствования структуры правоохранительных органов могут приводить к крайне тяжелым для государства и общества последствиям, а также вызывать значительный общественный резонанс. Кроме того, большие трудности вызывают и процессы согласования интересов различных слоев общества и социальных групп, а также мнений экспертов в различных предметных областях. Все это требует тщательного анализа возможных последствий принимаемых решений.

На рис.4 представлена графовая модель, обеспечивающая возможность сценарного анализа целесообразности интеграции органов предварительного следствия в единую структуру, а также оценки наиболее существенных положительных и негативных сторон формирования единого федерального следственного органа [7].

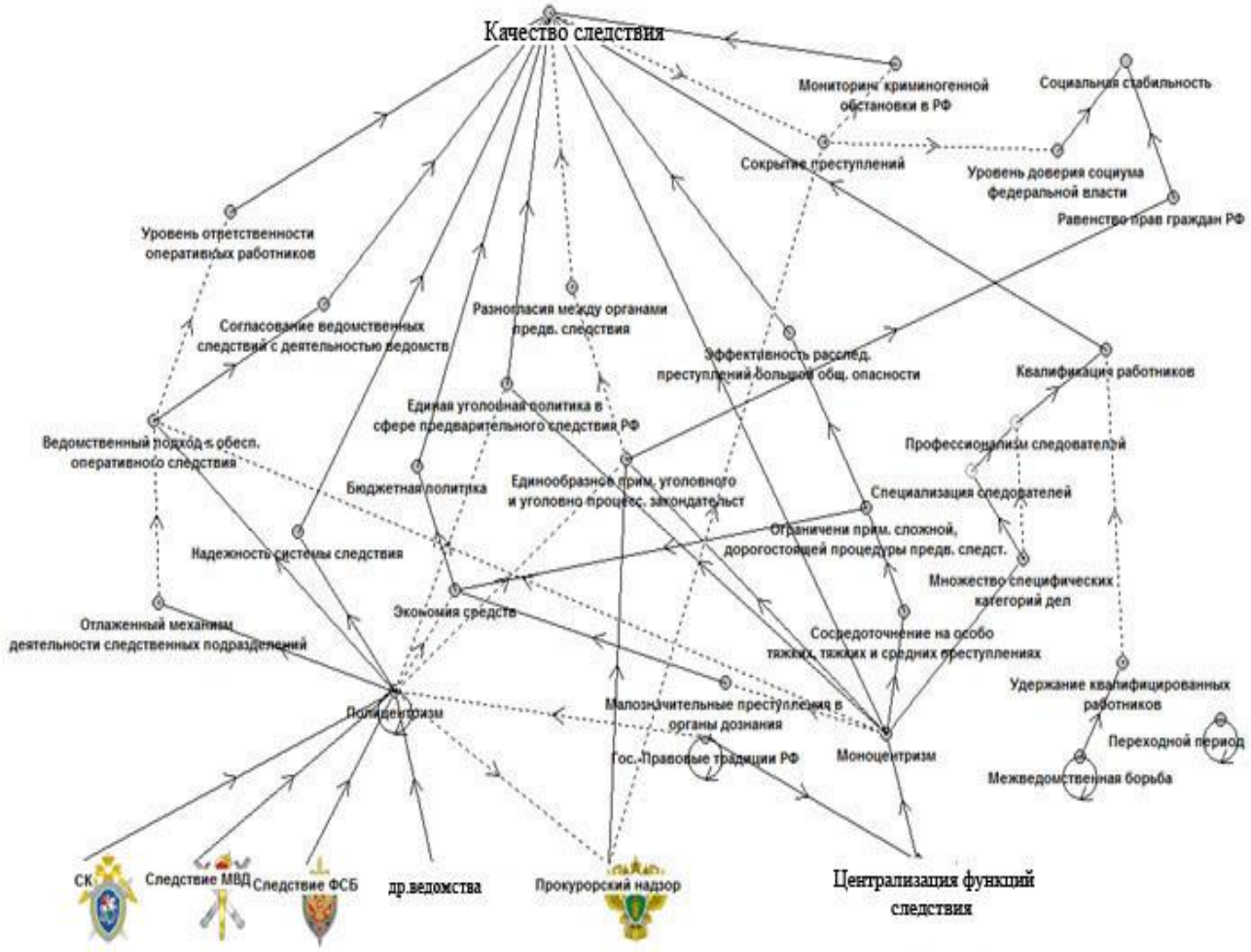

Рис. 4. Структура базовой имитационной модели

В процессе аналитического исследования данной имитационной модели разработан ряд альтернативных сценариев развития ситуации в политико-правовой и социальной сферах при различных условиях.

Сценарий 1. «Оценка организационных проблем перехода к единому следственному органу». Данный сценарий описывает типичные проблемы трансформации организационных структур управления, когда на начальном этапе функционирования новой структуры образуется определенный (желательно – кратковременный) и во многих случаях достаточно болезненный период «провала» показателей эффективности их функционирования. Объективной причиной такого положения является тот факт, что на начальном этапе старая структура уже должным образом не работает, а новая – еще не может функционировать на полную мощность, поскольку идут неизбежные переходные процессы в организации согласованной работы элементов новой управленческой структуры и их «притирки» друг к другу. Представленные на рис. 5 графические зависимости, отражающие динамику изменения значений ключевых параметров модели, по сути иллюстрируют описанные выше переходные процессы.

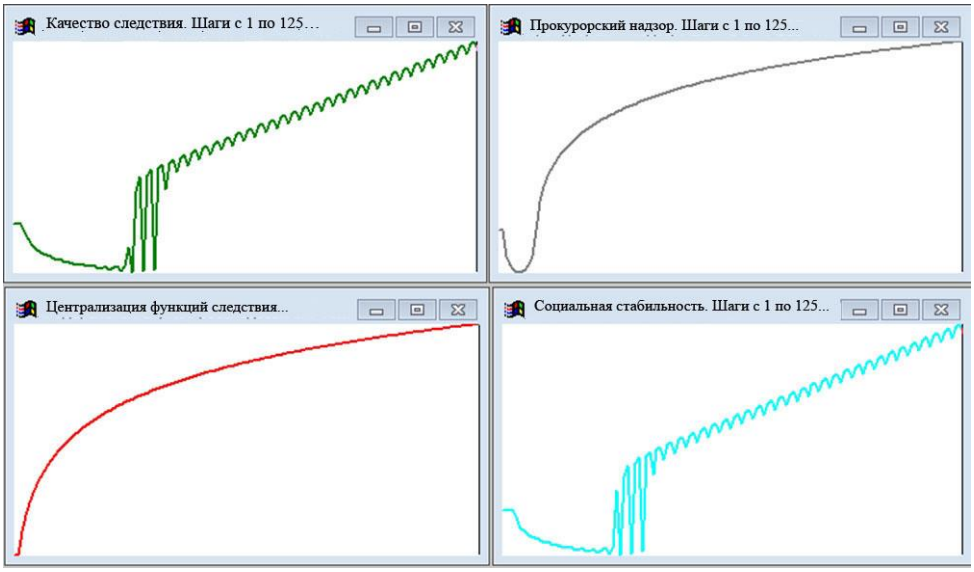

Рис. 5. Результаты моделирования (сценарий 1)

Сценарий 2. «Анализ угроз снижения качества и профессионализма следствия в результате создания единого следственного органа». В рамках данного сценария проведен анализ угроз негативного влияния структурной трансформации органов следствия на качество их работы. Как показали результаты моделирования, создание нового единого следственного органа неизбежно приводит к кардинальной перестройке отлаженного за многие годы механизма организации скоординированной деятельности следственных подразделений различных ведомств правоохранительной системы. Кроме того, возникает необходимость создания новых организационно-правовых механизмов взаимодействия между следственными и оперативно-розыскными подразделениями и службами, что неизбежно приведет к возникновению определенных трудностей в процессе совместного раскрытия и расследования преступлений. Существенно изменится и организация движения кадров, а также система карьерных лифтов.

Сценарий 3. «Анализ эффективности специализации предварительного следствия внутри единого следственного органа». В рамках данного сценария проведен анализ угроз разрушения системы специализации следователей по категориям и видам уголовных дел в процессе перехода к единой структуре управления предварительным следствием, что может привести к снижению качества следствия.

Сценарий 4. «Анализ динамики развития системы предварительного следствия в условиях изменения криминогенной обстановки». В рамках данного сценария проведена оценка возможности повышения эффективности следствия за счет организации единой системы криминологического мониторинга (особенно в киберсреде), результаты которого являются основой повышения эффективности работы предварительного следствия в целом, развития системы специализации следователей и повышения их квалификации.

Сценарий 5. «Анализ угроз концентрации полномочий в рамках данного единого следственного органа». В рамках данного сценария рассмотрена одна из отрицательных сторон создания единого следственного органа – возникновение рисков и угроз развития целого ряда имеющих признаки коррупционного характера негативных явлений, возникающих в результате, по сути, «монополизации» широкого спектра властных полномочий в единой организационной структуре.

Не вдаваясь в подробности причин, форм проявления и последствий подобного рода негативных явлений (это – отдельная и широкая тема исследований), отметим, что ситуация, когда рамках одного ведомства происходит концентрация значительного объема властных полномочий, чревата возможностью появления различных форм злоупотреблений этой властью, таких, например, как: коррупция (использование государственно-властных полномочий и прав в целях противоправного извлечения личной или групповой выгоды), сокрытие преступлений в интересах органа предварительного следствия, возбуждение «заказных» уголовных дел при отсутствии состава преступления, формальный характер внутренней надзорно-контрольной деятельности, необоснованное наращивание бюрократического аппарата, приводящее к снижению эффективности следственной деятельности и т.д.

Проведенный сценарный анализ влияния централизации органов следствия на рост коррупционных проявлений в процессе их деятельности показал, что подобные риски действительно реально существуют (рис. 6). Причем наличие в структуре правоохранительных органов нескольких ведомств, осуществляющих функции предварительного следствия, и, таким образом, препятствующих монополизации властных полномочий, при всех прочих недостатках все же в определенной степени препятствуют развитию коррупции.

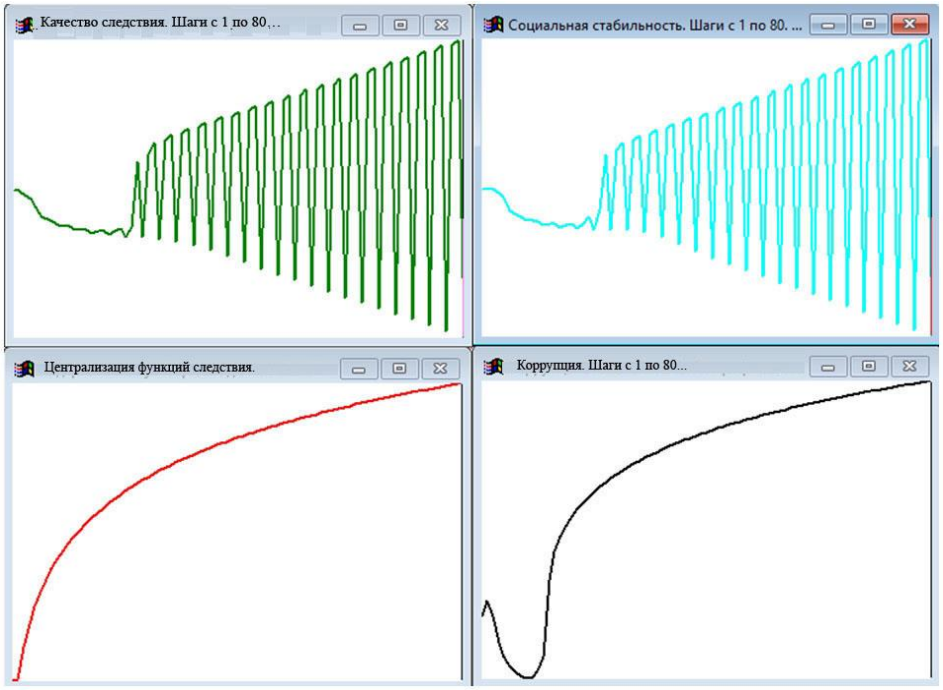

Рис. 6. Результаты моделирования (сценарий 5)

Сценарий 6. «Оценка необходимости усиления роли прокуратуры в осуществлении надзора за предварительным расследованием преступлений». В рамках данного сценария проведен анализ одного из ключевых факторов снижения рассмотренных в предыдущем сценарии рисков – усилении роли прокурорского надзора за органами предварительного следствия.

В частности, проведенный анализ показал, что необходимым и крайне важным условием создания единого следственного органа является усиление роли прокурорского надзора за соблюдением законности, поскольку усилий только внутриведомственного контроля явно недостаточно для обеспечения высокой эффективности выполнения данным органом своих функций. Таким образом, одновременно с созданием единого следственного органа на законодательном и организационном уровне должна быть решена задача усиления прокурорского надзора (контрольно-надзорной деятельности).

Наделение органов прокуратуры широкими надзорными полномочиями должно повысить эффективность предварительного следствия и снизить риск ошибок, нарушения прав и свобод граждан, а также усилить противодействие рассмотренным выше негативным явлениям, наиболее серьезными из которых являются, безусловно, коррупционные проявления.

Заключение

Результаты проведенных исследований показывают, что современные тенденции развития общества и государства требуют адекватной возникающим рискам и угрозам трансформации структуры правоохранительной системы с целью приведения ее в соответствие новым требованиям обеспечения общественной безопасности и социальной стабильности. Более того, происходящие и носящие устойчивый характер изменения общественных отношений в условиях широкомасштабной цифровизации приводят к появлению принципиально новых задач, стоящих перед правоохранительными органами, являющимися важнейшей составной частью системы управления государством и основой его устойчивого безопасного развития.

Интенсивное развитие цифровых технологий во всех сферах человеческой деятельности приводит, с одной стороны, к росту зависимости процессов общественного и государственного развития от

данных технологий, с другой – постепенному перемещению в «цифру» противоправных действий, наносящих все больший ущерб интересам личности, общества и государства. В этой связи существенно ужесточаются требования к правоохранительной системе, главной задачей которой становится совмещение борьбы как с традиционной, так и высокотехнологичной преступностью. Причем сегодня даже борьба с относительно простыми и архаичными преступлениями, требует от сотрудников правоохранительных органов обладания знаниями и практическими навыками работы с современными инфокоммуникационными технологиями. Как результат, возрастающая сложность и общественная значимость полноценного расследования совершенных с использованием высоких технологий преступлений и гарантированности неотвратимости наказания преступников объективно требует концентрации интеллектуальных, материальных и технических ресурсов.

Объективная трудность решения назревших и объективных проблем трансформации правоохранительной системы заключается в том, что любые ошибки, допущенные в процессе подготовки, принятия и реализации управленческих решений в рассматриваемой предметной области могут приводить к крайне негативным для государства и общества последствиям. Все это требует тщательного опережающего анализа возможных последствий уже на этапе подготовки решений в рассматриваемой предметной области. Именно этой цели и служит использование разработанных моделей и технологий анализа, основанных на методологии формирования сценариев развития сложных слабоформализуемых систем, позволяющей проводить исследования их поведения при различных стратегических управленческих воздействиях.

Литература

1. *Шульц В.Л. Бочкарев С.А., Кульба В.В., Шелков А.Б., Чернов И.В., Тимошенко А.А.* Анализ проблем трансформации систем законодательного регулирования и правоприменения в условиях цифровизации и методов оценки эффективности принимаемых решений // Национальная безопасность / nota bene. 2019. №4. – с. 19-74. [Электронный ресурс] – URL: https://e-notabene.ru/nb/article_30149.html. (Дата обращения: 04.06.2020)
2. *Широков В.А., Беспалова Е.В.* Компьютерные преступления: основные тенденции развития // Юрист. 2006. №10. – с.18-21.
3. *Коновалов А.А., Наумов С.А., Колесникова Д.Д.* Киберпреступность как глобальная угроза экономической безопасности: виды, особенности, проблемы противодействия // Ростовский научный журнал. 2018. №1. – с.20-27.
4. *Осипенко А.Л.* Сетевая компьютерная преступность: теория и практика борьбы. – Омск: Омск. акад. МВД России, 2009. – 480 с.
5. *Клаверов В.Б.* Проблемы противодействия компьютерной преступности. [Электронный ресурс]. URL: https://www.securitylab.ru/contest/382194.php. (Дата обращения: 31.05.2019).
6. *Шульц В.Л., Кульба В.В., Шелков А.Б., Чернов И.В.* Сценарный анализ в управлении геополитическим информационным противоборством. – М.: Наука, 2015. – 542 с.
7. *Шульц В.Л. Бочкарев С.А., Кульба В.В., Шелков А.Б., Чернов И.В., Тимошенко А.А.* Сценарный анализ проблем трансформации правоохранительной системы в условиях цифровизации // Вопросы безопасности. 2019. №4. – с. 36-65. – [Электронный ресурс] – URL: https://nbpublish.com/library_read_article.php?id=30588. (Дата обращения: 04.06.2020).