КРИТИЧЕСКИЕ ИНФРАСТРУКТУРЫ: УПРАВЛЕНИЕ РИСКАМИ И ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Ашот Тевикян[*]

Ключевые слова: инфраструктура, критические инфраструктуры, партнерские отношения, стратегический кризис-менеджмент, стратегическое прогнозирование, экономические войны.

Различные страны сталкиваются с растущим числом кризисов из-за все новых угроз, источниками которых могут быть как субъективные, так и объективные причины. Такие кризисы могут распространяться за пределы национальных границ и оказывать значительные негативные последствия на протекающие социально-экономические процессы и институты государств. Мировые лидеры остро осознают, что дальнейшие системные потрясения могут сильно затруднить возможности развития экономик стран, социальную сплоченность и политическую стабильность их обществ.

Осознается важность такого положения и в Армении. Вот как высказался начальник Национального исследовательского университета обороны МО РА Гайк Котанджян на состоявшемся 18-20 сентября 2017г. в Ереване заседании VI панармянского форума «Армения–Диаспора»: «Человечество вступает в эпоху четвертой научно-технической революции, которая характеризуется доминированием информационно-коммуникационных технологий во всех сферах жизнедеятельности государства, общества и личности <…> Республика Армения постоянно подвергается

[*] Эксперт Научно-образовательного фонда «Нораванк», преподаватель Ереванского филиала РЭУ имени Г.В.Плеханова.

вооруженному нападению со стороны своего агрессивного соседа. Эти нападения из физического пространства экстраполировались в виртуальное. Следовательно, национальная безопасность Армении и Арцаха в значительной степени обусловлены их не только традиционным оборонным потенциалом, но и кибервозможностями».

На фоне тревожного роста масштабов и сферы атак на экономические, институциональные и финансовые институты по всему миру – ***экономических войн,*** это актуализирует проведение направленных исследований на ***стыке экономики и национальной безопасности***.

Целью работы является обсуждение возможных угроз для Армении и наших союзников, которые стоят сейчас перед широким диапазоном враждебных актов, направленных на подрыв критически важных экономических активов и институциональных систем (*инфраструктур*) и причинение вреда возможностям по обеспечению безопасности государства. Соответственно, это станет призывом к правительству активизировать работы по разработке стратегии для противостояния таким угрозам и реализации вытекающих отсюда необходимых шагов.

1. Понятие критической инфраструктуры и ее контент

Во всей истории человечества овладевание и уничтожение или, наоборот, защита стратегически важных объектов были основой военного искусства. Понятие, которое применяется для совокупности таких объектов, – это «***инфраструктура***».

Национальный исследовательский совет США (*National Research Council*) дал следующее определение: «Инфраструктура – это, в самом общем смысле слова, совокупность взаимосвязанных структурных элементов, поддерживающих целостность всей структуры. Обычно применяется только для искусственно созданных (*физических* – ***прим. автора***) структур»[1].

Наше национальное благосостояние опирается на безопасную и устойчивую ***критическую инфраструктуру*** – те активы, системы и сети, которые лежат в основе любого общества, в том числе армянского. Эта ин-

[1] Infrastructure for the 21st Century Framework for a Research Age. Washington: National Academies Press, 1987. ISBN 978-030-9078-146.

фраструктура необходима для *поддержания жизненно важных общественных функций*. Одновременно существование общества зависит от уровня обеспечения поставок широкого спектра продуктов, услуг и функций.

Все более расширяющееся разнообразие угроз представляет все большую реальную опасность в процессе защиты критически важных инфраструктур. Новые уязвимости проявились с развитием информационных технологий, которые пронизывают все сферы жизни и, в первую очередь, деятельность экономически активного населения. Поэтому защита жизненно важных общественных структур и институтов является ключевой обязанностью правительства в контексте обеспечения государственной безопасности. Для достижения безопасности и устойчивости *жизненно важные партнеры*[1] по инфраструктуре должны коллективно определять приоритеты, формулировать четкие цели, избегать или смягчать риски, адаптируясь на основе обратной связи и изменяющейся среды. Партнерство в среде обеспечения безопасности и устойчивости критической инфраструктуры на национальном уровне направленно формирует защитные механизмы по управлению рисками, которым могут подвергаться критические инфраструктуры страны.

Традиционно в понятие инфраструктуры в первую очередь включаются крупные автомагистрали, дороги, мосты, сети общественного транспорта, аэропорты, поставку воды и источники воды, обращение сточных вод, обработку и ликвидацию отходов, обращение с опасными отходами, производство и передачу электроэнергии, телекоммуникации.

Однако мы не ограничиваемся данным перечнем. В условиях, когда на суше и на море, в воздухе, космосе и киберпространстве государства готовы вести войны гибридные и прокси-войны, асимметричные войны и войны, которые теперь называют «*конфликт*», сами понятия *инфраструктура и критическая инфраструктура* претерпевают изменения, точнее – наполняются новым смыслом.

При классификации инфраструктур их принято разделять на два типа: *жесткая инфраструктура* – это физические сети, необходимые для функционирования современно развитой нации; и *мягкая инфраструктура* – это институты, необходимые для поддержания социально-экономи-

[1] Наше понимание термина «*партнеры*» будет объяснено далее.

ческой системы, такие как здоровье, культурные и социальные стандарты страны, а также финансовая система, системы образования, здравоохранения, государственного управления и правоохранительных органов, и служб экстренной помощи[1].

Вот что пишет исполнительный директор Фонда «Нораванк» Гагик Арутюнян[2]: «В проводимых в «Нораванке» исследованиях особое внимание уделяется критическим инфраструктурам <…> Первоначально акцентировалась сфера информационной безопасности Армении. Однако скоро выяснилось, что все намного сложнее, т.к. практически невозможно было решать какие-то прикладные задачи без увязки возникших проблем с другими отраслями … научно-технологическая сфера является базовой критической инфраструктурой национальной безопасности, а остальные элементы являются производными от нее».

Это результат того, что наряду с хорошо известными во многих странах и отработанными направлениями вмешательства во внутриполитическую жизнь страны, подрыва её информационного суверенитета и т.п. при помощи таких испытанных технологий, как *«цветные революции», «управляемый хаос», «прямое финансовое поощрение внесистемной и системной оппозиции»,* НКО и т.п., запущены принципиально новые программы, связанные, прежде всего, с *финансово-экономическим и поведенческим* жесткими противоборствами[3], направленные на дезоргани-

[1] The soft infrastructure of a market economy Archived2011-03-28 at the Wayback Machine. William A. Niskanen, 1991, Cato Journal, Vol. 11, No. 2, 233–38, Cato Institute.

[2] «О критических инфраструктурах евразийской интеграции», декабрь, 2017. www.noravank.am/rus/issues/detail.php?ELEMENT_ID=16344.

В научно-образовательном фонде «Нораванк» исследования по данной тематике остаются важным направлением исследовательской деятельности фонда. См. на сайте фонда, например, такие публикации, как: *Арутюнян Г.*, Критические инфраструктуры и идеология; *Арутюнян Г.*, О критических инфраструктурах евразийской интеграции; *Ռոբերտ Խաչատրյան, Ֆրիդա Հակոբյան,* Բարձրագույն կրթության գործառույթները կրիտիկական ենթակառուցվածքների անվտանգության պաշտպանության գործընթացում (*Хачатрян Р., Акопян Ф.,* Функции высшего образования в процессе обеспечения безопасности критических инфраструктур (на арм.яз)); *Սամվել Մարտիրոսյան,* Հայաստանի տեղեկատվական անվտանգությունը և կրիտիկական ենթակառուցվածքները (*Мартиросян С.*, Информационная безопасность и критические инфраструктуры Армении (на арм.яз.)); *Գագիկ Հարությունյան*, Հայագիտությունը որպես «*կրիտիկական ենթակառուցվածք*» (*Арутюнян Г.*, Арменоведение как *«критическая инфраструктура»* (на арм.яз.)).

[3] *Ларина Е.,* Университеты США и американское разведывательное сообщество: как ведется война против России. http://communitarian.ru/posts/skrytaya_storona_vlasti/universitety_ssha_i_ amerikanskoe_razvedyvatelnoe_ soobschestvo_kak_vedetsya_voyna_protiv_rossii_17072015

зацию деятельности объектов/структур жизнедеятельности государства, которые можно и необходимо отнести к критическим инфраструктурам.

Рис. 1

Взаимозависимость критических инфраструктур [1]

Приводимые далее концептуальные определения задают *контент* критической инфраструктуры. Понимание этих ключевых определений является основой реалистического восприятия определяющей ее среды и формирует необходимый общественный подход по обеспечению ее безопасности и устойчивости. При этом воспользуемся опытом ряда стран (см. Таблица 1).

Критическая. В определениях большинства стран данное слово относится к той части инфраструктуры, которая оказывает *существенную* поддержку экономическому и социальному благополучию, общественной безопасности и обеспечивает выполнению ключевых обязанностей правительства.

[1] "Protecting Critical Infrastructures – Risk and Crisis Management. A guide for companies and government authorities." www.bmi.bund.de, Federal Ministry of the Interior, 2008.

Таблица 1

Определения критической инфраструктуры [1]

Австралия	Критическая инфраструктура определяется как физические объекты, цепи поставок, информационные технологии и сети связи, которые, если они будут уничтожены, деградированы или окажутся недоступными в течение длительного периода времени, окажут значительное влияние на социальное или экономическое благосостояние нации или повлияют на способность Австралии осуществлять национальную оборону и обеспечивать национальную безопасность.
Канада	Критическая инфраструктура Канады состоит из тех объектов физической инфраструктуры и информационных технологий, сетей, служб и активов, которые в случае их разрушения окажут серьезное воздействие на здоровье, безопасность или экономическое благополучие канадцев или эффективное функционирование правительств в Канаде.
Германия	Критическая инфраструктура – это организации и объекты, имеющие важное значение для общества, чья неудача или ухудшение могут вызвать постоянный дефицит поставок, значительные нарушения общественного порядка или другие драматические последствия.
Нидерланды	Критическая инфраструктура относится к продуктам, услугам и сопровождающим процессам, которые в случае нарушения или неудачи могут вызвать серьезные социальные беспорядки. Это может быть в виде огромных потерь и серьезного экономического ущерба.
Соединенное Королевство	[Национальная критическая инфраструктура] включает в себя те активы, услуги и системы, которые поддерживают экономическую, политическую и социальную жизнь Великобритании, важность которой такова, что потери могут: 1) вызвать крупномасштабную гибель людей; 2) оказать серьезное влияние на национальную экономику; 3) иметь другие серьезные социальные последствия для сообщества; или 4) иметь непосредственное отношение к правительству.

[1] Protection og Critical Infrastructure and the Role of Investment Policies Relating to National Security. OECD. 2008.

Соединенные Штаты	Определение критической инфраструктуры: системы и активы, будь то физические или виртуальные, настолько жизненно важные для Соединенных Штатов, что их неработоспособность или разрушение окажет негативное влияние на безопасность, национальную экономическую безопасность, национальное здравоохранение или любую их комбинацию. Для целей инвестиционной политики это определение более узкое: системы и активы, будь то физические или виртуальные, настолько жизненно важные для Соединенных Штатов, что неработоспособность или разрушение таких систем и активов окажет негативное влияние на национальную безопасность.

В определении Канады под критичностью подразумевается «*серьезное воздействие на здоровье, безопасность, безопасность или экономическое благополучие канадцев или эффективное функционирование правительств в Канаде*». Германия ссылается на «*значительные нарушения общественного порядка или другие драматические последствия*». Критическая инфраструктура в Нидерландах относится к инфраструктуре, разрушение которой может вызвать «*серьезные социальные беспорядки*», «*огромные потери жизней*» и «*экономический ущерб*». Таким образом, слово «*критическое*» эти государства относят к инфраструктуре, разрушение которой приведет к катастрофическим и далеко идущим последствиям для всей страны.

Инфраструктура. Определения «*инфраструктуры*», используемое в официальных описаниях критической инфраструктуры, как правило, являются довольно широкими. Выше мы уже приводили один из вариантов.

В Таблице 1 все 6 правительств к критическим инфраструктурам относят, в первую очередь, традиционные, физические инфраструктуры. Большинство из них также включают нематериальные активы и/или коммуникационные сети. Например, Австралия относит инфраструктуру к «*физическим объектам, цепочкам поставок, информационным технологиям и сетям связи*». Канада – к «*физическим и информационным технологи-*

ям, сетям, услугам и активам». Соединенное Королевство ссылается на «*активы, услуги и системы*», что является достаточно широким понятием.

Безопасность. Ее принято определять как «*состояние защищенности* (*или снижение риска через применения физических средств*) *критически важной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении нее действий в виде взломов, атак, последствий стихии или техногенных катастроф*».

Для эффективного функционирования системы обеспечения безопасности критически важных инфраструктур необходим непрерывный и последовательный мониторинг угроз, с постоянной и достоверной оценкой возможностей противодействия, нейтрализации и предотвращения этих угроз. Это позволяет своевременно устранить угрозы и уязвимости, способствует обмену точной, своевременной и действенной информацией, проведению анализа текущих и будущих рисков.

Устойчивость определяется как «*способность подготовиться и адаптироваться к изменяющимся условиям, а также оперативно противостоять и быстро восстанавливаться из-за сбоев*, *преднамеренных атак, несчастных случаев и/или, противостоять угрозам или инцидентам*».

Указывая на устойчивость инфраструктурных активов, систем и сети, предполагается, что они должны быть надежными, гибкими и адаптируемыми. Наличие точной, своевременной и действенной информации об угрозах и анализ ожидаемых рисков, определение мероприятий по смягчению их последствий, реагирование на угрозы, и, соответственно, способность на восстановление важны по укреплению устойчивости критических инфраструктур.

Повышение уровня безопасности и укрепление устойчивости критических инфраструктур обеспечивается через управления рисками. ***Риск*** определяется как «*вероятность потери или ущерба*» и относится к «*потенциально нежелательному результату, которое возможно возникнет в результате инцидента, события или события, определяемому его вероятностью* [*функция угроз и уязвимостей*] *возникновения и связанными с ним последствиями*».

Управление рисками является «*процессом идентификации, анализа с подготовкой информации о риске с передачей сообщения о ней, и при-*

знающее ее наличие, с возможностью избежать или контролировать его, с целью доведения до приемлемого уровня по приемлемой стоимости».

Партнерство (***партнерские отношения***) обеспечивает эффективное управление рисками.

Ущерб, нанесенный критической инфраструктуре, ее разрушение в результате стихийных бедствий, террористических действий, преступной деятельности или злонамеренного поведения могут оказать существенно негативное воздействие на безопасность страны и благосостояние его граждан.

В Российской Федерации (РФ) в понятие критически важного объекта (КВО) включают:

- Критически важные объекты инфраструктуры РФ – объекты, нарушение (или *прекращение)* функционирования которых приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению (или *разрушению)* экономики страны, субъекта или административно-территориальной единицы, или существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях на длительный период времени.
- Инфраструктура страны – совокупность объектов РФ, расположенных на территории РФ и иностранных государств, обеспечивающая функционирование институтов государства и жизнедеятельности его граждан.

В КВО включаются также такие понятия, как «*Объект защиты*», «*Потенциально опасный объект*» и « *Чрезвычайная ситуация*».

В «*Стратегии национальной безопасности Российской Федерации*» термин инфраструктура встречается в разнообразном контексте: военная, транспортная, информационная, жилищно-коммунальная инфраструктуры, инфраструктуры внутреннего рынка, социальная и образовательная инфраструктуры, национальные инфраструктуры финансовых рынков.

Секторальный охват. В Таблице 2 показана таблица секторального списка критической инфраструктуры для пяти западных стран и Евросоюза, которые, как считается, вызывают озабоченность в отношении их защиты.

Таблица 2

Секторальный охват критической инфраструктуры [1]

	Австралия	Канада	Нидерланды	Велико-британия	США	Евросоюз
Энергия (*в том числе ядерная*)	+	+	+	+	+	+
Информационные и коммуникационные технологии	+	+	+	+	+	+
Здравоохранение	+	+	+	+	+	+
Продовольствие	+	+	+	+	+	+
Вода	+	+	+	+	+	+
Транспорт	+	+	+	+	+	+
Обеспечение безопасности	Аварийные службы	+	+	Аварийные службы	Аварийные службы	+
Правительство и финансы		+	+	+	+	+
Химия		+	+		+	+
Оборонная промышленность	+	+	+		+	
Другие сектора и активы	Общественные/публичные собрания, национальные символы		Юридические / судебные органы		Плотины, коммерческие объекты, национальные памятники	Космические и исследовательские объекты

[1] OECD. 2008.

Как видно из перечня секторов в этом списке, большинство правительств принимают широкий секторальный взгляд на критическую инфраструктуру – они включают в себя сектора, на долю которых приходится значительная часть национального дохода и занятости.

2. Партнерские отношения, управлением рисками критической инфраструктуры, кризис-менеджмент

Партнерские отношения

Надо признать, что после развала СССР и включения в практику государственного управления принципов доктрины «Вашингтонского консенсуса», под шумок новоявленных, некомпетентных и крайне визгливых «*рыночных спецов*» в Армении была моментально приватизирована государственная собственность. И получилось так, что критическая инфраструктура страны в основном принадлежит частному сектору (*в том числе, иностранным компаниям*) и управляется им; однако правительство и местные органы власти также владеют и управляют отдельными объектами критической инфраструктуры.

И поскольку большинство инфраструктур, которые имеют решающее значение для нашего общества, находится в частной собственности, правительство и частный сектор должны работать рука об руку, добровольно сотрудничая для обеспечения эффективной защиты этих систем и объектов. Он должен стать и в дальнейшем оставаться основным механизмом для продвижения коллективных действий по обеспечению национальной безопасности и устойчивости критической инфраструктуры.

На эту проблему в распределении компетенции между государственными органами и организациями, обеспечивающими безопасность КВО, и собственниками (*владельцами*) КВО в сфере обеспечения безопасности таких объектов указывает, например союзник Армении по ОДКБ и Евразийскому союзу Белоруссия, выделяя современные задачи по обеспечению безопасности КВО[1].

Во-первых, необходимо установить точные сегменты ответственности за обеспечение безопасности КВО у уполномоченных государствен-

[1] «Современные проблемы обеспечения безопасности критически важных объектов». 2017. http://csp.by/blog-ekspert/obekty-kvo/sovremennye-problemy-obespecheniya-bezopasnosti-kr/.

ных органов и организаций в области обеспечения безопасности КВО и у собственников (*владельцев*) КВО. В ситуации, когда право собственности на значительное число объектов социально-экономической инфраструктуры, которые могут быть отнесены к КВО, перешло от государства в частные руки, центр тяжести в обеспечении безопасности таких объектов объективно смещается от государства в сторону собственников указанных объектов и негосударственных структур правоохранительной направленности и т.д.

Аналогичные проблемы имеются и в Армении.

Поэтому мы делаем упор на понятии ***партнерские отношения***, которое определяется как тесное сотрудничество между сторонами, имеющими общие интересы в достижении общего видения и целей. Поэтому, такое принципиально важное практическое значение приобретает понятие ***сообщество***, занимающееся управлением рисками для критически важных инфраструктур, включающее партнерские отношения между собственниками (*бизнес-сообщество*) и *операторами* (*государственные, местные органы власти, некоммерческие* (*экспертные*) *организации, академические круги)*.

Совместное управление предполагает, что государственные органы оказывают помощь частным компаниям в консультировании и в создании сетей связей, а также предоставляют конкретные рекомендации по их действиям в управлении рисками. И частный сектор вносит свой практический опыт в это партнерство.

Прямым преимуществом партнерских отношений является явная и общая заинтересованность в обеспечении безопасности и устойчивости критической инфраструктуры страны. Эта базовая ценность распространяется по всей сети партнерских отношений между собственниками и операторами, которые несут ответственность за управление рисками для повышения безопасности и устойчивости. Чтобы любое партнерство было эффективным, оно должно обеспечить ценность для его участников. Важность и ценность предложения для правительства очевидны: координация с заинтересованными сторонами инфраструктуры имеет важное значение для достижения предоставленного правительству мандата по сохранению общественной безопасности и обеспечению национальной безопасности.

В свою очередь, бизнес-сообщество делает многое для собственной инфраструктуры и благосостояния сообществ, которые она обслуживает. Правительство может преуспеть в том, чтобы стимулировать бизнес-сообщество выйти за рамки того, что является коммерческим интересом, и инвестировать в национальные интересы посредством активного участия в партнерских усилиях. Например, правительство может предоставить им доступ к точной, своевременной и действенной информации при появлении угроз и кризисов. Кроме того, правительство может помочь партнерам из частного сектора увидеть весь «*ландшафт*» рисков, повысив их способность делать целевые и эффективные инвестиции в область безопасности и устойчивости. Зависимость от критической инфраструктуры разделяется бизнес-сообществом и правительством, и необходимо разработать устойчивое партнерство на перспективу.

Управлением рисками критической инфраструктуры

Для ***управления рисками***, связанными с возможными существенными угрозами и опасностями, направленными на инфраструктуры, необходим комплексный подход со стороны указанного сообщества, который должен:

- Выявлять, сдерживать, обнаруживать, быть готовым и срывать угрозы и опасности, направленные на критические инфраструктуры страны.
- Снижать уязвимость критически важных активов, систем и сетей.
- Смягчать потенциальные последствия для критической инфраструктуры инцидентов или неблагоприятных событий, которые происходят с ними.

Историческая ремарка

Вопросами ликвидации последствий крупномасштабных стихийных бедствий ООН начала заниматься с 60-х годов прошлого века. В 1994г. в Иокогаме (Япония) состоялась первая Всемирная конференция по уменьшению стихийных бедствий. III Всемирная конференция по снижению риска бедствий проводилась в марте 2015г. в г.Сендае (Япония). Основным документом, принятым конференцией явилась «Сендайская рамочная

программа по снижению риска бедствий на 2015-2030 годы».

Большинство методов при выборе мер сокращения уровня рисков (*на основе выработанной стратегии приоритетов*) основывается на использовании критерия «*эффективность – стоимость*». Практика управления рисками и кризисом, которая используется в развитых странах (*например, Германия*) основана на общем цикле управления «*планирование-действие-проверка-корректировка*» (plan – do – check – act, PDCA) (рис. 2), также известен как Deming Cycle.

Рис. 2

Планирование-действие-проверка-корректировка (PDCA)

Одновременно выработка *стратегии* управления рисками и кризисом представляет собой систематический процесс и состоит из пяти этапов (рис. 3)[1].

Этап 1: Предварительное планирование

Предварительное планирование задает необходимые условия для успешного управления рисками и кризисами в сообществе.

[1] Protecting Critical Infrastructures – Risk and Crisis Management.

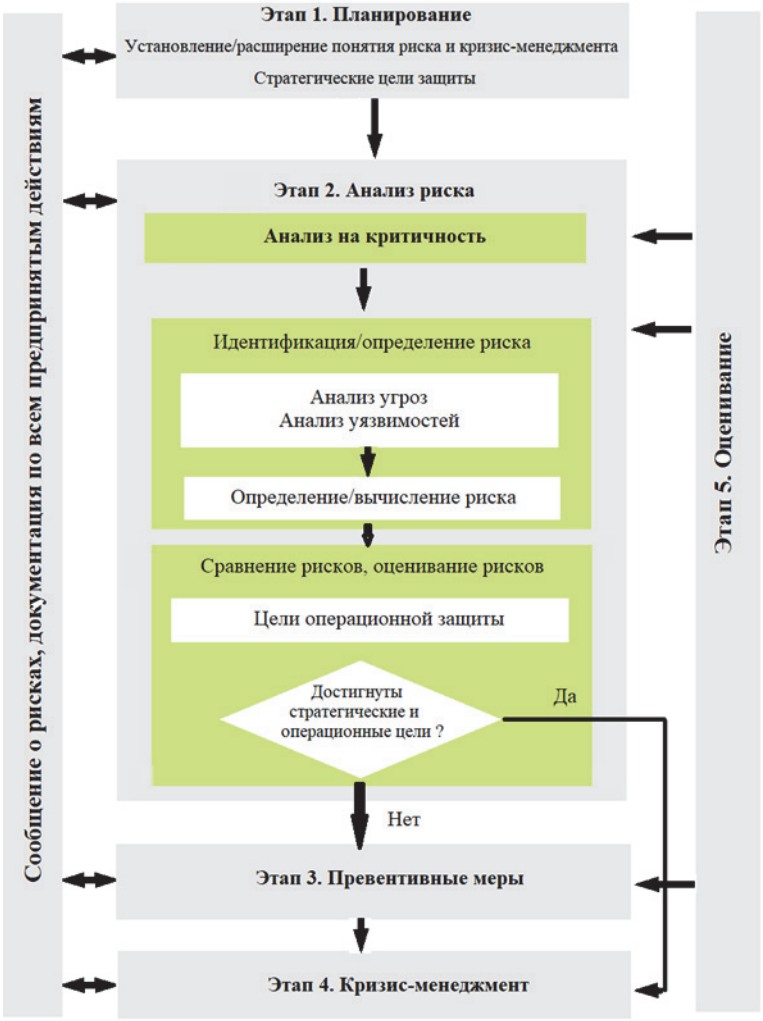

Рис. 3. Пять этапов управления рисками и кризисами

Этап 2: Анализ риска

Анализ риска объективирует информацию, собранную об угрозах и рисках в структурах сообщества. Анализируя возможный риск, исследуются различные процессы и их компоненты, и сравниваются имеющиеся различия рисков для организаций. Такого рода сравнения позволяют определить срочность и приоритетность мер, принимаемых при имеющемся риске, оказывая этим на них значительное влияние. Это создает основу для эффективного управления ограниченными финансовыми и кадровыми ресурсами.

Этап 3: Превентивные меры и стратегия

Превентивные меры помогают снизить риски для критических процессов. Они помогают достичь целей по их оперативной защите и тем самым повысить порог критичности по потенциальным кризисам, возможным в организациях. Это может уменьшить количество и/или интенсивность кризисных инцидентов.

Профилактические меры должны подвергаться анализу по направленным на них затратам и полученным результатам, с целью снижения общего риска.

Однако меры по снижению рисков, вероятность которых достаточна низка, но будут иметь драматические последствия, если они произойдут, часто невозможно оправдать, только на основе анализа по затратам и их результатом. В таких случаях нужно учитывать социальные и этические аспекты, а также правовые рамки при принятии решения о защитных мерах.

В превентивных стратегиях используются такие инструменты, как предотвращения рисков (*чтобы избежать риска*), смещения рисков и принятия риска (*если невозможно помочь уменьшить реальный риск*).

Этап 4: Кризис-менеджмент

Кризис определяется как отклонение от нормальной ситуации, с которой невозможно справиться с использованием обычных рабочих процедур. В Российской Федерации дается следующее определение: «***чрезвычайная ситуация*** *– обстановка на определенной территории, сложившаяся в результате аварии, опасного природного явления, катастрофы, стихийного или иного бедствия, которые могут повлечь или повлекли за собой человеческие жертвы, ущерб здоровью людей или окружающей природной среде, значительные материальные потери и нарушение условий жизнедеятельности людей*»[1].

Кризисы в критически важных инфраструктурных организациях могут иметь серьезные последствия для функционирования предприятий и государственных органов и, таким образом, наносить ущерб общественности или нарушать политическую, социальную или экономическую систему. Кризис следует четко отличать от менее серьезных инцидентов.

[1] Закон «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» (с изменениями на 15 февраля 2016 года) Ст. 1.

Управление кризисом (*кризис-менеджмент*) играет важную роль в защите организаций и, следовательно, критических инфраструктур и общественности.

Управление кризисом нельзя отделить от управления рисками. Концептуальная, организационная, процедурная и простая физическая подготовка к кризисам частично основана на результатах управления рисками. Поскольку меры по снижению риска не могут уменьшить все риски, и определенный риск всегда остается, кризис-менеджмент больше связан с кризисами, которые не могут быть предотвращены.

Цели кризисного управления для критически важных инфраструктурных организаций в случае наступившего кризиса:

- поддержание максимально возможной способности функционировать, и / или
- как можно быстрое восстановление критически важных функций.

Управление кризисом можно понимать как цикл *PDCA* в управлении рисками.

Важнейшими задачами кризис-менеджмента являются:

- создание концептуальных, организационных и процедурных условий, необходимых для максимально эффективного реагирования на экстремальный инцидент, и
- создание специальных структур для реагирования в случае кризиса, в частности, создание целевой группы по кризису.

Этап 5: Оценка управления рисками и кризисом

Оценка охватывает все этапы управления рисками и кризисом, определенные при предварительном планировании, для проверки того, эффективна ли система управления кризисом.

Управление рисками и кризисом может обеспечить долгосрочную «*добавленную стоимость»* только в том случае, если все этапы регулярно проверяются, тем самым закладывая основу для непрерывной оптимизации уровня безопасности организации.

Успех вышепредставленного ***интегрированного подхода*** зависит от использования всего спектра возможностей, компетентности и опыта в

рамках сообщества инфраструктуры и связанных с ним заинтересованных сторон.

3. Видение, миссия, цели и задачи по созданию и поддержанию безопасности и устойчивости критической инфраструктуры

Анализ действующего нормативного законодательства Республики Армения, изучение деятельности отдельных исполнительных органов власти, в частности, Министерства чрезвычайных событий позволяет утверждать, что критическая инфраструктура Армении – эта та среда, где отсутствует ее нормативное определение. Что касается связанной с защитой граждан деятельности по аварийному спасению, пожаротушению и координации первостепенной, срочной, аварийно-восстановительной деятельности при чрезвычайных ситуациях, то эти функции министерства регулируются рядом законодательных актов и нормативными решениями, направленными на снижение рисков бедствий.

С сожалением необходимо отметить, что и правительственная программа Армении на 2017-2022гг. имеет те же недостатки. Согласно пункту 1.5, «чрезвычайная ситуация и снижение опасности бедствий», осуществляемая правительством Армении в области чрезвычайной защиты, будет направлена на природные и антропогенные катастрофы по:

- снижению риска;
- предотвращению и устранению возможных последствий;

являясь составным элементом обеспечения безопасности государства, что будет способствовать ее устойчивому развитию».

Необходимо, чтобы руководство страны осознало и реализовало программу по выработке политики в области обеспечения безопасности и устойчивости к угрозам критических инфраструктур – ***Национальную программу защиты инфраструктур***.

Для достижения этих целей необходимо выработать видение, миссию, цели и задачи по созданию и поддержанию безопасности и устойчивости критической инфраструктуры (*носит сугубо обзорный характер*).

✓ Стратегическое направление усилий по созданию и поддержанию критической безопасности и устойчивости инфраструктуры зависит от общего ***видения:***

критическая инфраструктура защищена и устойчива, уровень уязвимостей очень низок, минимизированы возможные последствия по выявленным и разрушительным угрозам, эффективно и оперативно происходит реагирование на риски и угрозы и восстановление по их результатам.

✓ *Задачи/миссии*

Укрепление безопасности и устойчивости критической инфраструктуры через управления рисками, которые реализуются сообществом критической инфраструктуры совместными и комплексными действиями.

От видения и миссии зависят достижения целей (*далее выборочно приводятся*), которые представляют собой стратегическое направление, на котором необходимо сосредоточить всю важнейшую деятельность в области обеспечения безопасности и устойчивости критических инфраструктур.

✓ *Цели*:

- Оценить и проанализировать угрозы, уязвимости и последствия для критической инфраструктуры, которая, в свою очередь, необходима для оценки деятельности по управлению рисками.
- Защитить критическую инфраструктуру от антропогенных, стихийных и киберугроз, прилагая для этого усилия по снижению риска, с учетом затрат и выгод от инвестиций в обеспечение безопасности.
- Повысить критическую устойчивость инфраструктуры путем сведения к минимуму неблагоприятные последствия от инцидентов за счет превентивных усилий по планированию и смягчению их последствий.

✓ *Ключевые приоритетные задачи:*

- Укреплять партнерские отношения.
- Вводить инновации в управлении рисками.
- Сосредоточиться на результатах.

Ключевые принципы:

Установить основные принципы, представляющие ценность и предположения, которые сообщество критических инфраструктур должно учитывать при планировании работы с критически важной инфраструктуры по обеспечении ее устойчивости.

Выводы

Снижение уязвимостей критических инфраструктур и повышение их безопасности и устойчивости являются одной из основных целей страны. Это обеспечит адекватный уровень их защиты и, насколько возможно, позволит существенно ограничить рамки последствий от сбоев на жизнедеятельность общества и его граждан.

Например, большинство, из 35 стран-членов Организации Экономического Сотрудничества и Развития приняли во внимание наблюдаемые трансформации с рисками и «*ландшафтом*» кризисов и в последнее десятилетие направили свои усилия на реформирование системы управления кризисом, чтобы адаптироваться к ее новому контексту. Однако кризисы продолжают развиваться, бросая вызов даже самым новейшим и надежным системам. Идет процесс изменения типов, видов кризисов, с которым сегодня сталкиваются правительства.

Все вышесказанное выдвигает вопрос: как правительства адаптируют к новым угрозам свои подходы, возможности и инструменты в различных областях кризисного управления и как достигают большей гибкости, сохраняя наилучший опыт борьбы с кризисами и остающимися рисками?

Национальные усилия по укреплению критической безопасности и устойчивости инфраструктуры зависят от способности сообщества критически важных инфраструктур принимать обоснованные, с учетом риска, решения при распределении ограниченных ресурсов как для каждодневных, так и для кризисных операций. Поэтому управление рисками, которое должно стать краеугольным камнем Национальной программы защиты инфраструктур, актуально как на государственном, так и на местном уровнях. Безопасность и устойчивость на двух уровнях зависит от создания и поддержания надежных партнерских отношений между бизнес-сообществом и государственными, местными органами власти, общественными организациями. Необходимость координации также поднимает серьезные проблемы государственного управления.

Совершенствование понимания рисков нанесения ущерба или катастрофических последствий критическим инфраструктурам является важным шагом на пути к уменьшению опасности их возникновения, а также

основой планирования в деле обеспечения готовности к чрезвычайным ситуациям, адекватного реагирования на них и их преодоления.

Март, 2018г.

ԿՐԻՏԻԿԱԿԱՆ ԵՆԹԱԿԱՌՈՒՑՎԱԾՔՆԵՐ. ՌԻՍԿԵՐԻ ԿԱՌԱՎԱՐՈՒՄ ԵՎ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԱՊԱՀՈՎՄԱՆ ԽՆԴԻՐՆԵՐ

Աշոտ Թևիկյան

Ամփոփագիր

Հոդվածում քննարկվում են Հայաստանը և մեր դաշնակիցներին վտանգող հնարավոր սպառնալիքները, որոնք ներկայում ունեն թիրախային գործողությունների լայն շրջանակ՝ ուղղված կրիտիկական կարևոր տնտեսական ակտիվների և ինստիտուցիոնալ համակարգերի (*ենթակառուցվածքների*) խափանմանը, պետության անվտանգության ապահովման հնարավորությունների վնասմանը: Առաջարկվում է մշակել ռազմավարություն, որը հնարավորություն կտա դիմակայել նման սպառնալիքներին:

КРИТИЧЕСКИ ИНФРАСТРУКТУРЫ: УПРАВЛЕНИЕ РИСКАМИ И ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Ашот Тевикян

Резюме

В статье обсуждаются возможные угрозы для Армении и наших союзников, которые стоят сейчас перед широким диапазоном враждебных актов, направленных на подрыв критически важных экономических активов и институциональных систем (*инфраструктур*), с необходимостью причинить вред возможностям по обеспечению безопасности государства. Предлагаются направления работ по разработке стратегии и вытекающих отсюда возможностей, которые необходимы для противостояния таким угрозам.

CRITICAL INFRASTRUCTURES: RISK MANAGEMENT AND SECURITY PROBLEMS

Ashot Tevikyan

Resume

The article discusses possible threats to Armenia and its allies, which are now facing a wide range of hostile acts aimed at undermining critical economic assets and institutional systems (infrastructures), with the objective to harm opportunities of ensuring the security of the state. Areas of work are proposed to develop and create a strategy and resulting opportunities that are necessary to encounter such threats.