ЕС развивает регулирование кибербезопасности межгосударственных перетоков электроэнергии

Применим ли аналогичный подход в энергообъединении СНГ?

Исполнительный комитет Электроэнергетического Совета СНГ (ИК ЭЭС СНГ) в рамках деятельности по координации и поддержке взаимодействия профильных регуляторов в государствах — участниках СНГ анализирует соответствующий международный опыт с целью формирования условий для применения наиболее эффективных подходов как на национальном, так и на межгосударственном уровне.

Купчиков Т.В., председатель Исполнительного комитета ЭЭС СНГ;
Фролова О.Ю., директор департамента по стратегии ИК ЭЭС СНГ

В приоритетном порядке рассматриваются проблемные вопросы практического характера, позиция по которым в экспертной среде находится в активной стадии проработки либо назревает существенная корректировка регулирования.

Так, в рамках 62-го заседания Электроэнергетического Совета СНГ, прошедшего в июне 2023 года в Бишкеке с участием профильных министров и руководителей системообразующих организаций, по инициативе Российской Федерации был рассмотрен вопрос регулирования энергоснабжения майнинга. Были кратко представлены подходы Республики Беларусь, Республики Казахстан и Российской Федерации. В данный момент ожидается более подробный материал от Министерства энергетики Республики Казахстан, чей опыт является, по мнению ИК ЭЭС СНГ, наиболее продуктивным и будет представлен вниманию уважаемых читателей данного издания.

В № 6 (218) 2023 года был опубликован обзор подходов Европейского союза (ЕС, Союз) к долгосрочному развитию электрических сетей с описанием основных действий и межгосударственных механизмов поддержки развития. Нам представляется, что целесообразно рассмотреть подобные механизмы к возможности применения и на пространстве СНГ, что находит отражение в предложениях нашей организации.

Таким образом, настоящая статья продолжает цикл материалов, направленных на анализ отраслевой нормативной базы существующих в мире межгосударственных объединений, и представляет вашему вниманию первую часть обзора Предписания Европейской комиссии от 11 марта 2024 года о повышении коллективной кибербезопасности электроэнергетики — (EU) 2024/1366.

С учётом масштабов инвестиций и амбициозных планов по цифровой трансформации электроэнергетики, количества и динамики появления новых технологий в данной отрасли, вопросов доверия и контроля компонентной базы и программного обеспечения, а также систем управления, не говоря уже о растущей геополитической напряжённости, вопросы кибербезопасности критической инфраструктуры, к чему, безусловно, относится электроэнергетика, в частности, в контексте межгосударственных перетоков электроэнергии, становятся одними из приоритетных и со стратегической точки зрения начинают влиять на архитектуру технологического развития и потенциал расширения межгосударственных рыночных отношений в отрасли.

Данный тезис подтверждается, в частности, выходом в марте 2024 года Предписания Европейской комиссии (EU) 2024/1366 (далее — Предписание, Директива, Документ, Регламент) о повышении коллективной кибербезопасности в электроэнергетике в кратчайшие сроки.

В соответствии с Регламентом, принятым в развитие Предписания Европейского парламента и Европейского совета (EU) 2019/943 (внутренний рынок

электроэнергии), уполномоченные национальные регуляторы и организации ЕС должны в краткие сроки разработать методологию и планы по обеспечению высокого уровня коллективной безопасности в электроэнергетике.

Настоящий Регламент был разработан в тесном взаимодействии с Агентством Европейского союза по сотрудничеству регулирующих органов в области энергетики (ACER), Агентством Европейского союза по кибербезопасности (ENISA), европейскими ассоциациями операторов магистральных и распределительных сетей передачи электроэнергии (ENTSO-E и EU DSO Entity) и другими заинтересованными сторонами с целью принятия эффективных, сбалансированных и пропорциональных правил на прозрачной основе и с привлечением широкого круга участников.

Регламент не наносит ущерба компетенции государств-членов принимать необходимые меры для обеспечения защиты основных интересов своей безопасности, обеспечения политики и общественной безопасности, а также для обеспечения расследования, выявления и судебного преследования уголовных преступлений в соответствии с законодательством Союза. Согласно статье 346 Договора о функционировании Европейского союза, ни одно государство-член не обязано предоставлять информацию, раскрытие которой, по его мнению, противоречит существенным интересам его безопасности.

Необходимо отметить, что рассматриваемый Документ является частью взаимосвязанной нормативной архитектуры Европейского союза, которая, в частности, включает:

- Директиву (ЕС) 2022/2555 Европейского парламента и Совета, определяющую меры для обеспечения высокого общего уровня кибербезопасности на всей территории Европейского союза;
- Регламент (ЕС) 2019/941 Европейского парламента и Совета, дополняющий Директиву (ЕС) 2022/2555, гарантируя, что инциденты кибербезопасности в электроэнергетическом секторе должным образом идентифицируются как риски, и что меры, принимаемые для их устранения, должным образом учитываются в планах по обеспечению готовности к рискам;
- Регламент (ЕС) 2019/943 дополняет Директиву (ЕС) 2022/2555 и Регламент (ЕС) 2019/941, устанавливая конкретные правила для электроэнергетического сектора на уровне Союза, и дополняет положения Директивы (ЕС) 2022/2555, касающиеся электроэнергетического сектора, во всех случаях, когда речь идёт о трансграничных перетоках электроэнергии.

В Директиве ЕС отмечается, что, в контексте взаимосвязанности систем электроснабжения с высоким уровнем цифровизации, предотвращение и преодоление кризисов в сфере электроснабжения, связанных с кибератаками, не может рассматриваться как исключительно национальная задача.

Для разработки более эффективных и менее затратных мер в вышеуказанной области необходимо определить правила, порядок и процедуры скоординированного межгосударственного взаимодействия, чтобы государства-члены и другие субъекты (компетентные органы, ответственные за электроэнергетику и кибербезопасность) могли эффективно сотрудничать через границы в духе повышения прозрачности, доверия и солидарности.

... в контексте взаимосвязанности систем электроснабжения с высоким уровнем цифровизации, предотвращение и преодоление кризисов в сфере электроснабжения, связанных с кибератаками, не может рассматриваться как исключительно национальная задача.

Управление рисками кибербезопасности в рамках рассматриваемого Регламента способствует формированию структурированного процесса, включающего, среди прочего, идентификацию рисков для трансграничных перетоков электроэнергии, связанных с кибератаками, соответствующие операционные процессы и периметры, соответствующие механизмы контроля и проверки кибербезопасности. Несмотря на то, что сроки всего процесса, определённого Регламентом, растянуты на годы, каждый его этап должен способствовать достижению высокого общего уровня кибербезопасности в отрасли и снижению рисков. Все участники процесса должны приложить все усилия для скорейшей, без неоправданных задержек, и не позднее крайних сроков, определённых в Регламенте, разработки и согласования методологий.

Оценки рисков кибербезопасности на уровне Союза, государств-членов, регионов и организаций, предусмотренные настоящим Регламентом, могут быть ограничены рисками, возникающими в результате кибератак, как это определено в Регламенте (ЕС) 2022/2554 Европейского парламента и Совета, что исключает, например, физические нападения, стихийные бедствия и перебои в работе из-за потери оборудования или людских ресурсов.

Понятие «организации с высоким и критическим воздействием» в настоящем Регламенте является основополагающим для определения круга организаций, на которые будут распространяться обязательства, описанные в рассматриваемом Регламенте.

Основанный на оценке рисков подход, изложенный в различных положениях Регламента, направлен на выявление процессов, вспомогательных активов и управляющих ими организаций, которые влияют на трансграничные перетоки электроэнергии.

В зависимости от степени воздействия возможных кибератак на их деятельность трансграничные перетоки электроэнергии в ЕС могут рассматриваться как «оказывающие сильное воздействие» или «имеющие критическое воздействие». То же относится и к объектам, которые определяются как «существенные» (essential) и «значимые» (important) только исходя из их роли и влияния на процессы производства электроэнергии, влияющие на трансграничные перетоки.

... организационные и технические правила должны гарантировать, что большинство инцидентов с электричеством, связанных с первопричинами кибербезопасности, эффективно устраняются на оперативном уровне.

Для обеспечения эффективности и во избежание дублирования в достижении целей рассматриваемый Регламент использует существующие механизмы и инструменты, уже установленные в других законодательных актах.

С целью снижения рисков кибербезопасности, в соответствии с Документом, планируется разработать подробный свод правил, регулирующих действия и сотрудничество между заинтересованными сторонами, деятельность которых касается аспектов кибербезопасности трансграничных перетоков электроэнергии, с целью обеспечения безопасности энергосистемы.

Эти организационные и технические правила должны гарантировать, что большинство инцидентов с электричеством, связанных с первопричинами кибербезопасности, эффективно устраняются на оперативном уровне.

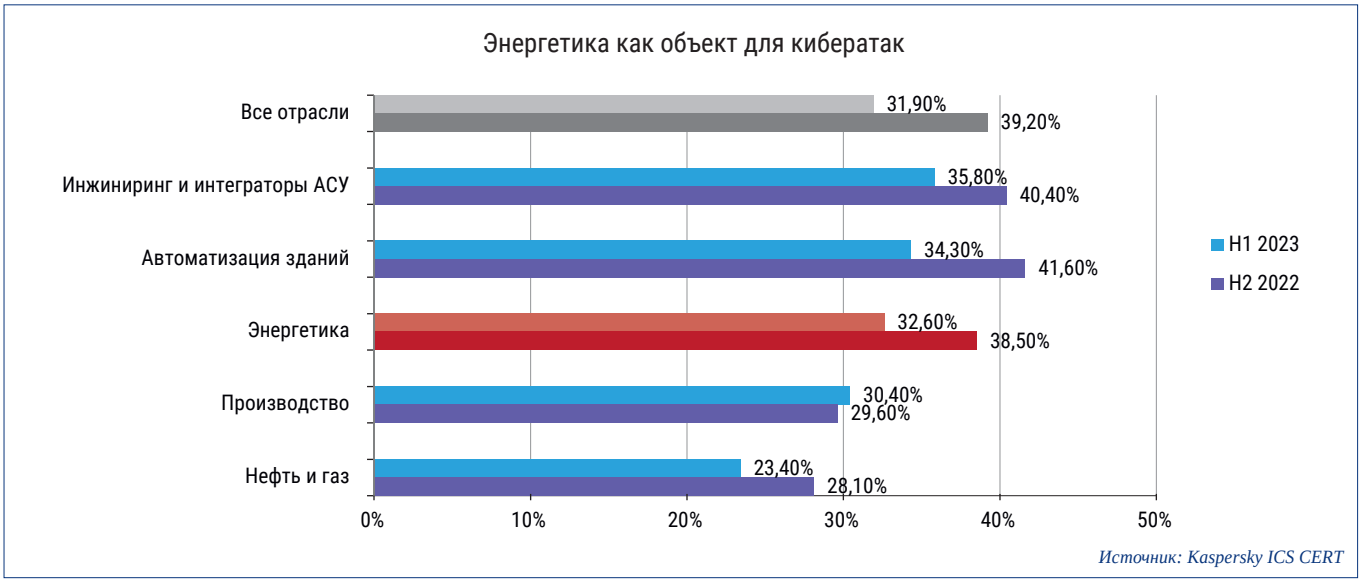
Планируется определить, что соответствующие заинтересованные стороны должны делать для предотвращения таких кризисов и какие меры они могут предпринять в том случае, если действующих правил работы системы уже недостаточно. Следовательно, необходимо разработать общую систему правил о том, как предотвращать, готовиться и справляться с одновременными кризисами в электроснабжении, первопричиной которых является кибербезопасность. Это обеспечивает большую прозрачность на этапе подготовки и во время одновременного энергетического кризиса и гарантирует скоординированное и эффективное принятие мер совместно с компетентными органами по кибербезопасности в государствах-членах.

В соответствии с Документом надёжность электроснабжения предполагает эффективное сотрудничество между государствами-членами, институтами Союза, органами, ведомствами и агентствами, а также соответствующими заинтересованными сторонами. Операторы систем распределения и передачи электроэнергии играют ключевую роль в обеспечении безопасной, надёжной и эффективной системы электроснабжения в соответствии со статьями 31 и 40 настоящей Директивы.

Общий подход к одновременному предотвращению и управлению кризисами в сфере электроснабжения требует общего понимания государствами-членами того, что представляет собой одновременный кризис в сфере электроснабжения, и когда кибератака является важным фактором. В частности, в целях устранения ситуации, в которой существует потенциальный риск значительного дефицита электроэнергии или невозможности снабжения потребителей электроэнергией, и это связано с кибератакой.

Чтобы избежать пробелов или дублирования обязательств по управлению рисками в области кибербезопасности, налагаемых на организации с высокой степенью воздействия и имеющих критическое значение, национальные органы в соответствии с Директивой (ЕС) 2022/2555 и компетентные органы в соответствии с настоящим Регламентом должны сотрудничать в отношении реализации мер по управлению рисками в области кибербезопасности и надзора за соблюдением этих мер на национальном уровне. Соответствие организации требованиям по управлению рисками кибербезопасности, изложенным в настоящем Регламенте, может быть рассмотрено компетентным органом в соответствии с Директивой (ЕС) 2022/2555 для обеспечения соблюдения соответствующих требований, изложенных в этой Директиве, или наоборот.

Общий подход к предотвращению и урегулированию кризисов в электроэнергетике, связанных с первопричинами кибербезопасности, также требует, чтобы все заинтересованные стороны использовали согласованные методы и определения для выявления рисков, связанных с кибербезопасностью электроснабжения. Это также требует наличия возможности эффективно сравнивать, насколько хорошо они и их соседи работают в этой области. Следовательно, необходимо определить процессы, роли и обязанности для разработки и обновления методологий управления рисками, шкал классификации инцидентов и меры кибербезопасности, адаптированные к рискам кибербезопасности, влияющим на трансграничные перетоки электроэнергии.



Процент российских компьютеров АСУ, на которых были заблокированы вредоносные объекты

Государства — члены ЕС через компетентный орган, назначенный для применения настоящего Регламента, несут ответственность за выявление организаций, которые отвечают критериям отнесения к субъектам с высоким и критическим воздействием. В целях устранения разногласий между государствами-членами в этом отношении и обеспечения правовой определённости в отношении мер по управлению рисками кибербезопасности и обязательств по представлению отчётности для всех соответствующих организаций планируется установить набор критериев, которые определяют организации, подпадающие под действие настоящего Регламента. Этот набор критериев должен регулярно обновляться в процессе разработки и принятия положений, условий и методологий, изложенных в настоящем Регламенте.

Положения настоящего Регламента должны применяться без ущерба для законодательства Союза, предусматривающего конкретные правила сертификации продуктов, услуг и процессов в области информационно-коммуникационных технологий (ИКТ), в частности, без ущерба для Регламента (ЕС) 2019/881 в отношении основы для создания Европейской системы сертификации в области кибербезопасности.

В контексте рассматриваемого Регламента продукты ИКТ должны также включать технические устройства и программное обеспечение, которые обеспечивают прямое взаимодействие с электротехнической сетью, в частности с промышленными системами управления, которые могут использоваться для передачи, распределения и производства энергии, а также для сбора и передачи соответствующей информации. Положения должны гарантировать, что соответствующие цели обеспечения безопасности, изложенные в статье 51 Регламента (ЕС) 2019/881, выполняются закупаемыми продуктами, услугами и процессами в области ИКТ.

Недавние кибератаки показывают, что предприятия все чаще становятся объектами атак на цепочки поставок. Такие атаки не только оказывают влияние на отдельные предприятия, но также могут оказывать каскадное воздействие на более крупные атаки на предприятия, к которым они подключены в электросети. Поэтому были добавлены положения и рекомендации, помогающие снизить риски кибербезопасности вследствие процессов, связанных с цепочкой поставок, в частности с закупками, которые влияют на трансграничные перетоки электроэнергии.

В Документе отмечается, что защита кибербезопасности не ограничивается границами Европейского союза. Безопасная система требует участия соседних третьих стран. Европейский союз и его государства-члены должны стремиться поддерживать соседние третьи страны, чья электроэнергетическая инфраструктура подключена к европейской энергосистеме, в применении аналогичных правил кибербезопасности, изложенных в рассматриваемом Регламенте.

На основании рассмотрения вышеуказанного документа ИК ЭЭС СНГ инициировал диалог с уполномоченными межгосударственными органами о целесообразности разработки аналогичных документов на пространстве СНГ.

В следующей статье мы продолжим обзор Предписания Европейской комиссии (EU) 2024/1366. Мы также будем рады услышать мнение уважаемой аудитории на поставленный в заголовке вопрос. ■