Об утверждении Правил обеспечения информационной безопасности в сфере топливно-энергетического комплекса

Приказ Министра энергетики Республики Казахстан от 15 сентября 2025 года № 349-н/қ. Зарегистрирован в Министерстве юстиции Республики Казахстан 16 сентября 2025 года № 36852

В соответствии с подпунктом 6-3) статьи 5 Закона Республики Казахстан "Об электроэнергетике" ПРИКАЗЫВАЮ:

1. Утвердить прилагаемые Правила обеспечения информационной безопасности в сфере топливно-энергетического комплекса.

2. Департаменту цифровизации Министерства энергетики Республики Казахстан в установленном законодательством Республики Казахстан порядке обеспечить:

1) государственную регистрацию настоящего приказа в Министерстве юстиции Республики Казахстан;

2) размещение настоящего приказа на интернет-ресурсе Министерства энергетики Республики Казахстан;

3) в течение десяти рабочих дней после государственной регистрации настоящего приказа представление в Департамент юридической службы Министерства энергетики Республики Казахстан сведений об исполнении мероприятий, предусмотренных подпунктами 1) и 2) настоящего пункта.

3. Контроль за исполнением настоящего приказа возложить на курирующего вице-министра энергетики Республики Казахстан.

4. Настоящий приказ вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования.

Министр энергетики
Республики Казахстан *Е. Аккенженов*

"СОГЛАСОВАН"
Министерство финансов
Республики Казахстан

"СОГЛАСОВАН"
Министерство национальной экономики
Республики Казахстан

"СОГЛАСОВАН"
Министерство цифрового развития,
инноваций и аэрокосмической
промышленности Республики Казахстан

утверждены приказом

Министр энергетики
Республики Казахстан
от 15 сентября 2025 года № 349-н/қ

Правила обеспечения информационной безопасности в сфере топливно-энергетического комплекса

Глава 1. Общие положения

1. Настоящие Правила обеспечения информационной безопасности в сфере топливно-энергетического комплекса (далее – Правила) разработаны в соответствии с подпунктом 6-3) статьи 5 Закона Республики Казахстан "Об электроэнергетике" (далее - Закон) и определяют порядок для обеспечения информационной безопасности в сфере топливно-энергетического комплекса, киберустойчивость критически важных объектов информационно-коммуникационной инфраструктуры топливно-энергетического комплекса.

2. К объектам информационной безопасности отраслевого центра информационной безопасности в сфере топливно-энергетического комплекса относятся промышленные системы управления топливно-энергетического комплекса.

Глава 2. Порядок обеспечения информационной безопасности в сфере топливно-энергетического комплекса и функционирования отраслевого центра информационной безопасности в сфере топливно-энергетического комплекса

3. Отраслевой центр информационной безопасности в сфере топливно-энергетического комплекса (далее – Отраслевой центр) функционирует на постоянной основе, руководствуясь принципами законности, централизации управления, оперативности реагирования на инциденты информационной безопасности и конфиденциальности информации.

4. Основной целью функционирования Отраслевого центра является создание единого защищенного информационного пространства для субъектов топливно-энергетического комплекса, обеспечивающего устойчивость критически важных объектов информационно-коммуникационной инфраструктуры топливно-энергетического комплекса в условиях современных киберугроз.

5. Отраслевым центром является юридическое лицо, определенное в соответствии с подпунктом 6-4) статьи 5 Закона, осуществляющее организацию и координацию мероприятий по формированию защищенного информационного пространства топливно-энергетического комплекса (далее - ТЭК).

6. Отраслевой центр запрашивает и получает от субъектов ТЭК и оперативных центров информационной безопасности (далее - ОЦИБ) информацию, необходимую для анализа угроз информационной безопасности, включая данные о киберинцидентах, параметрах работы защитных систем и результатах аудитов безопасности.

7. Отраслевой центр разрабатывает методические рекомендации, стандарты и регламенты по защите информационных систем субъектов ТЭК, которые учитываются субъектами ТЭК при организации мер информационной безопасности. Отраслевой центр направляет методические рекомендации, стандарты и регламенты по защите информационных систем субъектов ТЭК субъектам ТЭК для применения в работе, а также в уполномоченый орган в области электроэнергетики для сведения.

8. Отраслевой центр проводит обследование состояния защищенности информационных систем субъектов ТЭК, за исключением объектов, относящихся к государственным секретам.

9. Отраслевой центр по результатам обследования информационной безопасности субъектов ТЭК, направляет рекомендации по устранению выявленных нарушений со сроком их исполнения в течение одного месяца. При выявлении критических нарушений, создающих угрозу устойчивой работе объектов ТЭК, Отраслевой центр уведомляет уполномоченный орган в сфере обеспечения информационной безопасности в соответствии с Правилами проведения мониторинга событий информационной безопасности объектов информатизации государственных органов, утвержденных приказом исполняющего обязанности Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 16 августа 2019 года № 199/НҚ (зарегистрирован в Реестре государственной регистрации нормативных правовых актов под № 19286).

10. Отраслевой центр осуществляет мониторинг киберугроз посредством анализа данных о событиях информационной безопасности, поступающих от ОЦИБ.

Все поступающие данные анализируются с применением методов машинного обучения и поведенческого анализа для выявления аномальной активности. Особое внимание уделяется обнаружению целевых атак на промышленные системы управления ТЭК.

11. Для оперативного реагирования на инциденты информационной безопасности в Отраслевом центре действует трехуровневая система классификации угроз, из которых:

1) критические инциденты, создающие непосредственную угрозу устойчивой работе объектов ТЭК, требующие немедленного реагирования - в течение 1 (одного) часа с момента обнаружения;

2) для инцидентов высокого риска срок реагирования составляет до 4 (четырех) часов;

3) для инцидентов низкого уровня срок реагирования составляет до 24 (двадцати четырех) часов.

12. В каждом случае группа реагирования Отраслевого центра разрабатывает индивидуальный план мероприятий по локализации и устранению последствий атаки.

13. Субъекты ТЭК обеспечивают передачу в ОЦИБ данных, необходимых для осуществления мониторинга информационной безопасности, в форматах, объемах и порядке, установленных регламентом Отраслевого центра.

14. Субъекты ТЭК, при самостоятельном обнаружении инцидента информационной безопасности, оповещают Отраслевой центр в течении 30 (тридцать) минут с момента обнаружения.

15. Взаимодействие Отраслевого центра с уполномоченным органом в области электроэнергетики осуществляется через регулярный обмен информацией в следующих форматах и сроки:

1) уведомление обо всех инцидентах информационной безопасности предоставляется в течение 1 (одного) часа с момента их обнаружения для принятия срочных мер реагирования;

2) оперативные сводки о текущем состоянии информационной безопасности отрасли, включая статус (обработки) ранее выявленных инцидентов, направляются ежедневно до 10:00 часов по времени города Астаны;

3) еженедельные аналитические отчеты о состоянии информационной безопасности отрасли, направляемые каждую пятницу до 18:00 часов по времени города Астаны, с последующей обратной связью в течение 3 (трех) рабочих дней;

4) ежемесячные отчеты с оценкой эффективности принимемых мер информационной безопасности предоставляются до 5 (пятого) числа следующего месяца с получением сводного отзыва в течение 10 (десяти) рабочих дней.

16. Отраслевой центр участвует в разработке и реализации государственных программ по защите критической информационной инфраструктуры, вносит предложения по совершенствованию законодательства Республики Казахстан в области кибербезопасности ТЭК.

17. Отраслевой центр осуществляет постоянное и системное взаимодействие с Национальным координационным центром информационной безопасности (далее - НКЦИБ) в соответствии со статьей 7-5 Закона Республики Казахстан "Об информатизации". Техническое взаимодействие с НКЦИБ осуществляется через защищенные каналы связи с использованием сертифицированных средств криптографической защиты информации.

Глава 3. Порядок обеспечения конфиденциальности и защиты информации

18. Все данные, поступающие в Отраслевой центр от субъектов ТЭК, подлежат защите в соответствии Едиными требованиями в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденными постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832 (далее – Единые требования).

19. Отраслевой центр использует сертифицированные средства криптографической защиты информации, системы контроля доступа и технические средства обеспечения безопасности.

20. Защита информации о критически важных объектах информационно-коммуникационной инфраструктуры ТЭК и уязвимостях их информационных систем, основывается на выполнении следующих требовании:

1) отнесение сведений к служебной информации ограниченного распространения в порядке, установленном Правилами отнесения сведений к служебной информации ограниченного распространения и работы с ней, утвержденными постановлением Правительства Республики Казахстан от 24 июня 2022 года № 429;

2) обработка и хранение информации в Отраслевом центре осуществляются в специально выделенных защищенных сегментах информационной системы Отраслевого центра.

21. Требования к безопасности сегментов определяются на основе комплексного подхода к управлению рисками, в соответствии с СТ РК IEC 62443-3-3 "Сети коммуникационные промышленные. Безопасность сети и системы - Часть 3-3. Требования к системной безопасности и уровня безопасности" и Едиными требованиями.