Алексей А. Салкуцан[1], Григорий П. Гавдан[2], Андрей А. Полуянов[3]
[1,2]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
[3]ТЭЦ-8 филиал ПАО «Мосэнерго»,
Остаповский пр-д, 1, Москва, 109316, Россия
[1]e-mail: asalcutan@bk.ru, https://orcid.org/0000-0001-8282-3403
[2]e-mail: GPGavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076
[3]e-mail: andreapol_tec8@mail.ru, https://orcid.org/0000-0001-8648-5915

МЕТОДИКА ОПРЕДЕЛЕНИЯ КРИТИЧЕСКИХ ПРОЦЕССОВ НА ОБЪЕКТАХ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

DOI: http://dx.doi.org /10.26583/bit.2020.2.02

Аннотация. Целью статьи является попытка разработки методики определения критических процессов для упрощения деятельности субъектов критической информационной инфраструктуры (КИИ) по проведению категорирования объектов информационной инфраструктуры на примере химической промышленности. Актуальность рассматриваемых проблем обусловлены тем, что с каждым годом не уменьшается число кибератак на различные сферы деятельности государств, в том числе, и на значимые объекты (ЗО) КИИ. Для защиты национальных информационных ресурсов РФ в 2017 году был выбран вектор действий в направлении защиты объектов КИИ принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации», который определил важные направления политики российского государства в информационной сфере, и как минимум, на ближайшее десятилетие. Так, в ходе его выполнения, многим субъектам критической информационной инфраструктуры уже пришлось столкнуться с различного уровня трудностями. В статье разобраны некоторые фрагменты решения задач, поставленных при разработке методики определения критических процессов на объектах информационной инфраструктуры, устойчивое функционирование которых регламентировано рядом основополагающих нормативных правовых документов РФ. В работе установлены некоторые особенности определения критических процессов на объектах КИИ, например, химической промышленности, которые нашли свое применение в разработке авторами методики определения критических процессов информационной инфраструктуры.

Ключевые слова: значимые объекты, категорирование объектов, критические процессы, критическая информационная инфраструктура (КИИ), национальные информационные ресурсы, *субъекты КИИ.*

Для цитирования: САЛКУЦАН, Алексей А.; ГАВДАН, Григорий П.; ПОЛУЯНОВ, Андрей А. МЕТОДИКА ОПРЕДЕЛЕНИЯ КРИТИЧЕСКИХ ПРОЦЕССОВ НА ОБЪЕКТАХ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ. Безопасность информационных технологий, [S.l.], v. 27, n. 2, p. 18-34, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1268>. Дата доступа: 27 may 2020. doi: http://dx.doi.org/10.26583/bit.2020.2.02.

Alexei A. Salkutsan[1], Grigory P. Gavdan[2], Andrey A. Poluyanov[3]
[1,2]National Nuclear Research University MEPHI (Moscow Engineering Physics Institute),
Kashirskoe sh., 31, Moscow, 115409, Russia
[3]CHPP-8 branch of «Mosenergo» PJSC,
1 Ostapovsky Ave., Moscow, 109316, Russia
[1]e-mail: asalcutan@bk.ru, https://orcid.org/0000-0001-8282-3403
[2]e-mail: GPGavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076
[3]e-mail: andreapol_tec8@mail.ru, https://orcid.org/0000-0001-8648-5915

The method of identifying critical processes at information infrastructure facilities

DOI: http://dx.doi.org /10.26583/bit.2020.2.02

Abstract. The aim of the study is to develop a methodology for determining critical processes in order to simplify the activities of critical information infrastructure (CII) entities for categorizing information infrastructure objects on the example of the chemical industry. The actuality of the problems under consideration is based on the fact that the number of cyber attacks in various areas of state activity, including significant objects (ZO) of CII, is not decreasing. To protect the national information resources of the Russian Federation in 2017, the actions have been chosen in the direction of protecting CII objects with the adoption of the Federal law "on the security of critical information infrastructure of the Russian Federation", which defined important directions of the Russian state policy in the information sphere for the next decade. Thus during its implementation, many subjects of critical information infrastructure have already had to face difficulties of various levels. The paper analyzes some fragments of solving the tasks set in the development of methods for determining critical processes at information infrastructure facilities, the sustainable functioning of which is regulated by a number of fundamental regulatory legal documents of the Russian Federation. In the course of the study, some features of determining critical processes at CII facilities, for example, in the chemical industry, were established. These features were later used in the development of a unique methodology for determining critical processes in the information infrastructure.

Keywords: significant objects, object categorization, critical processes, critical information infrastructure (CII), national information resources, CII subjects.

For citation: SALKUTSAN, Alexei A.; GAVDAN, Grigory P.; POLUYANOV, Andrey A. The methodology for critical processes identifying at information infrastructure facilities. IT Security (Russia), [S.l.], v. 27, n. 2, p. 18-34, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1268>. Date accessed: 27 may 2020. doi:http://dx.doi.org/10.26583/bit.2020.2.02.

Введение

Непрерывное функционирование значимых объектов критической информационной инфраструктуры (КИИ) и состояние её безопасности в XXI веке играет ключевую роль в России в критических сферах экономики [1] и обеспечении национальной безопасности ведущих стран мира, включая и Российскую Федерацию (РФ). В настоящее время, обладая достаточными знаниями, ресурсами и используя современные технологии (ноу-хау) на мировой арене (и не только на уровне государств), появилась возможность проводить различного рода и вида специальные операции, как оборонительного, так и наступательного характера для достижения целей (политического, экономического, военного и др.) [2].

Для субъектов КИИ критических сфер экономики (государства), которые в своем составе имеют сотни и даже тысячи объектов КИИ выполнение Федерального закона (ФЗ) № 187 от 26 июля 2017 года[1] является не простой задачей.

В настоящее время возникает большое количество вопросов, на которые необходимо дать ответы, например, определение критических процессов в условиях неопределённости и др.[2] На IT&Security Forum Kazan 2019 представителем Национальным координационным центром по компьютерным инцидентам (НКЦКИ) Кореловым С. был представлен доклад на тему: «О практике взаимодействия с НКЦКИ».

Так, например, согласно данным НКЦКИ в 2019 году было выявлено:

6800 адресатов вредоносного программного обеспечения (ВПО);

215 рассылок ВПО с взломанных почтовых адресов;

[1]Федерального закона от 26.072017 года № 187 от 2017 г. «О безопасности критической информационной инфраструктуры Российской Федерации», принят Государственной Думой 12.07.2017 года.

[2]Проблемные вопросы процедуры категорирования объектов КИИ // Единый портал электронной подписи. URL: https://iecp.ru/news/item/423941-problemnyye-voprosy-protsedura-kategorirovaniya-kiya-obyekty (дата обращения: 12.12.2019).

186 случаев внедрения ВПО;
53 случая использования ресурсов для проведения DDoS-атаки;
51 случай подмены заглавной страницы сайта;
5 случаев внедрения майнеров и др.

Современные отрасли экономики активно внедряют новейшие цифровые решения, которые позволяют с помощью различных объектов информационной инфраструктуры, таких как: информационные системы (ИС) [3], автоматизированные системы управления технологическими процессами (АСУ ТП) [4] и информационно-телекоммуникационные сети (ИТКС) [5] повысить конкурентоспособность и модернизацию с целью ускорения своего инновационного развития. Чаще всего приобретая такие решения, предприятие или организация не задумываются или не хотят уделить должное внимание вопросам должного обеспечения защиты информации [6].

Например, авторами Leandros A. Maglaras, Ki-Hyung Kim, Helge Janicke в статье «Кибербезопасность критических инфраструктур» отмечается, что «современные АСУ ТП в последние годы подвергаются большому числу компьютерных атак, вследствие чего представляется серьезная угроза национальной безопасности государств» [7].

Так, согласно отчету Kaspersky ICS-CERT, в мире количество компьютерных атак с попытками внедрения вредоносных объектов на компьютеры АСУ в первом полугодии 2019 по сравнению с первым полугодием 2018 выросли незначительно, однако все равно находятся на высоких отметках (рис. 1). Так, работа химических предприятий в Российской Федерации основана на использовании различных технологических схем, методов и расчетов (химических формул, превращений одних веществ в другие вещества, изменениях свойств материалов, их строения и др.). В качестве примера в АСУ ТП (химическая отрасль) можно привести всем известную систему SCADA применяемую на базе устройств фирмы SIEMENS. Повсеместное внедрение таких систем в АСУ ТП, с одной стороны, способствовало (в отрасли) увеличению возможностей (отвечающих общим мировым стандартам): качеству конечного продукта, обеспечению его экологической безопасности и др., а с другой стороны, привело к увеличению угроз, способных нанести непоправимый ущерб не только самому предприятию, но зависимым и взаимозависимым с данным предприятием организациям из других сфер экономики [7].

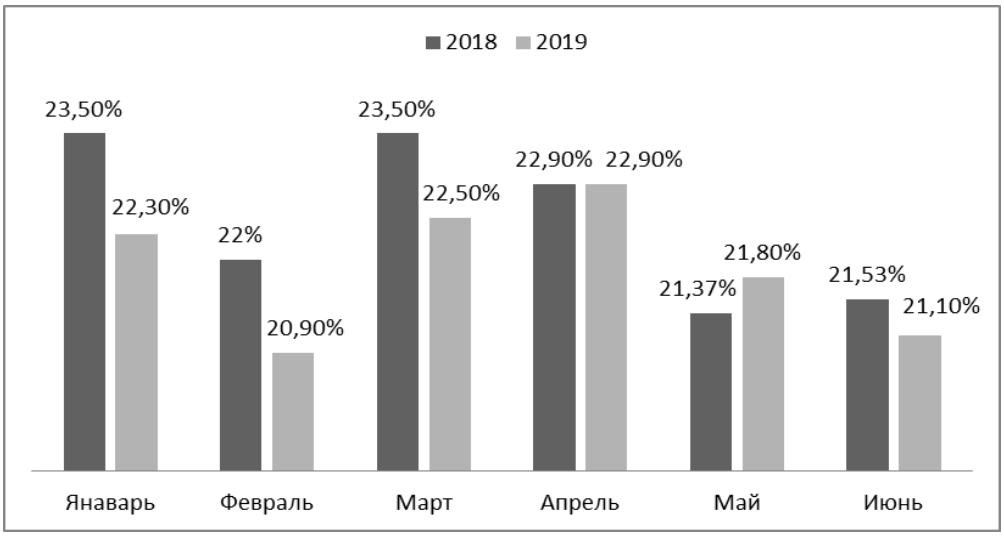

Рис. 1. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, по месяцам, первые полугодия 2018 и 2019 годов [8]
(Fig. 1. Percentage computers of vulnerable automatic process control systems where malicious objects were blocked by month, first half of 2018 and 2019 [8])

Так, при реализации угроз безопасности информации, например, «Угроза перехвата управления автоматизированной системой управления технологическими процессами» № 183[3] может привести к частичной или полной остановам технологических процессов (без выхода или с выходом оборудования из строя). Как следствие, произойдёт нарушение штатного хода технологических процессов на значимом объекте КИИ (ЗОКИИ).

Принятие Федерального закона № 187[4] от 2017 г. «О безопасности критической информационной инфраструктуры Российской Федерации», и появление связанных с ним других подзаконных актов, направлено именно на защиту ЗОКИИ государства, включая информационные системы органов власти. Поэтому для субъектов КИИ критических сфер экономики, имеющих сегодня сотни и даже тысячи значимых объектов КИИ, выполнение этого законодательства является не простой задачей. Так, например, при проведении мероприятий по категорированию нет утвержденной со стороны Федеральной службы по техническому и экспортному контролю России (ФСТЭК России) методики определения критических процессов. При этом также, необходимо отметить, что приказы о создании комиссии по категорированию и специальной комиссии по инвентаризации объектов КИИ и определению критических процессов (КП) являются внутренними нормативными документами предприятия (субъекта КИИ), где состав и форма определяется с субъектом[5].

В результате этого некоторые субъекты КИИ столкнулись с важной проблемой правильности отнесения того или иного объекта к категории значимого объекта КИИ, где в ряде случаев возврат документов со стороны ФСТЭК России происходит вследствие некорректности применения критериев значимости к объекту ИИ.

Отсутствие для сфер деятельности в РФ утвержденных методик для ЗОКИИ со стороны ФСТЭК России и Федеральной службой безопасности (ФСБ России) вынуждает многих представителей субъектов КИИ (в настоящее время) привлекать аутсорсинговые компании. В свою очередь аутсорсинговые компании (АК) для определения критических процессов в информационной инфраструктуре в своей работе применяют (наработанные) свои методы и подходы. Такое сотрудничество не всегда позволяет достигнуть требуемых гарантией в определении критических процессов у потенциально значимых объектов КИИ (ЗО КИИ) для этих субъектов. И здесь субъекту КИИ приходится делать свой выбор.

Необходимо также отметить, что многие отечественные методики и подходы по категорированию опираются только на метод экспертных оценок с последующим анализом полученных результатов для формирования отчета и включением в акт по категорированию того или иного объекта КИИ [9]. При этом в них не учитываются зависимости и взаимозависимости между объектами информационной инфраструктуры с другими объектами и их процессами, влияющими на появление рисков, например, возникновения каскадных и эскалационных сбоев в одном или нескольких регионах РФ из-за компьютерной атаки и т.д. И это достаточно важная проблема на ряду и с проблемой правильного определения значимости.

---

[3]Банк угроз информации ФСТЭК России // ФСТЭК России. URL: https://bdu.fstec.ru/threat/ubi.183 (дата обращения: 27.03.2020).

[4]Федерального закона № 187 от 2017 г. «О безопасности критической информационной инфраструктуры Российской Федерации».

[5]Приказ ФСТЭК России от 21 декабря 2017 г. № 235 «Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры российской федерации и обеспечению их функционирования» //. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/288-prikazy/1606-prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-235 (дата обращения: 27.03.2020).

Если обратимся к опыту рубежных специалистов, то обнаружим, что многими учеными, активно проводятся исследования и обсуждения в области КИИ, которые направлены на разработку комплексных инструментов для определения важнейших услуг информационной инфраструктуры [10]; методов выявления взаимозависимостей отказов инфраструктурных служб [11]; разработке оценок каскадированого (и др.) воздействия на системы КИИ [12]; комплексных подходов к оценке устойчивости критически важных элементов инфраструктуры [13]. Предполагается, что разрабатываемая методика позволит субъектам КИИ правильно определить имеющейся критические процессы, тем самым повысить ситуационную осведомленность государственных органов управления по наличию (у субъектов) объектов КИИ, что даёт возможность предвидеть (предупредить) сбои на ЗО КИИ для случаев с воздействием на КИИ. Так, важность этих объектов (химическая промышленность) для любого государства не требует доказательств, так как несет огромный ущерб людям, экономики и экологии [14].

Главной на сегодня трудностью, по мнению авторов, является отсутствие разработанных и утвержденных методик. Так, есть только отдельные как зарубежные, так и отечественные подходы и методы, которые освещались в научных статьях и конференциях по ИБ. Поэтому некоторые субъекты КИИ вынуждены (хотя и временно) заниматься анализом в отношении своих объектов КИИ без какой-либо утвержденной методической базы со стороны регуляторов.

Всё это послужило и легло в основу разрабатываемой авторами методики. Так, на рис. 2 представлены основные этапы предполагаемой авторами методики по определению значимости объекта (критических процессов) на объектах информационной инфраструктуры. В статье акцентировано внимание на некоторых её моментах.

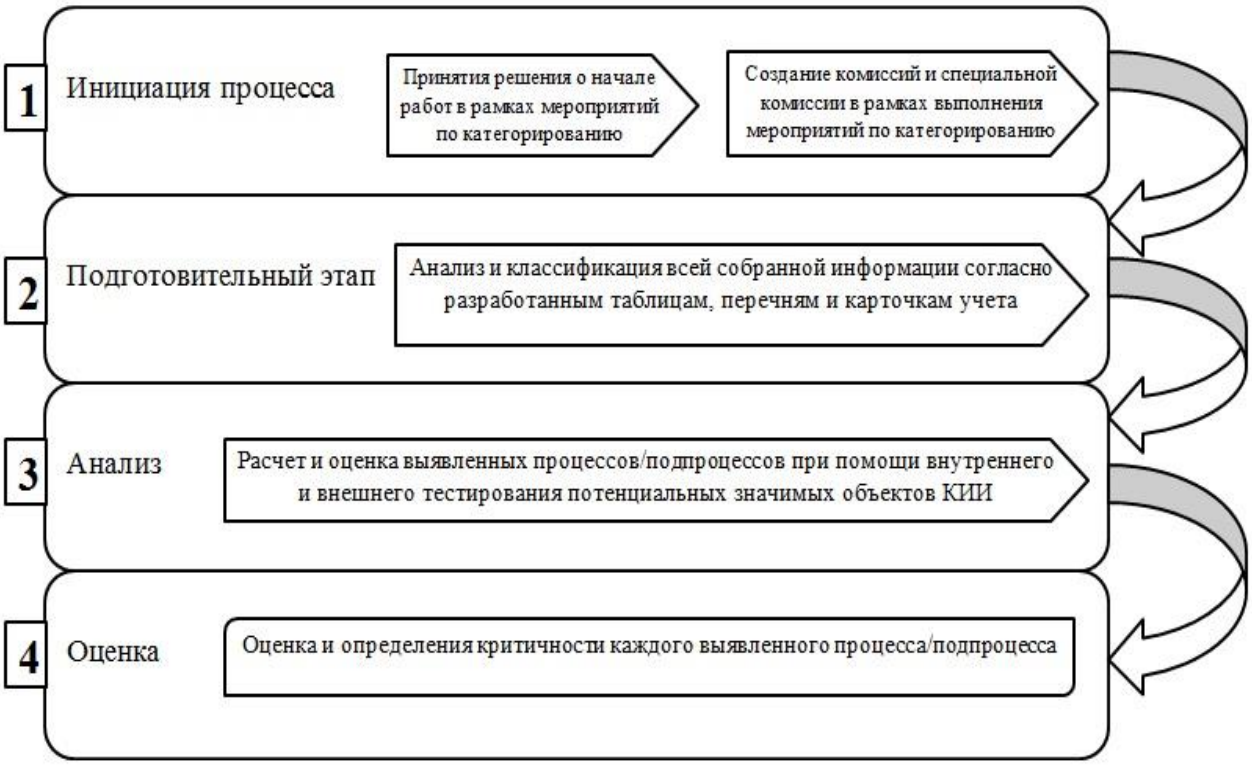

Рис. 2. Основные этапы методики определения критических процессов
(Fig. 2. The main stages of the methodology for determining critical processes)

1. Инициация процесса

После того, как субъект КИИ принял решение о начале работ по выполнению ФЗ №187, он создаёт комиссию по категорированию, которая начинает процесс инициации работ по выполнению мероприятий и одновременно принимает решения о начале работ по определению и обоснованию всех выявленных процессов в организации. Чтобы их выполнить, необходимо нанять соответствующих персонал, имеющий право в соответствии с законодательством РФ на ведение такой деятельности.

Здесь необходимо отметить, что содержать отдел по ИБ и ИТ, сотрудники которого смогли бы на достаточно высоком уровне проводить необходимые мероприятия на объектах КИИ (определять критические процессы, давать обоснованные решения на основе правильно полученных и оформленных результатах в ходе работы, выполнении обслуживания, проведении мониторинга (данных) объектов [15] и др.) с точки зрения финансирования вышестоящими министерствами и ведомствами для многих субъектов КИИ не представляется возможным. При этом, отдадим должное, некоторые субъекты КИИ имеют достаточные финансовые средства на содержание отдела (ИБ и ИТ), и как правило, предпочтения в этом случае отдают аутсорсинговым организациям [16] обладающим подготовленным персоналом, и опытом на рынке ИБ, готовых провести соответствующие мероприятия в рамках выполнения законодательства по КИИ (не безвозмездно) и это их законное право.

Первый этап. Инициация процесса по категорированию объектов КИИ. Для того чтобы избежать ошибок на первом этапе методики, авторами рекомендуется взять за основу нижеприведенную схему (рис. 3).

Рис. 3. Инициация процесса категорирования объектов критической информационной инфраструктуры
(Fig. 3. Initiating the process of categorizing critical information infrastructure objects)

Субъекты КИИ, у которых потенциально значимые объекты (ЗО) имеют выход в сеть Интернет, подвергают свои объекты угрозам. Это не означает, что необходимо отказаться от информационных Интернет-технологий в производстве и других сферах человеческой деятельности.

Важно при этом помнить, что в таких ситуациях в процессе эксплуатации (в последствии ЗОКИИ) существуют риски, например, от компьютерных атак, последствия которых могут наносить ущерб государству (приводить к жертвам среди населения, срыву государственного оборонного заказа, или к недоступности той или иной значимой системы и др.) [15].

2. Специальная комиссия по инвентаризации значимых объектов и определению критических процессов

Второй этап. Субъектом издается приказ о проведении инвентаризации всех информационных активов, после чего специальная комиссия приступает к выполнению возложенных на нее задач, которые представлены на рис.4 в виде схемы. Создание базы данных всех информационных активов находящейся на балансе предприятия основывается на тщательном сборе данных, на предприятии со всех структурных подразделении (таблица 1) может основываться как на зарубежных методах, например CRAMM, FRAP, OCTAVE, RiskWatch, Microsoft и т.д., так и на отечественных экспертных методах. Независимо от применения того или иного метода или подхода, главное, чтобы была собрана достаточная информация для заполнения базы данных обо всех выявленных информационных активах.

Таблица 1. База данных всех информационных активов на балансе предприятия

№ п.п.	Наименование актива	Адрес размещения	Назначение объекта	Количество	Документация на актив
1					
…					
n					

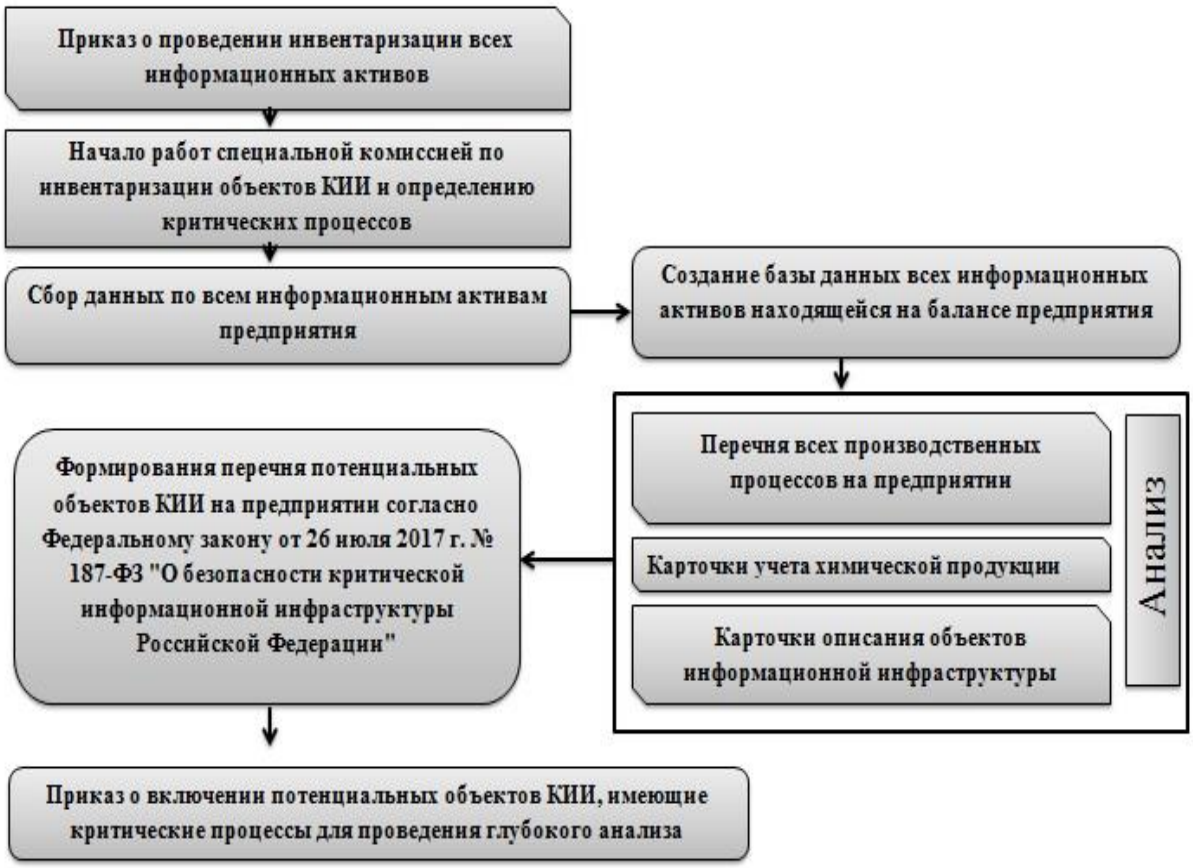

Рис. 4. Основные задачи специальной комиссии на подготовительном этапе
(Fig.4. The main tasks of the special commission at the preparatory stage)

После того, как специальной комиссией сформирована база данных всех информационных активов, далее формируется перечень потенциальный объектов КИИ на предприятии согласно Федеральному закону от 26 июля 2017 г. № 187-ФЗ[6]. Для того чтобы его сформировать необходимо, провести тщательный анализ всей технической документации, которая имеется на химическом предприятии, для того, чтобы разобраться какие объекты информационной инфраструктуры влияют или могут повлиять на технологические процессы [16]. Для этого необходимо:

1. Сформировать перечень всех производственных процессов на предприятии. Пример приведен в табл. 2.

Таблица 2. Перечень всех производственных процессов на предприятии

Критерии			**Описание**
Классификация химико-технологических процессов	Группа химических процессов		
	Тип процесса		
	Подтип процесса		
	По способу организации основные процессы		
Описание процесса	Вход (ресурсы преобразующейся в ходе процесса в выходы процесса)		
	Управление (условия выполнения процесса (документация, на основе которой осуществляется выполнение процесса)		
	Механизмы	Название оборудования	
		Серия и номер оборудования	
		Серия и номер лицензии	
		Количество	
		Наименование подразделения и № помещения	
		Ответственное лицо	
	Выход результаты (продукция)		

Результатом любого производственного процесса является выпуск определенной продукции. Однако здесь необходимо отметить, что в данном случае химическая продукция является очень специфичной. И поэтому для каждой химической продукции на предприятии необходимо создавать карточку учета (табл. 3).

Таблица 3. Карточка учета химической продукции на предприятии

№ п.п.	**Название химической продукции**	**Класс опасности [7]**	**Номер паспорта безопасности химической продукции**
1			
…			
n			

[6]Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // ФСТЭК России. Доступно на: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/285-zakony/1610-federalnyj-zakon-ot-26-iyulya-2017-g-n-187-fz (дата обращения: 10.02.2020).

[7]ГОСТ 12.1.007-76 Система стандартов безопасности труда (ССБТ). Вредные вещества. Классификация и общие требования безопасности (с Изменениями № 1,2) // Электронный фонд правовой и нормативно-технической документации. Доступно на: http://docs.cntd.ru/document/5200233 (дата обращения: 14.03.2020).

К карточке учета химической промышленности обязательно прикладывается приложение опасностей химической продукции согласно ГОСТ 32419-2013[8] «Классификация опасности химической продукции. Общие требования» информация представлена в табл. 4–6.

Таблица 4. Классификация химической продукции, опасность которой обусловлена ее физико-химическими свойствами

Критерии		**Описание**
Классификация опасности взрывчатой химической продукции	Классы опасности взрывчатой химической продукции	
Классификация опасности сжатых, сжиженных и растворенных под давлением газов	Классы опасности газов под давлением	
Классификация опасности воспламеняющихся газов, в том числе химически неустойчивых	Классы опасности воспламеняющихся газов	
	Дополнительные классы опасности для химически неустойчивых воспламеняющихся газов	
Классификация опасности химической продукции в аэрозольной упаковке	Классы опасности химической продукции в аэрозольной упаковке	
Классификация опасности химической продукции, представляющей собой воспламеняющуюся жидкость	Классы опасности химической продукции, представляющей собой воспламеняющуюся жидкость	
Классификация опасности химической продукции, представляющей собой воспламеняющееся твердое вещество	Классы опасности химической продукции, представляющей собой воспламеняющееся твердое вещество	
Классификация опасности саморазлагающейся химической продукции	Классы опасности саморазлагающейся химической продукции	
Классификация опасности пирофорной химической продукции	Классы опасности пирофорной химической продукции	
Классификация опасности самонагревающейся химической продукции	Классы опасности самонагревающейся химической продукции	
Классификация опасности химической продукции, выделяющей воспламеняющиеся газы при контакте с водой	Классы опасности химической продукции, выделяющей воспламеняющиеся газы при контакте с водой	
Классификация опасности окисляющей химической продукции	Классы опасности окисляющей химической продукции	
Классификация опасности органических пероксидов	Классы опасности органических пероксидов	
Классификация опасности химической продукции, вызывающей коррозию металлов	К химической продукции, вызывающей коррозию металлов, относится продукция, которая вызывает скорость коррозии стальной или алюминиевой поверхности > 6,25 мм в год при температуре 55 °С.	

[8]ГОСТ 32419-2013 Классификация опасности химической продукции. Общие требования // Электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/document/1200107879 (дата обращения: 14.03.2020).

Таблица 5. Классификация опасности химической продукции по воздействию на организм человека

Критерии (Классы опасности химической продукции)		**Описание**
Классификация опасности химической продукции, обладающей по воздействию на организм острой токсичностью	Обладающей острой токсичностью по воздействию на организм	
Классификация опасности химической продукции, вызывающей поражение (некроз)/раздражение кожи	Вызывающей поражение (некроз) / раздражение кожи	
	Вызывающей поражение (некроз)/раздражение кожи	
Классификация опасности химической продукции, вызывающей серьезные повреждения/раздражение глаз	Вызывающей серьезные повреждения / раздражение глаз	
	Вызывающей серьезное повреждение / раздражение глаз	
Классификация опасности химической продукции, обладающей сенсибилизирующим действием	Обладающей сенсибилизирующим действием	
Классификация опасности мутагенов	Классы опасности мутагенов	
Классификация опасности канцерогенов	Классы опасности канцерогенов	
Классификация опасности химической продукции, воздействующей на функцию воспроизводства	Классы опасности химической продукции, воздействующей на функцию воспроизводства	
Классификация опасности химической продукции, обладающей избирательной токсичностью на органы-мишени и/или системы при однократном воздействии	Классы опасности химической продукции, обладающей избирательной токсичностью на органы-мишени и/или системы при однократном воздействии	
Классификация опасности химической продукции, обладающей избирательной токсичностью на органы-мишени и/или системы при многократном / продолжительном воздействии	Классы опасности химической продукции, обладающей избирательной токсичностью на органы-мишени и/или системы при многократном/ продолжительном воздействии	
Классификация опасности химической продукции, представляющей опасность при аспирации	Классы опасности химической продукции, представляющей опасность при аспирации	

Таблица 6. Классификация опасности химической продукции по воздействию на окружающую среду

Критерии		**Описание**
Классификация опасности химической продукции, разрушающей озоновый слой		
Классификация опасности химической продукции, обладающей острой токсичностью для водной среды	Классы опасности химической продукции, обладающей острой токсичностью для водной среды	
Классификация опасности химической продукции, обладающей хронической токсичностью для водной среды	Классы опасности химической продукции, обладающей хронической токсичностью для водной среды	

Важно при проведении анализа понять, как устроена иерархия химико-технологических систем на химическом предприятии. Иерархия химического предприятия состоит из трех ступеней (рис. 5) [17].

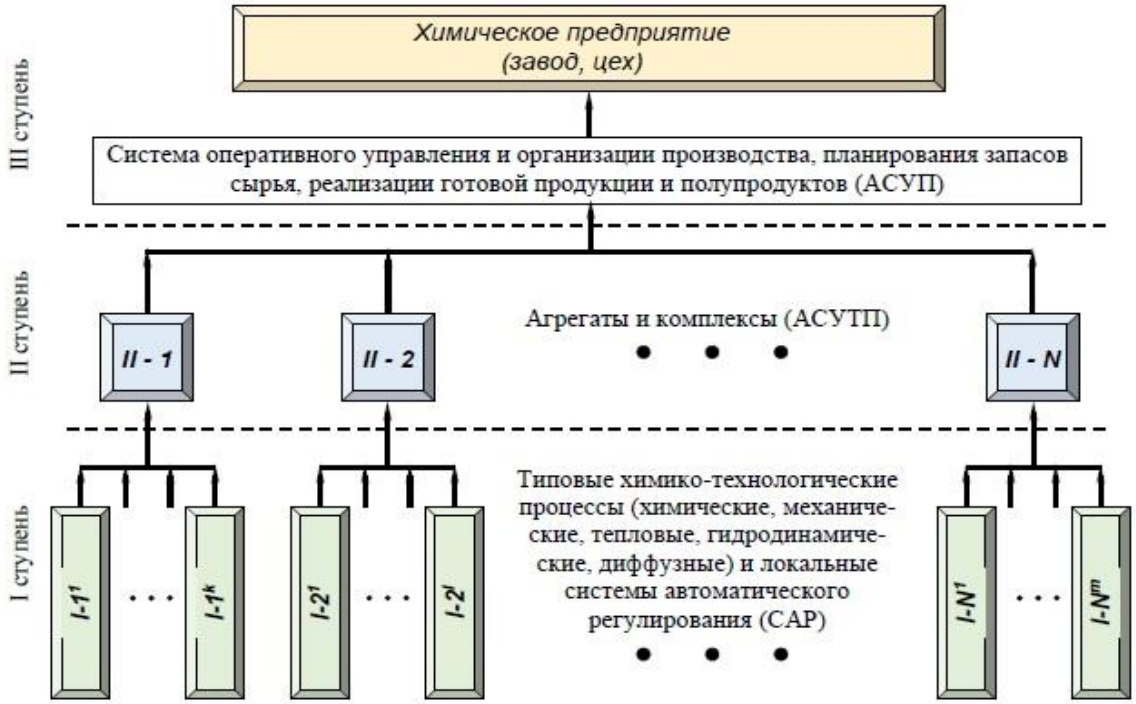

Рис. 5. Иерархия химического производства [17]
(Fig 5. Hierarchy of chemical production) [17]

На сегодняшний день цифровизация российских промышленных предприятий идет большими темпами, благодаря чему происходит положительное влияние на качественные [18] и количественные показатели деятельности [19], в том числе и химической отрасли [20].

2. Сформировать перечень потенциальный объектов КИИ согласно Федеральному закону от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (таблица 7).

Таблица 7. Перечень потенциальный объектов КИИ на предприятии

№ п.п.	Наименование объекта	Адрес размещения	Тип объекта	Вид права собственности	Количество	Номер карточки описания объекта

Для того чтобы заполнить вышеприведённую таблицу необходимо, чтобы каждый объект информационной инфраструктуры имел свою (заполненную) карточку описания (составлено на базе приказа № 236[9]) представленной в табл.8.

[9] Приказ от 22.12.2017 г. № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий» (в ред. приказа ФСТЭК России от 21 марта 2019 г. № 59).

Таблица 8. Учетная карточка описание объекта информационной инфраструктуры

Критерии		**Описание**
Общие сведения по объекту	Наименование объекта	
	Производитель	
	Серия и номер лицензии	
	Год поставки объекта	
	Количество	
	Описание	
Сведения о взаимодействии объекта и сетей электросвязи	Категория сети электросвязи или сведения об отсутствии взаимодействия объекта с сетями электросвязи	
	Наименование оператора связи и (или) провайдера хостинга	
	Цель взаимодействия с сетью электросвязи	
	Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводный), протоколов взаимодействия	
Сведения о силах обеспечения безопасности объекта	Структурное подразделение (работники) ответственные за обеспечение безопасности объекта	
	Структурное подразделения (работники), эксплуатирующие объект	
	Структурное подразделение (работники), обеспечивающие функционирование (сопровождение, обслуживание, ремонт) объекта	
Сведения о программных и программно-аппаратных средствах, используемых на объекте	Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, иных средств) и их количество	
	Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации - при наличии)	
	Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (прикладные программы, входящие в состав дистрибутивов операционных систем, не указываются)	
	Применяемые средства защиты информации (в том числе встроенные в общесистемное, прикладное программное обеспечение) (наименования средств защиты информации, реквизиты сертификатов соответствия, иных документов, содержащих результаты оценки соответствия средств защиты информации или сведения о не проведении такой оценки) или сведения об отсутствии средств защиты информации	
Организационные и технические меры, применяемые для обеспечения безопасности объекта	Организационные меры (установление контролируемой зоны, контроль физического доступа к объекту, разработка документов (регламентов, инструкций, руководств) по обеспечению безопасности объекта)	
	Технические меры по идентификации и аутентификации, управлению доступом, ограничению программной среды, антивирусной защите и иные в соответствии с требованиями по обеспечению безопасности значимых объектов	
Дополнительная информация по объекту	Документация на объект	
	Общая схема инфраструктуры производства на предприятии и архитектура объекта в этой схеме	

Также к вышеперечисленной таблице прилагается приложение, в котором прописаны технические данные, а именно системные и технические компоненты (табл. 9). Для каждого компонента заполнение таблицы происходит отдельно.

Таблица 9. Описание системных и технических компонентов объекта

<table>
<tr><td colspan="3">Критерии</td><td colspan="3">Описание компонентов (1,2,3..n)</td></tr>
<tr><td>1</td><td colspan="2">2</td><td>4</td><td>5</td><td>6</td></tr>
<tr><td colspan="3">Название компонента</td><td></td><td></td><td></td></tr>
<tr><td colspan="3">Описание</td><td></td><td></td><td></td></tr>
<tr><td colspan="3">Наименование объекта, с которым косвенно или прямо происходит взаимодействие</td><td></td><td></td><td></td></tr>
<tr><td colspan="3">Наименование процесса или процессов, которые включены в системные / технические компоненты</td><td></td><td></td><td></td></tr>
<tr><td rowspan="6">Наименование процесса или процессов, которые включены в системные/ технические компоненты</td><td colspan="2">Наименование процесса и его схема</td><td></td><td></td><td></td></tr>
<tr><td colspan="2">Наименование подпроцесса и его схема</td><td></td><td></td><td></td></tr>
<tr><td rowspan="4">Информация по программно-логические контроллеры (ПЛК)</td><td>Название</td><td></td><td></td><td></td></tr>
<tr><td>Серия и номер лицензии</td><td></td><td></td><td></td></tr>
<tr><td>Схема размещение</td><td></td><td></td><td></td></tr>
<tr><td>Перечень технической документации</td><td></td><td></td><td></td></tr>
<tr><td colspan="3">Перечень технической документации</td><td></td><td></td><td></td></tr>
<tr><td colspan="3">Наименование производственного процесса, над которым установлены компоненты</td><td></td><td></td><td></td></tr>
</table>

Следует отметить, что после сбора всей исходной информации последующее проведение процедуры анализа должно строго контролироваться (со стороны комиссией по категорированию) так, как сформированные отчеты будут использованы на последующих этапах методики. В ряде после неправильного предоставления данных (специальной комиссией), предприятие рискует увеличить сроки реализации мероприятий по категорированию.

Неправильное определение (в организации) ЗОКИИ – это шанс попасть под санкции со стороны регулирующих органов исполнительной власти РФ [21]. Это особенно важно на фоне громких заявлений (в средствах массовой информации) о проведенных кибератаках [22] со стороны различных преступных группировок в информационном пространстве. Такая преступная активность способна приводить к нарушению работы ЗОКИИ (вызвать дестабилизацию социальной, политической, экономической и др. систем государства). Так, например, государственные органы в РФ сегодня отказываются от использования иностранного ПО и оборудования, отдавая предпочтение отечественным разработкам (ПО, средствам защиты информации и другие) [23].

Данная мера помогает государственным структурам и российским компаниям не только снизить уровень угроз КИИ, но и оказывает поддержку отечественному производителю в условиях острого экономического и политического кризиса [24].

Заключение

Решение субъектами информационной инфраструктуры задач выявления значимых объектов на основе определения критических процессов остается на сегодня одним из важных направлений работы по защите ЗОКИИ, а значит и обеспечения национальной безопасности Российской Федерации. Отсутствие методик определения критических процессов субъекты ИИ заставляет субъекты КИИ испытывать определенные трудности, возникающие в ходе категорировании своих объектов для последующей их эксплуатации.

Необходимо отдать должное, что ФЗ-187 и пакет связанных с ним нормативных документов, дали запуск процессу позитивных изменений в сфере обеспечения безопасности КИИ и позволили в Российской Федерации пройти за два года в этом направлении путь, который занимал в некоторых государствах десятилетия. Доклады руководителей государственных структур и субъектов КИИ (на форумах, конференциях, совещаниях и др.) конечно же, вносят свою неоценимую пользу, но тоже не решают эту проблему в полной мере.

В настоящей работе приведены этапы проведения работ необходимых при определении категорирования и некоторые их особенности, нашедшие применение в разрабатываемой авторами методике по определению критических процессов субъектов (химическая промышленность) информационной инфраструктуры, где в основу методики был положен опыт Национальной образовательной инициативы США в области кибербезопасности. Только проведение дальнейших исследований, а затем и применение комплексных инструментов для определения важнейших услуг информационной инфраструктуры; методов выявления взаимозависимостей отказов инфраструктурных служб; комплексный подход к оценке устойчивости критически важных элементов инфраструктуры; разработок оценки каскадированого воздействия на системы позволит качественно выполнять категорирование объектов информационной инфраструктуры и эксплуатацию значимых объектов КИИ.

СПИСОК ЛИТЕРАТУРЫ:

1. Козырева А.А., Тарасов Д.А. Современное состояние государственной политики в сфере информационной безопасности. Вестник Воронежского института МВД России. 2018. № 4. С. 243–247. URL: https://cyberleninka.ru/article/n/sovremennoe-sostoyanie-gosudarstvennoy-politiki-v-sfere-informatsionnoy-bezopasnosti (дата обращения: 12.12.2019).
2. Родачин В.М. Гибридные войны и обеспечение национальной безопасности России. Гуманитарные науки. Вестник Финансового университета. 2019. № 4. С. 93–99. DOI: https://doi.org/10.26794/2226-7867-2019-9-4-93-99.
3. Жернова В.М. Информационные системы как источник повышенной опасности в условиях цифровизации. Вестник Южно-Уральского государственного университета. Серия: Право. 2019. Т. 19. № 3. С. 67–71. DOI: https://doi.org/10.14529/law190310.
4. Батьковский М. А., Кравчук П. В., Судаков В. А. Информационная система управления диверсификацией интегрированных структур оборонно-промышленного комплекса. Бюллетень науки и практики. 2020. Т. 6. № 1. С. 237–247. DOI: https://doi.org/10.33619/2414-2948/50/26.
5. Асалханова С.А. Формирование единого информационного пространства в цифровой экономике. Известия Санкт-Петербургского государственного экономического университета. 2020. № 1. С. 144–147. URL: https://cyberleninka.ru/article/n/formirovanie-edinogo-informatsionnogo-prostranstva-v-tsifrovoy-ekonomike (дата обращения: 27.03.2020).
6. Leandros A. Maglaras, Ki-Hyung Kim, Helge Janicke, Mohamed Amine Ferrag, Stylianos Rallis, Pavlina Fragkou, Athanasios Maglaras, Tiago J. Cruz. Cyber security of critical infrastructures. ICT Express, Vol. 4, Issue 1, March. 2018. P. 42–45. DOI: https://doi.org/10.1016/j.icte.2018.02.001.
7. Грачков, Игнатий А. Информационная безопасность АСУ ТП: возможные вектора атаки и методы защиты. Безопасность информационных технологий, [S.l.], Т. 25, № 1. С. 90–98, mar. 2018. ISSN 2074-

7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1097/1091 (дата обращения: 28.03.2020). DOI: http://dx.doi.org/10.26583/bit.2018.1.09.

8. Отчет Kaspersky ICS-CERT. Kaspersky ICS-CERT. URL: https://ics-cert.kaspersky.ru/reports/2019/09/30/threat-landscape-for-industrial-automation-systems-h1-2019/ (дата обращения: 27.03.2020).
9. Вавичкин, Александр Н. et al. К вопросу категорирования объектов критической информационной инфраструктуры высших учебных заведений. Безопасность информационных технологий, [S.l.], Т. 26, № 2. С. 44–57, june 2019. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1198> (дата обращения: 28.03.2020). DOI: http://dx.doi.org/10.26583/bit.2019.2.03.
10. Herrera, Luis-Carlos & Maennel, Olaf. (2019). A Comprehensive Instrument for Identifying Critical Information Infrastructure Services. International Journal of Critical Infrastructure Protection. DOI: https://doi.org/10.1016/j.ijcip.2019.02.001.
11. 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.
12. 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.
13. 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.
14. Кулясова Е. В. Химическая промышленность России: Современное состояние и проблемы развития. Вестник университета. 2019. № 5. С. 93–100. DOI: https://doi.org/10.26425/1816-4277-2019-5-93-100.
15. Миннуллина К.А. Смирнова А.Е. Стрелков Е.С. Татаринова Е.П. Договор как стратегия минимизации инновационных рисков. Вестник Волжского университета им. В.Н. Татищева. 2019. № 2. С. 122–128. URL: https://cyberleninka.ru/article/n/dogovor-kak-strategiya-minimizatsii-innovatsionnyh-riskov (дата обращения: 28.03.2020).
16. Остроцкая С.В., Калуцкий И.В. К вопросу анализа угроз безопасности критическим информационным инфраструктурам // Материалы II Всероссийской научной конференции с международным участием. В 2 частях. 2019 Издательство: Издатель Качалин Александр Васильевич. - Курск: Информационные технологии в моделировании и управлении: подходы, методы, решения, 2019. С. 212–217. URL: https://www.elibrary.ru/item.asp?id=39542201 (дата обращения: 23.03.2020).
17. Калашников А.О, Сакрутина Е.А. Модель прогнозирования рискового потенциала значимых объектов критической информационной инфраструктуры. Информация и безопасность. 2018. № 4. С. 466–471. URL: https://www.elibrary.ru/item.asp?id=36739588 (дата обращения: 28.03.2020).
18. Надеждина М.Е. Модель химико-технологических систем на принципах «Индустрии 4.0». Безопасность транспорта и сложных технических систем глазами молодежи. Материалы Всероссийской молодежной научно-практической конференции. Иркутск, 10-13 апреля 2018 г. - Иркутск: Иркутский государственный университет путей сообщения, 2018. С. 132–134. URL: https://www.elibrary.ru/item.asp?id=35307860 (дата обращения: 28.03.2020).
19. Кулясова Е.В., Вдовенко З.В. Цифровизация промышленных предприятий: возможности и угрозы новой реальности. Ученые записки российской академии предпринимательства. 2019. Том 18. № 3. С. 98–110. URL: https://www.elibrary.ru/item.asp?id=41311983 (дата обращения: 28.03.2020).
20. Кулясова Е.А, Вдовенко З.В. Перспективные инструменты цифровизации предприятий химического комплекса. Сборник методических рекомендаций по вопросам теоретических и практических разработок в области прикладных общественно-гуманитарных и технических наук. 2019. С. 128–133. URL: https://www.elibrary.ru/item.asp?id=38521969 (дата обращения: 28.03.2020).
21. Новичков В.Е., Пыхтин И.Г. Социально-правовое обоснование введения уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации. Психопедагогика в правоохранительных органах. 2018. № 2(73). С. 25–29. DOI: https://doi.org/10.24411/1999-6241-2018-12004.
22. Cyber Polygon Международный тренинг по борьбе с глобальными киберугрозами. Cyber Polygon. URL: https://cyberpolygon.com/upload/Cyber-Polygon-ru.pdf (дата обращения: 28.03.2020).

23. Жумаева А.П., Ялбаева В.А., Селифанов В.В., Макарова Д.Г., Звягинцева П.А., Чернов Д.В. О выборе средств защиты информации для государственных информационных систем. Известия Тульского государственного университета. Технические науки. 2018. №10. С. 52–58. URL: https://cyberleninka.ru/article/n/o-vybore-sredstv-zaschity-informatsii-dlya-gosudarstvennyh-informatsionnyh-sistem (дата обращения: 28.03.2020).
24. Габричидзе Т.Г., Куделькин В.А., Зайцев А.М., Болтовский А.В., Лебедева Т.Г. Анализ систем управления базами данных, используемых на территории Российской Федерации. Известия Самарского научного центра Российской академии наук. 2016. №1. С. 5–12. URL: https://cyberleninka.ru/article/n/analiz-sistem-upravleniya-bazami-dannyh-ispolzuemyh-na-territorii-rossiyskoy-federatsii (дата обращения: 28.03.2020).

REFERENCES:

[1] Kozyrev A. A., Tarasov D. A. Modern state policies in the field of information security. Vestnik Voronezhskogo instituta MVD Rossii. 2018. No. 4. P. 243–247. URL: https://cyberleninka.ru/article/n/sovremennoe-sostoyanie-gosudarstvennoy-politiki-v-sfere-informatsionnoy-bezopasnosti (accessed: 12.12.2019) (in Russian).
[2] Reducin V. M. Hybrid war and the national security of Russia. Gumanitarnye nauki. Vestnik finansovogo universitetam. 2019. No. 4. P. 93–99. DOI: https://doi.org/10.26794/2226-7867-2019-9-4-93-99 (in Russian).
[3] Zhernova V. M. Information systems as a source of increased danger in digitalization conditions. Bulletin of the South Ural State University. 68 Ser. Law. 2019. Vol. 19. No. 3. P. 67–71. DOI: https://doi.org/10.14529/law190310 (in Russian).
[4] Batkovskiy, M., Kravchuk, P., & Sudakov, V. (2019). Diversification Management Information System Integrated Structures of the Military-Industrial Complex. Bulletin of Science and Practice, 6(1). P. 237–247. DOI: https://doi.org/10.33619/2414-2948/50/26 (in Russian).
[5] Asalkhanova S. A. Formation of a single information space in the digital economy. Izvestiya Sankt-Peterburgskogo gosudarstvennogo ekonomicheskogo universiteta. 2020. No 1. P. 144–147. URL: https://cyberleninka.ru/article/n/formirovanie-edinogo-informatsionnogo-prostranstva-v-tsifrovoy-ekonomike. (accessed: 27.03.2020) (in Russian).
[6] Leandros A. Maglaras, Ki-Hyung Kim, Helge Janicke, Mohamed Amine Ferrag, Stylianos Rallis, Pavlina Fragkou, Athanasios Maglaras, Tiago J. Cruz. Cyber security of critical infrastructures. ICT Express, Vol. 4, Issue 1, March 2018. P. 42–45. DOI: https://doi.org/10.1016/j.icte.2018.02.001.
[7] Grachkov, Ignatiy A. Information security of industrial control systems: possible attack vectors and protection methods. IT Security (Russia), [S.l.], v. 25, n. 1. P. 90–98, mar. 2018. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1097> (accessed: 20.04.2020) DOI: http://dx.doi.org/10.26583/bit.2018.1.09.
[8] Kaspersky ICS-CERT report. Kaspersky ICS-CERT. URL: https://ics-cert.kaspersky.ru/reports/2019/09/30/threat-landscape-for-industrial-automation-systems-h1-2019/ (accessed: 27.03.2020).
[9] Vavichkin, Alexander N. et al. To the issue of categorization of critical informational infrastructure objects in higher education. IT Security (Russia), [S.l.], v. 26, n. 2. P. 44–57, june 2019. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1198> (accessed: 20.04.2020). DOI: http://dx.doi.org/10.26583/bit.2019.2.03.
[10] Herrera, Luis-Carlos & Maennel, Olaf. (2019). A Comprehensive Instrument for Identifying Critical Information Infrastructure Services. International Journal of Critical Infrastructure Protection. DOI: https://doi.org/10.1016/j.ijcip.2019.02.001.
[11] 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.
[12] 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.
[13] 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.
[14] Kulyasova E.V. Chemical industry of Russia: Current state and development problems. Bulletin of the University. 2019. No. 5. P. 93–100. DOI: https://doi.org/10.26425/1816-4277-2019-5-9-100 (in Russian).

[15] Minnullina K. A., Smirnova A. E., Strelkov E. S., Tatarinova E. P. Treaty as innovative risks minimization strategy. Vestnik Volzhskogo universiteta im. V.N. Tatishcheva. 2019. Vol. 2. P. 122–128. URL: https://cyberleninka.ru/article/n/dogovor-kak-strategiya-minimizatsii-innovatsionnyh-riskov (accessed: 28.03.2020) (in Russian).

[16] Ostrotskaya S. V., Kalutsky I. V. On the issue of analyzing security threats to critical information infrastructures. Materials of the II all-Russian scientific conference with international participation. In 2 parts. 2019 Publisher: Publisher Alexander Kachalin. - Kursk: Information technologies in modeling and management: approaches, methods, solutions, 2019. P. 212–217. URL: https://www.elibrary.ru/item.asp?id=39542201 (accessed: 28.03.2020) (in Russian).

[17] Kalashnikov A. O, Sakrutina E. A. Model of predicting risk potential of significant plants of critical information infrastructure. Informatsiya-i-bezopasnost. 2018. Vol. 4. P. 466–471. URL: https://www.elibrary.ru/item.asp?id=36739588 (accessed: 28.03.2020) (in Russian).

[18] Nadezhdina M.E. Model of chemical and technological systems based on the principles of "Industry 4.0". All-Russian youth scientific and practical conference. Irkutsk: Irkutsk state University of railway transport, 2018. P. 132–134. URL: https://www.elibrary.ru/item.asp?id=35307860 (accessed: 28.03.2020) (in Russian).

[19] Kulyasova E.V., Vdovenko Z.V. Digitalization of industrial enterprises: opportunities and threats of new reality. Uchenye zapiski rossijskoj akademii predprinimatel'stva. 2019. Vol. 18. No 3. P. 98–110. URL: https://www.elibrary.ru/item.asp?id=41311983 (accessed: 28.03.2020) (in Russian).

[20] Kulyasova E.A, Vdovenko Z.V. Promising directions of digitalization of chemical enterprises. Sbornik metodicheskih rekomendacij po voprosam teoreticheskih i prakticheskih razrabotok v oblasti prikladnyh obshchestvenno-gumanitarnyh i tekhnicheskih nauk. 2019. P. 128–133. URL: https://www.elibrary.ru/item.asp?id=38521969 (accessed: 28.03.2020) (in Russian).

[21] Novichkov V.E., Pykhtin I.G. Social and Legal Grounds providing Criminal Liability for Illegal Influence on Vital Informational Infrastructure of the Russian Federation. Psychopedagogy in Law Enforcement. No. 2(73). 2018. P. 25–29 DOI: https://doi.org/10.24411/1999-6241-2018-12004 (in Russian).

[22] Cyber Polygon international training to combat global cyber threats. Cyber Polygon. URL: https://cyberpolygon.com/upload/Cyber-Polygon-ru.pdf (accessed: 28.03.2020).

[23] Zhumaeva A.P., Erbaeva V.A., Selifanov V.V., Makarov G.D., Zvyagintsev P.A., Chernov D.V. On the choice of means of information security for government information systems. Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki. 2018. No. 10. P. 52–58. URL: https://cyberleninka.ru/article/n/o-vybore-sredstv-zaschity-informatsii-dlya-gosudarstvennyh-informatsionnyh-sistem (accessed: 02.12.2019) (in Russian).

[24] Gabrichidze T.G., Kudelkin V.A., Zaitsev A.M., Boltovskii A.V., Lebedeva T.G. Analysis of database management systems, used in the Russian Federation. Izvestiya Samarskogo nauchnogo centra Rossijskoj akademii nauk. 2016. No. 1. P. 5–12. URL: https://cyberleninka.ru/article/n/analiz-sistem-upravleniya-bazami-dannyh-ispolzuemyh-na-territorii-rossiyskoy-federatsii (accessed 02.12.2019) (in Russian).

Поступила в редакцию – 23 марта 2020 г. Окончательный вариант – 20 мая 2020 г.
Received – March 23, 2020. The final version – May 20, 2020.