Стандарты кибербезопасности Четвертой промышленной революции и Индустрии 4.0

En **Cybersecurity Standards of the Fourth Industrial Revolution and Industry 4.0**

A. S. Markov,
PhD (Eng., Grand Doctor), Member of Task Group JTC 27 ISO/IEC and Technical Committee 362
a.markov@bmstu.ru

Yu. A. Timofeev,
PhD (Eng.), Member of Task Group JTC 27 ISO/IEC, Vice-Chairman of Interindustry Technical Committee 22
yuritm@gmail.com

The article discusses the transformation of cybersecurity threats and challenges in the industry. The analysis of the conceptual and regulatory documents of the German industrial initiative – Industrie 4.0 Platform – is presented. The organizational and technical safety measures of Industrie 4.0 industrial facilities are shown. A comparison is given with the state of standardization of innovative industrial technologies in Russia. The need to harmonize Russian standards through industrial automation systems, information security management systems and it technology safety assessments is justified.

Keywords: cybersecurity, IT-security, industrial IoT security, Industrie 4.0 platform, Industry 4.0, RAMI 4.0

В статье рассмотрены вопросы трансформации угроз и вызовов кибербезопасности в промышленности. Представлен анализ концептуальных и нормативных документов немецкой инициативы – Платформы Industrie 4.0. Показаны организационно-технические меры безопасности промышленных объектов Industrie 4.0. Приведено сравнение с состоянием стандартизации инновационных промышленных технологий в России. Обоснована необходимость гармонизации российских стандартов по линии промышленных систем автоматизации, систем менеджмента информационной безопасности и оценки безопасности продукции ИТ-технологий.

Ключевые слова: информационная безопасность, промышленная безопасность, безопасное производство, платформа Industrie 4.0, Индустрия 4.0, RAMI 4.0

Алексей Сергеевич Марков,
доктор технических наук, член рабочей группы JTC 27 ISO/IEC, член ТК-362
a.markov@bmstu.ru

Юрий Андреевич Тимофеев,
кандидат технических наук, член рабочей группы JTC 27 ISO/IEC, заместитель председателя МТК-22
yuritm@gmail.com

1. Введение

Всемирный экономический форум (ВЭФ, WEF), объединивший в Давосе экономические структуры 70 стран, последние годы проходит под флагом Четвертой промышленной революции (4ПР). В рамках текущей зимней сессии ВЭФ основные дискуссии о 4ПР были сосредоточены на следующих глобальных проблемах:

- этика искусственного интеллекта;
- апробация ИТ-приложений в рамках борьбы с пандемией;
- кибербезопасность и «киберпандемия»;
- цифровое неравенство;
- выбросы углерода.

Как видно, напрямую или косвенно вопросы кибербезопасности неотрывно сопровождают период осмысления наступающей 4ПР. Актуальность тематики обусловливает статистика экономического форума: в период пандемии число кибератак и их последствий значительно возросло, а потенциальный ущерб на следующий год оценивается в 8 трлн долл[1].

Область нормативного регулирования кибербезопасности именно 4ПР в международном плане находится на начальном этапе, в то же время летописец новой экономической формации – Германия – уже завершила две «пятилетки», что мы рассмотрим в данной работе, отчасти – в сравнении с российской ситуацией.

[1] *Что, для сравнения, превышает 250 ВВП одной прибалтийской республики.*

2. Понятийный аппарат

Согласно ВЭФ (2015 год), понятие ***Четвертой промышленной революции*** (*Fourth Industrial Revolution*) предусматривает глобальное внедрение и объединение интернет/киберфизических систем и цифровизации производства, которое приведет, как ожидается, к масштабным изменения жизненного уклада человечества (в экономических, политических, социальных, личностных и иных сферах) в результате трансформации физического и виртуального мира [1].

Как известно, причинами указанной глобальной трансформации послужили всеобщая *связность* (доступный Интернет) и *интеллектуализация* устройств, что, в свою очередь, обусловило внедрение интеллектуальных систем (умные города» умные фабрики и пр.), создающих новый мир технологических возможностей и услуг [1, 2].

Полагается, что именно конвергенция и синтез ИТ- и ОТ-технологий в сочетании с итерационным интеллектуальным анализом больших неструктурированных интернет-данных (с целью перманентной генерации знаний) приведут к технологической сингулярности (гиперрадикальным изменениям) нескольких высокоиндустриальных стран относительно всего оставшегося мира.

По данной тематике существует достаточно много публикаций (например, [3–11]), однако терминология 4ПР еще находится на стадии дискуссии, главным образом, в рамках проведения очередных сессий ВЭФ.

По мнению авторов, следует понимать отличие 4ПР от ее технологических сегментов.

Так, ***Индустрия 4.0*** (Industry 4.0, I4.0) – промышленная составляющая 4ПР, целью которой является получение максимальной выгоды (добавленной стоимости) предприятия нового типа. Именно исходя из получения максимально возможной прибыли, согласно концепции I4.0, оценивается эффективность всех бизнес-процессов и адаптируются бизнес-модели предприятия. Не является исключением и менеджмент информационной безопасности, который также должен способствовать добавленной стоимости. В литературе часто I4.0 употребляют как синоним 4ПР в самом узком его смысле («умное производство»).

Платформа Industrie 4.0 – *национальная инициатива Германии по созданию и внедрению производств нового поколения с целью глобального конкурентного преимущества* (термин был введен еще в 2011 году). Данная инициатива ввела ныне широко употребляемое понятие «смарт», изначально являвшееся аббревиатурой – SMART (*Sustainable Manufacturing and Advanced Robotic Technologies*), то есть устойчивое производство и передовые роботизированные технологии, которое ныне утеряло свой первоначальный смысл вследствие популизма. По заявлениям ряда немецких специалистов, данная инициатива позволила Германии по уровню роботизации и автоматизации промышленности обогнать США на два года. Что касается кибербезопасности, то все исследования по данной тематике, согласно Industrie 4.0, должны проводиться исключительно для повышения конкурентоспособности Германии.

Следует отметить, что вопросы кибербезопасности пронизывают концепцию передового производства – I4.0. На первых обсуждениях ВЭФ кибербезопасность выделялась даже в отдельную прорывную (*disruptive*) технологию I4.0 (рис. 1); позже – в 2020 году – тематика кибербезопасности была обозначена в числе пяти глобальных рисков мировой экономики.

Что касается понятия ***кибербезопасности I4.0***, то его трактуют в узком и широком смыслах

Так, в первом случае под кибербезопасностью I4.0 понимают защищенность промышленных киберфизических систем (ИКФС, IIoT) от кибератак (*Industrial IoT Security*).

Согласно указанному определению, в сферу кибербезопасности I4.0 попадают безопасность проводных сенсорных сетей (WSN), межмашинных систем (M2M), больших данных, облачных сервисов и интеллектуальных приложений, а также систем радиочастотной идентификации (RFID). Вопросы защиты ресурсов касаются, соответственно, следующих этапов: слияния датчиков (сбор данных с помощью промышленных сенсоров), интеллектуального анализа и визуализации (поддерживается индустриальным облаком для управления огромными объемами данных) и интеграции в промышленные системы нового поколения (аддитивное производство, автономные роботы, цифровое проектирование и имитационное моделирование и др.).

В широком смысле (по аналогии с ISO/IEC 27032 [12]) кибербезопасность I4.0 представляет собой комбинацию свойств (состояний защищенности) целостности, доступности и конфиденциальности ресурсов в новой глобальной интегрированной киберпромышленной среде. В качестве угроз обычно указывают три класса: саботаж, шпионаж или манипуляции. Становление данного понятия связано с внедрением КФС и интернет-вещей, персональных гаджетов, их глобальной связностью (Интернет), а также гиперсложностью программ. Указанное обусловило рост технологических рисков, рост рисков приватности, а также эволюцию целенаправленных атак на КИИ и др. (рис. 2).

Основные аспекты кибербезопасности в рамках 4ПР можно свести к следующим:

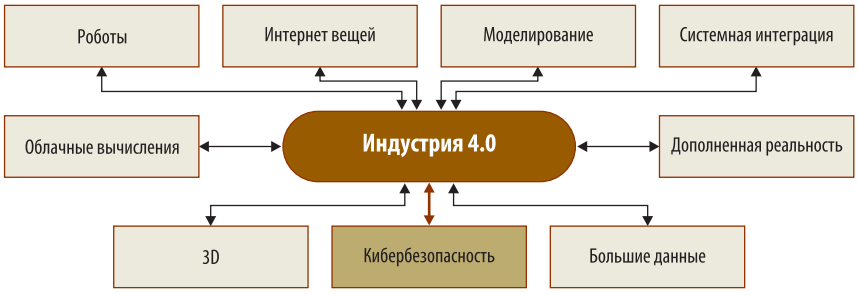

Рис. 1. ***Прорывные технологии Индустрии 4.0***

Рис. 2. ***Вызовы Индустрии 4.0 и их причины***

1) обеспечение безопасности ~~информации~~ в АСУ ТП (или объектов КИИ);

2) использование новых технологий для повышения безопасности объектов;

3) предотвращение компрометации систем защиты в условиях новых технологий.

Что касается использования новых технологий для повышения уровня кибербезосности, то в первую очередь отмечают системы искусственного интеллекта (ИИ), приложения квантовых вычислений, системы распределенного реестра, разного рода централизованные ИТ/ИБ-решения. Например, использование ИИ открывает совершенно новые возможности при обнаружении кибератак и нарушений, выявлении вредоносного кода, проверке программ на недекларированные возможности, создание новых направлений в криптографии (например, состязательной криптографии) и др.

В то же время, налицо новые угрозы и вызовы. Например, внедрение ИКФС элементарно создает дополнительные точки компрометации (несанкционированного перехвата данных, удаленного контроля или деструктивного воздействия) устройств. Однако системы ИИ уже порождают угрозы нового семантического типа, касающиеся изучения поведения средств защиты информации, в частности IDS/IPS. Другой пример представляют квантовые компьютеры, способные в перспективе решать большие задачи на почти бесконечных скоростях; соответственно, они могут представлять экзистенциальную угрозу для современных методов шифрования.

Примеры технологий кибербезопасности I4.0 приведены в табл. 1.

Нет смысла перечислять интуитивно понятные угрозы в отношении производственных систем нового поколения (Smart-X): к примеру, они подробно приведены в литературе, например в [2, 13]. Следует лишь сделать вывод о трансформации перечня угроз I4.0, а именно:

- состав угроз Третьей промышленной революции (и I3.0) в той или иной степени остался неизменным;
- векторы атак стали более совершенными, например, APT-атаки на КФС и цепи поставок [14];
- появился новый класс угроз, связанных с ИИ (противоборство с СЗИ) и квантовыми вычислениями (компрометация перебором).

Таким образом, полагаясь на актуальные угрозы I4.0 и соответствующие им контрмеры, целесообразно перейти к обзору тематических стандартов как основы технического регулирования отрасли (рис. 3).

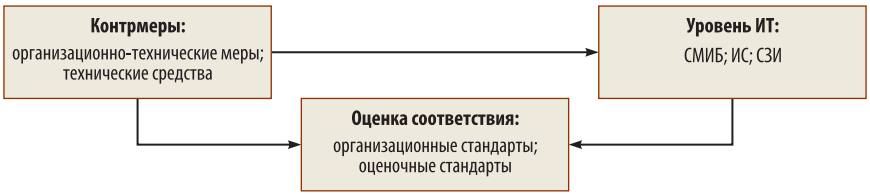

Рис. 3. ***Концептуальная схема формирования стандартов***

Как указывалось выше, темпы по унификации, стандартизации и сертификации в области 4ПР задает Германия, которая является уверенным наукоемким лидером на Западе (согласно IFR, по уровню концентрации роботов опережает Иран в 300 раз, а США – почти в два). Таким образом, имеет смысл привести сравнительный анализ на примере нормативной базы индустриальной платформы Германии[2].

3. Платформа Indusrtie 4.0 как пример стандартизации в области промышленной информационной и кибербезопасности

Сразу оговоримся, что тематика безопасности из-за особенностей немецкого языка имеет чуть более общий вид, так как безопасность по-немецки (*Sicherheit*) – это сохранность, функциональная надежность и информационная безопасность, которую также подразделяют на ИТ-безопасность и кибербезопасность («наступательную» безопасность). Однако в документах Industrie 4.0 подчеркивается, что в период 4ПР акцент делается именно на кибератаки, противодействие которым существенно осложняется с появлением новых высокоинтеллектуальных технологий, к примеру противоборствующих систем ИИ [15]. В связи с этим ниже авторы ограничатся общим термином «безопасность».

Нормативно-методическую базу безопасности Indusrtie 4.0 составляют технические публикации (их более 25, а по смежным тематикам – более 150), представленные на web-портале plattform-i40.de, который ор-

Таблица 1. ***Примеры новых технологий в области кибербезопасности***

Новые технологии кибербезопасности	Новые технологии, позволяющие решать текущие проблемы	Новые технологии, создающие угрозы
• Квантовые вычисления (перебор, связь) • Распределенные реестры (Blockchain) • Облачные вычисления • Виртуализация и контейнеризация	• Квантовые вычисления (безопасность связи) • ИИ ≡ Машинное обучение (автоматизация сервисов безопасности) • Big data ⇒ Smart data (обеспечение принятия решений)	• IIoT (IoT, WoT, IoS, IoD) • Автономные роботы и автоматические системы • Интеграция (горизонтальная, вертикальная) • ИИ (генеративно-состязательная сеть)

[2] *http://www.plattform-i40.de/.*

ганизован под эгидой Федерального министерства экономики и энергетики Германии и Федерального министерства образования и науки Германии, а также на web-сайте Союза машиностроителей Германии (industrialsecurity.vdma.org) [16].

Наиболее интересные документы, по мнению авторов, приведены в табл. 2.

Обзор представленных документов позволяет выделить ключевые принципы безопасности Industrie 4.0:

1) архитектурные решения Industrie 4.0 опираются на эталонную 3D-модель RAMI 4.0 (Reference Architecture Model for Industrie 4.0) (рис. 4);

2) объектами защиты выступают производственные объекты как носители информации;

3) документы придерживаются системного подхода к безопасности, а именно:

- проблематика безопасности затрагивает различные свойства ее систем, как-то: сохранность, защищенность программно-аппаратных ресурсов, персональных данных и знаний (Safety, Security, Privacy and Knowledge Protection) с приоритезацией целостности процессов и ресурсов;
- безопасность рассматривается как часть доверия (Trustworthiness) к Industrie 4.0 (на всех этапах цепочки создания добавленной стоимости);
- выделяются два сегмента безопасности: безопасность КФС и интернет-безопасность (Cyber-Physical Systems & Internet Technology Security);
- по уровню преднамеренности (и сложности противодействия) выделяются IT-Security и Cybersecurity;
- детально разбираются актуальные угрозы и атаки на цепи поставки.

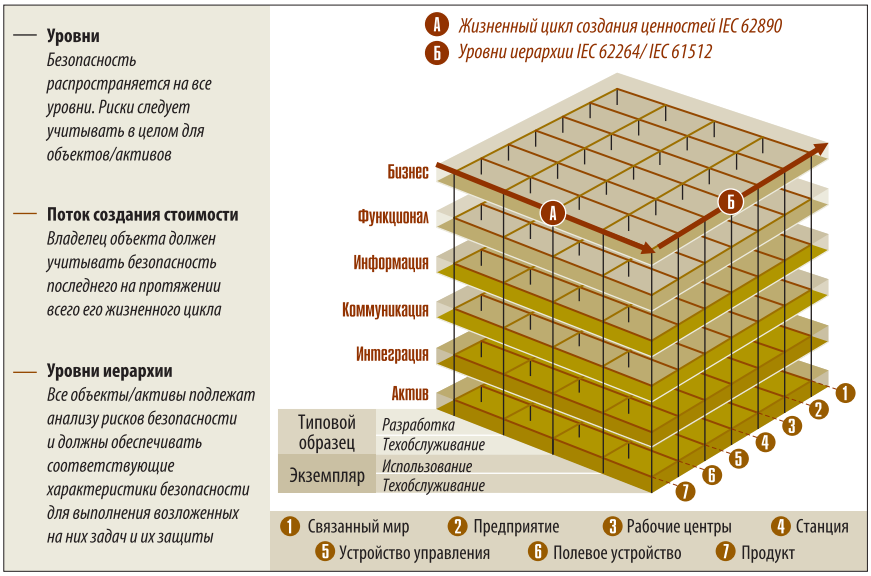

*Рис. 4. **Эталонная 3D-модель Industrie 4.0***

4. Технические документы (в соответствии с Немецким законом об информационной безопасности, а также логикой интеграции) соответствуют стандартам европейского происхождения, а именно, IEC и ISO.

Собственно, рис. 4 еще раз подтверждает востребованность процедур безопасности.

Анализ руководящих документов позволяет сделать вывод, что

Таблица 2. Примеры технических публикаций по тематике безопасности Indusrtie 4.0

Название документа	Целевая направленность
Access control for Industrie 4.0 components for application by manufacturers, operators and integrators. Discussion paper. Berlin: BMWi, 2019, 50 p.	• Обоснование использования RBAC и ABAC; • рекомендации по внедрению ABAC
Artificial Intelligence (AI) in Security Aspects of Industrie 4.0. Result paper. Berlin: BMWi, 2019, 32 p.	• Раскрытие проблематики безопасности систем ИИ; • описание новых классов ИИ-атак; • краткие рекомендации
Blockchain and the law in the context of Industrie 4.0. Working paper. Berlin: BMWi, 2019, 32 p.	• Описание правовых ограничений применения Blockchain; • краткие рекомендации по использованию Blockchain
Industrie 4.0 security in vocational and advanced training. New issues for business organisation and expertise. Working paper. Berlin: BMWi, 2016, 20 p.	Компетенции специалистов по безопасности
Integrity of Data, Systems and Processes as the Core Element of Networking and Digitalization. Discussion paper. Berlin: BMWi, 2018, 24 p.	• Обоснование соблюдения правильности, полноты и целостности данных, систем и процессов; • требования к участникам
IT Security in Industrie 4.0. Action fields for operators Berlin: BMWi, 2016, 52 p.	Изложение контрмер: СМИБ и риск-менеджмент, сегментирование, управление инцидентами, безопасность производства программ, безопасность приобретения, справочники и стандарты
IT security in Industrie 4.0. First steps towards secure production. Guideline. Berlin: BMWi, 2019, 6 p.	Краткие рекомендации
Leitfaden Industrie 4.0 Security. Handlungsempfehlungen für den Mittelstand. Frankfurt am Main: VDMA, 47 p.	Организационно-технические меры
Secure Communication for Industrie 4.0. Discussion paper. Berlin: BMWi, 2016, 24 p.	Базовая схема и протоколы коммуникации
Security in RAMI4.0. Guidline. Berlin: BMWi, 2016, 4 p.	Эталонная архитектурная модель
Technical Overview: Secure Identities. Working paper. Berlin: BMWi, 2016, 28 p.	Требования и рекомендации по идентификаторам/аутентификаторам

безопасность Industrie 4.0 опирается на нормативно-методический аппарат трех базовых международных стандартов (рис. 5):

- ISA/IEC 62443 – линейка стандартов по безопасности для промышленных систем автоматизации и управления;
- ISO/IEC 27xxx – серия стандартов по менеджменту информационной безопасности;
- ISO/IEC 15408 – линейка стандартов по критериям оценки ИТ-безопасности.

При этом, конечно, максимально используются международные стандарты и нормы по смежным и частным подсистемам безопасности, а именно:

- ISO/IEC 25000 – требования и оценка качества систем и программного обеспечения;
- ISO/IEC 15459, 29003, 29115, 29146, 29191 и IEC 24760-1 – ряд стандартов по подсистемам идентификации, аутентификации и авторизации;
- IEC 61512 и 62890 – стандарты по управлению серийным производством и по управлению жизненным циклом производственных систем (в части обоснования эталонной модели RAMI 4.0).

Следует заметить, что, опираясь на организационно-технические меры ISO/IEC 27001, технические документы Industrie 4.0 детализируют их (собственно, что и требует ISO/IEC 27001.) К примеру, руководящий документ Leitfaden Industrie 4.0 Security (см. табл. 2) включает 17 организационно-технических мер безопасности Industrie 4.0 (рис. 6), технический документ Integrity of Data, Systems and Processes as the Core Element of Networking and Digitalization – 13 мер по обеспечению целостности, а IT Security in Industrie 4.0 – 15 мер по безопасности приобретения.

Любопытно сравнить базовые контрмеры (см. рис. 6) с мерами, приведенными в приказе ФСТЭК России по защите значимых объектов критической информационной инфраструктуры нашей страны (по иронии судьбы число их совпадает – 17 классов). Очевидно, что приказ ФСТЭК России, по сути, зеркалирует к ISO/IEC 27000, в то время как рассматриваемый документ детализирует его относительно производственных предприятий Германии.

В связи с последним утверждением, кратко рассмотрим соотношение международной стандартизации в области информационной и кибербезопасности 4ПР и аналогичного сегмента «Цифровой России».

4. Международные и российские стандарты в области информационной и кибербезопасности Четвертой промышленной революции

В соответствии с рис. 5, рассмотрим соотношение стандартов по безопасности промышленных систем, систем менеджмента информационной безопасности и оценки безопасности продукции ИТ-технологий.

1. Что касается безопасности систем промышленной автоматизации и управления, то в нашей стране актуальны четыре стандарта:

- ГОСТ Р 56205-2014 (аналог IEC/TS 62443-1-1: 2009);
- ГОСТ Р МЭК 62443-2-1-2015 (IEC 62443-2-1: 2010);
- ГОСТ Р 56498-2015 (IEC/PAS 62443-3: 2008);
- ГОСТ Р МЭК 62443-3-3-2016 (IEC 62443-3-3: 2013).

Это означает, что 11 актуальных стандартов линейки IEC 62443 не переведены на русский язык.

2. Если обратиться к организационным стандартам серии 27000, то на начало ~~лета~~ на портале iso.org представлено 84 документа, на gost.ru – 21.

Конечно, количество стандартов не является исключительным показателем, более того, сегодня в нашей стране организационно-технические меры к промышленным системам определены в известных приказах ФСТЭК России. Однако, при всей

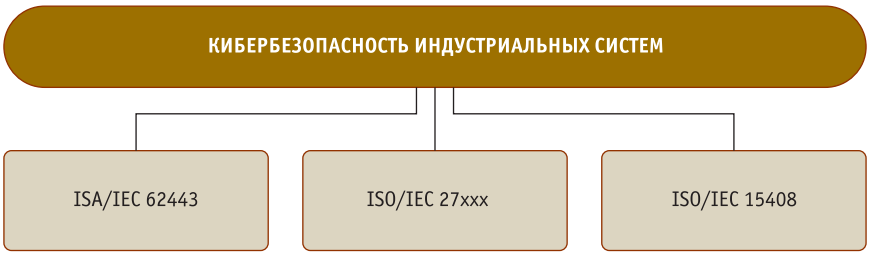

Рис. 5. ***Базовые линейки стандартов Industrie 4.0***

Рис. 6. ***Базовые меры по защите объектов Industrie 4.0***

прогрессивности отечественных нормативно-методических документов, надо понимать уровень критического анализа и выделяемых ресурсов на международную стандартизацию. К примеру, по опыту авторов, в обсуждении стандартов ISO активно участвуют профессионалы из 100 стран. И метаданные обсуждаемых международных стандартов ISO/IEC серии 27000 говорят сами за себя, например: cloud computing (ISO/IEC 27017), application security (27034), supplier relationships (27036), big data security (27045), cloud services (27071), IoT security and privacy (27402), smart cities (27570) и т. д.

В табл. 3 приведены примеры стандартов, которые активно обсуждаются в Евросоюзе и мировом сообществе, но никак не представлены (пока) в нашей стране.

В табл. 4 приведены примеры инновационных стандартов по тематике 4ПР и I4.0, разрабатываемые международной организацией по стандартизации за рамками серии 27000, но также отсутствующих в нашей стране.

Справедливости ради следует сообщить, что в этом году в рамках реализации задач национальной программы «Цифровая экономика РФ» МТК-22 предполагает выпустить на русском языке более 20 новых стандартов ИСО/МЭК (и в основном по тематике менеджмента ИБ).

3. Что касается оценки соответствия ИТ-продукции (средств защиты информации), то международное сообщество завершило четвертую итерацию совершенствования документов линейки «Общих критериев» (релевантных линейке стандартов ISO/IEC 15408 1, 2, 3, 4, 5 – *Information security, cybersecurity and privacy protection – Evaluation criteria for IT security*). Все индустриальные страны, разумеется, де-юре или де-факто придерживаются метастандарта для формирования нормативных документов к продукции (профилей защиты и заданий по безопасности). Несмотря на то, что Россия находится вне международного тренда (даже не является подписчиком), все-таки, благодаря активности ТК-362, накоплен богатый опыт разработки внутрироссийских профилей защиты и проведения соответствующих сертификационных испытаний, а некоторые идеи (требования доверия) задействованы при подготовке современных НПА ФСТЭК России.

Таким образом, сравнительный анализ говорит, что в нашей стране имеется определенный задел по всем направлениям стандартизации технологий кибербезопасности 4ПР и I4.0, но, в то же время, есть моменты, которым следует уделить внимание (рис. 7). Учитывая гиперактивность международного сообщества по стандартизации, видимо, Россия на текущей итерации индустриального развития вынуждена придерживаться ассиметричного подхода: воспринимая международную нормативно-методическую базу, детализировать ее применительно к отечественным индустриальным решениям.

Таблица 3. ***Примеры инновационных стандартов серии 27000***

Прорывные технологии 4ПР и I4.0	ISO/IEC	ENISA[3]
IoT	ISO/IEC 27030 – IT – Security techniques – Guidelines for security and privacy in Internet of Things (IoT) [проект]	ENISA: Baseline Security Recommendations for IoT
Cloud Computing	ISO/IEC 27017:2015 IT – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services; ISO/IEC 27036-4 IT. Security techniques – information security for supplier relationships – Part 4: Guidelines for security of cloud services [на стадии разработки]	ENISA: • Cloud and Big Data; • Cloud Security; • Cloud Computing Security; • Security Framework for Governmental Clouds
Big Data	ISO/IEC WD 27045 Information technology – Big data security and privacy – Processes [на стадии разработки]	ENISA: • Big Data Security; • Good Practices and Recommendations on the Security of Big Data Systems
Smart-X	SO/IEC CD TS 27570.2 IT – Security techniques – privacy guidelines for smart cities [на стадии разработки]	—

Таблица 4. ***Примеры стандартов, затрагивающих тематику безопасности 4ПР***

Прорывные технологии 4ПР и I4.0	ISO или IEC
Blockchain	ISO/CD TR 23245 Blockchain and distributed ledger technologies – security risks, threats and vulnerabilities [на стадии разработки]
Artificial intelligence	ISO/IEC CD 22989 Artificial intelligence – concepts and terminology [на стадии разработки]
Quantum computing	ISO/IEC WD 23837 IT security techniques – Security requirements, test and evaluation methods for quantum key distribution [на стадии разработки]
Cyber-physically	ISO/AWI 23704 Reference model for cyber-physically controlled smart machine tool systems (CPSMT) [на стадии разработки]

[3] *European Union Agency for Cybersecurity.*

Рис. 7. ***Соотношение стандартов и норм по тематике 4ПР***

5. Заключение

Цель представленной работы состояла, главным образом, в кратком информировании читателя о состоянии стандартизации перспективных технологий в области кибербезопасности на примере технологического лидера Четвертой промышленной революции – Германии.

При этом можно сделать ~~ряд~~ 1 вытекающих друг из друга утверждений:

1. Технологии кибербезопасности оказывают существенное влияние на различные стороны производственной и общественной деятельности, а ряд из них (например, квантовые вычисления и технологии ИИ) инициирует глобальные вызовы для всех стран. Очевидно, что регулирование этой ситуации требует проведения исключительно грамотного, ответственного и комплексного подхода в области стандартизации по указанной тематике [17].

2. Платформа Industrie 4.0 как лидирующее мировое индустриальное движение придерживается международных стандартов европейского происхождения (IEC, IEC) и активно инициирует развитие новых норм с учетом полномасштабного критического анализа.

При этом можно выделить три направления стандартизации кибербезопасности Industrie 4.0:

- современные аспекты промышленной безопасности;
- меры информационной безопасности, кибербезопасности и защиты персональных данных;
- критерии оценки ИТ-продукции.

В свою очередь, немецкая платформа Industrie 4.0 активно поддерживает собственные концептуальные технические документы информативного плана, позволяющие обсуждать генеральные направления во избежание стратегических и проектных ошибок, а с другой стороны, разрабатывает методические документы, уточняющие международные стандарты согласно специфике немецкой индустрии.

3. В настоящее время Германия проводит гармонизацию своих норм и моделей с рядом индустриальных стран, в первую очередь, разумеется, с Китаем. Этой тематике посвящен уже почти десяток документов. Любознательный читатель может ознакомиться с ними на web-портале Industrie 4.0. Возможно, это следует учесть при решении тематических международных вопросов отечественной инициативы «Цифровая экономика России» в части информационной безопасности.

4. Анализ нормативно-методической базы России в области информационной безопасности позволяет сделать вывод о возможности наметить точки соприкосновения с передовыми индустриальными странами в случае сотрудничества или же определить свой путь развития (с учетом политических аспектов), понимая какие технологии наиболее востребованы в мире (судя по гиперактивной работе зарубежных технических комитетов) и работая только на опережение. ■

ЛИТЕРАТУРА

1. Шваб К. Технологии четвертой промышленной революции. – М.: Эксмо. – 2018. – 320 с.

2. Шваб К. Четвертая промышленная революция. – М: Эксмо. – 2016. – 208 с.

3. Артамонов В. А., Артамонова Е. В. Цифровая трансформация экономики как предвестник 4-й промышленной революции // Защита информации. Инсайд. – 2019. – № 3. – С. 2–10.

4. Зегжда Д. П., Васильев Ю. С., Полтавцева М. А., Кефели И. Ф., Боровков А. И. Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации // Вопросы кибербезопасности. – 2018. – № 2 (26). – С. 2–15.

5. Корнеев Н. В., Меркулов В. Д. Интеллектуальная аналитика в обеспечении защищенности от комплексных угроз // В сб.: Безопасные информационные технологии. Сборник трудов Десятой международной научно-технической конференции. – 2019. – С. 215–219.

6. Массель Л. В., Воропай Н. И., Сендеров С. М., Массель А. Г. Киберопасность как одна из стратегических угроз энергетической безопасности России // Вопросы кибербезопасности. – 2016. – № 4 (17) . – С. 2–10.

7. Петренко С. А., Олифиров А. В., Маковейчук К. А. Метод повышения киберустойчивости цифровой экономики // В сб.: Финансово-экономическое и информационное обеспечение инновационного развития региона в Ялте. Посвящается 75-летию Гуманитарно-педагогической академии (филиал) ФГАОУ ВО «КФУ им. В. И. Вернадского». – 2019. – С. 412–418.

8. Петренко С. А. Киберустойчивость систем Индустрии 4.0 // Защита информации. Инсайд. – 2019. – № 3 (87). – С. 6–15.

9. Dakhnovich A. D., Moskvin D. A., Zegzhda D. P. An Approach to Building Cyber-Resistant Interactions in the Industrial Internet of Things // Automatic Control and Computer Sciences. 2019. V. 53, № 8. P. 948–953.

10. Petrenko S. La Administraciyn de la Ciberseguridad. Industria 4.0. Publicado segъn la decisiyn del consejo de redacciyn de la Universidad de Innopolis. Universidad de Oviedo, Universidad de Innopolis. Oviedo, Asturias. 2019. 294 p.

11. Shaping a globally secure Industrie 4.0 Ecosystem. / By ed. E. Winkelmeier-Becker – Conference Volume. Berlin: Federal Ministry for Economic Affairs and Energy, Germany. 2021. 147 p.

12. Марков А. С., Цирлов В. Л. Руководящие указания по кибербезопасности в контексте ISO 27032 // Вопросы кибербезопасности. – 2014. – № 1 (2) . – С. 28–35.

13. Ervural B. C., Ervural B. B. Overview of Cyber Security in the Industry 4.0 Era – Industry 4.0: Managing the Digital Transformation. In: Industry 4.0: Managing the Digital Transformation. 2017. P. 267–284. DOI: 10.1007/978-3-319-57870-5_16.

14. Барабанов А. В., Марков А. С., Цирлов В. Л. О систематике информационной безопасности цепей поставки программного обеспечения // Безопасность информационных технологий. – 2019. – Т. 26, № 3. – С. 68–79.

15. Cybersecurity for Industry 4.0. Analysis for Design and Manufacturing / By ed. L. Thames and D. Schaefer – Springer. 2017. 273 p.

16. German Standardization Roadmap Industrie 4.0 / Foreword by D. Wegener – Version 4. – Berlin: DIN e. V., DKE. 2020. 138 p.

17. Головин С. А., Лоцманов А. Н., Позднеев Б. М. Стратегия информационного обеспечения эффективного вхождения промышленности России в современные условия // Стандарты и качество. – 2020. – № 7. – С. 68–73.