Роман В. Наталичев[1], Виктор С. Горбатов[2], Григорий П. Гавдан[3], Анатолий П. Дураковский[4]
Национальный исследовательский ядерный университет «МИФИ», Каширское ш., 31, Москва, 115409, Россия
[1]*e-mail*: *r.natalichev2015@yandex.ru, https://orcid.org/0000-0002-8985-7144*
[2]*e-mail: VSGorbatov@mephi.ru, https://orcid.org/0000-0001-9998-9733*
[3]*e-mail: GPGavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076*
[4]*e-mail: APDurakovskiy@mephi.ru, https://orcid.org/0000-0002-8311-7735*

ЭВОЛЮЦИЯ И ПАРАДОКСЫ НОРМАТИВНОЙ БАЗЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

DOI: http://dx.doi.org/10.26583/bit.2021.3.01

Аннотация. В настоящее время в России проводится активная работа по реализации относительно нового механизма государственного регулирования в области информационной безопасности, законодательно определяемого как обеспечение безопасности значимых объектов критической информационной инфраструктуры (КИИ). Субъектами данного законодательства выполнен достаточно большой объем организационных мероприятий, поддержанных научными исследованиями отечественных и зарубежных специалистов. Настоящая работа посвящена исследованию вопросов обеспечения безопасности значимых объектов КИИ на основе проведения критического системного анализа нормативной базы с указанием неоднозначности толкования и возможных вариантов практического выполнения требований применительно к конкретной сфере деятельности. Высокий уровень напряженности дискуссий по данному направлению на различных форумах показывает, что формирование новой системы на местах, на уровне отдельных субъектов, вызывает много сложностей и даже порой неприятие по некоторым аспектам нормативных требований. Как правило, это происходит всегда на начальных этапах становления любой новой системы в силу неоднозначности формулировок и наличия существенных внутренних противоречий в отдельных нормативных актах различных регуляторов. Одной из существенных проблем является определенное недопонимание на местах, особенно в реальном секторе экономики, необходимости введения и роли нового механизма обеспечения безопасности в общем комплексе мер обеспечения информационной безопасности, уже реализуемых в России более четверти века. Проведение системного анализа такой проблемной ситуации особенно актуален для образовательного сообщества, уже приступившего к реализации новых программ обучения различного уровня подготовки, переподготовки и повышения квалификации специалистов в области информационной безопасности. На основе описания эволюции отечественного законодательства в области информационной безопасности дано обоснование необходимости нового механизма государственного регулирования. Приводятся примеры неоднозначности и внутренних противоречий (парадоксов) некоторых положений нормативно-правовых актов по безопасности объектов КИИ, показывающие насущную необходимость их совершенствования и дополнительных усилий по толкованию основных положений, исходя из принципа креативного подхода по разъяснению сложных вопросов.

Ключевые слова: информационная безопасность, критическая информационная инфраструктура, значимый объект, значимые последствия, показатель значимости, нормативные правовые акты системный анализ, угрозы безопасности, подготовка специалистов.

Для цитирования: НАТАЛИЧЕВ, Роман В. и др. ЭВОЛЮЦИЯ И ПАРАДОКСЫ НОРМАТИВНОЙ БАЗЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ. Безопасность информационных технологий, [S.l.]. Т. 28, № 3, с. 6–27, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1359. DOI: http://dx.doi.org/10.26583/bit.2021.3.01.

Roman V. Natalichev[1], Viktor S. Gorbatov[2], Grigory P. Gavdan[3]
Anatoly P. Durakovskiy[4]
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe sh., 31, Moscow, 115409, Russia
[1]e-mail: r.natalichev2015@yandex.ru, https://orcid.org/0000-0002-8985-7144
[2]e-mail: VSGorbatov@mephi.ru, https://orcid.org/ /0000-0001-9998-9733
[3]e-mail: GPGavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076
[4]e-mail: APDurakovskiy@mephi.ru, https://orcid.org/0000-0002-8311-7735

Evolution and paradoxes of the regulatory framework for ensuring the security of critical information infrastructure facilities

DOI: http://dx.doi.org/10.26583/bit.2021.3.01

Abstract. Today in Russia the active work is going on the implementation of a relatively new mechanism of state regulation in the field of information security, which is legally defined as ensuring the security of significant objects of critical information infrastructure (CII). The subjects of this legislation have carried out a fairly large amount of organizational measures supported by scientific research of domestic and foreign specialists. The paper is devoted to the study of the issues of ensuring the safety of significant CII objects based on a critical system analysis of the regulatory framework and indicating the ambiguity of interpretation and possible options for the practical implementation of the requirements related to a specific field. The high level of tension of discussions in this area at various forums demonstrates that the formation of a new system at the level of individual subjects causes many difficulties and even sometimes leads to rejection of some aspects of regulatory requirements. As a rule, this always happens at the initial stages of the formation of any new system due to ambiguity of the wordings and the presence of significant internal contradictions in certain regulatory acts. One of the significant problems, in our opinion, is a certain misunderstanding, especially in the real sector of the economy, of the need to introduce and the role of a new security mechanism within the overall set of information security measures that have already been implemented in Russia for more than a quarter of a century. Conducting a system analysis of such a problematic situation is especially relevant for the educational community that has already started implementing new training programs of various levels of training, retraining and advanced training of specialists in the field of information security. Based on the description of the evolution of domestic legislation in the field of information security, for the need for a new mechanism of state regulation is justified. Examples of ambiguity and internal contradictions (paradoxes) of some provisions of regulatory legal acts on the safety of CII facilities are given, showing the urgent need for their improvement as well as for additional efforts to interpret the main provisions, based on the principle of a creative approach to explaining complex issues.

Keywords: information security, critical information infrastructure, significant object, significant consequences, significance indicator, regulatory legal acts, system analysis, threats to security, training of specialists.

For citation: NATALICHEV, Roman V. et al. Evolution and paradoxes of the regulatory framework for ensuring the security of critical information infrastructure facilities. IT Security (Russia), [S.l.], v. 28, n. 3, p. 6–27, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1359. DOI: http://dx.doi.org/10.26583/bit.2021.3.01.

Введение

Прошло уже несколько лет от вступления в действие относительно нового механизма государственного регулирования в области информационной безопасности, законодательно[1] определяемого как обеспечение безопасности объектов критической информационной инфраструктуры (КИИ). За это время данное направление нормативно

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

поддержано на законодательном уровне путем внесения поправок в Уголовный Кодекс[2] (УК РФ) и Кодекс об административных правонарушениях[3], соответствующими Федеральными законами[4,5], и имеет достаточно обширную нормативно-методическую базу основных регуляторов в области информационной безопасности – ФСТЭК России и ФСБ России[6].

В период подготовки настоящей статьи вышел в свет новый вариант Стратегии национальной безопасности[7], в которой в пункте 51 в качестве одной из существенных угроз безопасности указано стремление и отработка действий иностранных государств по выведению из строя объектов КИИ Российской Федерации. В пункте 57 (подпункт 3) дается директива по реализации противодействия такой угрозе в рамках государственной политики по обеспечению информационной безопасности России.

Государственными и бизнес-структурами, законодательно определенными как субъекты этого направления нормативного регулирования, проведен достаточно обширный перечень организационных и методико-просветительных мероприятий по его практической реализации. Среди них разработка и реализация новых образовательных программ подготовки, переподготовки и повышению квалификации работников соответствующих сил обеспечения [1, 2].

Активно проводятся научно-технические исследования по данной тематике как отечественных [3, 4], так и зарубежных специалистов, по разработке, в частности, комплексных инструментов определения важнейших услуг информационной инфраструктуры [5]; оценок каскадированного воздействия на системы КИИ [6]; методов выявления взаимозависимостей отказов инфраструктурных служб организаций [7]; комплексных подходов по оценке устойчивости критически важных элементов инфраструктуры [8].

В то же время формирование новой системы на местах, на уровне отдельных субъектов, вызывает много сложностей и даже порой неприятие по некоторым аспектам нормативных требований. Об этом свидетельствуют достаточно напряженные дискуссии в ходе профильных конференций, совещаний и семинаров[8]. Это происходит, как правило, всегда на начальных этапах становления любой новой системы в силу неоднозначности формулировок и наличия существенных внутренних противоречий в отдельных нормативных актах различных регуляторов. Но, в данном случае, одним из существенных,

[2]«Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ.

[3]«Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 № 195-ФЗ.

[4]Федеральный закон от 26.05.2021 № 141-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях».

[5]Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 194-ФЗ.

[6]Приказ ФСТЭК России № 235 от 21.12.2017 «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования», Приказ ФСТЭК России № 239 от 25.12.2017 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ», Приказ ФСБ России от 24.07.2018 № 366 «О Национальном координационном центре по компьютерным инцидентам», Приказ ФСБ России от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ РФ».

[7]Указ Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации».

[8]ТБ Форум, конференции: Защита информации в АСУ ТП. Безопасность критической информационной инфраструктуры (16.07.2020, 09.02.2021, 08.04.2021, 15.07.2021), Защита критической инфраструктуры в государственных и бизнес-структурах (29.10.2020). URL: https://www.tbforum.ru/program (дата обращения: 16.03.2021).

на наш взгляд, факторов является определенное недопонимание на местах, особенно в реальном секторе экономики, необходимости введения, а главное, роли нового механизма в общем комплексе уже существующих мер обеспечения информационной безопасности. Тем более, что нововведение принято в декларируемых условиях «регуляторной гильотины»[9] с целью развития бизнеса за счет повышения эффективности государственного управления.

На наш взгляд, многие субъекты реального сектора экономики, особенно крупные корпорации [9, 10], а также банковская система[10], объективно мотивированные необходимостью обеспечивать устойчивость своих бизнес-процессов, уже имеют необходимые силы обеспечения противодействия кибератакам. По данным исследователей [11] 95% отечественных компаний, подвергшихся атакам, построены с учетом прежних и действующих в настоящее время, нормативно-правовых требований и/или на основе гармонизированных с лучшими мировыми практиками стандартов открытых систем, использующих риск-ориентированные подходы по оценке их безопасности.

Очевидно, что для выполнение новых государственных требований необходимо выделение дополнительных ресурсов, как правило, в условиях их недостаточности. Поэтому очевидна и скептическая позиция субъектов реальных секторов экономики, которые в лучшем случае выполняют формальные организационные процедуры, а в худшем занимают выжидательную позицию, что само по себе можно расценивать как своеобразную угрозу национальной безопасности.

Ссылки на реальную возможность практической реализации угроз безопасности КИИ[11], а также, например, на результаты кибератаки по блокированию нефтяного трубопровода в США 6 мая 2021 г. с целью получения выкупа[12], явно не могут поколебать эту скептическую позицию, особенно субъектов, использующих в своей деятельности риск-ориентированные подходы.

Возникает необходимость проведения системного анализа указанной проблемной ситуации, что особенно актуально для образовательного сообщества. В целом образовательные учреждения не являются субъектами рассматриваемого законодательства, хотя по разъяснению регулятора в их число должны быть включены крупные вузы с большой научной составляющей своей деятельности [12]. Но, главное, как упомянуто выше, данное сообщество уже приступило к практической реализации новых образовательных программ. Поэтому в силу своего целевого предназначения и необходимости реализации креативного подхода по подготовке специалистов высокой квалификации оно не может занимать ни выжидательную, ни тем более формальную позицию. То есть при изучении нормативной базы как основы становления всей практической деятельности специалиста, необходимо, с одной стороны, доказательно обосновать объективную необходимость того или иного вида государственного регулирования. В то же время даже простое изложение основных положений действующих нормативных актов при нынешнем их объеме выходит за рамки нормативно заданных объемов учебного времени, включая самостоятельные

[9]Реформа контрольно-надзорной деятельности, нацеленная на повышение уровня безопасности и устранение избыточной административной нагрузки на субъекты предпринимательской деятельности. Определена Федеральным законом от 31.07.2020 № 247-ФЗ «Об обязательных требованиях в Российской Федерации». URL: http://www.consultant.ru/document/cons_doc_LAW_358670/ (дата обращения: 16.03.2021).

[10]«Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0-2014» (принят и введен в действие Распоряжением Банка России от 17.05.2014 № Р-399)

[11]Аналитики заявили о росте кибератак на критическую инфраструктуру на 150%. URL: https://www.rbc.ru/technology_and_media/12/07/2021/60eb7ca69a7947b2f91f6a8d?from=newsfeed (дата обращения: 16.03.2021).

[12]Байден заявил о предложении Путину защитить 16 секторов от кибератак. URL: https://www.rbc.ru/politics/16/06/2021/60ca35199a7947191c7a646d (дата обращения: 16.03.2021).

занятия. Необходим критический системный анализ нормативной базы с указанием возможности неоднозначного толкования, наличия внутренних противоречий и вариантов практического выполнения применительно к конкретной сфере деятельности.

Исследованию этих вопросов для сферы обеспечения безопасности КИИ и посвящена настоящая работа, ориентированная, прежде всего, на образовательное сообщество по обучению специалистов в области информационной безопасности, но может быть полезной и для специалистов реального сектора экономики при принятии соответствующих управленческих решений.

Первый вопрос, а именно обоснование объективной необходимости новых подходов государственного регулирования, рассмотрен в сжатом историческом обзоре развития нормативно-правовой базы со ссылками на научные публикации по комплексу обеспечения информационной безопасности. Данный обзор не претендует на полноту исследования и изложения всех возможных нюансов, но, на наш взгляд, достаточно доказательно, без ссылок на директивные акты, показывает актуальность рассматриваемых вопросов и их роль в общем комплексе обеспечения информационной безопасности.

В качестве примеров неоднозначности и внутренних противоречий (парадоксов) проводится критический анализ некоторых положений нормативно-правовых актов по безопасности объектов КИИ, показывающий насущную необходимость их совершенствования и дополнительных усилий по толкованию основных положений, исходя из принципа креативного подхода по разъяснению сложных вопросов: «не как и что надо делать, а почему это надо».

1. Эволюция законодательной базы КИИ

1.1. Традиционные элементы правовой базы информационной безопасности

Условной точкой отсчета начала формирования российской нормативно-правовой базы в области информационной безопасности, не считая традиционной, очень устойчивой части по защите государственной тайны, можно считать 1995 г., с момента принятия, так называемого в кругах узких специалистов, «трехглавого» федерального закона[13].

Системный анализ его основных положений позволяет выделить несколько ключевых элементов, в той или иной степени послуживших импульсом к дальнейшему формированию действующей нормативной базы на уровнях иных правовых актов и нормативно-методических документов уполномоченных федеральных органов государственной исполнительной власти, для краткости далее называемых регуляторами. Как будет показано ниже, этот процесс формирования активно продолжается и в настоящее время с учетом новых достижений *социально-технологической революции* [13].

Первый и основной момент анализируемого закона – разделение общей государственной системы защиты информации с ограниченным доступом на две подсистемы, во многом похожих по методологическим подходам их организации, но законодательно разделенными по совокупности отдельных нормативных требований. Наряду с государственной тайной, выделенной в отдельный объект правового регулирования, введен правовой режим защиты, так называемой, конфиденциальной информации, в частности, многочисленных профессиональных тайн [14]. Это заложило основу формирования устойчивого отечественного рынка технических средств и оказания услуг в области информационной безопасности, регулируемого достаточно прозрачной и/или непротиворечивой нормативной базой.

[13]Федеральный закон от 20 февраля 1995 года № 24-ФЗ «Об информации, информатизации и защите информации».

Второй элемент – выделение в особую категорию конфиденциальной, то есть требующей защиты, информации так называемых персональных данных. Период становления этого направления государственного регулирования в силу чрезвычайной сложности проблемы растянулся до условного срока завершения в 2011 г. после принятия основополагающих поправок в специальное законодательство[14]. В настоящее время это направление фактически стало самостоятельным, так как получило новый законодательный импульс[15] для дальнейшего развития в части определения механизмов государственного регулирования процессов распространения так называемых общедоступных персональных данных.

Таким образом, эти первые два элемента, претерпевая за прошедшее время значительные изменения, как на законодательном, так и на нормативном уровнях, заложили правовую основу обоснования актуальности государственных требований для такого наиболее традиционного показателя безопасности информации (по общепринятой методологии информационной безопасности) как *конфиденциальность*. Справедливости ради отметим, что в настоящих реалиях это утверждение для персональных данных не совсем верно, о чем и свидетельствует упомянутая выше тенденция развития этого законодательства, но это предмет отдельного обсуждения.

Третий элемент – законодательная «путевка в жизнь» для электронного документооборота на основе электронно-цифровой подписи (ЭЦП), уже активно используемой в реальном секторе экономики, в частности, в платежных банковских системах. Актуальность этого направления нормативного регулирования и в настоящее время определяется необходимостью выполнения такого показателя безопасности передаваемых сведений как *целостность* и ее производных: достоверности, доверия, юридической значимости. Так как все технологии электронной подписи требуют выполнения условий конфиденциальности и «привязаны» к определенному физическому лицу, то можно утверждать о взаимосвязи и, соответственно, системности всех трех рассмотренных элементов. Становление нормативно-правовой базы регулирования электронного документооборота также заняло немалый период времени и условно завершилось в 2011 г. с выходом специального закона[16]. Стоит отметить, что в обозримом будущем и этот элемент будет существенно трансформирован в аспекте государственного регулирования в связи с бурным внедрением в финансовую сферу[17], а также сферу государственного управления и в реальный сектор экономики, систем обеспечения бизнес-процессов на основе технологии блокчейн [15, 16].

Вывод. Очевидно, что все рассмотренные выше элементы, даже с терминологической точки зрения, не могут быть положены в основу анонсированного выше обоснования для выделения рассматриваемой проблемы безопасности КИИ. Они либо достаточно устойчивы на текущий момент, либо тенденции их дальнейшего существенного развития определяются необходимостью их совершенствования с учетом новых современных вызовов в деле обеспечения информационной безопасности. Но, без

[14]Федеральный закон «О внесении изменений в Федеральный закон "О персональных данных» от 25 июля 2011 г. № 261-ФЗ.

[15]Федеральный закон «О внесении изменений в Федеральный закон «О персональных данных» от 30.12.2020 № 519-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_372682/ (дата обращения: 16.03.2021).

[16]Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения: 16.03.2021).

[17]Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31.07.2020 № 259-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_358753/ (дата обращения: 16.03.2021).

понимания этой структуры сложно определить роль и место нового механизма госрегулирования в общем комплексе обеспечения информационной безопасности.

1.2. Предыстория законодательного регулирования безопасности КИИ

Анализ публикаций периода подготовки «трехглавого закона» показывает, что уже тогда у специалистов по защите информации было понимание того, что указанных выше устойчивых до настоящего времени основных элементов недостаточно для полноты общей системы (комплекса) информационной безопасности. Так, например, банковская сфера, как и другие сектора реальной экономики, мотивированные на обеспечение непрерывности и устойчивости своего бизнеса, развивали свои системы безопасности на основе риск-ориентированных подходов, не предполагающих существенного государственного регулирования, но и, не выходя за его рамки. Но, к сожалению, в литературе применительно к теме нашего исследования можно указать лишь одну монографию [17] с научным обоснованием этого вопроса и оставшейся незамеченной профильными специалистами, возможно из-за ее названия, терминологически не связанного с проблемой защиты информации. В этой работе автором показана взаимосвязь общепринятых основных показателей безопасности информации: *доступности, целостности и конфиденциальности* с очевидным понятием качества *информационных ресурсов*, необходимых согласно законам *кибернетики* наряду с другими ресурсами для эффективного функционирования любой системы управления. Именно эта системная взаимосвязь может быть логическим обоснованием для часто используемых в СМИ и научно-популярной литературе терминов «кибербезопасность», «кибератаки», киберфизические системы и т.д. Но в действующей нормативно-правовой базе они практически нигде не используются, что иногда затрудняет ее толкование с точки зрения методологических основ информационной безопасности.

Такое киберпредставление, правда, своеобразным образом, нашло свое отражение в описанном выше «трехглавом» законе при легальном определении «первой головы» – информации как объекта права. Это своеобразие заключалось в том, что, нарушая, с точки зрения правоведов, каноны вещного права на отдельно выделенную категорию информации под названием информационные ресурсы, независимо от категории доступа, было распространено классическое право собственности, то есть защита законом в рамках гражданских правоотношений как элемента состава имущества. Эта норма была поддержана Гражданским Кодексом путем включения информации в объекты гражданских прав, нормой о возможности информации быть товаром и т.д. Взаимосвязь указанных норм с киберпредставлением работы Герасименко В.А. [17] становится очевидной не просто в силу чисто терминологического совпадения, а потому, что в терминах «трехглавого» закона информационные ресурсы – это документированная информация, то есть документы или массивы документов, которые и обращаются в любой системе управления. Таким образом, логически начинает проявляться необходимый четвертый элемент системы нормативного регулирования.

В общепринятых методологических терминах информационной безопасности его можно трактовать как требование обеспечения доступности, так как остальные показатели безопасности в аспекте госрегулирования заданы описанными выше элементами.

В то же время собственники (в терминах нынешнего законодательства обладатели) информации – это по определению санкционированные пользователи, иначе декларированное право собственности оказывается ничтожным, обладающие правовой возможностью защиты своих ресурсов даже при отсутствии у них свойства конфиденциальности. Самый главный вывод из приведенного анализа состоит в том, что таким, хотя и «экзотическим», образом определялась системность критериев и взглядов на

проблему правовой защиты информации, исходя из всех трех основных показателей информационной безопасности. И, на наш взгляд, четвертый элемент «трехглавого» закона можно рассматривать как предтечу рассматриваемого нового механизма госрегулирования. Но, в силу наличия существенных внутренних противоречий с позиций вещного права, обсуждение которых выходит за рамки настоящей работы, такое «киберпредставление» не получило сколь-нибудь существенного развития в нормативной базе, включая стандарты открытых систем. Более того, эти противоречия в совокупности с другими факторами привели к принятию в 2006 г. нового закона[18], анализ которого применительно к данному исследованию, в том числе по отношению к показателю доступности, будет дан далее.

Дальнейшая предыстория появления законодательства о безопасности КИИ связана уже с феноменом все возрастающего влияния современных информационно-коммуникационных технологий. Переход на рубеже XX–XXI века к глобальному постиндустриальному (именуемого иногда информационным) сообществу развитых стран зафиксировано впервые Окинавской Хартией. В то же время по мере развития информационных технологий актуализировались проблемы обеспечения их безопасности [18]. Адекватным отечественным ответом на новые вызовы стало утверждение в этот период информационной безопасности как одного из приоритетного направления в рамках Стратегии национальной безопасности и государственной политики по ее реализации.

В 2000 г. принимается первый обширный вариант Доктрины информационной безопасности, который по своей структуре и содержанию являлся директивой прямого действия [19]. Так одним из важных положений Доктрины стал достаточно короткий обобщенный перечень угроз национальной безопасности в информационной сфере, не потерявшим актуальности и в настоящее время в силу фундаментальности предложенных формулировок.

Среди них, имеющие прямое отношение к предмету данного исследования, хотя и с отсутствием прямой терминологической связи с понятием «информационная инфраструктура»:

– нарушения технологии обработки информации;

– внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;

– разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;

– уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;

– воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации.

Доктрина стала мощным стимулом для развития научных исследований и формирования отечественной целостной системы обеспечения информационной безопасности, включая системную структуру и распределение полномочий органов государственной власти.

В 2004 г. в ходе административной реформы Гостехкомиссия России, выполнявшая функции одного из регуляторов в сфере защиты информации с ограниченным доступом, была преобразована в Федеральную службу по техническому и экспортному контролю

[18]Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 16.03.2021).

(ФСТЭК России)[19]. При этом наряду с традиционными полномочиями Гостехкомиссии служба также получила статус уполномоченного органа по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры (ОБИ КСИИ). Этот момент можно условно считать исходной точкой начального периода становления анализируемого нового направления госрегулирования, которое и на настоящий момент еще далеко от своего завершения.

Исходя из общепринятой иерархии, верхним уровнем любой нормативной базы госрегулирования является базовый специальный закон либо, Указ Президента Российской Федерации.

Как показывает опыт формирования законодательства по электронному документообороту и персональным данным, период от исходной точки до принятия такого закона занимает от пяти, а то и более десяти лет с возможной вариацией базовых терминов. Такая же ситуация произошла и в сфере безопасности информационной инфраструктуры, хотя можно указать довольно существенную фундаментальную проработку правовых аспектов этой проблемы в рамках научных исследований.

В [20] научно обоснована необходимость выделения в качестве отдельного направления правового противодействия угрозам безопасности информационной инфраструктуре. Оно направлено «на нормативное регулирование отношений в области обеспечения сохранности объектов и сооружений связи, работоспособности средств связи, рационального использования радиочастотного ресурса, обслуживания абонентов сети связи, устойчивого функционирования сетей связи, информационных и компьютерных систем, глобальных информационных сетей и иных организационно-технических систем, предназначенных для повышения эффективности деятельности субъектов информационной сферы, а также производства и распространения продукции систем массовой информации и книгоиздания. Это противодействие основывается на нормах конституционного, административного, информационного и уголовного права».

Научное обоснование актуальности таких вопросов с позиций субъекта реального сектора экономики, например, Российские железные дороги (РЖД), представлено в [21]. В ней авторы ввели понятие *«функциональной безопасности»* как способности сложной системы устойчиво (штатно) функционировать в условиях наличия дестабилизирующих факторов. В свою очередь, такая устойчивость определяется *надежностью* ее аппаратно-технологических элементов и элементов обеспечения *информационной безопасности,* представление которой базировалось на перечне угроз, данном в Доктрине информационной безопасности.

Тем не менее, специальный законодательный акт отсутствовал, так как основные усилия законодателей и регуляторов в этот период были сосредоточены на совершенствовании базового «трехглавого» закона и нормативной базы трех основных его элементов. Показателен в этом смысле новый закон[18], принятый в 2006 г. вместо «трехглавого» закона. В аспекте данного исследования этот закон положение не исправил, а в некотором смысле даже усугубил, так как:

– информация в связи с отменой права собственности на информационные ресурсы юридически перестала быть объектом права, что было далее закреплено в Гражданском Кодексе;

– раздел о защите информации структурно и содержательно остался практически тем же, за исключением некоторых норм, понимание которых невозможно без дополнительных комментариев с указанием серьезных внутренних противоречий. В

[19]Указ Президента РФ от 16.08.2004 № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

частности, введена норма о возможности технологической защиты общедоступной информации, об актуальности этого отмечено выше. Но, сформулированные в законе условия такой возможности полностью разрушают всю логическую системную структуру самого раздела о защите информации, что является предметом отдельного анализа;

– замена «информатизации» как объекта правового регулирования на «информационные технологии» привело к тому, что в дальнейшем этот закон развивался в направлении правового регулирования вопросов создания и функционирования, прежде всего, глобальной сети Интернет. Поэтому закон фактически перестал быть базовым для области обеспечения информационной безопасности.

Несмотря на отсутствие специального закона, продолжалась работа по развитию директивной базы анализируемого направления, особенно после 2011 г., отмеченного выше как условный срок завершения формирования законодательной базы основных элементов правового обеспечения информационной безопасности. Так, можно еще рассмотреть директивный документ[20], в котором в пункте 3 (подпункт в) появилось определение *критической информационной инфраструктуры* Российской Федерации как *совокупности автоматизированных систем* ***управления критически важными объектами*** *и обеспечивающих их взаимодействие информационно-телекоммуникационных сетей, предназначенных для решения задач государственного управления, обеспечения обороноспособности, безопасности и правопорядка, нарушение (или прекращение) функционирования которых может стать причиной наступления тяжких последствий*.

В новом варианте Доктрины информационной безопасности в пункте 8 (подпункт б) (Указ Президента Российской Федерации от 5 декабря 2016 г. № 646) данное направление обозначено как одно из приоритетных в аспекте национальных интересов в информационной сфере. Следует также указать на интересную работу [22] общепризнанного специалиста в области информационной безопасности, в которой автор системно анализирует данную проблему в терминах «промышленной кибербезопасности», имеющей отличительные особенности от традиционной безопасности офисной информационной инфраструктуры. Но, как уже упомянуто выше такие «кибер» представления практически не используются в отечественной законодательной, а соответственно, и в нормативной базе.

Не будем выдвигать конспирологические причины еще почти пятилетнего срока до принятия базового закона[1], просто отметив 2017 г. как начало практического формирования действующей нормативной базы в сфере безопасности КИИ.

Вывод. описание эволюции законодательной и директивной базы, итогом которой стало приведенное выше легальное определение КИИ, методически увязанное с киберпредставлением безопасности информации, данным в работе Герасименко В.А. [17], на наш взгляд, полностью отвечает цели постановки в данном исследовании первой задачи по обоснованию понимания необходимости разработки новой нормативной базы государственного регулирования наряду с традиционно используемыми элементами.

2. Парадоксы нормативной базы безопасности объектов КИИ

2.1. Субъекты и предмет государственного регулирования безопасности КИИ

[20]«Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации». Утверждены Президентом Российской Федерации Д. Медведевым 3 февраля 2012 г., № 803.

Субъекты и предмет нового направления государственного регулирования по букве Федерального закона № 187-ФЗ[1] во многом отличны, не всегда в лучшую сторону, от вышеприведенного определения критической информационной инфраструктуры[20].

Критерий ***субъектности*** не привязан к понятию «критически важный объект» (КВО), а задается по факту принадлежности к одной из 13 сфер деятельности, охватывающих значительный объем предприятий и организаций, как реального сектора экономики, так и социальной сферы. Они по умолчанию объявляются критическими в связи с предполагаемым наличием потенциально опасных процессов, показателем опасности которых, естественно, задан возможный ущерб нарушения штатного (устойчивого) функционирования. Очевидно, что анализируемое направление сближается с широко применяемым в бизнесе риск-ориентированным подходом. Но, отличие состоит в том, что в рассматриваемом случае неприемлемый уровень риска в интересах государства заранее задан в виде некоторых показателей значимости.

Предметом регулирования является безопасность объектов КИИ, к которым отнесены не только АСУ, но и ИС, а также ИТКС, принадлежащие субъектам «на праве собственности, аренды или ином законном основании».

Дополнительно к вышеупомянутым субъектам и объектам КИИ, естественно, добавляются владельцы и их сети электросвязи, используемые для организации ***взаимодействия*** указанных выше объектов. То есть, формально по «букве закона», если сетевая структура используется только для ***обеспечения*** функционирования конкретно заданной ИС или АСУ (что, как правило, и происходит на практике), то она не задает ни субъектность, ни объектность данного законодательства. Этот пример одной из неточностей нормативной базы, так как задать критерий по выделению процессов взаимодействия из простого обеспечения довольно затруднительно. Хотя заметим, что эта неточность не является большим препятствием на практике, так как обеспечение устойчивости функционирования сетей, относится скорее к проблеме надежности технических средств, чем к информационной безопасности. И, как следствие, эта проблема всегда имела адекватное решение, в том числе на уровне отраслевого нормативно-правового регулирования, начиная с принятия в 2003 г. первоначального варианта Закона «О связи»[21]. Но, формальное толкование этого положения создает, как будет показано ниже, определенные сложности при разработке нормативных актов отраслевого уровня для операторов связи.

Основная сложность практической реализации нормативных требований для субъектов, в нашем случае, возникает на этапе инвентаризации своих информационных объектов, объективно необходимого для дальнейшего категорирования и обеспечения безопасности. Особенно актуальна такая ситуация для крупных субъектов реального сектора экономики. Напомним, что их функциональная безопасность во многом определяется и адекватно обеспечивается надежностью производственных и технологических процессов [21]. В то же время выделить свою КИИ в виде отдельных, достигающих десятки и сотни ИС, АСУ и ИТКС крайне сложно. Какая-либо обоснованная методика инвентаризации, использующая непротиворечивые критерии отсутствует. Организация и определение процедур этого объективно необходимого этапа отдана на «откуп» самим субъектам. Поэтому очевидной становится возможная экономическая мотивация выжидательной позиции большой части субъектов, особенно реального сектора экономики.

[21]Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_43224/ (дата обращения: 16.03.2021).

Не помогает, а наоборот усложняет процедуру инвентаризации, привязка отдельных объектов КИИ к критическим процессам, которые они обеспечивают. (подпункты «а», «б» пункта 5 Постановления Правительства 127[22]. Нормативный перечень таких процессов охватывает практически все возможные виды, а именно – «управленческие, технологические, производственные, финансово-экономические и другие процессы в рамках выполнения функций (полномочий) или осуществления деятельности субъектов КИИ».

Такой парадокс продемонстрируем на примере, приведенном в методическом пособии АРСИБ[23], когда АС «Бухгалтерия 1С» металлургического предприятия (субъекта КИИ), обеспечивающая финансово-экономический процесс (*критический*, по указанным выше формальным критериям), должна быть отнесена к объектам КИИ. По мнению авторов пособия, в силу того, что эта АС не осуществляет управление, контроль или мониторинг (заметим, что последние являются обязательными элементами любой системы управления) потенциально опасных производственных процессов данного субъекта, она включается в инвентаризационный перечень (табл. 1), но не подлежит категорированию. В то же время в соответствии с нормативно установленной процедурой категорирования такому объекту присваивается четвертая категория как незначимого. И далее можно сделать парадоксальный вывод о ненужности защиты такого объекта.

Таблица 1. Пример заполнения инвентаризационной таблицы в методическом документе АРСИБ

№	Наименование ИС (АСУ, ИТКС)	ОКВЭД 2	Относимость к КИИ
1	Бухгалтерия 1С	69.20.2	-
2	АСУ металлургического цеха	24.10.1	+
3	ИС конструкторского отдела	72.19.2	+
п/п...	ИС склада	52.10.9	-

Вывод. Разрешение различных противоречий на текущий момент находится на уровне субъекта наряду с его ответственностью, что, очевидно, снижает адекватность нового механизма государственного регулирования. Поэтому, на наш взгляд, существующая нормативно-методическая база должна быть дополнена унифицированной методикой проведения инвентаризационного этапа так же, как и этапа категорирования. Методологической базой такой методики должно стать научно обоснованное киберпредставление [17] безопасности информационных ресурсов и понятие функциональной безопасности [21] критических процессов. При этом для мотивации субъектов по упомянутому выше критерию экономической целесообразности (снижению затрат на инвентаризацию) достаточно ограничиться объектами КИИ, встроенными в систему управления потенциально опасными процессами. А их дальнейшее нормативное категорирование и обеспечение безопасности в соответствии с государственными показателями значимости позволит формализовать (и в определенной степени

[22]Постановление Правительства Российской Федерации № 127 от 08.02.2018 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» (с изменениями от 13 апреля 2019 г.).

[23]Безопасность объектов критической информационной инфраструктуры организации. Общие рекомендации (версия 2.0). Подготовлены Ассоциацией руководителей служб информационной безопасности (АРСИБ) The Association of Heads of Information Services security (AHISS) URL: http://aciso.ru/files/docs/metodichka_2.0.pdf (дата обращения: 16.03.2021).

унифицировать) требования ко всему комплексу обеспечения информационной безопасности субъекта.

2.2. Парадокс категорирования объектов КИИ

Далее покажем на отдельном примере категорирования объекта из сферы топливно-энергетического комплекса, что отдельные объекты КИИ, определенные по формальным признакам, могут и не являться таковыми.

Основные элементы приведенного примера установленной процедуры категорирования (рис. 1).

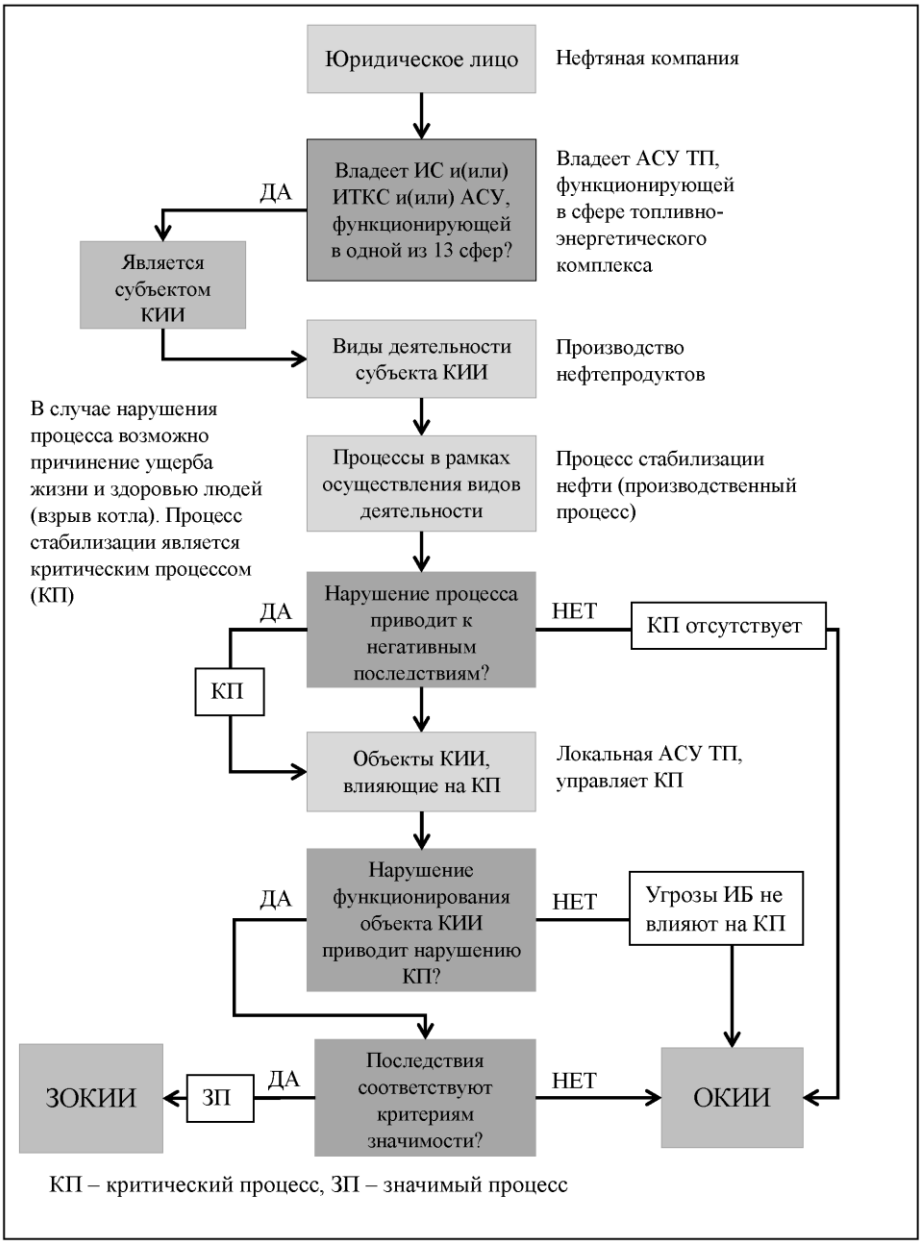

Рис. 1. Пример категорирования объекта КИИ
Fig. 1. Example of object categorization

1) ***Субъект КИИ*****:** нефтяная компания – российское юридическое лицо, которому на праве собственности принадлежит АСУ ТП, функционирующая в сфере топливно-энергетического комплекса согласно статье 2 пункт 8 закона 187-ФЗ[1]);

2) ***Вид деятельности как критерий субъектности КИИ*****:** производство нефтепродуктов в соответствии с пунктом 5 «а» Постановления Правительства 127[22]);

3) ***Критический процесс*****:** стабилизация нефти в ходе ее переработки, когда в случае нештатной ситуации, например, несанкционированного перекрытия технологической заслонки, может произойти взрыв и потенциальное причинение ущерба жизни и здоровью людей (п. 5 «б» Постановления Правительства 127[22]);

4) ***Объект КИИ*****:** локальная АСУ ТП стабилизации нефти, осуществляющая обеспечение указанного критического процессом (п. 5 «в» Постановления 127[22]) и подлежащая включению в перечень объектов КИИ и, соответственно, категорированию (п. 5 «г» Постановления Правительства 127[22]).

5) ***Этап оценки соответствию показателям критериев значимости*** масштаба возможных последствий в случае возникновения компьютерных инцидентов

В соответствии с 187-ФЗ[1] компьютерным инцидентом является факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки (т.е. причины нарушения могут быть любые). Предположим, что обеспечение противодействия указанному выше условию критичности, а именно, перекрытие технологической заслонки возможно лишь механическим способом по специальному регламенту. Как правило, так и происходит в большинстве случаев в реальном секторе экономики, когда нарушение и (или) прекращение функционирования АСУ ТП не может привести к последствиям, масштаб которых соответствует установленным показателям значимых последствий. Тогда, соответственно, должна быть присвоена 4-ая категория, как критерий незначимости.

В итоге рассмотренная локальная АСУ ТП, относящаяся к объектам КИИ по формальным признакам, таковой не является в силу того, что выполнение условий безопасности заложены непосредственно в регламент технологического процесса, а не в систему автоматизированного управления, что является типовой реализацией риск-ориентированного подхода субъектов реального сектора.

Разрешение такого парадокса требует уточнения самого понятия КИИ, определяющего область действия нового законодательства. Выше было показано[20], что информационная инфраструктура директивно определяется как ***совокупность*** объектов, хотя и без указания какой либо их взаимосвязи. А в анализируемой нормативной базе отсутствует даже термин совокупность, что, видимо, должно приниматься по умолчанию. Такой подход противоречит методологии разработки нормативной базы, не допускающей неясность и неоднозначное толкование основных положений.

Одно из возможных общепринятых определений инфраструктуры формулируется как комплекс взаимосвязанных обслуживающих структур или объектов, составляющих и обеспечивающих основу функционирования системы[10]. Если увязать это определение с киберпредставлением [17], то такой основой для КИИ любого субъекта выступает структурно определенная совокупность элементов (в нашем случае объектов КИИ) управления критическими процессами. Их устойчивость обеспечивается необходимым уровнем качества (безопасности) используемых информационных ресурсов.

Иными словами между объектами инфраструктуры должна существовать какая-либо взаимосвязь – физическая, информационная, функциональная и т.п., и именно она

определяет сущность самого понятия инфраструктуры. То есть, локальная АСУ ТП, не имеющая взаимосвязи с другими критическими объектами, не включается в КИИ по определению. Принимая во внимание ее функциональное предназначение с позиций представления, данного в [21], методологически она может быть отнесена к инфраструктуре топливно-энергетического комплекса, к производственной (промышленной) инфраструктуре в целом, но никак не к рассматриваемой нами проблеме.

В связи с важностью вопроса о легальном, прозрачном определении понятия КИИ целесообразно привести мировой опыт развитых стран.

1) В США основой методологии разрешения анализируемой проблемы является фундаментальное понятие «*Критическая инфраструктура* (КИ)»[24].

Во избежание лингвистических неточностей приведем оригинальное определение: «Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters».

В переводе с комментариями КИ США – это системы и активы, будь то физические (аналог отечественных КВО и/или значимых объектов КИИ) или виртуальные (в нашем понимании информационные ресурсы), настолько жизненно важные для Соединенных Штатов, что неспособность или разрушение таких систем и *активов* (в частности, в нашем понимании информационных ресурсов) окажет ослабляющее воздействие на *кибербезопасность*, национальную экономическую безопасность, национальное общественное здравоохранение или безопасность или любую комбинацию этих вопросов. То есть, основополагающим в такой формулировке является государственный интерес, выраженный в масштабе последствий нарушения их устойчивого функционирования. При этом не важно, в какой сфере они функционируют и являются-ли они «физическими» либо «виртуальными». В практической плоскости в США имеются естественные приоритетные ограничения, которые по сообщениям СМИ оцениваются в 16 наименований объектов.

2) Аналогичный подход использует и Европейский Союз, в частности, его политико-экономический лидер Германия. Ее к*ритически важная инфраструктура* представлена как организации или объекты, имеющие важное значение для государства, отказ или нарушение работы которых может привести к долгосрочным перебоям в поставках, значительным сбоям в общественной безопасности или другим серьёзным нарушениям. То есть основу КИ составляют «важные» объекты, совокупность которых далее [23] подразделяется на базовую техническую инфраструктуру (энергетика, информационные и коммуникационные технологии, транспорт и движение, водоснабжение и водоотведение) и инфраструктуру социально-экономических услуг (здравоохранение, «питание», аварийно-спасательные службы, борьба с бедствиями, парламент, правительство, государственное управление, судебные учреждения, финансы и страхование, СМИ и культурные ценности). Безопасность объектов КИ Германии выражается в терминах обеспечения их *кибербезопасности, то есть безопасности систем управления*.

Вывод. Проведенный выше анализ настоятельно подчеркивает актуальность совершенствования анализируемой нормативной базы в аспекте более четкого и однозначного толкования базового понятия КИИ. При этом необходимо выстроить логическую цепочку взаимосвязи действующих процессов в КВО (физических объектах)

[24]NIST Special Publication 800-30 Revision 1 - Специальная публикация Национального института Стандартов и Технологий США.

с «виртуальными» (в нашем понимании, информационными) объектами КИ. Тем более, что в ближайшее время в состав КИ России должны войти так называемые киберфизические системы управления[25], анализ свойств которых как объектов КИИ выходит за рамки данной работы.

2.3. Взаимопересечение различных объектов КИИ

Как было показано выше предметом нового механизма госрегулирования является безопасность законодательно заданных видов объектов, а именно ИС, АСУ, ИТКС и сетей их взаимодействия. Несмотря на кажущуюся по умолчанию простоту определения объектов регулирования, на практике при проведении организационных процедур по реализации нормативных требований могут возникнуть определенные сложности по их выделению из общей информационной инфраструктуры.

Так в соответствии с ГОСТ Р 50922-2006[26] ИС как некий объект проектирования представляет собой **совокупность** содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. Без специального разъяснения формально такая дефиниция может быть распространена и на бумажное делопроизводство, часто осуществляемое в настоящее время с использованием компьютеров. Поэтому, на наш взгляд целесообразнее было бы использование понятия автоматизированной системы обработки информации (АСОИ). Тем более, что термин автоматизированная система (АС) достаточно часто использован в традиционной нормативной базе ФСТЭК России.

Понятие АСУ как объекта, обеспечивающего устойчивость критического процесса и, соответственно, обоснованно включенного в КИИ, уже было рассмотрено ранее, поэтому останавливаться на нем специально не имеет смысла.

В нашем случае отметим тот факт, что многие ИС (АС) и АСУ на практике как объекты КИИ являются распределенными системами, поэтому отделить их от ИТКС практически невозможно (рис. 2). Именно ИТКС по определению (ГОСТ Р 52653-2006[27]) соединяет все компоненты (объекты) в единую информационную инфраструктуру.

Конечно, данную «размытость» границ законодательно заданных объектов КИИ можно попытаться разрешить на уровне локальных нормативных актов отдельных отраслей деятельности субъектов КИИ. Уже изданы различные методические рекомендации по категорированию, в которых разъясняются отдельные неоднозначные моменты: в сфере связи, в сфере здравоохранения, в области топливно-энергетического комплекса и т.д. Но, жесткая привязка этих актов к вышестоящим законодательным нормам дает прямо противоположные результаты.

В соответствии с методическими рекомендациями в сфере связи[28] выделенная сеть передачи данных для ***управления и мониторинга*** сетей электросвязи является ИТКС,

[25]Национальная программа «Цифровая экономика Российской Федерации». Утверждена протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7.

[26]ГОСТ Р 50922-2006 Национальный стандарт Российской Федерации «Защита информации. Основные термины и определения», разработан ФГУ «ГНИИИ ПТЗИ ФСТЭК России» (далее – ГОСТ Р 50922-2006).

[27]ГОСТ Р 52653-2006 Национальный стандарт Российской Федерации «Информационно-коммуникационные технологии в образовании. Термины и определения», утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 419-ст (далее – ГОСТ Р 52653-2006).

[28]Методические рекомендации по категорированию объектов критической информационной инфраструктуры, принадлежащих. субъектам критической информационной инфраструктуры, функционирующим в сфере связи. Введены в действие для опытного использования в тестовом режиме

хотя по функционалу, как видно из названия, она должна входить в состав автоматизированной системы управления и мониторинга сетей электросвязи, являясь частью АСУ.

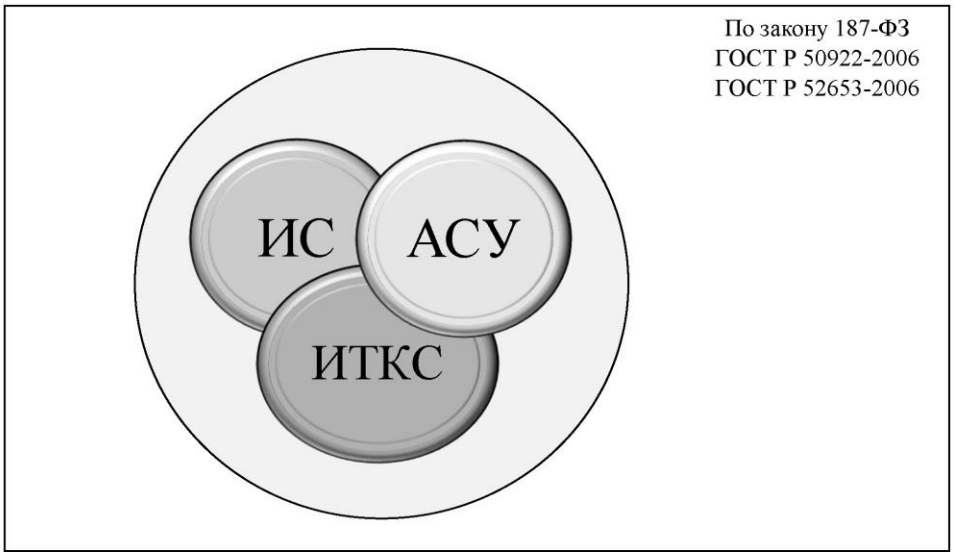

Рис. 2. Терминологическое пересечение понятий ИС, АСУ и ИТКС
Fig. 2. Terminological intersection of the concepts of Information Systems, Automated Control Systems and Information and Telecommunications Systems

Помимо вышеуказанного пересечения ИС и АСУ с ИТКС, сами ИС и АСУ также имеют терминологическое взаимопересечение. Например (в соответствии с теми же рекомендациями в сфере связи), система самообслуживания абонентов является ИС. Хотя по своему функционалу она обеспечивает автоматизацию управления (подключения/отключения) услуг связи (то есть управление критическим процессом) и должна являться АСУ. На данном примере видно, что АСУ является той же самой ИС (и наоборот), разница лишь в том, что в АСУ обрабатывается исключительно служебная информация, и целью этой обработки является управление определенным процессом, т.е. сама обработка информации не является целью функционирования АСУ.

Примером положительного выхода из указанной понятийной размытости может служить нормативно-методический акт[29] основного регулятора в рассматриваемой сфере – ФСТЭК России. В п. 1.3. данной методики, не привязанной к Постановлению Правительства 127, значительно расширена как субъектность, так и объектность применения данного акта на государственные и муниципальные ИС, системы персональных данных (ИСПДн), ИС управления производством, используемым организациями оборонно-промышленного комплекса, АСУ П и АСУ ТП на критически важных объектах (потенциально опасных), представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. Это подтверждает тот факт, что подход к обеспечению защиты иных «критических» информационных структур по своей сути должен быть такой же, как и к объектам КИИ.

решением Исполкома Общественно-государственного объединения «Ассоциация документальной электросвязи» от 26 июня 2019 г. Согласовано: 8 Центр ФСБ России и ФСТЭК России. URL: https://www.rans.ru/images/metrecKII.pdf (дата обращения: 16.03.2021).

[29] Методика оценки угроз безопасности информации, утверждена ФСТЭК России 5 февраля 2021 г. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021 (дата обращения: 16.03.2021).

Помимо этого, в новую методику было добавлено понятие «информационно-телекоммуникационная инфраструктура, на базе которой функционируют объекты КИИ», а также прописана возможность разработки модели угроз для «совокупности взаимодействующих систем и сетей оператора».

Не останавливаясь подробно на анализе основных положений методики, что является предметом отдельного анализа, заметим, что они дают возможность исключения необходимости определения угроз безопасности (и соответственно установления мер защиты) строго для отдельного объекта КИИ, границы которого, как уже отметили ранее, могут быть достаточно размыты.

Так как задание модели угроз безопасности с методологической точки зрения – это определяющий этап создания и совершенствования любой системы информационной безопасности, то принятие указанного нормативно-методического документа, безусловно, положительный факт. В то же время многие его положения расходятся с нормами анализируемого законодательства по безопасности КИИ. Достаточно указать только, что расширяя перечень объектов, методика ограничивает сферу применения для субъектов только в виде государственных и муниципальных образований. Другие субъекты, частности, реального сектора экономики, в силу ограничений механизмов госрегулирования на основе общего законодательства, выведены из сферы действия данного нормативного акта. Следовательно, их действия, по-прежнему, остаются на уровне принятия самостоятельных реальных решений вопросов обеспечения безопасности своих критических процессов.

Вывод. Терминологическая размытость границ объектов защиты вследствие неоднозначности толкования законодательно заданных понятий приводит к трудностям в их выявлении с целью дальнейшего категорирования. В итоге это может оказать влияние и на обоснованность предполагаемых мероприятий по обеспечению их безопасности (устойчивости) – «проблематично» защищать то, что однозначно не определено.

3. Нормативное регулирование и ответственность субъектов КИИ

Основой системы государственного регулирования является задание и реализация мер юридической ответственности за невыполнение субъектами правоотношений нормативных требований. В этом аспекте проблемой по обеспечению безопасности КИИ, на наш взгляд, будет являться то, что основой для определения субъектности, а, следовательно, и ответственности служит принадлежность к одной из 13 сфер деятельности.

В то же время очевидно, что в данном случае такой основой, как принято в методологии правоведения, должны быть последствия или ущерб национальным интересам, к которым может привести невыполнение нормативных требований. Именно такой подход был заложен в рассмотренном выше определении[20] понятия «критическая информационная инфраструктура». В данной формулировке присутствует понятие «совокупность», причем все объекты, входящие в совокупность, объединены в некую систему своим предназначением, а, главное, масштабом последствий их устойчивого функционирования.

Если сравнить указанное определение с нормами нового законодательства, то не трудно заметить, часть сфер деятельности «образца» 2012 г. законодательно «выпали» из состава КИИ, хотя сама область расширилась путем включения наряду с АСУ также ИС и ИТКС.

Усугубляет проблему и формулировка определения значимого объекта КИИ[1], в которой нет указанной выше причинно-следственной связи, а значение имеют не свойства

объекта регулирования, а наличие его записи в соответствующем государственном реестре.

И опять на передний план для субъектов реального сектора экономики выходит мотивация их выжидательной позиции, исходя из экономической целесообразности включения их объектов в состав государственного реестра. Тем более, что функциональная безопасность этих субъектов во многом и так обеспечивается выполнением требований технологической устойчивости. В этой ситуации применение новых норм *административной ответственности,* на наш взгляд, вряд ли будет адекватным в аспекте существенного развития анализируемого направления государственного регулирования. Это может лишь способствовать к переходу субъектами от выжидательной позиции к формальному выполнению установленных процедур, что как уже указывалось не меньшая угроза национальной безопасности.

Нестыковки и неточности директивной и нормативно-правовой базы вряд ли дадут возможность адекватного применения соответствующих расширенных норм об уголовной ответственности в соответствии с п. 3 статьи 274.1 УК РФ[2]. Должностные лица субъектов КИИ можно привлечь к уголовной ответственности за нарушение «***правил эксплуатации*** средств хранения, обработки или передачи *охраняемой компьютерной информации*, содержащейся в *критической информационной инфраструктуре* Российской Федерации, или ***информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре*** Российской Федерации ... если оно **повлекло причинение вреда критической информационной инфраструктуре** Российской Федерации».

Учитывая вышеуказанные проблемы, в данной формулировке нормы уголовной ответственности либо не будут работать вообще, так как принципиально невозможно причинить вред сразу всем объектам КИИ (в том числе никак не взаимосвязанным), либо нарушения на одном объекте КИИ априори будут приравнены к причинению вреда всей КИИ, что, будет не совсем логично, учитывая «некритичность» отдельных объектов КИИ.

Кроме того, в данном случае вред рассматривается не в отношении государства и его граждан, который оценивается по установленным критериям значимости[22], а в отношении такого правового объекта как КИИ, нынешнее нормативное определение которой, как показано выше, достаточно спорно и неоднозначно.

Вывод. Хотя новая система госрегулирования безопасности КИИ на текущий момент и поддержана нормами административной и уголовной ответственности, но в силу размытости, нестыковок и неоднозначности нормативной базы возможность их практического применения в условиях «регуляторной гильотины» является очень дискуссионной.

Заключение

Анализ предыстории развития и действующей нормативно-правовой базы по обеспечению безопасности объектов КИИ показал необходимость применения нового механизма государственного регулирования, а также его место в общем комплексе информационной безопасности страны.

Тем не менее, приведенные в работе примеры неоднозначности и внутренних противоречий (парадоксов) некоторых положений нормативно-правовых актов по безопасности объектов КИИ, показывают существующий общественный запрос по их совершенствованию. Необходимы дополнительные усилия, как со стороны научных специалистов, так и регуляторов по толкованию основных положений нормативно-

правовой базы. Основная цель этих усилий – снижение излишних затрат субъектов за счет более четкого нормативного определения самого понятия КИИ, ее структуры, объектов защиты и их взаимосвязей, исходя из общих принципов системного подхода к анализу сложных систем.

Изложенные в работе результаты могут быть полезны всем субъектам анализируемого законодательства, а также образовательным организациям, приступившим к практической реализации новых образовательных программ подготовки, переподготовки и повышения квалификации работников сил обеспечения, ответственных за реальный уровень безопасности отечественной КИИ.

СПИСОК ЛИТЕРАТУРЫ:

1. Горбатов В.С., Дураковский А.П., Лобанов М.И. О профессиональных стандартах в интересах подготовки кадров по безопасности объектов критической информационной инфраструктуры. Безопасность информационных технологий, [S.l.]. Т. 26, № 4. С. 54–68. 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.4.04.
2. Каннер Т.М. Особенности повышения квалификации специалистов по обеспечению безопасности значимых объектов критической информационной инфраструктуры. безопасность информационных технологий. Безопасность информационных технологий, [S.l.]. Т. 26, № 3. С. 22–31, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.3.02.
3. Грачков И.А., Малюк А.А. Проблемы разработки доверенного программного обеспечения, применяемого на объектах критической информационной инфраструктуры (организационные и методические аспекты). Безопасность информационных технологий, [S.l.]. Т. 26, №. 1. С. 56–63, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.1.06.
4. Грачков И.А Информационная безопасность АСУ ТП: возможные вектора атаки и методы защиты. Безопасность информационных технологий, [S.l.]. Т. 25, №. 1. С. 90–98, 2018. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2018.1.09.
5. Herrera Luis-Carlos & Maennel Olaf. (2019). A Comprehensive Instrument for Identifying Critical Information Infrastructure Services. International Journal of Critical Infrastructure Protection. Vol. 25. P. 50–61. DOI: https://doi.org/10.1016/j.ijcip.2019.02.001.
6. Rehak David & Senovsky Pavel & Hromada Martin & Lovecek Tomas & Novotny Petr. (2018). Cascading Impact Assessment in a Critical Infrastructure System. International Journal of Critical Infrastructure Protection. Vol. 22. P. 125–138. DOI: https://doi.org/10.1016/j.ijcip.2018.06.004.
7. Hannes Seppänen, Pekka Luokkala, Zhe Zhang, Paulus Torkki, Kirsi Virrantaus. Critical infrastructure vulnerability – a method for identifying the infrastructure service failure interdependencies. International Journal of Critical Infrastructure Protection. 2018. Vol. 22. P. 25–38. DOI: https://doi.org/10.1016/j.ijcip.2018.05.002.
8. David Rehak, Sciprofile linkPavel Šenovský, Martin Hromada, Tomas Lovecek. An integrated approach to assessing the stability of critical infrastructure elements. International Journal of Critical Infrastructure Protection. Vol. 25. P. 125–138. DOI: https://doi.org/10.1016/j.ijcip.2019.03.003.
9. В РЖД заявили о небольшом ущербе от атаки вируса WannaCry // Interfax.ru//. URL: https://www.interfax.ru/russia/563900/ (дата обращения: 16.03.2021).
10. Трунина А., Рождественский И., Фадеева А., Вовнякова А. «Роснефть» сообщила о мощной хакерской атаке на свои серверы // URL: https://www.rbc.ru/technology_and_media/27/06/2017/595247629a7947dc9d430d2c/ (дата обращения: 16.03.2021).
11. Макарова О.С., Поршнев С.В. Оценивание вероятностей компьютерных атак на основе метода анализа иерархий с динамическими приоритетами и предпочтениями. Безопасность информационных технологий, [S.l.]. Т. 27, № 1. С. 6–18, 2020. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2020.1.01.
12. Вавичкие А.Н., Горбатов В.С., Дураковский А.П., Чжен Д.А. К вопросу категорирования объектов критической информационной инфраструктуры высших учебных заведений. Безопасность информационных технологий, [S.l.]. Т. 26, № 2. С. 44–57, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.2.03.
13. Ахромеева Т.С., Малинецкий Г.Г., Посашков С.А. Стратегии и риски цифровой реальности // Стратегические приоритеты. 2017. № 2 (14). С. 88–102. URL: http://sec.chgik.ru/ctrategii-i-riski-tsifrovoy-realnosti/ (дата обращения: 16.03.2021).

14. Фатьянов А.А. Тайна и право (основные системы ограничений на доступ к информации в российском праве) / М.: МИФИ. 1999. – 288 с. URL: https://elibrary.ru/item.asp?id=29067845& (дата обращения: 16.03.2021).
15. Будзко В.И., Мельников Д.А. Информационная безопасность и блокчейн // Системы высокой доступности. 2018. Т. 14. № 3. С. 5–11. DOI: http://dx.doi.org/10.18127/j20729472-201803-02.
16. Запечников, Сергей В. Системы распределенного реестра как инструмент обеспечения доверия между участниками бизнес-процессов. Безопасность информационных технологий, [S.l.]. Т. 26, № 4. С. 37–53, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.4.03.
17. Герасименко В.А. Основы информационной грамоты. М.: Энергоатомиздат, 1996. – 320 с.
18. Тарасов, Анатолий М. Окинавская хартия и конгрессы ООН: Вопросы противодействия киберпреступности. Безопасность информационных технологий, [S.l.]. Т. 26, № 4. С. 120–131, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.4.09.
19. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические - и методологические основы. /Под редакцией В.А. Садовничего, В.П. Шерстюка. (Монография). М.: МЦНМО – МГУ им. М.В Ломоносова, 2002. – 351 с. URL: http://www.iisi.msu.ru/UserFiles/File/publications/Streltsov.pdf (дата обращения: 16.03.2021).
20. Стрельцов А.А. Теоретические и методологические основы правового обеспечения информационной безопасности России : Дис. д-ра юрид. наук : 05.13.19 : Москва, 2004. – 371 с. РГБ ОД, 71:05-12/1. URL: https://static.freereferats.ru/_avtoreferats/01002635074.pdf (дата обращения: 16.03.2021).
21. Шубинский И.Б., Тарасов А.А. Современная парадигма безопасности критически важных систем информационной инфраструктуры. Безопасность информационных технологий. 2005, № 3. С. 7–13.
22. Касперский Е.В. В заложниках у автоматики: как защитить промышленность от кибератак. Безопасность информационных технологий, [S.l.]. Т. 23, № 3. С. 7–10, 2016. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/12 (дата обращения: 16.03.2021).
23. Котов А. Развитие критических инфраструктур в Германии: выход из тени // Научно-аналитический вестник ИЕ РАН, 2021, №1. С. 96–102. DOI: http://dx.doi.org/10.15211/vestnikieran1202196102.

REFERENCES

[1] Gorbatov Viktor S., Durakovskiy Anatoly P., Lobanov Maxim I. On professional standards for personnel training on safety of critical information infrastructure objects. IT Security (Russia), [S.l.]. Vol. 26, no. 4. P. 54–68, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.4.04 (in Russian).
[2] Kanner Tatiana M. Features of advanced training of specialists in ensuring safety of significant objects of critical information infrastructure. IT Security (Russia), [S.l.]. Vol. 26, no. 3. P. 22–31, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.3.02 (in Russian).
[3] GRACHKOV, Ignaty A.; MALYUK, Anatoly A. Development problems of trusted software applied at critical information infrastructure objects (organizational and methodological aspects). IT Security (Russia), [S.l.]. Vol. 26, no. 1. P. 56–63, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.1.06 (in Russian).
[4] Grachkov Ignatiy A. Information security of industrial control systems: possible attack vectors and protection methods. IT Security (Russia), [S.l.]. Vol. 25, no. 1. P. 90–98, 2018. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2018.1.09 (in Russian).
[5] Herrera Luis-Carlos & Maennel Olaf. (2019). A Comprehensive Instrument for Identifying Critical Information Infrastructure Services. International Journal of Critical Infrastructure Protection. Vol. 25. P. 50–61. DOI: https://doi.org/10.1016/j.ijcip.2019.02.001.
[6] Rehak David & Senovsky Pavel & Hromada Martin & Lovecek Tomas & Novotny Petr. (2018). Cascading Impact Assessment in a Critical Infrastructure System. International Journal of Critical Infrastructure Protection. Vol. 22. P. 125–138. DOI: https://doi.org/10.1016/j.ijcip.2018.06.004.
[7] Hannes Seppänen, Pekka Luokkala, Zhe Zhang, Paulus Torkki, Kirsi Virrantaus. Critical infrastructure vulnerability – a method for identifying the infrastructure service failure interdependencies. International Journal of Critical Infrastructure Protection. 2018. Vol. 22. P. 25–38. DOI: https://doi.org/10.1016/j.ijcip.2018.05.002.
[8] David Rehak, Sciprofile linkPavel Šenovský, Martin Hromada, Tomas Lovecek. An integrated approach to assessing the stability of critical infrastructure elements. International Journal of Critical Infrastructure Protection, Vol. 25. P. 125–138. DOI: https://doi.org/10.1016/j.ijcip.2019.03.003.
[9] Russian Railways announced a small damage from the attack of the WannaCry virus. Interfax.ru. URL: https://www.interfax.ru/russia/563900 (accessed: 16.03.2021) (in Russian).
[10] Trunina A., Rozhdestvensky I., Fadeeva A., Vovnyakova A. Rosneft reported a powerful hacker attack on its servers. URL: https://www.rbc.ru/technology_and_media/27/06/2017/595247629a7947dc9d430d2c (accessed: 16.03.2021) (in Russian).

[11] Makarova Olga S., Porshnev Sergey V. Assessment of probabilities of computer attacks based on the method of analysis of hierarchies with dynamic priorities and preferences. IT Security (Russia), [S.l.]. Vol. 27, no. 1. P. 6–18, 2020. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2020.1.01 (in Russian).
[12] Vavichkin Alexander N. et al. To the issue of categorization of critical informational infrastructure objects in higher education. IT Security (Russia), [S.l.]. Vol. 26, no. 2. P. 44–57, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.2.03 (in Russian).
[13] Akhromeeva T.S., Malinetskiy G.G., Posashkov S.A. Strategies And Risks Of Digital Reality. Strategic Priorities. 2017. No 2 (14). P. 88–102. URI: http://sec.chgik.ru/ctrategii-i-riski-tsifrovoy-realnosti/ (accessed: 16.03.2021) (in Russian).
[14] Fatyanov A.A. Secrecy and law (the main systems of restrictions on access to information in Russian law). M.: MEPHI. 1999. – 288 p. URL: https://elibrary.ru/item.asp?id=29067845& (accessed: 16.03.2021) (in Russian).
[15] Budzko V.I., Melnikov D.A. Information security and blockchain. Highly available systems. 2018. Vol. 14. No. 3. P. 5–11. DOI: http://dx.doi.org/10.18127/j20729472-201803-02 (in Russian).
[16] Zapechnikov, Sergey V. Distributed ledger as a tool to ensure trust among business process participants. IT Security (Russia), [S.l.]. Vol. 26, no. 4. P. 37–53, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.4.03 (in Russian).
[17] Gerasimenko V.A. Fundamentals of information literacy. M.: Energoatomizdat, 1996. – 320 p.
[18] Tarasov, Anatoly M. The Okinawa Charter and the Congress of the United Nations: cybercrime countering issues. IT Security (Russia), [S.l.]. Vol. 26, no. 4. P. 120–131, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.4.09 (in Russian).
[19] Streltsov A.A. Ensuring information security of Russia. Theoretical - and methodological foundations. Edited by V. A. Sadovnichy, V. P. Sherstyuk. (Monograph). Lomonosov Moscow State University, 2002. – 351 p. URL: http://www.iisi.msu.ru/UserFiles/File/publications/Streltsov.pdf (accessed: 16.03.2021) (in Russian).
[20] Streltsov A. A. Theoretical and methodological foundations of legal support of information security in Russia: Dis. Dr. yurid. sciences': 05.13.19: Moscow, 2004. – 371 p. URL: https://static.freereferats.ru/_avtoreferats/01002635074.pdf (accessed: 16.03.2021) (in Russian).
[21] Shubinsky I. B., Tarasov A. A. Modern security paradigm of critical information infrastructure systems. IT Security (Russia). 2005, no. 3. P. 7–13 (in Russian).
[22] Kaspersky E.V. Automation hostage: how to protect the industry againts cyber attacks. IT Security (Russia), [S.l.]. Vol. 23, no. 3. P. 7–10, 2016. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/12 (accessed: 16.03.2021) (in Russian).
[23] Kotov A. Development of Critical Infrastructures in Germany: Out of the Shadow. Scientific and Analytical Bulletin of the IE RAS, 2021, no. 1. P. 96–102. DOI: http://dx.doi.org/10.15211/vestnikieran1202196102 (in Russian).

Поступила в редакцию – 02 апреля 2021 г. Окончательный вариант – 17 августа 2021 г.
Received – April 02, 2021. The final version – August 17, 2021.