О внесении изменений в приказ Министра энергетики Республики Казахстан от 15 сентября 2025 года № 349-н/қ "Об утверждении Правил обеспечения информационной безопасности в сфере топливно-энергетического комплекса"

Приказ Министра энергетики Республики Казахстан от 13 апреля 2026 года № 148-н/қ. Зарегистрирован в Министерстве юстиции Республики Казахстан 20 апреля 2026 года № 38484

Примечание ИЗПИ!

Вводится в действие с 11.07.2026.

ПРИКАЗЫВАЮ:

1. Внести в приказ Министра энергетики Республики Казахстан от 15 сентября 2025 года № 349-н/қ "Об утверждении Правил обеспечения информационной безопасности в сфере топливно-энергетического комплекса" (зарегистрирован в Реестре государственной регистрации нормативных правовых актов под № 36852) следующие изменения:

заголовок приказа изложить в новой редакции:

"Об утверждении Правил обеспечения кибербезопасности в сфере топливно-энергетического комплекса";

пункт 1 приказа изложить в новой редакции:

"1. Утвердить прилагаемые Правила обеспечения кибербезопасности в сфере топливно-энергетического комплекса.";

Правила обеспечения информационной безопасности в сфере топливно-энергетического комплекса, утвержденные указанным приказом, изложить в новой редакции согласно приложению к настоящему приказу.

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 после его официального опубликования;

3) в течение десяти рабочих дней после государственной регистрации настоящего приказа в Министерстве юстиции Республики Казахстан 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 с 11 июля 2026 года и подлежит официальному опубликованию.

Министр энергетики
Республики Казахстан *Е. Аккенженов*

"СОГЛАСОВАН"
Министерство искусственного
интеллекта и цифрового развития
Республики Казахстан

"СОГЛАСОВАН"
Министерство финансов
Республики Казахстан

"СОГЛАСОВАН"
Министерство национальной экономики
Республики Казахстан

Приложение к приказу
Министр энергетики
Республики Казахстан
от 13 апреля 2026 года № 148-н/қ
Утверждены приказом
Министра энергетики
Республики Казахстан
от 15 сентября 2025 года № 349-н/қ

Правила
обеспечения кибербезопасности в сфере топливно-энергетического комплекса

Глава 1. Общие положения

1. Настоящие Правила обеспечения кибербезопасности 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 кибербезопасности в сфере топливно-энергетического комплекса, киберустойчивость критически важных цифровых объектов топливно-энергетического комплекса.

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

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

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

4. Основной целью функционирования Отраслевого центра является создание единого защищенного цифрового пространства для субъектов топливно-энергетического комплекса, обеспечивающего устойчивость критически важных цифровых объектов 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 цифрового пространства топливно-энергетического комплекса.

6. Отраслевой центр запрашивает и получает от субъектов топливно-энергетического комплекса и оперативных центров кибербезопасности информацию, необходимую для анализа угроз кибербезопасности, включая данные о киберинцидентах, параметрах работы защитных систем и результатах аудитов кибербезопасности.

7. Отраслевой центр разрабатывает методические рекомендации, стандарты и регламенты по защите цифровых систем субъектов топливно-энергетического комплекса, которые учитываются субъектами топливно-энергетического комплекса при организации мер кибербезопасности. Отраслевой центр направляет методические рекомендации, стандарты и регламенты по защите цифровых систем субъектов топливно-энергетического комплекса субъектам топливно-энергетического комплекса для применения в работе, а также в уполномоченый орган в области электроэнергетики для сведения.

8. Отраслевой центр проводит обследование состояния защищенности цифровых систем субъектов топливно-энергетического комплекса, за исключением объектов, относящихся к государственным секретам.

9. Отраслевой центр по результатам обследования кибербезопасности субъектов топливно-энергетического комплекса, направляет рекомендации по устранению выявленных нарушений со сроком их исполнения в течение одного месяца. При выявлении критических нарушений, создающих угрозу устойчивой работе объектов топливно–энергетического комплекса, Отраслевой центр уведомляет уполномоченный орган в сфере обеспечения кибербезопасности в соответствии с Правилами проведения мониторинга событий кибербезопасности цифровых объектов государственных органов, утверждаемыми уполномоченным органом в сфере обеспечения кибербезопасности в соответствии с подпунктом 6) статьи 7–1 Закона Республики Казахстан "О кибербезопасности".

10. Отраслевой центр осуществляет мониторинг киберугроз посредством анализа данных о событиях кибербезопасности, поступающих от оперативных центров кибербезопасности.

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 топливно-энергетического комплекса.

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

1) критические инциденты, создающие непосредственную угрозу устойчивой работе объектов топливно-энергетического комплекса, 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 топливно–энергетического комплекса обеспечивают передачу в оперативные центры кибербезопасности данных, необходимых для осуществления мониторинга кибербезопасности, в форматах, объемах и порядке, установленных регламентом Отраслевого центра.

14. Субъекты топливно-энергетического комплекса, при самостоятельном обнаружении инцидента кибербезопасности, 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 кибербезопасности предоставляется в течение 1 (одного) часа с момента их обнаружения для принятия срочных мер реагирования;

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

3) еженедельные аналитические отчеты о состоянии кибербезопасности 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 принимаемых мер кибербезопасности 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 цифровой инфраструктуры, вносит предложения по совершенствованию законодательства Республики Казахстан в области кибербезопасности топливно-энергетического комплекса.

17. Отраслевой центр осуществляет постоянное и системное взаимодействие с Национальным координационным центром кибербезопасности в соответствии со статьей 9 Закона Республики Казахстан "О кибербезопасности". Техническое взаимодействие с Национальным координационным центром кибербезопасности 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 топливно-энергетического комплекса, подлежат защите в соответствии Едиными требованиями в сферах цифровизации и обеспечение кибербезопасности, утверждаемыми Правительством Республики Казахстан в соответствии с подпунктом 3) статьи 6 Закона Республики Казахстан "О кибербезопасности" (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 цифровых объектах топливно-энергетического комплекса и уязвимостях их цифровых систем, основывается на выполнении следующих требований:

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 цифровой 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.