# О несоизмеримости подходов стран Южного Кавказа и Евросоюза к нормативному обеспечению ИКБ для национальных КВИ

БАГДАСАРЯН Г.С., академик Инженерной академии Армении

**Аннотация.** Показан глубокий разрыв между нынешними составами НТД по информационно-кибернетической безопасности (ИКБ), применяемыми для критически важных инфраструктур (КВИ) в Евросоюзе и в республиках бывшего Закавказья, который вряд ли будет устранен последними по крайней мере в ближайшей перспективе.

**Ключевые слова:** Евросоюз и страны Южного Кавказа; обеспечение кибербезопасности КВИ; несопоставимость нормативно-технических документов.

Согласно исследованию [1] Federation of the European electricity industry (Eurelectric), представляющей интересы более 3500 энергетических компаний Евросоюза (ЕС), занятых производством, распределением и поставкой электроэнергии, с 2020 по 2022 годы число кибератак на энергетическую инфраструктуру ЕС удвоилось.

Вдобавок к всё более ухудшающейся ситуации [2] не меньшую тревогу у стран ЕС вызывают, судя по различным источникам, также и факты публикации [3] той же Eurelectric, посвящённой в основном киберинцидентам, случившимся в ходе продолжающегося российско-украинского конфликта. В том числе в виде повреждений энергетической инфраструктуры на Украине и их последствий, со своей стороны повысивших до ключевого уровня значимость высоконадёжного решения проблемы информационно-кибернетической безопасности (ИКБ) для всех стран ЕС, в том числе в целях обеспечения совместной их энергобезопасности.

При таком отношении к нарастающим разного рода киберугрозам вполне, полагаем, естественно, что в ЕС предприняты и непрерывно предпринимаются различные шаги по укреплению киберустойчивости (*Cyber resilience*). В их числе — принятый и введённый в действие в последнее десятилетие целый ряд новых законодательных и нормирующих документов, призванных совместно обеспечить максимальное повышение ИКБ для критически важных инфраструктур (КВИ) Евросоюза. Включая электроэнергетическую отрасль и, в частности, электросети на различные классы напряжения.

На данный момент из немалого числа такого рода европейских документов к первоочередным относят:

- Директиву 2022/2555 по сетевой и информационной безопасности (NIS 2 Directive) [4];
- Регламент ЕС под номером 2024/2847, называемый также Законом о киберустойчивости (Cyber Resilience Act — CRA) [5];
- Сетевой кодекс кибербезопасности (Regulation (EU) 2024/1366 [6]).

Обладая особенностями, вкратце изложенными в табл. 1, эти три документа ЕС считаются особо важными ещё и потому, что во многом дополняют друг друга выдвигаемыми требованиями к ИКБ. В частности, к аппаратно-программным средствам, избираемым для оцифровывания управленческих и иного рода технологических процессов в тех или иных национальных КВИ, включая электроэнергетические.

Для обоснований в данной публикации можно было бы, в принципе, сослаться на весь состав требований, предъявляемых совместно названными действующими документами Евросоюза. Но для этого, полагаем, достаточен пример требуемого одним лишь Регламентом ЕС # 2024/2847/CRA, дополненный нами относительно небольшим иным, относящимся конкретно к цифровизации электроэнергетических систем (ЭЭС).

Уже из полного названия указанного Регламента ЕС понятно, что его требования по кибербезопасности распространяются на виды так называемых продуктов с цифровыми элементами (*Products with digital elements*), разделённые в [5] на два класса: важные (*Important products with digital elements*) и важнейшие (*Critical products with digital elements*). Подразумевае-

мые при этом их составы названы совместно в табл. 2. Что же касается самих требований, предъявляемых в этом документе, с одной стороны, к свойствам упомянутых видов продуктов (*Cybersecurity requirements relating to the properties of products with digital elements*), а с другой — к работе с возможными их уязвимостя-

*Таблица 1*

| Особо важные нормативно-правовые акты Евросоюза по ИКБ |
|---|
| Директива NIS 2 (Directive (EU) 2022/2555) [4]:<br>а) Основана на предшественнице (NIS 1 Directive).<br>б) Имеет целью создание более надёжного и согласованного подхода к ИКБ во всём Евросоюзе. В связи с чем охватывает существенно увеличенную целевую аудиторию (распространяется также и на поставщиков цифровых услуг; государственное управление на центральном и региональном уровнях; публичные электронные коммуникации; управление отходами и сточными водами; производство критически важных продуктов, почтовые и курьерские услуги; электрические, нефтяные и газовые сети.<br>в) Содержит: более строгие меры по управлению рисками для энергетических операторов; улучшенные решения по отчётности об инцидентах для национальных органов власти, а также по более тесной координации между государствами — членами ЕС при реагировании на киберугрозы. |
| Закон о киберустойчивости (CRA — Regulation (EU) 2024/2847) [5]:<br>а) Введён в дополнение к Директиве NIS 2.<br>б) Имеет назначением дальнейшее повышение безопасности цифровых инфраструктур Евросоюза.<br>в) С этой целью устанавливает для продуктов с цифровыми компонентами требования кибербезопасности, гарантирующие, что они будут строжащим образом защищёнными от возможных киберугроз, в том числе для применяемых в энергосистемах. |
| Сетевой кодекс кибербезопасности [6]:<br>а) Принят и действует с целью устранения рисков КБ, характерных для энергетического сектора ЕС.<br>б) Ввёл правила КБ, адаптированные к электрическим сетям, с акцентом при этом на:<br>• меры защиты электросетей для предотвращения несанкционированного доступа;<br>• протоколы реагирования на инциденты, требуемые для выявления и сдерживания киберугроз;<br>• ужесточение требований КБ для сторонних вендоров, поставляющих информационно-коммуникационные и операционные технологии (ИКТ и ОТ) энергетическим компаниям. |

*Таблица 2*

| Важные продукты с цифровыми элементами |
|---|
| Класс I:<br>1. Системы управления идентификацией, программное и аппаратное обеспечение для управления привилегированным доступом, в том числе считыватели аутентификации и контроля доступа, включая биометрические;<br>2. Автономные и встроенные браузеры;<br>3. Менеджеры паролей;<br>4. Программное обеспечение, ищущее, удаляющее или изолирующее вредоносное ПО;<br>5. Продукты с цифровыми элементами с функцией виртуальной частной сети (Virtual Private Network — VPN);<br>6. Системы менеджмента управления сетями;<br>7. Системы управления информацией и событиями безопасности (Security Information and Event Management — SIEM);<br>8. Менеджеры загрузки;<br>9. Инфраструктура открытых ключей и программное обеспечение для выдачи цифровых сертификатов;<br>10. Физические и виртуальные сетевые интерфейсы;<br>11. Операционные системы;<br>12. Маршрутизаторы, модемы, предназначенные для подключения к интернету, и коммутаторы;<br>13. Микропроцессоры с функциями, связанными с безопасностью;<br>14. Микроконтроллеры с функциями, связанными с безопасностью;<br>15. Специализированные интегральные схемы (Application specific integrated circuits — ASIC) и программируемые в полевых условиях управляющие матрицы (Field-programmable gate arrays — FPGA) с функциями, связанными с безопасностью;<br>16. Универсальные виртуальные помощники для «умного» дома;<br>17. Продукты для «умного» дома с функциями безопасности, включая «умные» дверные замки, камеры наблюдения, системы наблюдения за детьми и сигнализацию;<br>18. Интернет-подключённые игрушки, подпадающие под действие Директивы 2009/48/ЕС Европейского парламента и Совета (социальные интерактивные функции (например, разговор или съёмка) или с функциями отслеживания местоположения [1]), которые имеют;<br>19. Персонально носимые товары, надеваемые на человека с целью мониторинга здоровья, и к которым применяются Регламент (ЕС) 2017/745 или (ЕС) № 2017/746, а также товары, предназначенные для детей. |

*Таблица 2. Продолжение*

| |
|---|
| Класс II:<br>1. Гипервизоры и контейнерные системы выполнения, поддерживающие виртуализированное выполнение операционных систем и аналогичных сред;<br>2. Межсетевые экраны, системы обнаружения и предотвращения вторжений (Intrusion detection and prevention systems);<br>3. Микропроцессоры, устойчивые к вскрытию;<br>4. Микроконтроллеры, устойчивые к вскрытию. |
| Важнейшие (критические) продукты с цифровыми элементами |
| 1. Аппаратные устройства с охранными блоками;<br>2. Шлюзы «умных» счётчиков в системах «умного» учёта (см. статью 2, п. 23 Директивы (ЕС) 2019/944 от 5 июня 2019 года), другие виды устройства для целей продвинутой безопасности, включая безопасную криптообработку;<br>3. Смарт-карты или аналогичные устройства, включая защищённые элементы. |

*Источники: соответственно приложения III и IV к* [5].

*Таблица 3*

| Основные требования, предъявляемые в CRA к свойствам продуктов с цифровыми элементами |
|---|
| 1) Продукты с цифровыми элементами должны проектироваться, разрабатываться и производиться таким образом, чтобы обеспечить соответствующий уровень кибербезопасности (КБ) с учётом рисков.<br>2) На основании оценки рисков КБ и где это применимо, продукты с цифровыми элементами должны:<br>a) быть без известных уязвимостей;<br>b) иметь конфигурации, защищённые по умолчанию (если между производителем и бизнес-пользователем не согласовано иное в отношении индивидуального продукта с цифровыми элементами, включая возможность сброса продукта в исходное состояние);<br>c) обеспечивать устранение уязвимостей с помощью обновлений безопасности, включая, где применимо, автоматические обновления безопасности, установленные в соответствующий срок и включённые по умолчанию, с понятным и простым в использовании механизмом отключения, путём уведомления пользователей о доступных обновлениях и возможности временного отсроченного их выпуска;<br>d) обеспечивать защиту от несанкционированного доступа с помощью соответствующих механизмов контроля, включая, но не ограничиваясь, системами аутентификации, управления идентификацией или доступом, а также сообщать о возможном несанкционированном доступе;<br>e) защищать конфиденциальность хранимых, передаваемых или иным образом обработанных данных, личных или других, например, шифруя соответствующие данные в состоянии покоя или в передаче с помощью современных механизмов, а также с помощью других технических средств;<br>f) защищать целостность хранимых, передаваемых или иным образом обработанных данных, личных или иных команд, программ и конфигураций от любых манипуляций или модификаций, не санкционированных пользователем, и сообщать о повреждениях;<br>g) обрабатывать только те личные или иные данные, которые являются достаточными, релевантными и ограниченными, необходимыми для предполагаемой цели продукта с цифровыми элементами (минимизация данных);<br>h) защищать доступность основных и базовых функций, в том числе после инцидента, включая меры по устойчивости и смягчению от атак типа «отказ в обслуживании»;<br>i) минимизировать негативное влияние самих продуктов или подключённых устройств на доступность услуг, предоставляемых другими устройствами или сетями;<br>j) быть спроектированными, разработанными и произведёнными с минимально возможными поверхностями атаки, включая внешние интерфейсы;<br>k) быть спроектированными, разработанными и произведёнными для снижения воздействия инцидента с использованием соответствующих механизмов и методов смягчения эксплуатации;<br>l) предоставлять информацию, связанную с безопасностью, путём записи и мониторинга соответствующей внутренней активности, включая доступ к данным, сервисам или функциям, с механизмом отказа пользователя;<br>m) предоставить пользователям возможность легко удалять все данные и настройки, если такие данные могут быть переданы другим продуктам или системам, и обеспечить выполнение этого в безопасном порядке. |

*Источник: Часть I из приложения 1 (Essential cybersecurity requirements) к* [5].

ми (*Vulnerability handling requirements*), то они названы по отдельности соответственно в табл. 3 и 4.

К требованиям из табл. 3 и 4 добавим, что их необходимость и практическая важность обусловлены, по всей видимости, также и всё более расширяющимся применением в различных инфраструктурах ЕС так называемого «промышленного интернета вещей» (*Industrial Internet of Things — IIoT*), который, согласно, к примеру, [7] и [8], вместе с предоставлением различных существенных выгод, значительно рас-

*Таблица 4*

| Основные требования, предъявляемые в CRA к работе с уязвимостями |
|---|
| Производители продуктов с цифровыми элементами должны:<br>1) Выявлять и документировать уязвимости и компоненты, содержащиеся в предлагаемых продуктах, в том числе путём составления спецификации программного обеспечения в широко используемом и машиночитаемом формате, охватывающем, по крайней мере, зависимости продуктов верхнего уровня;<br>2) Незамедлительно устранять обнаруживаемые уязвимости, в том числе путём предоставления обновлений для системы безопасности. При этом там, где это технически возможно, новые обновления для системы безопасности должны предоставляться отдельно от обновлений функциональности;<br>3) Проводить для них эффективные и регулярные тесты и проверки безопасности;<br>4) Как только обновление для системы безопасности станет доступно — делиться и публиковать информацию об исправленных уязвимостях, включая: описание уязвимостей; информацию, позволяющую пользователям идентифицировать продукт с затронутыми цифровыми элементами: последствия уязвимостей, их серьёзность; чёткую и доступную информацию, помогающую пользователям устранять уязвимости; в надлежащим образом обоснованных случаях, когда производители считают, что риски для безопасности, связанные с публикацией, перевешивают преимущества для безопасности, они могут отложить публикацию информации об исправленной уязвимости до тех пор, пока пользователям не будет предоставлена возможность применить соответствующий патч;<br>5) Внедрить и обеспечить соблюдение политики скоординированного раскрытия уязвимостей;<br>6) Принимать меры для облегчения обмена информацией о потенциальных уязвимостях в своём продукте с цифровыми элементами, а также в сторонних компонентах, содержащихся в этом продукте, в том числе путём предоставления контактного адреса для сообщения об обнаруженных уязвимостях в продукте с цифровыми элементами;<br>7) Предусмотреть механизмы безопасного распространения обновлений для продуктов с цифровыми элементами, гарантирующие своевременное устранение уязвимостей и, где это применимо для обновлений системы безопасности, автоматическое;<br>8) Обеспечить, чтобы при наличии обновлений для системы безопасности, направленных на устранение выявленных проблем безопасности, они распространялись без задержек и, если иное не согласовано между производителем и бизнес-пользователем в отношении специально разработанного продукта с цифровыми элементами, бесплатно и с передачей пользователям соответствующей рекомендательной информации, в том числе касательно защитных мер, которые необходимо предпринять. |

*Источник: Часть II из приложения 1 (Essential cybersecurity requirements) к* [5].

ширяет возможности для совершения киберпреступлений. Из-за того, в частности, что при использовании IIoT-технологии [8]:

- естественное для неё разнообразие стандартов и протоколов, применяемых для создания, например, автоматизированных промышленных систем контроля и управления (*IACS — Industrial Automation Control System*), приводит к различным по степени преодолимости сложностям и, как следствие, к возможным от них дополнительным уязвимостям при осуществлении для такого рода систем интеграции избираемых для них разнообразных устройств с цифровыми элементами;
- обновление ПО одного устройства созданной системы может вызвать при эксплуатации сбои в работе других связанных с ним устройств, и, следовательно, во избежание этого потребуется плотное сотрудничество и оперативное взаимодействие с разработчиками других устройств с целью внесения соответствующих требуемых изменений в заложенное в них ПО (особенно уже устаревших версий) для достижения их совместной надёжной работы.

Требования в таблицах 3 и 4, в сущности, обобщённого содержания. В различных разрезах они развёрнуты в [5], с кратным, как следствие, увеличением их численности. К примеру, в случае с 8-ю требованиями из табл. 4, которые в статьях 13, 19 и 20 основного текста этого Регламента/Закона ЕС увеличены до следующих по численности требований-обязательств: 24 — для производителей продуктов с цифровыми элементами, 14 в сумме — для их импортёров и дистрибьютеров.

Если в целом говорить о содержимом Регламента [5], то оно изложено на 81 странице, из которых 67 занимает 71 статья основного текста, а остальное — 8 приложений к ним. Но даже краткий пересказ всего этого был бы большим излишеством, поскольку для данной публикации вполне достаточно требований, приведённых в таблицах 3 и 4.

Опыт показывает, что требования в документах законодательного уровня выражаются обычно посредством сугубо терминологических понятий типа «должен», «обязан», «необходимо» и т.п. Без уточнения при этом, с одной стороны, каким конкретно образом это задаваемое может или должно быть *достигнуто*, а с другой — *проверено* на полноту и/или степень качественности исполнения.

Восполнение этого недостающего звена является, как правило, прерогативой, если не главной функцией

соответствующих стандартов, технических спецификаций и отчётов, руководств по применению, иных возможных разновидностей нормативно-технических документов (НТД), в том числе в виде специально разрабатываемых форм, в которых определены как правила и порядок проведения испытаний на соответствие, так и необходимое в качестве официально подтверждающего их результаты. На практике определение состава НТД, который в достаточной мере охватывал бы требования из того или иного законодательного акта, — не простая в решении задача.

Помимо различного иного, без преувеличения весьма важного в практическом отношении, Регламент/Закон ЕС [5] о киберустойчивости, избранный нами в данной публикации в качестве более чем показательного примера, имеет ещё и ту особенность, что указанная выше задача, известная также под названием «привязка к стандартам» (*Mapping on standards*), во многом решена организацией European Union Agency for Cybersecurity (ENISA). С публикацией детального Отчёта [9] по итогам выполненного специального исследования на названную тему.

Прежде о методологии, применённой ENISA в этом исследовании. В подробностях она приведена в Разделе 2 из [9], а в более сжатом виде — в верхней части табл. 5, к которой в качестве дополняющего добавлены ещё и составляющие полного жизненного цикла (*Generic life-cycle*), рассматривавшиеся для любого из продуктов с цифровыми элементами из табл. 2. Что же касается полученного результата, то это совокупность из 57 европейских и международных НТД из табл. 6 в привязке к требованиям из таблиц 3 и 4, повторённый также и в таблицах 7 и 8 (причём в точности в той же последовательности, в какой названы в первоисточнике).

В целом НТД из табл. 7 и 8 относятся к средствам контроля безопасности, управлению системами информационной безопасности, криптографическим и другим механизмам обеспечения безопасности, к различным по содержанию сервисам, различным

*Таблица 5*

| Методология определения НТД, применённая ENISA к требованиям к КБ из табл. 2 и 3 |
|---|
| 1) Выбор требований; 2) Определение ключевых целей в области безопасности и потенциальных дополнительных требований; 3) Листинг наиболее актуальных стандартов; 4) Обоснование охвата; 5) Потенциальные пробелы; 6) Определение соответствующего этапа (–ов) цикла |
| Жизненный цикл условного продукта с цифровыми элементами |
| Проектирование ⇒ Внедрение⇒ Валидация ⇒ Ввод в эксплуатацию ⇒ Надзор/техническое обслуживание ⇒ Завершение срока службы |

*Источники: Схемы 1 и 2 из Раздела 2 в* [9].

*Таблица 6*

| Минимальный состав НТД [1, 2], в соответствующей мере охватывающих требования CRA [4] к кибербезопасности и обработке уязвимостей продуктов с цифровыми элементами (57) |
|---|
| EN ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection — Information security controls.<br>EN ISO/IEC 27005:2022, Information security, cybersecurity and privacy protection — Guidance on managing information security risks.<br>EN IEC 62443–3–2:2020, Security for industrial automation and control systems — Security risk assessment for system design.<br>EN IEC 62443–4–1:2018, Security for industrial automation and control systems — Secure product development lifecycle requirements.<br>ISO/IEC 18045:2022 [3], Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation.<br>ITU-T X.1214 (2018), Security assessment techniques in telecommunication/information and communication technology networks.<br>ETSI EN 303 645 [3] V2.1.1 (2020), CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements.<br>ISO/IEC 18031:2011 [3], Information technology — Security techniques — Random bit generation.<br>ISO/IEC 9798, IT — Security techniques — Entity authentication:<br>• Part 1 (2010) — General;<br>• Part 2 (2019) — Mechanisms using authenticated encryption;<br>• Part 3 (2019) — Mechanisms using digital signature techniques;<br>• Part 4 (1999) — Mechanisms using a cryptographic check function;<br>• Part 5 (2009) — Mechanisms using zero-knowledge techniques;<br>• Part 6 (2010) — Mechanisms using manual data transfer. |

*Таблица 6. Продолжение*

ISO/IEC 24760, Information security, cybersecurity and privacy protection — A framework for identity management:
- Part 1 (2019[3]) — Core concepts and terminology;
- Part 2 (2015[3]) — Reference architecture and requirements;
- Part 3 (2016[3]) — Practice.

ITU-T X.812 (1995), Information technology — Open Systems Interconnection — Security frameworks for open systems: Access control framework.
ITU-T X.1253 (2011), Security guidelines for identity management systems.
EN IEC 62443–4–2:2019, Security for industrial automation and control systems — Technical security requirements for IACS components.
ITU-T X.805 (2003), Security architecture for systems providing end-to-end communications.
ISO/IEC 18033, Information security — Encryption algorithms:
- Part 1 (2021) — General;
- Part 2 (2006[3]) — Asymmetric ciphers;
- Part 3 (2010[3]) — Block ciphers;
- Part 4 (2011[3]) — Stream ciphers;
- Part 5 (2015) — Identity-based ciphers;
- Part 6 (2019) — Homomorphic encryption;
- Part 7 (2022) — Tweakable block ciphers.

ITU-T X.814 (1995), Information technology — Open Systems Interconnection — Security frameworks for open systems: Integrity framework.
ISO/IEC 9796, Information technology — Security techniques — Digital signature schemes giving message recovery:
- Part 2 (2010) — Integer factorization-based mechanisms;
- Part 3 (2006) — Discrete logarithm-based mechanisms.

ISO/IEC 9797, Information technology — Security techniques — Message Authentication Codes (MACs):
- Part 1 (2011) — Mechanisms using a block cipher;
- Part 2 (2021) — Mechanisms using a dedicated hash-function;
- Part 3 (2011) — Mechanisms using a universal hash-function.

ISO/IEC 14888, IT Security techniques — Digital signatures with appendix:
- Part 1 (2008) — General;
- Part 2 (2008) — Integer factorization-based mechanisms;
- Part 3 (2018) — Discrete logarithm-based mechanisms.

ITU-T X.815 (1995), Information technology — Open Systems Interconnection — Security frameworks for open systems: Integrity framework.
ISO/IEC 27701:2019[3], Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines.
ISO/IEC 29100:2011[3], Information technology — Security techniques — Privacy framework.
ETSI TS 103 485 V1.1.1 (2020), CYBER; Mechanisms for privacy assurance and verification.
ISO/IEC 22237–1:2021, Information technology — Data center facilities and infrastructures — Part 1: General concepts.
ITU-T Y.4810 (2021). Requirements for data security of heterogeneous Internet of things devices.
ISO/IEC TS 19249:2017, Information technology — Security techniques — Catalogue of architectural and design principles for secure products, systems and applications.
EN ISO/IEC 15408–2:2020[3] [ISO/IEC 15408–2:2008], Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Security functional components.
ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements.
ISO/IEC 27034–1:2011, Information technology — Security techniques — Application security — Overview and concepts
EN ISO/IEC 15408–3:2020[3] [ISO/IEC 15408–3:2008], Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Security assurance components.
ISO/IEC 13888–1:2020, Information security — Non-repudiation — General.
ISO/IEC 30111:2019, Information technology — Security techniques — Vulnerability handling processes.
IEC 62443–2–1:2010[3], Security for industrial automation and control systems — Security program requirements for IACS asset owners.
ISO/IEC 27036. Cybersecurity — Supplier relationships:
- Part 1 (2021) — Overview and concepts;
- Part 2 (2022) — Requirements;
- Part 3 (2023) — Guidelines for hardware, software, and services supply chain security.

ISO/IEC 27034–5–1:2018, Information technology — Application security — Protocols and application security controls data structure, XML schemas.

*Таблица 6. Окончание*

| |
|---|
| ISO/IEC 29146:2016[3], Information technology — Security techniques — A framework for access management.<br>EN ISO/IEC 29147:2020 [ISO/IEC 29147:2018], Information technology — Security techniques — Vulnerability disclosure. |

*[1] См. примечание 3 к табл. 5 касательно текущего статуса ряда НТД из данной таблицы.*

*[2] В скобках к охватываемым частям серийных стандартов ИСО/МЭК (равно как и ко всем приводимым НТД разработки ITU-T и ETSI), названы годы публикации.*

*[3] Действуют на данный момент соответственно в версиях ISO/IEC 18045:2026, ISO/IEC 24760–1:2025, ISO/IEC 24760–2:2025, ISO/IEC 18033–2:2017, ISO/IEC 18033–3:2021, ISO/IEC 18033–4:2020, ISO/IEC 29146:2024, ISO/IEC 27034–1:2011+COR1:2014, ISO/IEC 18031:2025, IEC 62443–2–1:2024, EN ISO/IEC 15408–2:2023 [ISO/IEC 15408–2:2022 *], EN ISO/IEC 15408–3:2023 [ISO/IEC 15408–3:2022*], ISO/IEC 24760–1:2025, ISO/IEC 24760–2:2025, ISO/IEC 24760–3:2025, ISO/IEC 27701:2025, ISO/IEC 29100:2024, ETSI EN 303 645 V3.1.3 (2024–09).*

** Заменены уже соответственно на ISO/IEC 15408–2:2026 и ISO/IEC 15408–3:2026, к которым добавлены ещё и три других стандарта той же серии (Information security, cybersecurity and privacy protection — Evaluation criteria for IT security):*

*— ISO/IEC 15408–4:2026 (Framework for the specification of evaluation methods and activities);*

*— ISO/IEC 15408–5:2026 (Pre-defined packages of security requirements).*

аспектам управления идентификацией и оценки соответствия требуемому, ко взаимодействию в сфере кибербезопасности с поставщиками продуктов с цифровыми элементами, конфиденциальности и прочему. При этом считается, что организации должны следовать установленному, по крайней мере в основных (essential) из этих множественных документов, чтобы обеспечить целостность своих ИТ- и ОТ-систем и минимизировать риски кибератак.

Следует, полагаем, также сказать, что эти многочисленные стандарты, становящиеся всё более жёсткими, содержат, с другой стороны, разнообразные чёткие рекомендации по защите информационных и операционных сред особо значимых (критически важных) национальных инфраструктур, то расцениваются в нашем случае в ЕС важнейшим инструментом обеспечения их защищённости в условиях всё более растущей вероятности оказаться целью разнообразных кибератак. Без большого при этом упования на широко распространяемое в том числе в ЕС, будто для устойчивости к деструктивному их воздействию достаточно обзавестись нужной по функциональности системой обнаружения и предупреждения кибервторжений (*Intrusion detection and prevention systems — IDPS*).

Приведённое в табл. 6–8 — это НТД с так называемыми горизонтальными (общими/базовыми) требованиями к кибербезопасности, при этом универсальными в том отношении, что:

а) применимы к любым организациям и объектам, независимо от отрасли;

б) охватывают устанавливаемым в целом все компоненты их ИТ-инфраструктуры (серверы, рабочие места, сеть);

в) определяют в качестве основных необходимых мер обеспечения киберзащиты:

- цифровую гигиену (использование антивирусного и антишпионского ПО; регулярное обновление используемого ПО, в том числе защитного для операционных систем и приложений; использование сложных паролей, менеджеров паролей и обязательной двухфакторной аутентификации (2FA);
- защиту инфраструктуры (обеспечение безопасности пользовательских доменов, рабочих станций, локальных и глобальных сетей (LAN/WAN));
- управление рисками (путём реализации действий, к примеру, из пятифункциональной модели американского национального института стандартов — NIST);
- защиту сети (контроль горизонтального трафика между рабочими станциями; защита периметра, использование VPN и брандмауэров);
- защиту данных (шифрование важных файлов, резервное копирование (backup), контроль за физическим доступом к цифровому оборудованию);
- обучение персонала (постоянный инструктаж сотрудников по соответствующим вопросам обеспечения кибербезопасности).

Между тем НТД из табл. 5 имеет определённые издержки в покрытии требований из табл. 3 и 4. В некоторой мере они раскрыты в [6] в примечаниях под названием «Overall coverage and possible gaps / Общее покрытие и возможные пробелы», приводимых к каждому из требований из указанных таблиц.

Так, например, для выполнения горизонтального требования за номером 7 из табл. 4 (предусмотреть механизмы безопасного распространения обновлений для надёжного гарантирования своевременного устранения уязвимостей, которыми могут воспользоваться киберпреступники) в [9] считается недостаточным полагаться только на положения, приведённые в стандартах ISO/IEC 27002:2022 и ISO/IEC 62443–4–1:2018. Потому что, согласно записанному в примечании к этому требованию, хотя данные два стандарта и вносят весомый вклад в различные аспекты выполнения рассматриваемого требования, они: а) не дают

*Таблица 7*

| Состав НТД, отнесённых ENISA в [9] к требованиям из CRA к свойствам продуктов с цифровыми элементами | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Обозначения НТД[1] | Требования[2] | | | | | | | | | | | | |
| | 1 | 2 | 3a | 3b | 3c | 3d | 3e | 3f | 3g | 3h | 3i | 3j | 3k |
| EN ISO/IEC 27002:2022 | X | | X | | | | | X | | | X | X | X |
| EN ISO/IEC 27005:2022 | X | | | | | | | | | | | | |
| EN IEC 62443–3–2:2020 | X | | | | | | | | | | X | | |
| EN IEC 62443–4–1:2018 | X | X | | | | | | | | | | | |
| ISO/IEC 18045:2022 [2] | | X | | | | | | | | | X | | |
| ITU-T X.1214 (03/2018) | | X | | | | | | | | | | | |
| ETSI EN 303 645 V2.1.1 [2] | X | X | X | X | X | X | X | X | X | X | X | X | X |
| ISO/IEC 18031:2011 | | | X | | | | | | | | | | |
| ISO/IEC 9798–1:2010 | | | | X | | | | | | | | | |
| ISO/IEC 9798–2:2019 | | | | X | | | | | | | | | |
| ISO/IEC 9798–3:2019 | | | | X | | | | | | | | | |
| ISO/IEC 9798–4:1999 | | | | X | | | | | | | | | |
| ISO/IEC 9798–5:2009 | | | | X | | | | | | | | | |
| ISO/IEC 9798–6:2010 | | | | X | | | | | | | | | |
| ISO/IEC 24760–1:2019 | | | | X | | | | | | | | | |
| ISO/IEC 24760–2:2015 | | | | X | | | | | | | | | |
| ISO/IEC 24760–3:2016 | | | | X | | | | | | | | | |
| ISO/IEC 29146:2016 | | | | X | | | | | | | | | |
| ITU-T X.812 (11/1995) | | | | X | | | | | | | | | |
| ITU-T X.1253 (09/2011) | | | | X | | | | | | | | | |
| EN IEC 62443–4–2:2019 | | | | X | X | X | | X | | X | | X | X |
| ITU-T X.805 (10/2003) | | | | | X | | | X | | | | | |
| ISO/IEC 18033–1:2021 | | | | | X | | | | | | | | |
| ISO/IEC 18033–2:2017 | | | | | X | | | | | | | | |
| ISO/IEC 18033–3:2021 | | | | | X | | | | | | | | |
| ISO/IEC 18033–4:2020 | | | | | X | | | | | | | | |
| ISO/IEC 18033–5:2015 | | | | | X | | | | | | | | |
| ISO/IEC 18033–6:2019 | | | | | X | | | | | | | | |
| ISO/IEC 18033–7:2022 | | | | | X | | | | | | | | |
| ITU-T X.814 (11/1995) | | | | | X | | | | | | | | |
| ISO/IEC 9796–2:2010 | | | | | | X | | | | | | | |
| ISO/IEC 9796–3:2006 | | | | | | X | | | | | | | |
| ISO/IEC 9797–1:2011 | | | | | | X | | | | | | | |
| ISO/IEC 9797–2:2021 | | | | | | X | | | | | | | |
| ISO/IEC 9797–3:2011 | | | | | | X | | | | | | | |
| ISO/IEC 14888–1:2018 | | | | | | X | | | | | | | |
| ISO/IEC 14888–2:2008 | | | | | | X | | | | | | | |
| ISO/IEC 14888–3:2018 | | | | | | X | | | | | | | |
| ITU-T X.815 (11/1995) | | | | | | X | | | | | | | |
| ISO/IEC 27701:2019 | | | | | | | X | | | | | | |
| ISO/IEC 29100:2011 | | | | | | | X | | | | | | |

*Таблица 7. Продолжение*

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ETSI TS 103 485 V1.1.1 | | | | | | | X | | | | | | |
| ISO/IEC 22237–1:2021 | | | | | | | | X | | | | | |
| ITU-T Y.4810 (11/2021) | | | | | | | | | X | | | | |
| ISO/IEC TS 19249:2017 | | | | | | | | | | X | | | |
| EN ISO/IEC 15408–2:2022 | | | | | | | | | | X | | | |
| ISO/IEC 27001:2022 | | | | | | | | | | | X | | |
| ISO/IEC 27034–1:2011 | | | | | | | | | | | X | | |
| EN ISO/IEC 15408–3:2022 | | | | | | | | | | | X | | |
| ISO/IEC 13888–1:2020 | | | | | | | | | | | | X | |
| ISO/IEC 30111:2019 | | | | | | | | | | | | | X |
| IEC 62443–2–1:2010 | | | | | | | | | | | | | X |

[1] *См. примечание 6 к табл. 5 касательно текущего статуса ряда НТД из данной таблицы.*

[2] *В определениях из табл. 3.*

*Источник: Таблица 22 из Отчёта* [9].

*Таблица 8*

| Состав НТД, отнесённых ENISA в [9] к требованиям из CRA к обработке уязвимостей продукции с цифровыми элементами | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Обозначения НТД[1] | Требования[2] | | | | | | | |
| | (1) | (2) | (3) | (4) | (5) | (6) | (7) | (8) |
| ISO/IEC 27001:2022 | | X | X | | | | | |
| ISO/IEC 27002:2022 | | X | X | | | | X | X |
| ISO/IEC 27005:2022 | | | X | | | | | |
| ISO/IEC 27034–5–1:2018 | | | X | | | | | |
| ISO/IEC 27036–1:2021 | X | | | | | | | |
| ISO/IEC 27036–2:2022 | X | | | | | | | |
| ISO/IEC 27036–3:2023 | X | | | | | | | |
| EN ISO/IEC 29147:2020 | | X | | X | X | X | | |
| ISO/IEC 30111:2019 | | X | | X | X | X | | X |
| EN IEC 62443–4–1 2018 | | X | | X | | | X | X |
| ETSI EN 303 645 V2.1.1 | | | | X | X | | | |

[1] *См. примечание 3 к табл. 5 касательно текущего статуса ряда НТД из данной таблицы.*

[2] *В определениях из табл. 4.*

*Источник: Таблица 23 из Отчёта* [9].

подробных рекомендаций по безопасным механизмам установки и внедрения обновлений; б) не регулируют вопрос уведомления пользователей о доступности обновлений. Вследствие чего для покрытия таких пробелов авторами [9] признаётся обоснованным использование этих стандартов в комбинации с НТД, адаптированными к конкретным потребностям и считающимися лучшими в этой части на основе опыта отраслевых практик. Как, скажем, в совместности с NIST SP 800–53, NIST SP 800–63B и OWASP SSDLC (в частности, последнее из которых являет собой, напомним, подход международного сообщества OWASP (*Open Web Application Security Project*) специалистов по ИБ, интегрирующий меры безопасности на всех этапах жизненного цикла разработки защищённого ПО (*Secure Software Development Lifecycle — SSDLC*), предназначающегося для создания безопасных приложений, обеспечивающих устойчивость к распространённым киберугрозам.

Со своей стороны могли бы добавить в табл. 5–7 немало и другого. В том числе, к примеру:

— Британский BS ISO IEC 27039–2015, датский DANSK DS/ISO/IEC 27039:2015 или норвежский NS-ISO/IEC 27039:2015, идентичные международному

ISO/IEC 27039:2015 (*Information technology — Security techniques — Selection, deployment and operations of intrusion detection and prevention systems (IDPS)*), каждый из которых:

- весьма важен в том отношении, что при применении возводит достаточно серьёзные преграды выбору и использованию для/в требующих кибер-защиты информационно-коммуникационных инфраструктур недостаточно надёжных или же вовсе ненадёжных систем определения и предупреждения возможных кибервторжений;
- имеет предшественницей и, судя по всему, в основе специальную публикацию NIST SP 800–94 (*Guide to Intrusion Detection and Prevention Systems (IDPS). Recommendations of the National Institute of Standards and Technology*) 2007 года национального института стандартов и технологий США.

— Европейский EN IEC 62443–4–2:2019 (*Security for industrial automation and control systems — Technical security requirements for IACS components),* который будучи полностью идентичным международному стандарту IEC 62443–4–2:2019:

- также содержит подробные технические требования к компонентам (*Component requirements — CRs*) промышленных систем автоматизации и управления (IACS), связанные, в свою очередь, с семью основными требованиями (*Foundational requirements — FRs*), описанными в IEC TS 62443–1–1, включая определение требований к уровням безопасности возможностей указанного рода систем и их компонентов;
- имеет целевой аудиторией поставщиков и разработчиков компонентов IACS, а также владельцев и операторов такого рода цифровых систем (для определения требований к закупкам и оценки безопасности компонентов при проектировании их архитектуры).

Взамен отметим, что целям обеспечения ИКБ призваны служить в Европе также и стандарты с так называемыми вертикальными требованиями. Разнящиеся, в частности, тем, что содержат соответствующие требования по ИКБ и, вместе с тем, рекомендуемые для их исполнения различные специализированные защитные меры, разработанные для конкретных секторов экономики (вертикалей). С учётом при этом уникальных для них видов киберугроз, регуляторных норм и возможных уязвимостей.

В качестве примеров ряд такого рода нормирующих документов, предназначенных конкретно для электроэнергетической отрасли, назван в табл. 9. Причём в основном европейских (в их числе 2 британских, 2 германских и по одному из итальянских, албанских и датских), являющихся, главным образом, полностью идентичными аналогами тех международных нормирующих документов, что приписаны к ним в квадратных скобках.

К приведённому в табл. 9 надо добавить, что в ней не упомянуты многие иные «европеизированные» или же не подвергшиеся этому международные НТД по ИКБ, также предъявляющие вертикальные требования к разнообразным специфическим компонентам оцифровываемых ЭЭС. Тогда как существуют не только в виде десятка других документов из названных в этой таблице серий, но и виде множества других. Это, в частности, несколько десятков НТД серий IEC 61968 (*Application integration at electric utilities — System interfaces for distribution management*), IEC 61970 (*Energy management system application program interface (EMS-API)*) и IEC 62325 (*Framework for energy market communications*), также высокозначимых в деле достижении безопасности при оцифровке объектов энергосферы — см. на данный счёт показанное, к примеру, в [10]).

Однако и то относительно немногое, что представлено выше в табл. 5 и 8, вполне, полагаем, достаточно для выводов о степени удалённости стран Южного Кавказа (бывшего советского Закавказья) от того, к чему они якобы сильно стремятся — перенять и начать практиковать подходы, применяемые в ЕС. В том числе к ИКБ критически важных инфраструктур этого союза и, в частности, для обслуживающих их ЭЭС.

Возникновение такого объявленного желания относится, как минимум, к появлению инициативы Европейского Союза EU4Digital, призванной, согласно [11], поддержать страны так называемого «Восточного партнёрства» (Армению, Азербайджан, Беларусь, Грузию, Молдову и Украину) в реализации программ и мер по цифровизации ключевых областей экономики и общества в соответствии с нормами и практиками ЕС. С тем, в том числе, чтобы (опять же согласно [11]) помочь упомянутым шести странам бывшего Советского Союза обеспечить экономический рост, создать больше рабочих мест, улучшить жизнь людей и т.п.

Из всего намечавшегося «европейской инициативой» особо, считаем, интересен проект «EU4Digital: Cybersecurity East», реализовывавшийся в 2019–2022 гг. с вкладом в него Евросоюзом 3 121 600 евро [12]. Однако в ещё большей мере содержащееся в относящемся к этому проекту руководящем документе [13], в котором:

а) главной целью указанной инициативы определена, как и в [11], разработка для шести упоминавшихся бывших советских республик технических механизмов и механизмов сотрудничества для укрепления кибербезопасности и лучшей подготовленности к кибератакам в соответствии со стандартами Евросоюза.

*Таблица 9*

| Примеры важных вертикальных стандартов по КБ, предназначенных конкретно для энергосферы[1] |
|---|
| EN ISO/IEC 27019:2020 [ISO/IEC 27019:2017[2]], Information technology — Security techniques — Information security controls for the energy utility industry.<br>CEI IEC TS 60870–5–7:2025[3] [IEC TS 60870–5–7:2025 (2013)], Telecontrol equipment and systems — Part 5–7: Transmission protocols — Security extensions to IEC 60870–5–101 and IEC 60870–5–104 protocols (applying IEC 62351).<br>EN IEC 62645:2020 [IEC 62645:2019 (2015)], Nuclear power plants — Instrumentation, control and electrical power systems — Cybersecurity requirements.<br>BS IEC 63096:2020[4] [IEC 63096:2020 (–)], Nuclear power plants — Instrumentation, control and electrical power systems — Security controls. |
| Из НТД серии «Communication networks and systems for power utility automation»:<br>• EN 61850–3:2014 [IEC 61850–3:2013], General requirements;<br>• EN 61850–4:2011 + A1:2020 [IEC 61850–4:2011 + AMD1:2020], System and project management;<br>• EN 61850–5:2013 + A1:2022 [IEC 61850–5:2013 + AMD1:2022 (2013, 2005)], Communication requirements for functions and device models;<br>• EN 61850–10:2013 + A1:2025 [IEC 61850–10:2012 + AMD1:2025], Conformance testing;<br>• IEC TR 61850–10–3:2022, Functional testing of IEC 61850 systems;<br>• IEC TR 61850–90–1:2010, Use of IEC 61850 for the communication between substations;<br>• IEC TR 61850–90–2:2016, Using IEC 61850 for communication between substations and control centers. |
| Из НТД серии «Power systems management and associated information exchange — Data and communications security»:<br>• EN IEC 62351–3:2023 [IEC 62351–3:2023 (2020, 2018, 2014)], Communication network and system security — Profiles including TCP/IP;<br>• EN IEC 62351–4:2020 [IEC 62351–4:2020 (2018)], Profiles including MMS and derivatives;<br>• EN IEC 62351–5:2023 [IEC 62351–5:2023 (2013)], Security for IEC 60870–5 and derivatives;<br>• EN IEC 62351–6:2020 [IEC 62351–6:2020 (–)], Security for IEC 61850;<br>• EN IEC 62351–7:2026 [IEC 62351–7:2025(2017)], Network and System Management (NSM) data object models;<br>• EN IEC 62351–8:2020 [IEC 62351–8:2020 (–)], Role-based access control for power system management;<br>• EN IEC 62351–9:2023 [IEC 62351–9:2023(2017)], Cyber security key management for power system equipment;<br>• IEC TR 62351–10:2012 (–), Security architecture guidelines IEC 62351–9:2023;<br>• EN IEC 62351–11:2017 [IEC 62351–11:2016 (–)], Security for XML documents;<br>• IEC TR 62351–12:2016 (–), Resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems;<br>• IEC TR 62351–13:2016 (–), Guidelines on security topics to be covered in standards and specifications;<br>• PD IEC TS 62351–100–1:2018[5] [IEC TS 62351–100–1:2018], Conformance test cases for IEC TS 62351–5 and IEC TS 60870–5–7;<br>• DIN IEC TS 62351–100–3:2020[6] [IEC TS 62351–100–3:2020 (–)], Konformitätstestfälle für IEC 62351–3, die sichere. Kommunikationserweiterung für Profile einschließlich TCP/IP/Conformance test cases for the IEC 62351–3, the secure communication extension for profiles including TCP/IP;<br>• DS IEC TS 62351–100–4:2023[7] [IEC TS 62351–100–4:2023 (–)], Cybersecurity conformance testing for IEC 62351–4;<br>• DIN IEC TS 62351–100–6:2023[5] [IEC TS 62351–100–6:2022 (–)], Cybersecurity — Konformitätsprüfung für IEC 61850–8–1 und IEC 61850–9–2 /Cybersecurity conformance testing for IEC 61850–8–1 and IEC 61850–9–2. |

*[1] В квадратных скобках к НТД из данной таблицы названы международные документы, которым они идентичны, а в круглых скобках дополнение к последним — также и годы издания предшествовавших им версий.*

*[2] Действует в версии ISO/IEC 27019:2024 (Information security, cybersecurity and privacy protection — Information security controls for the energy utility industry).*

*[3–5] Соответственно итальянский и британские НТД.*

*[6] Германские и албанский нормативно-технические документы (технические спецификации — TS). Приведены как примеры того, что, хотя рассматриваемые международные НТД не имеют общеевропейских аналогов (под грифом EN), но, тем не менее, приняты теми или иными европейскими странами в виде национальных идентичных прообразов.*

б) В виде отдельных приложений сделан обзор по состоянию на 2020 год в целом ситуации с решением в вышеназванных странах Восточного партнёрства проблемы обеспечения ИКБ для критически важных национальных информационных инфраструктур;

в) На этой основе обобщены (в разделе 5) основные вызовы и определяемые ими различные защитные меры, необходимые для каждой из этих национальных инфраструктур и для всех них вместе.

Представленное в табл. 10 более чем кратко выражает то, что содержится в [11] применительно к Армении, Азербайджану и Грузии. Что касается достигнутого к настоящему времени в деле достижения цели / решения задачи из пункта а), то во многом, на наш взгляд, очевидно из приведённого в табл. 11.

При всех своих количественно-содержательных различиях, составы национальных НТД из табл. 10 имеют ещё и общее: это настолько большое отличие

*Таблица 10*

| Основные проблемы стран Южного Кавказа в деле обеспечения кибербезопасности[1] |
|---|
| Армения (AM):<br>• недостаток средств и интереса властей;<br>• нехватка знаний и экспертизы;<br>• устаревшее аппаратное и программное обеспечение, создающее очень высокий риск киберинцидентов. |
| Азербайджан (AZ):<br>• недостаточное финансирование;<br>• нехватка квалифицированных кадров и ресурсов в области кибербезопасности;<br>• недостаточная приверженность национальных органов решению вопросов кибербезопасности. |
| Грузия (GE):<br>• недостаточное финансирование;<br>• недостаточная приверженность национальных органов решению вопросов кибербезопасности;<br>• недостаток осведомлённости и нехватка квалифицированного персонала и ресурсов. |

[1] *По состоянию на июнь 2020 года* [10].

*Таблица 11*

| НТД стран Южного Кавказа из числа подразумеваемых CRA Евросоюза |
|---|
| Армения: ГОСТ Р ИСО/МЭК 15408–2–2013[1] [ISO/IEC 15408–2:2008], ГОСТ Р ИСО/МЭК 15408–3–2013[1] [ISO/IEC 15408–3:2008], ISO/IEC 27001:2022 + AMD1:2024[2], ISO/IEC 27002:2022[2], ISO/IEC 27005:2022[2], ISO/IEC 27701:2025[2]. АСТ ИСО/МЭК 9796–2–2009 [ISO/IEC 9796–2–2002], АСТ ИСО/МЭК 9796–3–2009 [ISO/IEC 9796–3:2006], ГОСТ ISO/IEC 24760–2–2021[3] [ISO/IEC 24760–2:2015], АСТ ИСО/МЭК 14888–1–2008 [ISO/IEC 14888–1:2008], АСТ ИСО/МЭК 14888–2–2008 [ISO/IEC 14888–2:2008], АСТ ИСО/МЭК 14888–3–2008 [ISO/IEC 14888–3:2001], ГОСТ ISO/IEC TS 19249–2021[3] [ISO/IEC TS 19249:2017], ГОСТ ISO/IEC 29100–2021[3] [ISO/IEC 29100:2011], ISO/IEC 29147:2018 [2)], ISO/IEC 30111:2019[2], IEC 62443–4–1:2018[2]. |
| Азербайджан: AZS 356.2–2009 [ISO/IEC 15408–2:2005], AZS 356.3–2009 [ISO/IEC 15408–3:2005], AZS ISO/IEC 27001:2022 [ISO/IEC 27001:2022], AZS ISO/IEC 27002:2022 [ISO/IEC 27002:2022], AZS 492–2010 [ISO/IEC 27005:2008]. |
| Грузия[4]: ISO/IEC 15408–2:2008[5], ISO/IEC 15408–3:2008[5], SST ISO IEC 27001:2026 [ISO/IEC 27001:2022 + AMD1:2024], SST ISO IEC 27002:2022 [ISO/IEC 27002:2022], SST ISO IEC 27005:2022 [ISO/IEC 27005:2022], ISO/IEC 18045:2008[5], SST ISO/IEC 27701:2022 (ISO/IEC 27701:2019], SST ISO/IEC 27036–1:2022 [ISO/IEC 27036–1:2021]. |

[1] *Российские стандарты, введённые в действие также и на территории Армении.*

[2] *Включены в таблицу условно, поскольку, по крайней мере на данный момент, не включены в каталог национальных стандартов РА (см. на https://www.armstandard.am/en/standarts). Несмотря на то, что правительственным решением от 24.05.2026 г. № 662-Ն в том числе и они определены как приемлемые (?!) для страны.*

[3] *Приняты Арменией в качестве межгосударственных стандартов для стран ЕАЭС.*

[4] *В Грузии действуют SST EN 18031–1:2025 [EN 18031–1:2024] и SST EN 18031–2:2025 [EN 18031–3:2024], которые, однако, не имеют какого-либо отношения к ISO/IEC 18031:2011 из табл. 6–8.*

[5] *В каталоге стандартов страны отсутствуют. Включены в данную таблицу лишь потому, что, согласно статье 9 из постановления правительства Грузии от 28.06.2018 № 343, в этой республике при сертификации средств создания квалифицированной электронной подписи / квалифицированной электронной печати:*

– *критерии безопасности должны определяться согласно установленному в стандартах ISO/IEC 15408–1:2009, ISO/IEC 15408–2:2008 и ISO/IEC 15408–3:2008 из серии «Информационные технологии — Методы безопасности — Критерии оценки ИТ-безопасности).*

– *Методологией оценки безопасности ИТ должна избираться содержащаяся в отменённом уже стандарте ISO/IEC 18045:2008 (заменён на ISO/IEC 18045:2022, который, в свою очередь, отменён вводом в действие одноимённого с ним ISO/IEC 18045:2026: Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Requirements and methodology for IT security evaluation).*

каждого пакета от стандартов, приведённых в табл. 6 и 9, что невольно вспоминается изречение: «Где Кура и где твой дом» из известного водевиля советского времени. В этом контексте мы видим совершенно далёкие друг от друга вещи: отношение в Евросоюзе к требуемому в качестве нормативного обеспечения ИКБ национальных КВИ и отношение к этому же властей Армении, Азербайджана и Грузии. Причём степень отсталости последних столь глубока, что вряд ли будет устранена в каждой из этих трёх стран не только в ближайшей перспективе, но и, совершенно не исключаем, даже в обозримом будущем. Тем более, что:

1) ни одно из мероприятий из инициативы EU4Digital не предусматривало переход к применению европейских стандартов. Во всяком случае напрямую (см. табл. 12).

2) Финансирование упомянутой европейской инициативы полностью завершено ещё в 2022 году и, судя

*Таблица 12*

| Мероприятия, предусматривавшиеся в целом инициативой EU4Digital |
|---|
| 1. Разработка Национальной стратегии кибербезопасности.<br>2. Перенос Директивы NIS в национальное регулирование.<br>3. Разработка критериев определения критической информационной инфраструктуры (CII).<br>4. Создание, поддержание и расширение перечня национальных CII.<br>5. Постоянное усиление устойчивости, честности и надёжности CII.<br>6. Сотрудничество в области кибербезопасности:<br>— улучшение сотрудничества внутригосударственного, государственного и частного секторов;<br>— международное сотрудничество.<br>7. Принятие общей методологии и проведение национальной оценки киберрисков.<br>8. Укрепление закона о кибербезопасности, его гармонизация с Директивами ЕС.<br>9. Создание национальных CERT[1]/CSIRT[2] и т.д. |

[1] *CERT (Computer Emergency Response Team) обычно означает компьютерную группу реагирования на чрезвычайные ситуации.*

[2] *CSIRT (Computer Security Incident Response Team) — команда экспертов, занимающаяся предотвращением, анализом и устранением последствий кибератак, а также мониторингом угроз и поддержкой систем.*

*Источник: приведённое в* [13] *на рис. 1.*

по всему, продолжено не будет. Разве только при появлении какой-то новой инициативы ЕС той направленности — обеспечения ИКБ для КВИ шести стран так называемого «восточного партнёрства» (*Eastern Partner countries*). В чём, однако, также крайне сильно сомневаемся.

3) Судя по всему, как и прежде, власти каждой из рассматриваемых здесь республик бывшего советского Закавказья — стран Южного Кавказа не видят резона самостоятельно переходить к применению НТД, используемых в ЕС в целях ИКБ наднациональных и национальных КВИ. Даже тех, что названы в табл. 6 и 9.

В пользу истинности нашего предположения-догадки по поводу последнего из этих пунктов свидетельствуют, на наш взгляд, даже данные, приведённые в табл. 10. Но в гораздо большей мере — более десятка других фактов, из которых ограничимся здесь упоминанием только двух примеров, относящихся к Азербайджану и Грузии.

Как известно [14], выступая в первых числах июня 2024 года в Баку в рамках панельной дискуссии III-го Национального форума по кибербезопасности, глава Национального центра по борьбе с киберинцидентами (USOM) Турецкой Республики М.Э. Йылдырым предложил установить единые стандарты кибербезопасности для всей Организации тюркских государств (включающей, помимо Азербайджана, также Казахстан, Кыргызстан, Турцию и Узбекистан). Более того, было бы, полагаем, вполне естественно, что под этими общими стандартами подразумевались соответствующие турецкие. И, как минимум, названные в табл. 13, являющиеся полностью идентичными аналогами 57 из 81 в сумме НТД, приводившихся в табл. 6 и 9.

Так как ещё много лет назад Азербайджан провозгласил себя братом Турции, то, казалось бы, её вышеупомянутое предложение этим южнокавказским государством должно было быть принято. В том числе ещё и как свидетельство тому, что оно вроде бы готовится стать европейским в подходах к безопасному развитию.

Однако из-за чего-то неизвестного нам такой шаг до сих пор не совершён. Несмотря даже на то, что уже и на уровне Национального центра кибербезопасности (*Milli Kibertəhlükəsizlik Mərkəzi*) этого государства стали, кажется [16], видеть резон в переходе к применению передовой нормативной базы по ИКБ для эксплуатируемых и нововводимых в стране операционных технологий (ОТ). В том числе таких НТД, как стандарты серий IEC 62443 и NIST SP 800. Включая применительно к цифровой технике, внедряемой в национальную ЭЭС как для решения отдельных задач (скажем, по релейной защите), так и в составе разнообразных готовых комплексов аппаратно-программных средств, относимых в целом к разряду промышленных автоматизированных систем управления (*Industrial Automation Control System — IACS*).

Сюда же надо, полагаем, добавить также и следующее, при современных возможностях являющееся во многом «секретом Полишинеля». Имеем в виду встреченные нами в процессе работы немалые и, скорее всего, искусственно созданные сложности для доступа к нынешней нормативной базе Азербайджана по ИКБ. Чего, кстати, не испытали во всех остальных исследовавшихся нами случаях (по США, ЕС, Армении, Грузии, Казахстану, Российской Федерации, Турции, др.).

Из-за этих испытанных нами сложностей не исключаем, что к приведённому в табл. 11 для Азербайджана, возможно, надо будет добавить ещё

*Таблица 13*

| Турецкие идентичные аналоги международных и европейских НТД из табл. 6 и 9 |
|---|
| Для НТД из табл. 6 (всего 44):<br>TS EN ISO/IEC 15408–2:2024 [EN ISO/IEC 15408–2:2023], TS EN ISO/IEC 15408–3:2024 [EN ISO/IEC 15408–3:2023], TS ISO/IEC 27001:2023 [ISO/IEC 27001:2022], TS EN ISO/IEC 27002:2022 [EN ISO/IEC 27002:2022], TS EN ISO/IEC 27005:2024 [EN ISO/IEC 27005:2024], TS EN IEC 62443–2–1:2024 [EN IEC 62443–2–1:2024], TS EN IEC 62443–3–2:2020 [EN IEC 62443–3–2:2020], TS EN IEC 62443–4–1:2018 [EN IEC 62443–4–1:2018], TS EN IEC 62443–4–2:2018/AC:2022 [EN IEC 62443–4–2:2019/AC:2022], TS ISO/IEC 18031:2025 [ISO/IEC 18031:2025], TS EN ISO/IEC 18045:2023 [EN ISO/IEC 18045:2023], TS ISO/IEC 9796–2:2021 [ISO/IEC 9796–2:2010}, TS ISO/IEC 9796–3:2007 [ISO/IEC 9796–3:2006], TS ISO/IEC 9797–1/Amd 1:2023 [ISO/IEC 9797–1:2011/Amd 1:2023], TS ISO/IEC 9797–2/Cor 1:2025 [ISO/IEC 9797–2:2021/Cor 1:2024], TS ISO/IEC 9797–3/Amd 1:2021 [ISO/IEC 9797–3:2011/Amd 1:2020], TS ISO/IEC 9798–1:2019 [ISO/IEC 9798–1:2010], TS ISO IEC 9798–2:2019 [ISO/IEC 9798–2:2019], TS ISO/IEC 9798–3:2019 [ISO/IEC 9798–3:2019], TS ISO/IEC 9798–4/Cor 2:2019 [ISO/IEC 9798–4:1999/COR 2:2012], TS ISO/IEC 9798–5:2012 [ISO/IEC 9798–5:2009], TS ISO/IEC 9798–6:2012 [ISO/IEC 9798–6:2010], TS EN ISO/IEC 24760–1:2022[EN ISO/IEC 24760–1:2022], TS EN ISO/IEC 24760–2:2022 [EN ISO/IEC 24760–2:2022], TS EN ISO/IEC 24760–3:2022 [EN ISO/IEC 24760–3:2022], TS EN ISO/IEC 29146:2023 [EN ISO/IEC 29146:2023], TS ISO/IEC 18033–1:2021 [ISO/IEC 18033–1:2021], TS ISO/IEC 18033–2/Amd 1:2021[ISO/IEC 18033–2:2006/AMD 1:2017], TS ISO/IEC 18033–3/Amd 1:2021 [ISO/IEC 18033–3:2010/AMD 1:2021], TS ISO/IEC 18033–4/Amd 1:2021 [ISO/IEC 18033–4:2011/AMD 1:2020], TS ISO/IEC 18033–5/Amd 1:2021 [ISO/IEC 18033–5:2015/AMD 1:2021], TS ISO/IEC 18033–6:2021 [ISO/IEC 18033–6:2019], TS ISO/IEC 18033–7:2022 [ISO/IEC 18033–7:2022], TS ISO/IEC 14888–1:2015, [ISO/IEC 14888–1:2008], TS ISO/IEC 14888–2:2015 [ISO/IEC 14888–2:2008], TS ISO/IEC 14888–3:2021 [ISO/IEC 14888–3:2018], TS EN ISO/IEC 27701:2025, [EN ISO/IEC 27701:2025], TS EN ISO/IEC 29100:2020 [EN ISO/IEC 29100:2020], TS ISO/IEC 22237–1:2021 [ISO/IEC 22237–1:2021], TS EN ISO/IEC 30111:2020 [EN ISO/IEC 30111:2020], TS ISO/IEC 27036–1:2021 [ISO/IEC 27036–1:2021], TS ISO/IEC 27036–2:2022 [ISO/IEC 27036–2:2022], TS ISO/IEC 27036–3:2023 [ISO/IEC 27036–2:2023], TS EN ISO/IEC 29147:2020 [EN ISO/IEC 29147:2020]. |
| Для НТД из табл. 9 (всего 13):<br>TS EN ISO/IEC 27019:2025 [EN ISO/IEC 27019:2025], TS EN IEC 62645:2020 [EN IEC 62645:2020], TS EN 61850–3:2014 [EN 61850–3:2014], TS EN 61850–4/A1:2021 [EN 61850–4:2011/A1:2020], TS EN 61850–5/A1:2022 [EN 61850–5:2013/A1:2022], TS EN 61850–10/A1:2025 [EN 61850–10:2013/A1:2025], TS EN IEC 62351–3:2023 [EN IEC 62351–3:2023], TS EN IEC 62351–4/A1:2020 [EN IEC 62351–4:2018/A1:2020], TS EN IEC 62351–5:2023 [EN IEC 62351–5:2023], TS EN IEC 62351–6:2021 [EN IEC 62351–6:2020], TS EN IEC 62351–7:2026 [EN IEC 62351–7:2026], TS EN IEC 62351–8:2020 [EN IEC 62351–8:2020], TS EN IEC 62351–9:2023 [EN IEC 62351–9:2023]. |

*Источник:* [15].

и 2–3 других её национальных стандарта по рассматриваемой здесь тематике. Однако вряд ли больше этого количества, что, конечно же, никоим образом не способно смягчить применимость — в том числе и к этой южнокавказской стране — наших крайне отрицательных оценок насчёт какой-либо соизмеримости европейских подходов с необходимыми для национальных КВИ в качестве нормативной базы по ИКБ.

В сравнении с приведённым выше фактом-примером по Азербайджану, не менее вопросительным и, к тому же, в немалой степени показательным, считаем, также и следующее, относящееся к Грузии.

Ещё в проектном документе Еврокомиссии под названием «Укрепление в Грузии потенциала в области кибербезопасности» [17] было определено (см. там пункт 3.4), что повесткой дня сотрудничества между Евросоюзом и Грузией в области цифровой экономики и общества является приложение «усилий по повышению киберустойчивости ключевых секторов критической инфраструктуры и государственных организаций, опираясь на релевантный опыт ЕС и в соответствии с нормами ЕС». Для чего, в свою очередь, этим партнёрским проектом в качестве приоритетов Грузии обозначалось перенятие у ЕС установленного, в частности:

- в ряде заключений и оперативных рекомендаций Совета ЕС июня 2018 года по руководящим принципам наращивания внешнего потенциала Евросоюза в области кибербезопасности (*EU External Cyber Capacity Building Guidelines*), содержащим политические указания по масштабам, принципам, приоритетам и подходу к участию ЕС в этой области;
- в Директиве (ЕС) 2016/1148 Европейского парламента и Совета от 06.07.2016 г., касающейся мер по обеспечению высокого общего уровня безопасности сетей и информационных систем по всему Евросоюзу (NIS Directive concerning measures for a high common level of security of network and information systems across the Union);
- в исполнительном регламенте Еврокомиссии (ЕС) 2018/151 от 30.01.2018 г. (Commission Implementing Regulation (EU) 2018/151), относящемся к управлению рисками, исходящими от цифровых провайдеров, связанных с безопасностью сетей и информационных систем, и определения существенного влияния инцидентов.

Помимо этого, в том же партнёрском (Twinning) проекте в качестве необходимых были определены разработка и внедрение в Грузии новых положений и предписаний, нормативных актов, правил и стандартов — с целью покрытия существующих пробелов между национальным и европейским законодательством.

Особо отметим, что необходимость приведения подхода в Грузии к кибербезопасности в соответствие с установленным, в частности, в Директиве NIS (кстати, отменённой ещё 2022-м [4]) нашло своё отражение сперва в «Стратегии кибербезопасности Грузии и плане действий на 2017–2018 годы», а затем в «Национальной стратегии кибербезопасности Грузии и плане действий на 2020–2022 годы». При этом на реализацию упомянутого выше евро-грузинского проекта было выделено со стороны ЕС миллион триста тысяч евро (EUR 1 300 000): как бы в дополнение к тому, что составляло долю Грузии из 8 миллионов евро (*Factsheet_Georgia_april2021.pdf*), опять же безвозмездно предоставлявшихся ЕС шести странам Восточного партнёрства для реализации ими в 2018 и 2020 годах неких работ по обеспечению киберустойчивости

К чему указанные планы и затраты ЕС по Грузии в итоге привели, подсказывают в немалой степени данные по этой стране, приведённые в табл. 11.

Для паритетности к примерам-фактам по Азербайджану и Грузии можно, в принципе, добавить и что-либо сходное по Армении. Благо, оно не только имеется, но и до сих пор продолжает накапливаться. Однако считаем более целесообразным сделать это в составе всего того, что привело страну к, мягко выражаясь, незавидному состоянию из соответствующей части табл. 11.

*СПИСОК ЛИТЕРАТУРЫ*


1. *Cybersecurity in the power sector (https://www.eurelectric.org/in-detail/cybersecurity-in-the-power-sector/).*
2. *ENISA Threat Landscape 2025. //The European Union Agency for Cybersecurity (ENISA). October 2025. P. 89.*
3. *Battle-tested power systems. Resilience and preparedness for Europe's electricity sector. // Eurelectric, February 2026. P. 32. (20260212-Battle-tested-power-systems-FINAL.pdf).*
4. *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) № 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). // Official Journal of the European Union, 27.12.2022. P. 73.*
5. *Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) № 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). // Official Journal of the European Union, 20.11.2024. P. 81.*
6. *Regulation (EU) 2024/1366 of 11 March 2024 supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows. // Official Journal of the European Union, 24.5.2024. P. 44. (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401366).*
7. *Industrial internet of things (https://en.wikipedia.org/wiki/Industrial_internet_of_things?ysclid=mq27bqnyhu868952072)*
8. *Что такое промышленный интернет вещей (IIoT)? (https://leo.ru/faq/articles/chto-takoe-promyshlennyy-internet-veshchey-iiot-/).*
9. *Cyber Resilience Act Requirements Standards Mapping. //Office of the European Union/The European Union Agency for Cybersecurity (ENISA), 2024. P. 69 (https://publications.jrc.ec.europa.eu/repository/handle/JRC137340).*
10. *Maik G. Seewald. IEC 62351: Security for Grid Automation and Control Protocols. // CISSP. March 2025. P. 8 (https://www.ieee802.org/1/files/public/docs2025/x-seewald-iec62351–0325-v01.pdf).*
11. *Инициатива EU4Digital (https://eufordigital.eu/ru/discover-eu/the-eu4digital-initiative/).*
12. *EU4Digital: Cybersecurity East (https://eufordigital.eu/ru/discover-eu/eu4digital-improving-cyber-resilience-in-the-eastern-partnership-countries/).*
13. *Cybersecurity guidelines for the Eastern Partner countries. EU4Digital: supporting digital economy and society in the Eastern Partnership. // EU4Digital, June, 2020. P. 46.*
14. *Türk dövlətləri arasında kibertəhlükəsizlik standartlarının müəyyən olunması təklif edilir. (https://akta.az/az/news/tuerk-doevletleri-arasinda-kibertehluekesizlik-standartlarinin-mueeyyen-olunmasi-teklif-edilir).*
15. *https://intweb.tse.org.tr/Standard/Standard/StandardAra.aspx.*
16. *Kritik informasiya infrastrukturu obyektləri yeni növ kiberhücumların əsas hədəfindədir. (https://ncsc.gov.az/news-page?tag=CII&index=4).*
17. *EuropeAid/168–164/ACT/GE: Strengthening Cybersecurity Capacities in Georgia. // European Commission. 48p. (8a7bd7d-e7bd-af0b-8f61-d7da4428f2c9).*