Предисловие

Представляемая монография посвящена изучению закономерностей развития нормативно-технического регулирования в области обеспечения безопасности использования и устойчивости функционирования критической информационной инфраструктуры общества, составляющей основу среды информационно-коммуникационных технологий (ИКТ-среда).

Актуальность данной работы во многом обусловлена особенностями современного этапа развития общества, которое на пути «цифровой трансформации» столкнулось не просто с угрозами информационной безопасности человека, общества и государства, но и с серьезным вызовом самим основам его существования.

С одной стороны, критическая информационная инфраструктура теперь включает информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергетики, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности. Критическая информационная инфраструктура де-факто стала необходимым условием жизнедеятельности всех субъектов общественной жизни.

Уровень развития критической информационной инфраструктуры и используемых в ней ИКТ начал оказывать определяющее влияние на реализацию конституционных прав и свобод человека и гражданина, на экономическую и социальную конкурентоспособность общества, на политическую культуру, на обороноспособность страны и безопасность государства.

С другой стороны, серьезным препятствием для дальнейшего расширения использования ИКТ и критической информационной инфраструктуры в интересах общественного развития становится их уязвимость по отношению к злонамеренному внедрению вредоносного программного обеспечения и данных, нарушающих устойчивое функционирование вычислительных и коммуникационных устройств, сетей связи.

Серьезность вызова, с которым столкнулось общество в области безопасности использования ИКТ и устойчивости функционирования критической информационной инфраструктуры, подтверждается продолжающимся, несмотря на принимаемые меры как у нас в стране, так и за рубежом, ростом количества и увеличением опасности компьютерных преступлений. Усилия международного сообщества на переговорной площадке в ООН, на площадках региональных международных организациях, направленные на применение международного права к отношениям в ИКТ-среде не приводят к снижению напряженности в отношениях между государствами, возникающих в связи с необоснованными обвинениями в провоцировании инцидентов в ИКТ-среде.

Фактически сложилась ситуация, в которой апробированные правовые и иные средства противодействия угрозам международной безопасности не демонстрируют прежнюю эффективность.

Представляется, что в определенной мере сложившаяся ситуация обусловлена новизной, необычностью ИКТ-среды как пространства национального регулирования и межгосударственного сотрудничества в области международной безопасности.

В этих условиях одним из перспективных направлений развития как системы национального, так и международного нормативного регулирования становится взаимодействие правовых механизмов воздействия на социальные отношения с механизмами воздействия на субъектов, непосредственно связанных с развитием ИКТ, информационной инфраструктуры посредством нормативного технического регулирования.

С этой точки зрения трудно переоценить своевременность представляемой работы.

Монография включает три главы.

В первой главе исследуются существующие постановки проблемы обеспечения безопасности использования критической информационной инфраструктуры как объекта нормативного технического регулирования.

Отмечается, что безопасность жизнедеятельности общества в областях, базирующихся на использовании критических информационных инфраструктур, в настоящее время обеспечивается посредством создания и применения высокоэффективных программно-технических средств, криптостойких алгоритмов и интеллектуально насыщенных эвристических методов в области разработки и поддержания правил, условий и ограничений.

Управляющее воздействие технической нормы направлено на создание условий для применения перечисленных средств для сни-

жения стоимости рисков нарушения безопасности — интенсивности возникновения инцидентов и опасности негативных последствий.

Во второй главе исследуются механизмы нормативного технического регулирования, нацеленные на обеспечение безопасности критической информационной инфраструктуры посредством применения средств активного мониторинга, реализующих прогностическую и адаптивную функции, а также рассматриваются подходы к оценке эффективности отдельных элементов этих механизмов.

В третьей главе рассмотрены возможности применения в механизмах технического регулирования средств искусственного интеллекта и машинного обучения для обеспечения безопасности критических информационных инфраструктур.

Прошло 30 лет с тех пор, как в Законе Российской Федерации «О безопасности» (№ 2446-1 от 5 марта 1992 г., ст. 13) среди факторов, определяющих безопасность страны, появилась информационная составляющая.

С тех пор термин «информационная безопасность» прочно вошел в лексикон политического руководства Российской Федерации, во внешнюю и внутреннюю политику. Представление об обеспечении информационной безопасности страны непрерывно трансформируется в соответствии с расширением областей применения информационно-коммуникационных технологий в жизни человека, общества и государства, развитием информационной инфраструктуры, а также с появлением новых угроз национальным интересам в информационной сфере. При этом обеспечение безопасности использования ИКТ и информационной инфраструктуры остается важным направлением государственной политики Российской Федерации.

Предлагаемая монография вносит заметный вклад в формирование научной теории нормативного регулирования социальных отношений в ИКТ-среде в целях достойного ответа на вызов информационной безопасности Российской Федерации, повышения эффективности реализации государственной политики в этой области.

Член Президиума Национальной Ассоциации
международной информационной безопасности,
заведующий отделом Центра проблем информационной
безопасности факультета вычислительной математики
и кибернетики МГУ имени М.В. Ломоносова,
Заслуженный деятель науки Российской Федерации,
доктор тех. наук, доктор юрид. наук, профессор
А.А. Стрельцов

Введение

Различные страны сталкиваются с растущим числом кризисов, которые могут распространяться за пределы национальных границ и оказывать значительные негативные последствия на протекающие социально-экономические процессы и институты государств. Зреет понимание, что дальнейшие системные потрясения могут сильно затруднить возможности развития экономик стран, социальную сплоченность и политическую стабильность их обществ. На фоне тревожного роста интенсивности атак на экономические, административные и финансовые институты по всему миру это актуализирует проведение направленных исследований вопросов безопасности стратегически важных объектов. Понятие, которое применяется для совокупности таких объектов, — это «инфраструктура», т. е. в самом общем смысле слова совокупность взаимосвязанных структурных элементов, поддерживающих целостность всей структуры (обычно термин применяется только для искусственно созданных (физических) структур).

Национальное благосостояние опирается на безопасную и устойчивую критическую инфраструктуру — те активы и системы, которые лежат в основе любого общества, в том числе российского. Эта инфраструктура необходима для поддержания жизненно важных общественных функций. Кроме того, благосостояние и развитие современного общества зависит от уровня предоставления широкого спектра продуктов, услуг и функций. Разнообразие угроз, расширяющееся в связи с ростом этого уровня, представляет большую и реальную опасность для критических инфраструктур. Поэтому защита жизненно важных общественных структур и институтов является ключевой обязанностью страны в контексте обеспечения государственной безопасности.

При классификации инфраструктур их принято разделять на два типа: «жесткая инфраструктура» — это физические системы, необходимые для функционирования современно развитой нации (крупные технологические производства, сети общественного транспорта, аэропорты, средства поставки и источники воды, обращение с опасными отходами, производство и передачу электроэнергии, телекоммуникации и т. п.) и «мягкая инфраструктура» — это институты, необходимые для поддержания социально-экономической струк-

туры, такие как финансовая система, системы образования, здравоохранения, государственного управления и правоохранительных органов и служб экстренной помощи.

Это разделение представляет собой одно из свидетельств того, что наряду с известными и отработанными направлениями вмешательства во внутриполитическую жизнь страны и подрыва её информационного суверенитета сегодня запущены новые программы, связанные с жестким финансово-экономическим и политическим противоборством, направленным на дезорганизацию деятельности объектов и структур жизнедеятельности государства, которые следует отнести к критическим инфраструктурам.

Понимание ключевых определений контента критической инфраструктуры является основой реалистического восприятия определяющей ее среды и формирует необходимый общественный подход по обеспечению ее безопасности и устойчивости. В определениях большинства стран слово «критическая» относится к той части инфраструктуры, которая оказывает определяющую поддержку экономическому и социальному благополучию и общественной безопасности.

Под критичностью может подразумеваться серьезное воздействие на здоровье, безопасность или экономическое благополучие людей, термин может ссылаться на значительные нарушения общественного порядка или другие драматические последствия. Критическая инфраструктура может относиться к инфраструктуре, разрушение которой вызывает серьезные социальные беспорядки, огромные потери жизней и колоссальный экономический ущерб. Таким образом, слово «критическая» относят к инфраструктуре, разрушение которой приведет к катастрофическим негативным последствиям для людей, общества и государства.

Многие национальные источники к критическим инфраструктурам относят в первую очередь традиционные, физические инфраструктуры, а также включают в это понятие нематериальные активы и/или коммуникационные сети. Например, некоторые страны относят критическую инфраструктуру к физическим объектам, цепочкам поставок, информационным технологиям и сетям связи* или еще шире — к физическим и информационным технологиям**.

---

* Trusted Information Sharing Network for critical infrastructure resilience. — http://www.tisn.gov.au/Pages/default.aspx

** Critical Infrastructures. Federal Office for Information Security, Federal Office of Civil Protection and Disaster Assistance. — http://www.kritis.bund.de/SubSites/Kritis/EN/introduction/introduction_node.html

Одно из наиболее распространенных определений критической инфраструктуры — системы и активы, будь то физические или виртуальные, настолько жизненно важные, что их неработоспособность или разрушение окажет негативное влияние на безопасность, национальную экономическую безопасность, национальное здравоохранение или любую их комбинацию*. Иногда к активам и системам добавляют услуги**, что является достаточно широким понятием. В «Стратегии национальной безопасности Российской Федерации» термин «инфраструктура» встречается неоднократно и в разнообразном контексте: военная, транспортная, информационная, жилищно-коммунальная инфраструктуры, инфраструктуры внутреннего рынка, социальная и образовательная.

Безопасность критически важной инфраструктуры принято определять как состояние защищенности (или снижение риска через применения физических средств***), обеспечивающее ее устойчивое функционирование при проведении в отношении нее целенаправленных вредоносных действий (взломов, атак). Для эффективного функционирования системы обеспечения безопасности критических инфраструктур необходим непрерывный контроль рисков нарушения их функционирования с постоянной и достоверной оценкой возможностей противодействия соответствующим угрозам. Это позволяет своевременно предупреждать угрозы и устранять уязвимости, способствует обмену точной, своевременной и действенной информацией для проведения анализа текущих и будущих рисков.

В ряде источников используется еще термин «устойчивость», который определяется как способность подготовиться и адаптироваться к изменяющимся условиям, а также оперативно противостоять и быстро восстанавливаться после преднамеренных атак и/или противостоять угрозам или инцидентам. Говоря об устойчивости инфраструктурных активов, систем и сетей, 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

---

* Critical Infrastructure Sectors. U.S. Department of Homeland Security. — https://www.dhs.gov/criticalinfrastructure-sectors

** The national infrastructure. Centre for the Protection of National Infrastructure. — http://www.cpni.gov.uk/about/cni/

*** Critical Infrastructure Protection Market Expected to Reach 144.82 Billion USD by 2021. Market Watch, 13 June 2016. — http://www.marketwatch.com/story/critical-infrastructure-protection-market-expectedto-reach?14482?billion-usd-by?2021-2016-06-13-92033051

их последствий, реагирование на угрозы и, соответственно, способность на восстановление важны для укрепления устойчивости критических инфраструктур.

Под защитой критической инфраструктуры понимаются меры по обеспечению безопасности взаимозависимых систем, сетей и активов, лежащих в основе служб, жизненно необходимых для функционирования общества. Большинство критических инфраструктур невозможно без инфраструктуры информационной, т. е. без компьютеров и сетей, представленных в первую очередь системами диспетчерского управления и сбора данных (SCADA), взаимосвязанность которых позволяет им обмениваться информацией и выполнять анализ по всем критически важным функциям. К этим инфраструктурам относятся банковская сфера, производство и распределение электроэнергии, медицинские услуги, государственные аварийно-спасательные службы, а также воздушные и наземные перевозки и много другое.

Важной особенностью обеспечения безопасности критических инфраструктур является то, что каждый проект такого рода уникален — так же, как и каждая промышленная инфраструктура, защиту которой невозможно ограничить установкой только стандартизированных решений. Подбор оптимальной конфигурации защитных технологий и набора сервисов осуществляется в процессе функционирования текущей системы безопасности критической инфраструктуры.

Уничтожение или выведение из строя критических инфраструктур может нанести большой ущерб населению, компаниям и административным органам. Но ни один человек, ни один продукт и ни одна организация не способны бороться с киберпреступностью в одиночку. Особенно это касается объектов критической инфраструктуры, которые изо дня в день подвергаются атакам со стороны противоборствующих государств и международных преступных группировок. Заинтересованность в обеспечении безопасности критической инфраструктуры ощущается на национальном и международном уровне. Однако в настоящее время одни лишь распоряжения и предписания, видимо, не смогут исчерпывающе способствовать полному решению задач защиты критической инфраструктуры, потому что, если попытаться с помощью нормативных актов установить необходимость обеспечивать защиту от угроз сегодняшнего дня, то они могут оказаться не готовыми к защите от вновь возникающих угроз. Кроме того, если предписания будут касаться технических вопросов, то это, скорее всего, приведет к формальному обеспечению соответствия этим предписаниям в ущерб гибко-

сти управления подлинной безопасности. Тем более, что в обеспечении безопасности критических инфраструктур действует вполне определенное соотношение критериев, при котором основной задачей является поддержание непрерывности критических процессов и оперативное устранение любых сбоев.

Новые проблемы проявились с развитием информационных технологий, которые пронизывают все сферы жизни и в первую очередь деятельность экономически активного населения. Среди критических объектов и их организационно-технологических компонентов особую (а в ряде случаев — доминирующую) роль с точки зрения безопасности несомненно играют критические информационные инфраструктуры (КИИ), представляющие собой информационные системы, телекоммуникационные сети и автоматизированные системы управления, входящие в состав объектов, функционирующих в критически важных индустриях*. Прежде всего это вызвано тем, что современные технологии практически во всех областях человеческой деятельности немыслимы без развитой информационной поддержки и многочисленных автоматизированных контуров информационного обеспечения, управления и контроля, и дефекты функционирования этих связей делают невозможной нормальную деятельность критических инфраструктур. Более того, существуют критические инфраструктуры, работа которых практически исчерпывается информационными процессами и услугами (например, системы сотовой связи).

С другой стороны, именно информационная сфера более других подвержена всевозможным вредоносным воздействиям (кибератакам). Спектр источников такого воздействия весьма широк — это могут быть как отдельные лица, преследующие мошеннические или террористические цели, так и структуры, выполняющие задачи нанесения информационного ущерба в рамках процессов более высокого уровня, вплоть до государственного противостояния. Интенсивность кибератак неуклонно растет, поэтому решение вопросов информационной безопасности КИИ и повышение эффективности защитных мер представляются актуальными. В настоящей работе обсуждаются вопросы управления информационной безопасностью КИИ.

В первой главе обсуждается методологическая парадигма управления безопасностью КИИ, учитывающая особенности и факторы, формирующие это понятие, предлагается подход асимптоти-

* Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ.

ческого управления, направленного на неуклонное повышение уровня защищенности, показывается соответствие такого подхода современной практике управления безопасностью критических информационных инфраструктур.

Безопасность в индустриях, изобилующих критическими информационными инфраструктурами, является доминирующим фактором, и сегодня основная проблематика обеспечения безопасности неуклонно перемещается из области создания высокоэффективных программно-технических средств, криптостойких алгоритмов и интеллектуально насыщенных эвристических методов в область разработки и поддержания правил, условий и ограничений, т. е. в область управления безопасностью.

Управление рассматривается как целенаправленное формирование решений и реализующее эти решения воздействие субъекта на управляемый объект. Применение столь широкого определения для конкретного случая (информационной безопасности) требует раскрытия используемых понятий (субъекта управления, управляемого объекта и его состояния, цели в виде целевого состояние объекта и способов формирования и реализации решений).

Целью управления информационной безопасностью является защищенность, которая в традиционном понимании возникает и существует как приемлемая реакция на возможное вредоносное воздействие, нарушающее нормальное функционирование защищаемого объекта. В любом случае управление безопасностью имеет в качестве цели некоторое состояние свойств, факторов и характеристик (критериев) безопасности объекта, которое полагается удовлетворительным (целевым и безопасным). Неотъемлемой особенностью традиционных моделей управления безопасности является их рекурсивность — в составе модели управления всегда есть способ, позволяющий отличить целевое (безопасное) состояние объекта от всех остальных состояний.

Объектами управления являются активности и контроли. Активности реализуют ограничения, накладываемые на отношения субъектов и объектов информационной деятельности. Контроли поддерживают наблюдение за объектом для оценки и прогнозирования защищенности объекта (пребывания в целевом состоянии). Руководствуясь предположениями о формах и интенсивностях агрессивности среды и дефектах защищенности объекта, конфигурируется арсенал активностей так, чтобы обеспечить достижение целевого состояния. Контроли служат для удержания объекта в целевом состоянии при изменении предположений об угрозах и уязвимостях.

В случае информационной безопасности представление о целевом состоянии объекта может как устанавливаться в явном (эксплицитном) статическом виде, так и определяться в процессе управления (имплицитный вид). В соответствии с этим определяется характер управляющего воздействия.

Эксплицитная форма содержит заранее сформулированные в явном виде условия (требования), выполнение которых соответствует достижению объектом управления целевого состояния. Цели формируются за пределами управляемого объекта (нормативы и руководства регулятора, ведомственные установки, общеметодические решения и т. п.). Это внешние аксиоматические положения, и формально предполагается, что они полностью описывают целевое состояние объекта управления (декларативная методология), управляющее воздействие состоит в реализации и удержании этих положений.

Имплицитная форма нашла свое наиболее развитое воплощение в риск-ориентированном подходе, предполагающем идентификацию, спецификацию и метризацию возможностей возникновения инцидентов. Управляющее воздействие состоит в том, чтобы реализовать меры, снижающие факторы стоимости рисков: интенсивность возникновения инцидентов и размер негативных последствий. Целевое состояние характеризуется величиной остаточного риска, означающего достижение некоторого уровня защищенности, а приемлемость этого уровня соответствует допустимому остаточному риску.

Еще одна распространенная методология управления безопасностью, изложенная в документах «Общих критериев» («исчисление доверия»), использует смешанную эксплицитно-имплицитную форму, реализуя управляющее воздействие в виде формирования на базе принятой аксиоматики (цели, угрозы, политики, предположения) заданных требований (функциональных и доверия), полному выполнению которых соответствует целевое состояние.

В этой главе также выявляются и рассматриваются особенности управления безопасностью КИИ, вводится понятие асимптотического управления. В качестве ключевой категории асимптотического управления предлагается обобщенное понятие события безопасности и его сигнатуры, а в качестве инструментария — модель механизма безопасности (активного мониторинга), реализующего прогностическую и адаптивную функции асимптотического управления, рассматриваются подходы для оценки эффективности элементов такой модели.