Сергей Е. Парьев[1], Дмитрий И. Правиков[2], Владимир Г. Карантаев[3]
[1]Независимый эксперт
[2]Российский государственный университет
(национальный исследовательский университет) имени И.М. Губкина
Ленинский пр-кт, 65, корп. 1, Москва, 119991, Россия
[3]Центр НТИ МЭИ
ул. Красноказарменная, 17, Москва, 111250, Россия
[1]e-mail: sergey.pariev@mail.ru, https://orcid.org/0000-0001-5698-7471
[2]e-mail: dip@gubkin.pro, https://orcid.org/0000-0001-5217-4537
[3]e-mail: vladimir.karantaev@gmail.com, https://orcid.org/0000-0003-1628-7635

ОСОБЕННОСТИ ПРИМЕНЕНИЯ РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА ДЛЯ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ОБЪЕКТОВ

DOI: http://dx.doi.org/10.26583/bit.2020.4.04

Аннотация. В статье анализируется взаимосвязь понятия «безопасность» с производными понятиями. Выделена объективная научно-практическая потребность в научном и регуляторном закреплении термина «кибербезопасность», дано его определение. В результате анализа перспективных подходов к обеспечению безопасности отмечена сохраняющаяся актуальность риск-ориентированного подхода. При этом в качестве методов оценки рисков кибербезопасности в ближайшей перспективе будут рассматриваться экспертные методы на основе возможного ущерба. Сделан вывод о необходимости развития инструментов автоматизации оценки рисков кибербезопасности при применении инженерных методик расчета cyberPHA, Security PHA Review и других. В академическом плане наиболее приоритетным направлением исследований остается проблема разработки моделей вычисления вероятности наступления рисков кибербезопасности в киберфизических системах.

Ключевые слова: кибербезопасность, комплексная безопасность, оценка рисков, риск-ориентированный подход, киберфизические системы, АСУ ТП.
Для цитирования: ПАРЬЕВ, Сергей Е.; ПРАВИКОВ, Дмитрий И. Правиков; КАРАНТАЕВ, Владимир Г. ОСОБЕННОСТИ ПРИМЕНЕНИЯ РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА ДЛЯ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ОБЪЕКТОВ. Безопасность информационных технологий, [S.l.], v. 27, n. 4, p. 37–52, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1304>. Дата доступа: 20 nov. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.4.04.

Sergey E. Pariev[1], Dmitry I. Pravikov[2], Vladimir G. Karataev[3]
[1]Independent expert, Russia
[2]National University of Oil and Gas «Gubkin University»,
Leninsky av. 65, bd. 1, Moscow, 119991, Russia
[3]Center for Scientific and technical information of the Moscow power engineering Institute (MEI)
17 Krasnokazarmennaya str., Moscow, 111250, Russia
[1]e-mail: sergey.pariev@mail.ru, https://orcid.org/0000-0001-5698-7471
[2]e-mail: dip@gubkin.pro, https://orcid.org/0000-0001-5217-4537
[3]e-mail: vladimir.karantaev@gmail.com, https://orcid.org/0000-0003-1628-7635

Features of the risk-based approach to ensure cyber security of industrial facilities

DOI: http://dx.doi.org/10.26583/bit.2020.4.04

Abstract. We analyze a relationship between the concept of "security" and derived concepts. The objective scientific and practical need for scientific and regulatory consolidation of the term "cybersecurity" is highlighted, and its definition is given. As a result of the analysis of promising approaches to security, the

risk-based approach remains relevant. At the same time, expert methods based on possible damage will be considered as methods for assessing cybersecurity risks in the near future. It is concluded that it is necessary to develop tools for automating cybersecurity risk assessment when using engineering calculation methods cyberPHA, Security PHA Review, and others. In academic terms, the most priority area of research remains the problem of modeling and developing models for calculating the probability of occurrence of cybersecurity risks in cyberphysical systems.
Keywords: cybersecurity, risk assessment, risk-oriented approach, IACS, ICS, cyber physical systems, integrated safety and security.
For citation: PAREVE, Sergey E.; PRAVIKOV, Dmitry I.; KARATAEV, Vladimir G. Features of the risk-based approach to ensure cyber security of industrial facilities IT Security (Russia), [S.l.], v. 27, n. 4, p. 37–52, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1304>. Date accessed: 20 nov. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.4.04.

Введение

В общем случае безопасность можно трактовать достаточно широко и для того, чтобы очертить предмет дальнейшего рассмотрения, сформулируем ряд исходных постулатов.

Объектом исследования выбрана безопасность промышленного объекта, оснащенного средствами автоматизации технологических (например, АСУ ТП) и вспомогательных процессов. Далее такой объект мы будем называть защищаемым объектом. В соответствии с ГОСТ Р 53704-2009 «Системы безопасности комплексные и интегрированные. Общие технические требования» *безопасность защищаемого объекта* – состояние защищенности объекта от угроз причинения ущерба (вреда) жизни или здоровью людей; имуществу физических или юридических лиц; государственному или муниципальному имуществу; техническому состоянию, инфраструктуре жизнеобеспечения; внешнему виду, интерьеру(ам), ландшафтной архитектуре; окружающей природной среде.

Традиционно по отношению к указанным выше составляющим защищаемого объекта, рассматриваемого как социотехническая система, – физическим лицам, имуществу, оборудованию, окружающей среде рассматривались угрозы различного вида (технические сбои; пожары; информационные, химические, бактериологические, радиационные виды воздействий и т.д.), противодействие которым обеспечивал соответствующий «вид безопасности». Вместе с тем, усложнение структуры самих защищаемых объектов, процессов, работу которых они обеспечивают, а также широкое внедрение средств автоматизации и информатизации в различные подсистемы, в том числе в подсистемы обеспечения безопасности, привело к тому, что различные виды безопасности начали тесно переплетаться.

Помимо «видов безопасности», связанных с соответствующим видом угроз (например, пожарная безопасность) используются и «виды безопасности», в которых во главу угла ставится тип защищаемого объекта или вида деятельности. Например, охрана труда (как вид безопасности) нацелена в первую очередь на защиту жизни и здоровья сотрудников предприятия от любых негативных воздействий, а охрана окружающей среды – соответственно на защиту окружающей среды также от любого негативного воздействия. Наличие таких двух групп «видов безопасности», которые по сфере своего применения имеют множественные пересечения, еще больше запутывает картину их взаимосвязей.

В российской научной литературе предлагался подход, определяемый как комплексная безопасность, и описанный, в частности, в [1]. Суть данного подхода можно описать следующим образом. Безопасность современного предприятия, например, предприятия ТЭК рассматривается как комплекс безопасностей: функциональной, производственной, физической, пожарной, химической, информационной и т.д. При этом,

по каждому направлению безопасности на современном предприятии развертывается система, обеспечивающая мониторинг состояния объекта, своевременное выявление предпосылок к нарушению безопасности, обработку событий безопасности (фильтрацию, нормирование, обогащение, реагирование и др.), расследование и ликвидацию последствий, а также своевременное информирование персонала. По отдельным направлениям система безопасности может автоматически включать средства нейтрализации угроз, например, средства пожаротушения. Перечисленные системы, как правило, создаются с использованием программно-аппаратных средств, которые в свою очередь подвержены угрозам информационной безопасности.

Необходимо отметить, что комплексный характер безопасности на более высоком, междисциплинарном уровне рассматривался раньше в других работах, например, [2]. При этом на уровне технической реализации под комплексными системами безопасности, как правило, понимались интегрированные системы пожарной и охранной сигнализации, управления доступом, системы видеонаблюдения и т.п. [3].

Изучение зарубежного опыта, в частности применительно к предприятиям в нефтегазовой отрасли, показывает, что в настоящее время понятие безопасности также начинает носить комплексный характер так, как это было отмечено в [1]. Так, например, на рис. 1 показано, на какие документы опираются методические рекомендации, подготовленные Cisco, Schneider Electric и Aveva, для защиты (в части кибербезопасности) нефте- и газопроводов[1].

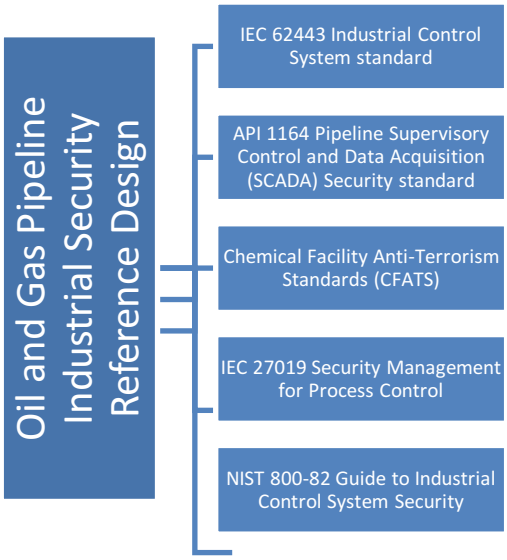

Рис. 1. Методическая основа рекомендаций по безопасности нефте- и газопроводов
(Fig. 1. Methodological basis of recommendation for security of the oil and gas pipe lines)

Осознание факта связанности «отдельных видов безопасности» привело к тому, что стали больше говорить о безопасности «в целом» (или «комплексной безопасности»). По нашему мнению, это понимание получило свое отражение и в последних российских нормативных документах. В частности, можно отметить Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», в названии которого использован именно термин «безопасность», а не «информационная безопасность». В ст. 1 ФЗ-187 при определении целей закона акцент сделан на

[1]URL:https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Oil_and_Gas/Pipeline/SecurityReference/Security-IRD.pdf (accessed: 08.10.2020).

«устойчивости функционирования» объектов критической инфраструктуры как цели обеспечения безопасности, а не на традиционном для информационной безопасности сохранении конфиденциальности, целостности и доступности информации. Это говорит о комплексности охватываемой этим документом проблематики и о возможном желании авторов документа привести рассматриваемые угрозы (т.е. компьютерные атаки) к общему знаменателю с другими видами угроз.

Данный подход разделяется и другими исследователями, которые отмечают, что под критической информационной инфраструктурой понимаются системы, нарушение работы которых приведет к неблагоприятным последствиям, а именно нарушение или остановка деятельности и/или нарушение безопасности информации [4], т.е. негативное воздействие не обязательно связано с воздействием на информацию.

Уточним, что в нашем понимании «устойчивость функционирования» защищаемого объекта – это способность объекта сохранять свои основные функции с заданным качеством (в заданных пределах) под воздействием деструктивных факторов (в частности, под воздействием компьютерных атак). При этом не должно оказываться негативного влияния, выходящего за заранее заданные пределы, на жизнь и здоровье персонала, населения, на окружающую среду и т.д.

В данной статье ограничимся рассмотрением только такого вида негативного воздействия на защищаемый объект как компьютерные атаки, т.е. актов целенаправленного предумышленного или непредумышленного воздействия на информатизированные и (или) автоматизированные подсистемы защищаемого объекта посредством программных и (или) программно-аппаратных средств.

Может показаться, что критериями обеспечения безопасности защищаемого объекта являются такие параметры как количество атак на объект, количество отраженных атак, количество пропущенных атак. Однако они вторичны и, более того, могут давать ложное ощущение защищенности. Основным критерием может быть только нахождение/не нахождение объекта в определенном состоянии (наборе состояний), в котором он способен продолжать функционировать в допустимых пределах (это могут быть, в том числе, и какие-то деградированные состояния), т.е. исполнять свои основные функции с заданным качеством и при этом продолжать обладать способностью отражать, ограничивать и бороться с последствиями воздействия деструктивных факторов.

Исходя из изложенного, дадим определение кибербезопасности защищаемого (промышленного) объекта. Кибербезопасность защищаемого (промышленного) объекта – все аспекты, связанные с определением, достижением и поддержанием состояния безопасности защищаемого объекта, при котором обеспечивается его устойчивое функционирование в условиях проведения в отношении него компьютерных атак.

Необходимо отметить, что приведенное определение весьма сходно с другим определением кибербезопасности, приведенным в [5]: «кибербезопасность – безопасность защищаемого объекта, системы которого функционируют в условиях деструктивных информационных воздействий».

Аналогичный подход к определению кибербезопасности рассматривался в [6]: «Цифровая трансформация промышленного уклада привела к эволюции понятия «информационная безопасность», превратив его в понятие «кибербезопасность», в основе которого лежит не столько обеспечение конфиденциальности, целостности и доступности информации, сколько защита автоматизированных и киберфизических систем от компьютерных атак. Для таких систем сохранение способности к корректному функционированию в условиях киберугроз является приоритетной задачей».

Отличием предлагаемого авторами определения от сформулированных ранее определений кибербезопасности является выделение не только свойства устойчивого функционирования защищаемого объекта, но и состояние его безопасности, а также негативных воздействий на его окружение.

В качестве итогов рассмотрения понятий безопасности их взаимосвязь представлена на рис. 2.

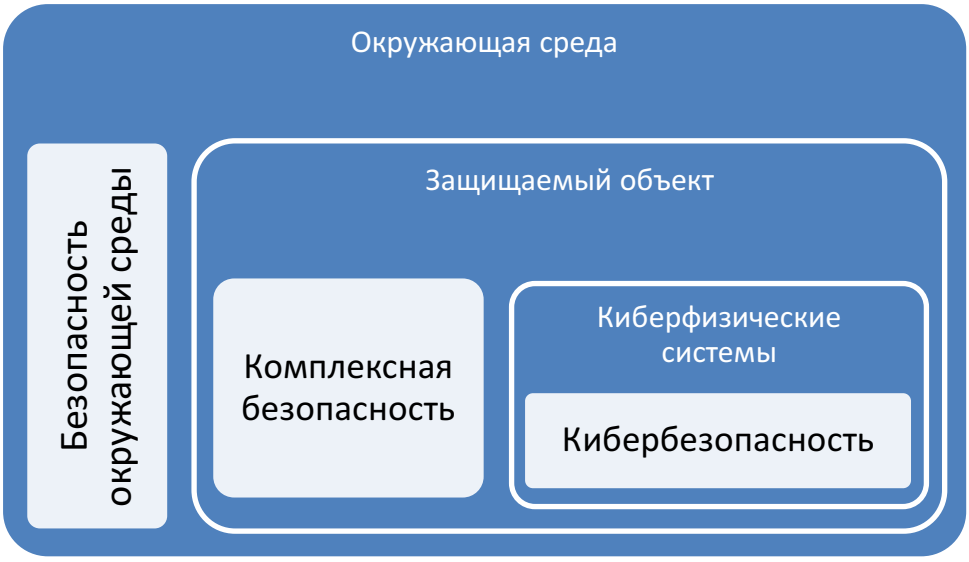

Рис. 2. Взаимосвязь понятий безопасности
(Fig. 2. Interrelation of the notions of security)

1. Риск-ориентированный подход в обеспечении информационной безопасности

Наличие свойства безопасности у защищаемых объектов обуславливает поиск путей достижения (обеспечения) указанного свойства. В качестве наиболее перспективного как за рубежом, так и в Российской Федерации, рассматривается риск-ориентированный подход, давно применяемый для обеспечения различных видов безопасности, в том числе для обеспечения безопасности критической информационной инфраструктуры [7]. Тем не менее, его применение к обеспечению кибербезопасности имеет свои особенности.

Краеугольным камнем риск-ориентированного подхода является оценка рисков, поэтому в последнее время в Российской Федерации начали подниматься вопросы развития методических подходов по оценке рисков кибербезопасности промышленных объектов [8].

Системное обсуждение назрело по целому ряду причин:

- отсутствие официальных методик оценки риска, оценки угроз безопасности информации, а тем более угроз кибербезопасности. Одним из значимых шагов в этом направлении стало Постановление Правительства РФ от 08.02.2018 №127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры …», в котором были введены критерии значимости (фактически это виды негативных последствий, которые относятся как к самому предприятию, так и населению, окружающей среде и государству) и был задан в общем виде процесс выявления и оценки этих критериев, что в целом представляет собой процесс оценки рисков. Однако говорить о готовой методике оценки рисков, конечно, не представляется возможным. В последнее

время начали появляться отдельные отраслевые методики категорирования, но пока они также носят довольно общий характер;

- всё большая зависимость рисков HSE (Health, Safety & Environmental) – зарубежный аналог, покрывающий промышленную безопасность, охрану труда и безопасность окружающей среды, связанную с жизнедеятельностью промышленного объекта) от рисков кибербезопасности, практически никак не отраженная в нормативной и методической базе;
- слабость или полное отсутствие отраслевых методических подходов, которые бы создавали «систему координат» для всех участников процесса: компаний реального сектора экономики, поставщиков решений и услуг, разработчиков средств защиты информации и средств автоматизации промышленных объектов;
- нормативно технические требования, относящиеся к разным видам безопасности не гармонизированы между собой.

Рассматривая методические подходы по оценке рисков кибербезопасности промышленных объектов невозможно обойти стороной обсуждение ряда международных документов:

- IEC 62443-2-1 (2010);
- ISO/IEC 27001 (2013);
- ISA TR84.00.09 (2017).

Необходимо отметить, что семейство стандартов 62443 в русскоязычных научных статьях в основном упоминалось, но детально не анализировалось. Из известных работ можно отметить [9], в которой рассматривались вопросы построения защищенной архитектуры АСУ ТП. За рубежом, очевидно в силу более активного использования, можно отметить руководство по стандарту 62443 [2].

Стандарт ISO/IEC 27001 в русскоязычных научных работах по сравнению с семейством стандартов 62443 рассмотрен более глубоко. В качестве примера можно привести [9]. Из зарубежных источников можно отметить соответствующее руководство по анализу угроз[3].

Стандарт ISA TR84.00.09 в русскоязычных научных источниках практически не упоминается, поэтому его рассмотрение велось на основании материалов, находящихся в открытом доступе[4].

Рассмотрим более детально принципы, заложенные в серию стандартов ISA/IEC 62443. На рис. 3 представлен текущий статус разработки серии стандартов ISA/IEC 62443.

Второй документ серии ISA/IEC 62443 гармонизирован в Российской Федерации в виде национального стандарта ГОСТ Р МЭК 62443-2-1-2015 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 2-1. Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики», который посвящен методическим вопросам построения системы управления кибербезопасностью промышленного объекта (если более точно, то рассматривается не весь промышленный объект, а только его система автоматизации и технологического управления) и базируется на применявшихся ранее

[2]Quick Start Guide: An Overview of the ISA/IEC 62443 Standards. URL: https://gca.isa.org/blog/download-the-new-guide-to-the-isa/iec-62443-cybersecurity-standards (accessed: 31.03.2020).
[3]Cyber-related process hazard analysis. URL: https://www.isa.org/templates/news-detail.aspx?id=160155 (accessed: 31.03.2020).
[4]Cyber Process Hazards Analysis (PHA) to Assess ICS Cybersecurity Risk. URL: https://youtu.be/8oZGYcRDjzc (accessed: 31.03.2020).

стандартах построения систем менеджмента в ИТ системах: ИСО/МЭК 17799 и ИСО/МЭК 27001.

			Название	Дата
Обзор	1-1	TS	Терминология, концепции и модели	2007
	1-2	TR	Основной список терминов и сокращений	
	1-3		Показатели эффективности систем кибербезопасности	
	1-4		Жизненный цикл безопасности и сценарии использования систем промышленной автоматики и контроля (IACS)	
Политика и процедуры	2-1	IS	Создание программы обеспечения безопасности систем промышленной автоматики и контроля (IACS)	2009
	2-2		Основные параметры программ безопасности систем промышленной автоматики и контроля (IACS)	2022
	2-3	TR	Управления обновлениями программного обеспечения (ПО) в среде систем промышленной автоматики и контроля (IACS)	2015
	2-4	IS	Требования к программам безопасности для поставщиков услуг систем промышленной автоматики и контроля (IACS)	2018
	2-5	TR	Руководство по внедрению для владельцев активов систем промышленной автоматики и контроля (IACS)	
Системы	3-1	TR	Технологии безопасности для систем промышленной автоматики и контроля (IACS)	
	3-2	IS	Оценка рисков безопасности, системное разделение и уровни безопасности	2020
	3-3	IS	Требования к безопасности системы и уровни безопасности	2013
Компонент	4-1	IS	Требования к жизненному циклу разработки безопасности продукта	2018
	4-2	IS	Технические требования безопасности для компонентов систем промышленной автоматики и контроля (IACS)	2019

Рис. 3. Статус разработки серии стандартов ISA/IEC 62443
(Fig. 3. Status of development of the standard series IEC 62443)

Стандарт, фактически, фиксирует происходящие перемены, связанные с технологиями, которые находят все более массовое использование во вновь создаваемых и модернизируемых промышленных объектах. Речь идет о, так называемых, готовых коммерческих технологиях (COTS Software – Commercial Off-The-Shelf Software), использование которых сильно повышает риски кибербезопасности.

Согласно стандарту система управления кибербезопасностью (Cyber Security Management System – CSMS) промышленного объекта состоит из элементов, относящихся к трем основным категориям:

- анализ рисков;
- устранение риска при помощи CSMS;
- контроль и усовершенствование CSMS.

В свою очередь категория «анализ рисков» включает:

- экономическое обоснование;
- выявление, классификация и оценка рисков.

В категории «выявление, классификация и оценка рисков» стандарт представляет 14 обобщенных требований к работам, связанным с оценкой рисков. Отмечается, что могут применяться количественные и качественные методы оценки, при этом делается вывод о том, что в виду отсутствия накопленной статистики инцидентов на текущем этапе целесообразно применять качественные (экспертные) методы.

Требования к процессу оценки рисков детализируется в проекте международного стандарта IEC 62443-3-2 ED1 «Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design», принятого в виде окончательного документа в 2020 г.

Место стандартов МЭК 62443-2-1 и МЭК 62443-3-2 в общей иерархии серии IEC 62443 представлено на рис. 4.

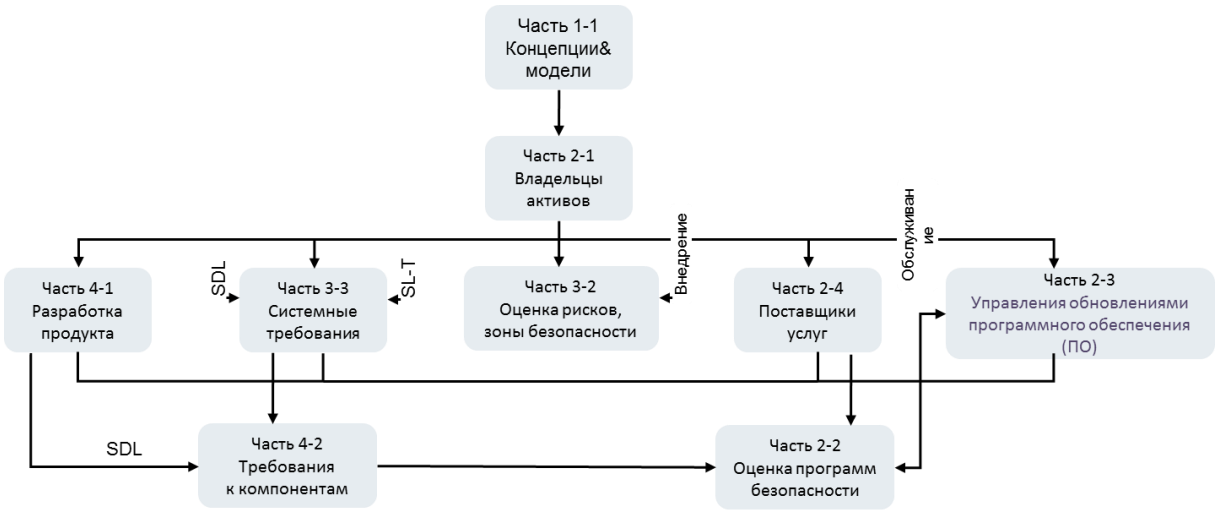

Рис. 4. Общая структура серии стандартов ISA/IEC 62443
(Fig. 4. A structure of the standard series ISA/IEC 62443)

Описание процесса оценки рисков кибербезопасности промышленного объекта приведено на рис. 5.

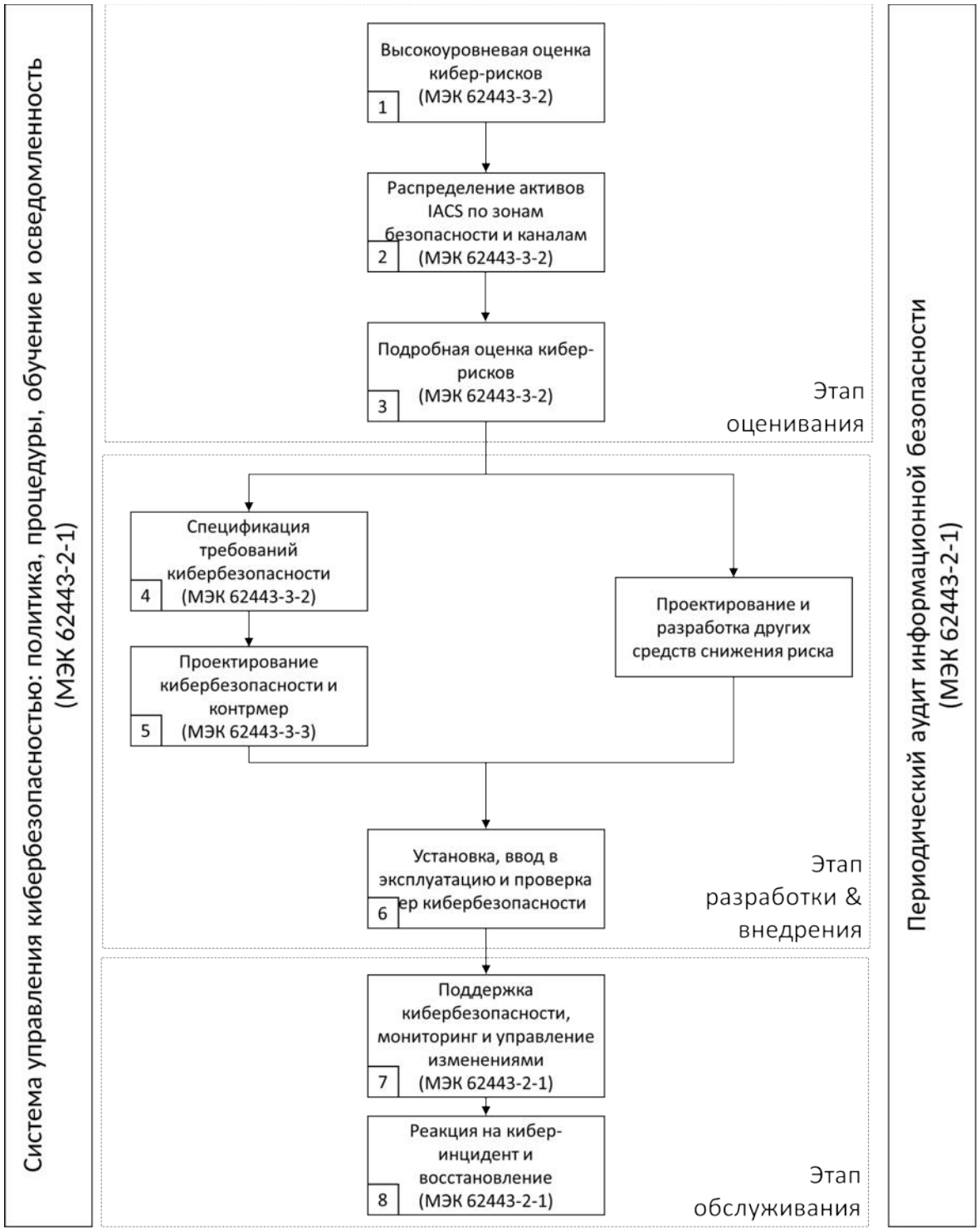

Рис. 5. Процесс оценки рисков кибербезопасности системы автоматизации и технологического управления промышленного объекта ISA/IEC 62443-3-2
(Fig. 5. Process of cybersecurity risk assessment of Industrial Automation and Control System of Industrial object ISA/IEC 62443-3-2)

Подтверждением выше сформулированного тезиса о том, что сообщество специалистов задумалось о «комплексной безопасности» является вектор развития другого международного стандарта IEC 61511.

Вторая редакция IEC 61511-1 (2016) «Functional safety. Safety instrumented systems for the process industry sector. Part 1. Terms, definitions and technical requirements» требует проводить оценку рисков с целью выявления уязвимостей систем противоаварийной защиты (ПАЗ, SIS – Safety Instrumented System). Вместе с тем стандарт не содержит подробных требований по оценке рисков, но п. 8.2.4. содержит ссылки на документы, применение которых позволит реализовать это требование.

Наибольший интерес из них вызывает новая редакция технического отчета ISA TR84.00.09 (2017), который на данный момент является одним из самых полных документов, описывающих реализацию требований по обеспечению кибербезопасности ПАЗ на всех стадиях жизненного цикла систем. Документ ISA TR84.00.09 (2017) содержит положения IEC 62443 и NIST «Cybersecurity Framework». В российском нормативном поле подобных документов, к сожалению, не разработано.

Таким образом, приведенный краткий обзор международных нормативно технических документов позволяет утверждать, что методическая база для оценки HSE-рисков с учетом оценки рисков кибербезопасности сформировалась. Методическая база объединяет как количественные, так и качественные методы анализа. Динамика работы и сформированные планы по развитию международных документов всех типов в ISA и IEC позволяет сделать вывод, что данный методический подход будет развиваться и далее.

2. Пример метода оценки рисков HSE, учитывающего риски кибербезопасности

Можно утверждать, что в международной практике сформировался подход Cyber Process Hazard Analysis (Cyber PHA), основанный на классическом подходе к выявлению, оценке и управлению опасностями технологического процесса – PHA (Process Hazard Analysis), но включающем в себя и аспекты, связанные с рисками кибербезопасности.

Так, например, в рамках одной из ведущих конференций S4[5], проходившей в США в 2017 г. компания aeSolutions представляла этот подход, а в 2018 г. в рамках конференции «Промышленная кибербезопасность: цифровая трансформация – вызовы и возможности»[6] американская компания Kenexis представила еще одну практическую модификацию классического подхода под названием Security PHA Review.

Особый интерес вызывает востребованность данных подходов и соответствующих услуг в реальном секторе экономики, в частности в США. В 2019 г. на форуме ARC Industry Forum, компания Shell представила доклад[7], в котором был представлен практический опыт компании, по совместному применению методик оценки HSSE-рисков (Health, Safety, Security and Environment) традиционными методиками оценки, используемыми в рамках PHA: HAZOP и LOPA и методики оценки рисков кибербезопасности (Security Risk Assessment).

Практическая деятельность компании Shell, основана на реализации положений технического отчета ISA-TR84.00.09. Компания Shell также называет свой подход Cyber PHA, который основан на оценке факторов эскалации, приводящих к нарушению целостности функций безопасности, реализуемых защитными барьерами, в частности ПАЗ

[5]Cyber Process Hazards Analysis (PHA) to Assess ICS Cybersecurity Risk. URL: https://youtu.be/ (accessed: 31.03.2020).
[6]Security PHA review for analyzing process plant vulnerability to cyberattack. URL: https://youtu.be/QnfBRlgBaHg, URL: https://ics.kaspersky.ru/media/ics-conference-2018/Edward-Marszal-Security-PHA-review-for-analyzing-process-plant-vulnerability-to-cyberattack-En.pdf (accessed: 31.03.2020).
[7]Cyber-related process hazard analysis. URL: https://www.isa.org/templates/news-detail.aspx?id=160155 (accessed: 31.03.2020).

(SIS), вследствие возможного наличия актуальных угроз кибербезопасности (сценариев эксплуатации уязвимостей), которые есть или могут быть в программно-аппаратных комплексах применяемых средств автоматизации. В рамках представленного подхода оцениваться не только HSSE риски, но и риски коммерческих потерь (в данной части риски, не связанные с реализаций угроз safety), репутационных потерь, рисков снижения эффективности функционирования защитных барьеров. Данный подход сочетает применение количественных и качественных методов анализа. Для визуализации процесса применяется модель «галстук-бабочка». Пример такой модели представлен на рис. 6.

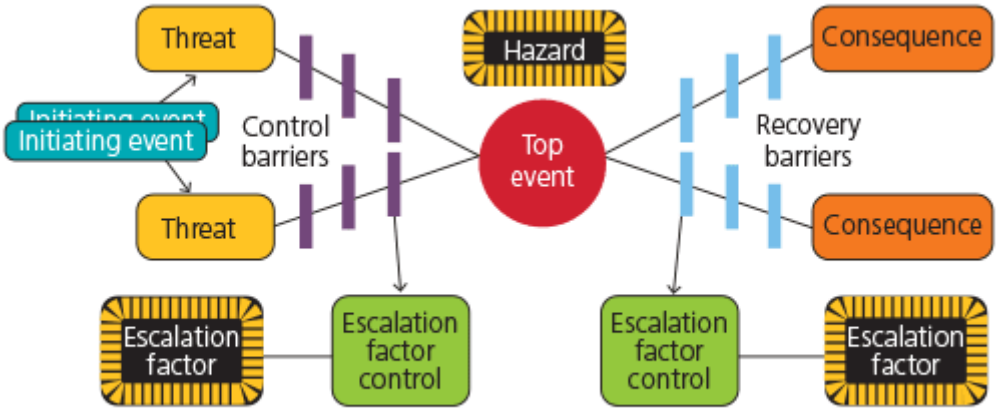

Рис. 6. Модель процесса анализа рисков «галстук-бабочка»
(Fig. 6. Model of the "bow tie" risk analysis process)

3. Проблематика риск-ориентированного подхода

Помимо преимуществ, описанных выше, и, несмотря на достаточную распространенность, накопленный практический опыт позволил выявить также ряд ограничений и недостатков текущих методик применения риск-ориентированного подхода. Ограничения связаны с тем, что в настоящее время информатизация затрагивает практически все основные процессы современного предприятия. В результате возникают сложные цепочки типа: «пожарная безопасность влияет на состояние вычислительной среды, безопасность вычислительной среды влияет на промышленную и, как следствие, экологическую безопасность» и просчитать риски в отдельных ситуациях становится затруднительно. Более того, режим реального времени работы многих функциональных систем и систем их защиты практически отсекает человека от принятия тактических решений, а значит и непосредственного управления рисками.

Одной из проблем применения риск-ориентированного подхода является проблема определения вероятности наступления риска. Вероятность хорошо оценивается для физических детерминированных процессов с более-менее устойчивым распределением вероятности различных событий (например, для физических отказов оборудования). Но определение вероятности для разных типов атак (или использования разного рода технических приемов нарушителем) представляется практически невозможным. Более того, сама постановка такой задачи является некорректной из-за самой природы рисков кибербезопасности. Попытки определения вероятности наступления рисков рассматривались, в частности, в [11].

В настоящее время подходы к определению вероятности наступления определенного события сводятся либо к анализу статистики предыдущих периодов, либо к применению экспертного метода.

Одной из трудностей получения достоверных статистических данных по компьютерным инцидентам является тот факт, что реальные инциденты в промышленных системах в настоящее время сравнительно редки (а большая часть, скорее всего, не замечается, либо приписывается физическим отказам, а то и замалчивается) и собрать даже для однотипных промышленных объектов какую-либо релевантную статистику по реальным инцидентам практически невозможно.

Следует отметить, что после принятия Федерального закона № 116-ФЗ «О промышленной безопасности опасных производственных объектов» в качестве актуальной научной задачи рассматривалась разработка и внедрение в отечественную практику научно обоснованных методов анализа и оценки техногенного риска, позволяющих всесторонне оценить возникновение чрезвычайных ситуаций на опасном производственном объекте. В работе [12] отмечено, что «основная проблема количественного анализа риска опасного производственного объекта на основе методов теории вероятности, математической статистики и др. связана с нахождением частотной оценкой возникновения чрезвычайной ситуации вследствие неопределённости исходных данных».

Даже оставляя за скобками отсутствие в данный момент накопленной и статистически релевантной информации по инцидентам, вероятностный подход имеет и куда более серьезные недостатки. Использование статистики предыдущих периодов подразумевает определенную устойчивость распределения вероятности, причем устойчивость не только во времени, но и по месту (объекту, типу объекта). Предположим, известно, что в мире есть единственная преступная группа, которая на протяжении 10 лет раз в год атакует один из 1000 однотипных защищаемых объектов с использованием эксплойтов в определенном сетевом сервисе. Какова вероятность, что в следующем году выбранный защищаемый объект будет атакован? Ответ не может быть дан на основании данной статистики. Неизвестно на основании чего преступная группа выбирает тот или иной объект (может быть атаки проводятся равновероятно по всему списку, тогда вероятность атаки для выбранного объекта будет 0,001, а может конкуренты каждый год платят за атаку на выбранный объект, тогда вероятность будет равна единице) или тот или иной способ атаки, даже обладая какой-то статистикой за предыдущие периоды.

Еще больше неопределенности в определении вероятности сценария (метода, техники, использования конкретных типов уязвимостей) проведения атаки и наступления соответствующих сценарию рисков. По мнению авторов, говорить, например, о вероятности использования злоумышленником конкретной уязвимости абсолютно некорректно. Даже о вероятности атаки на конкретную подсистему промышленного объекта говорить практически бессмысленно, т.к., если злоумышленник принял решение атаковать промышленный объект, то он проверит все доступные (с учетом ресурсных ограничений) ему способы атаки, пока не придет к необходимому ему результату. В терминах риск-ориентированного подхода это означает, что в общем случае необходимо принимать вероятность осуществления атаки по конкретному сценарию как равной единице.

Экспертный метод в свою очередь имеет как очевидные, так и скрытые от неискушенного взора недостатки. Основным недостатком является субъективизм таких оценок – два разных эксперта в одной и той же ситуации могут дать совершенно разные оценки и привести их к какому-то общему знаменателю не так просто. Кроме того, сейчас не существует объективных способов оценки квалификации самих экспертов, которых в экспертные группы обычно приглашают соответствующие руководители, ориентирующиеся на собственные представления об уровне экспертизы. Менее очевидной проблемой является проблема усреднения экспертных оценок нескольких экспертов из-за

чего крайние (т.е. минимальные и максимальные) значения в такой усредненной оценке будут встречаться существенно реже, чем должны были быть. Также необходимо учитывать психологическую склонность любого человека оценивать вероятность событий, с которыми в реальности он никогда не встречался, меньше, чем тех, с которыми приходилось иметь дело на практике.

Выходом из сложившейся ситуации, на наш взгляд, может быть переход к оценке риска на основе возможного ущерба в результате наступления негативных последствий (что в какой-то степени коррелирует с подходом, приведенном в Постановлении Правительства РФ №127 и новой методике моделирования угроз безопасности информации ФСТЭК России, проект которой в настоящее время стал доступен для публичного обсуждения) без учета вероятности наступления этого события (т.е. в предположении, что вероятность наступления этого события равна единице). Дополнительным фактором ранжирования рисков может служить сложность (например, выраженная в количестве затрачиваемых ресурсов) проведения соответствующей атаки.

Подводя итог можно отметить, что риск-ориентированный подход к управлению кибербезопасностью, несмотря на все его недостатки, в ближайшей перспективе будет применяться за отсутствием других продуктивных подходов.

Как было отмечено выше, обеспечение кибербезопасности является необходимым, но не достаточным условием для обеспечения безопасности защищаемого объекта. Риск-ориентированный подход хорошо себя зарекомендовал для управления разнородными рисками из разных предметных областей. Если посмотреть на историю развития методов обеспечения информационной безопасности, то можно отметить, что используемые концепции принципиально не отбрасывались, а становились частью подходов, приходящих им на смену. Так и сейчас, риск-ориентированный подход еще не исчерпал себя и как существенный элемент общей системы защиты может использоваться в дальнейшем.

Можно также предположить дальнейшее развитие риск-ориентированных подходов. Так, в работе [13] разрабатывается модель угроз для цифровых подстанций для оценки рисков, возникающих в результате кибератак. Более того, есть ряд случаев, например, при управлении высокоавтоматизированным транспортным средством [14], когда риск, выраженный в стоимостном выражении, определяется ситуативно, упрощенного говоря, с транспортным средством какой стоимости произошла авария. В общем случае, для систем промышленной автоматизации как развитие риск-ориентированных подходов в качестве перспективных следует рассматривать подходы, связанные с пониманием и управлением комплексной безопасностью [15].

Заключение

Основной проблемой применения риск-ориентированного подхода является оценка вероятности компьютерных атак. Применение традиционных, основанных на исторических данных, количественных методик оценки рисков кибербезопасности на настоящий момент себя не оправдали в силу самой природы рисков кибербезопасности помноженной на всё увеличивающуюся сложность киберфизических систем. Единственной областью, где достигнуты сколько-нибудь значимые количественные результаты, можно считать только методы сравнительной оценки уязвимостей (например, CVSS 3.1). Как следствие, исходя из принципов риск-ориентированного подхода, вероятность наступления соответствующих событий (т.е. реализации риска) приходится принимать равной единице, а риск – равным ущербу от наступления этого события (точнее его негативных последствий). При этом оценка ущерба проводится на основе экспертных и полуэкспертных методов.

На основе анализа, проведенного в статье, авторы предлагают две группы выводов: первая группа – относится к вопросам практической реализации риск-ориентированного подхода и обеспечения кибербезопасности, вторая – лежит в плоскости развития академических исследований:

- с точки зрения практического применения риск-ориентированного подхода продолжат развиваться и адаптироваться гибридные методы анализа угроз кибербезопасности. То есть подходы, объединяющие методы функциональной (промышленной) и информационной безопасности. Продолжатся попытки перехода к оценке рисков в денежном эквиваленте или других параметрах, оценивающих эффективность и непрерывность ведения бизнеса;
- при условии гармонизации требований серии стандартов МЭК 62443 компании реального сектора экономики с высоким уровнем зрелости процессов управления информационной безопасностью и имеющие опыт практического применения серии стандартов МЭК 27000 начнут использовать предлагаемые методические подходы по оценке и управлению рисками;
- в ближайшей перспективе будут превалировать качественные оценки на основе экспертных мнений;
- потенциалом применения обладают методы теории системного анализа, которые могут позволить добавить объективности экспертным методам оценки;
- возрастает потребность в разработке прикладных информационных систем, позволяющих разрабатывать гибридные модели угроз и (отчасти) автоматизировать процесс оценки рисков.

С академической точки зрения процесс формирования теоретической и методологической базы кибербезопасности социотехнических и киберфизических объектов (и промышленных объектов, имеющих в своем составе системы АСУ ТП, как типичных представителей таких объектов) нельзя признать законченным и исследования должны быть продолжены. До сих пор нет сколько-нибудь значимых онтологий базовых понятий, описывающих все аспекты кибербезопасности промышленного объекта, более того нет онтологий современного состояния как комплексной безопасности, так и, казалось бы, более академически развитой информационной безопасности (за исключением отдельных узких областей).

Учитывая, тот факт, что в ближайшей перспективе экспертные методы оценки будут превалировать, потенциалом обладают исследования в области систем искусственного интеллекта – систем, основанных на знаниях, применение которых позволит масштабировать накапливаемые экспертные знания.

СПИСОК ЛИТЕРАТУРЫ:

1. Гриняев С.Н., Правиков Д.И., Медведев Д.А. Комплексная безопасность ТЭК как объект научного анализа. // Естественные и технические науки № 3/2. 2019. С. 24–30. URL: https://www.elibrary.ru/item.asp?id=38506340 (дата обращения: 08.10.2020).
2. Губайдуллина И.Н., Ковтунова С.Ю. К вопросу обеспечения комплексной безопасности. // Инновационная экономика: перспективы развития и совершенствования № 2 (7). 2015. С. 92–95. URL: https://cyberleninka.ru/article/n/k-voprosu-obespecheniya-kompleksnoy-bezopasnosti (дата обращения: 08.10.2020).
3. Ильин А.П., Мальцев А.В., Мальцев А.С. Анализ современных комплексных систем безопасности // Современные технологии обеспечения гражданской обороны и ликвидации последствий чрезвычайных ситуаций № 1(7). Т. 2. 2016. URL: https://cyberleninka.ru/article/n/analiz-sovremennyh-kompleksnyh-sistem-bezopasnosti. (дата обращения: 08.10.2020).
4. Горелик В.Ю., Безус М.Ю. О безопасности критической информационной инфраструктуры Российской Федерации // student № 9. 2020. С. 1438–1448. URL: https://cyberleninka.ru/article/n/o-bezopasnosti-kriticheskoy-informatsionnoy-infrastruktury-rossiyskoy-federatsii (дата обращения: 08.10.2020).

5. Правиков Д.И., Петухов А.В. Кибербезопасность как новое фундаментальное направление в области информационной безопасности // Вестник современны цифровых технологий № 1. 2019. С. 19–25. URL: https://www.elibrary.ru/item.asp?id=41496052 (дата обращения: 08.10.2020).
6. Лаврова Д.С. Методология предотвращения компьютерных атак на промышленные системы на основе адаптивного прогнозирования и саморегуляции. Диссертация на соискание ученой степени доктора технических наук. – СПбПУ. 2019. URL: https://www.dissercat.com/content/metodologiya-predotvrashcheniya-kompyuternykh-atak-na-promyshlennye-sistemy-na-osnove-adapti (дата обращения: 08.10.2020).
7. Калашников А.О. Управление информационными рисками объектов критической информационной инфраструктуры Российской Федерации // Вопросы кибербезопасности № 3 (4). 2014. С. 35–40. URL: https://cyberleninka.ru/article/n/upravlenie-informatsionnymi-riskami-obektov-kriticheskoy-informatsionnoy-infrastruktury-rossiyskoy-federatsii (дата обращения: 08.10.2020).
8. Колосок И.Н., Гурина Л.А. Оценка рисков кибербезопасности информационно-коммуникационной инфраструктуры интеллектуальной энергетической системы // Информационные и математические технологии в науке и управлении № 2 (14). 2019. С. 40–51. URL: https://cyberleninka.ru/article/n/otsenka-riskov-kiberbezopasnosti-informatsionno-kommunikatsionnoy-infrastruktury-intellektualnoy-energeticheskoy-sistemy (дата обращения: 08.10.2020).
9. Сухих, Ян А.; Правиков, Дмитрий И.; Кузичкин, Алексей А. Разработка защищенных архитектур автоматизированных систем управления технологическими процессами. Безопасность информационных технологий, [S.l.]. Т. 27, № 2. С. 97–117, 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1274 (дата обращения: 08.10.2020). DOI: http://dx.doi.org/10.26583/bit.2020.2.08.
10. Пащенко И.Н., Васильев В.И. Разработка требований к системе защиты информации в интеллектуальной сети Smart Grid на основе стандартов ISO/IEC 27001 и 27005 // Известия Южного федерального университета. Технические науки № 12 (149). 2013. URL: https://cyberleninka.ru/article/n/razrabotka-trebovaniy-k-sisteme-zaschity-informatsii-v-intellektualnoy-seti-smart-grid-na-osnove-standartov-iso-iec-27001-i-27005 (дата обращения: 08.10.2020).
11. Крундышев В.М. Построение безопасных крупномасштабных динамических сетей. // Материалы 29-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 2020. СПб: Изд-во Политехнического университета. С. 5–6. URL: https://www.elibrary.ru/item.asp?id=44017238 (дата обращения: 08.10.2020).
12. Протасов А.В., Вильвер П.Ю. Особенности использования метода индексирования при анализе техногенного риска в России // Вестник Иркутского государственного технического университета. 2011. URL: https://cyberleninka.ru/article/n/osobennosti-ispolzovaniya-metoda-indeksirovaniya-pri-analize-tehnogennogo-riska-v-rossii (дата обращения: 08.10.2020).
13. Карантаев В.Г., Карпенко В.И.. Возможные методы анализа последствий влияния кибератак на системы релейной защиты и автоматики цифровых и высокоавтоматизированных подстанций. // РУМ №3 (593). 2020. С. 4–12.
14. Правиков Д.И., Пономарева Е.А., Куприяновский В.П. Проблемы обеспечения информационной безопасности высокоавтоматизированных транспортных средств. International Journal of Open Information Technologies. Т. 8. № 6. 2020. С. 98–103. URL: http://www.injoit.org/index.php/j1/article/view/949 (дата обращения: 08.10.2020).
15. Правиков Д.И., Щербаков А.Ю., Корнеев Н.В., Тихоненко О.О. Комплексная безопасность систем промышленного оборудования // Вестник современных цифровых технологий № 2.2020. С. 30–35. URL: https://www.elibrary.ru/item.asp?id=42533459 (дата обращения: 08.10.2020).

REFERENCES:

[1] Grinyaev S.N., Pravikov D.I., Mededev D.A. Kompleksnaya bezopasnost` toplivno energeticheskogo kompleksa kak ob`ekt nauchnogo analyza. Estestvennye i technicheskie nauki № 3/2. 2019. S. 24–30. URL: https://www.elibrary.ru/item.asp?id=38506340 (accessed: 08.10.2020) (in Russian).
[2] Gubaidullina I.N., Kovtunova S.U. K voprosu obespecheniya kompleksnoy bezopasnostyю Innovacionnaya economica: perspecrivy razvitiya i sovershenstvovania. № 2 (7). 2015. S. 92–95. URL: https://cyberleninka.ru/article/n/k-voprosu-obespecheniya-kompleksnoy-bezopasnosti (accessed: 08.10.2020) (in Russian).
[3] Il`in A.P., Maltsev A.V., Maltsev A.S. Analyz sovremennykh kompleksnyh system bezopasnosty. Sovremennye tehnologii obespecheniay grazdanskoy oborony I likvidacii posledstvii chrezvychainikh situaciy № 1(7). Vol 2. 2016. URL: https://cyberleninka.ru/article/n/analiz-sovremennyh-kompleksnyh-sistem-bezopasnosti (accessed: 08.10.2020) (in Russian).

[4] Gorelik V.U., Bezus M.U. O bezopasnosti kriticheskoy informacionnoy infrastructury Rossiskoi Federacii. Student № 9. 2020. S. 1438–1448. URL: https://cyberleninka.ru/article/n/o-bezopasnosti-kriticheskoy-informatsionnoy-infrastruktury-rossiyskoy-federatsii (accessed: 08.10.2020) (in Russian).

[5] Pravikov D.I., Petukhov A.V., Kiberbezopasnost` kak novoe fundamental`noye napravleniey v oblasty informacionnoy bezopasnosty. Vestnik sovremennyh cifrovykh tehnologii № 1. 2019. S. 19–25. URL: https://www.elibrary.ru/item.asp?id=41496052 (accessed: 08.10.2020) (in Russian).

[6] Lavrova D.S. Mtodologiya predotvrasheniya komputernykh atak na promyshlennye systemy na osnove analyza adptivnogo prognozirovaniya I samoregulacii. Dissertacia na soiskanie uchenoy stepeni doctora technicheskyh nauk. SPbTU. 2019. URL: https://www.dissercat.com/content/metodologiya-predotvrashcheniya-kompyuternykh-atak-na-promyshlennye-sistemy-na-osnove-adapti (accessed: 08.10.2020) (in Russian).

[7] Kalashnikov A.O. Upravlenie informatsionnimi riskami obektov kriticheskoy informacionnoy infrastructury Rossiskoi Federacii. Voprosy kiberbezopasnosty № 3 (4). 2014. S. 35–40. URL: https://cyberleninka.ru/article/n/upravlenie-informatsionnymi-riskami-obektov-kriticheskoy-informatsionnoy-infrastruktury-rossiyskoy-federatsii (accessed: 08.10.2020) (in Russian).

[8] Kolosok I.N., Gurina L.A. Ocenka riskov kiberezopasnosty informacionno-kommunikacionnoy infrastructury intellectualnoy energeticheskoy systemy. Informacionnye I matematicheskie technologii v nauke I upravlenii. № 2 (14). 2019. S. 40–51. URL: https://cyberleninka.ru/article/n/otsenka-riskov-kiberbezopasnosti-informatsionno-kommunikatsionnoy-infrastruktury-intellektualnoy-energeticheskoy-sistemy (accessed: 08.10.2020) (in Russian).

[9] Sukhikh, Yan A.; Pravikov, Dmitry I.; Kuzichkin, Alexey A. Development of secure architectures for process control systems. IT Security (Russia), [S.l.]. Vol. 27, no. 2. P. 97–117, 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1274. (accessed: 08.10.2020). DOI: http://dx.doi.org/10.26583/bit.2020.2.08 (in Russian).

[10] Pashnko I.N., Vasilyev V.I. Razrabotka trebovaniy k systeme zashity informacii v intellectualnoy sety Smart Grid na osnove standartov ISO/IEC 27001 i 27005. Izvestiay Uznogo federal1nogo universiteta. Technicheskie nauki № 12 (149). 2013. URL: https://cyberleninka.ru/article/n/razrabotka-trebovaniy-k-sisteme-zaschity-informatsii-v-intellektualnoy-seti-smart-grid-na-osnove-standartov-iso-iec-27001-i-27005 (accessed: 08.10.2020) (in Russian).

[11] Krundyhev V.M. Postoyenie bezopasnykrh krupnomashtabnykrh dinamicheslyh setey // Materialy 29 nauchno-technicheskoy konferencii “Metody I tehnicheskie sredstva obespecheniay bezopasnosty informacii”. – 2020. – SPb: Izdatel`svo Polytehnicheskogo universiteta. S. 5– 6. URL: https://www.elibrary.ru/item.asp?id=44017238 (accessed: 08.10.2020) (in Russian).

[12] Protasov A.V., Vil`ver P.U. Osobennosty ispol`zovania metoda indeksirovania pri analyze technogennogo riska v Rossii. Vestnik Irkutskogo gosudarstvennogo tecknicheskogo univeriteta. 2011. URL: https://cyberleninka.ru/article/n/osobennosti-ispolzovaniya-metoda-indeksirovaniya-pri-analize-tehnogennogo-riska-v-rossii (accessed: 08.10.2020) (in Russian).

[13] Karantayev V.G., Karpenko V.I. Vozmoznye metody analyza posledstviy vliyania kiberatak na systemy releynoy zashity i avtomatiky cifrovykh I visokoavtomatizirovannykh podstanciy. RUM №3 (593). 2020. S. 4–12 (accessed: 08.10.2020) (in Russian).

[14] Dmitry Pravikov, Evgeniya Ponomareva, Vasily Kupriyanovsky. Problems of ensuring information security of highly automated vehicles. International Journal of Open Information Technologies. Vol. 8. № 6. 2020. P. 98–103. URL: http://www.injoit.org/index.php/j1/article/view/949 (accessed: 08.10.2020) (in Russian).

[15] Pravikov D.I., Sherbakov A.U., Korneev N.V., Tikhonenko O.O. Kompleksnaya bezopasnost` system promyshlennogo oborudovania. Vestnik sovremennyh cifrovykh tehnologii № 2. 2020. S. 30–35. URL: https://www.elibrary.ru/item.asp?id=42533459 (accessed: 08.10.2020) (in Russian).

Поступила в редакцию – 07 сентября 2020 г. Окончательный вариант – 20 ноября 2020 г.
Received – September 07, 2020. The final version – November 20, 2020