"Отын-энергетика кешені саласындағы ақпараттық қауіпсіздікті қамтамасыз ету қағидаларын бекіту туралы" Қазақстан Республикасы Энергетика министрінің 2025 жылғы 15 қыркүйектегі № 349-н/қ бұйрығына өзгерістер енгізу туралы

Қазақстан Республикасы Энергетика министрінің 2026 жылғы 13 сәуірдегі № 148-н/қ бұйрығы. Қазақстан Республикасының Әділет министрлігінде 2026 жылғы 20 сәуірде № 38484 болып тіркелді

ЗҚАИ-ның ескертпесі!

Осы бұйрық 11.07.2026 ж. бастап қолданысқа енгізіледі

БҰЙЫРАМЫН:

1. "Отын-энергетика кешені саласындағы ақпараттық қауіпсіздікті қамтамасыз ету қағидаларын бекіту туралы" Қазақстан Республикасы Энергетика министрінің 2025 жылғы 15 қыркүйектегі № 349-н/қ бұйрығына (Нормативтік құқықтық актілерді мемлекеттік тіркеу тізілімінде № 36852 болып тіркелген) мынадай өзгерістер енгізілсін:

бұйрықтың тақырыбы жаңа редакцияда жазылсын:

"Отын-энергетика кешені саласындағы киберқауіпсіздікті қамтамасыз ету қағидаларын бекіту туралы";

бұйрықтың 1-тармағы жаңа редакцияда жазылсын:

"1. Отын-энергетика кешені саласындағы киберқауіпсіздікті қамтамасыз ету қағидалары бекітілсін.";

Көрсетілген бұйрықпен бекітілген Отын-энергетика кешені саласындағы ақпараттық қауіпсіздікті қамтамасыз ету қағидалары осы бұйрықтың қосымшасына сәйкес жаңа редакцияда жазылсын.

2. Қазақстан Республикасы Энергетика министрлігінің Цифрландыру департаменті Қазақстан Республикасының заңнамасында белгіленген тәртіппен:

1) осы бұйрықты Қазақстан Республикасының Әділет министрлігінде мемлекеттік тіркеуді;

2) осы бұйрықты Қазақстан Республикасы Энергетика министрлігінің интернет-ресурсында ресми ресми жарияланғаннан кейін орналастыруды;

3) осы бұйрық Қазақстан Республикасы Әділет министрлігінде мемлекеттік тіркелгеннен кейін он жұмыс күні ішінде Қазақстан Республикасы Энергетика министрлігінің Заң қызметі департаментіне осы тармақтың 1) және 2) тармақшаларында көзделген іс-шаралардың орындалғаны туралы мәліметтерді ұсынуды қамтамасыз етсін.

3. Осы бұйрықтың орындалуын бақылау жетекшілік ететін Қазақстан Республикасының энергетика вице-министріне жүктелсін.

4. Осы бұйрық 2026 жылғы 11 шілдеден бастап қолданысқа енгізіледі және ресми жариялануға тиісті.

Қазақстан Республикасы Энергетика министрі *Е. Аккенженов*

"КЕЛІСІЛДІ"
Қазақстан Республикасының
Жасанды интеллект және
цифрлық даму министрлігі
"КЕЛІСІЛДІ"
Қазақстан Республикасының
Қаржы министрлігі
"КЕЛІСІЛДІ"
Қазақстан Республикасының
Ұлттық экономика министрлігі

Қазақстан Республикасы
Энергетика министрі
2026 жылғы 13 сәуірдегі
№ 148-н/қ бұйрығына
қосымша
Қазақстан Республикасы
Энергетика министрінің
2025 жылғы 17 қыркүйектегі
№ 349-н/қ бұйрықпен
бекітілген

Отын-энергетика кешені саласындағы киберқауіпсіздікті қамтамасыз ету қағидалары

1-тарау. Жалпы ережелер

1. Осы Отын-энергетика кешені саласындағы киберқауіпсіздікті қамтамасыз ету қағидалары (бұдан әрі – Қағидалар) "Электр энергетикасы туралы" Қазақстан Республикасы Заңы (бұдан әрі – Заң) 5-бабының 6-3) тармақшасына сәйкес отын-энергетика кешені аса маңызды цифрлық объектілерінің кибертұрақтылығын, отын-энергетика саласындағы киберқауіпсіздікті қамтамасыз ету тәртібін айқындайды.

2. Отын-энергетика кешені саласындағы киберқауіпсіздіктің салалық орталығының киберқауіпсіздік объектілеріне отын-энергетика кешенін басқарудың өнеркәсіптік жүйелері жатады.

2-тарау. Отын-энергетика кешені саласындағы киберқауіпсіздікті қамтамасыз ету және отын-энергетика кешені саласындағы киберқауіпсіздіктің салалық орталығының жұмыс істеу тәртібі

3. Отын-энергетика кешені саласындағы киберқауіпсіздіктің салалық орталығы (бұдан әрі – Салалық орталық) заңдылық, басқаруды орталықтандыру,

киберқауіпсіздіктің оқыс оқиғаларына ден қою жеделдігі және ақпараттың құпиялылығы қағидаттарын басшылыққа ала отырып, тұрақты негізде жұмыс істейді.

4. Салалық орталықтың жұмыс істеуінің негізгі мақсаты қазіргі заманғы киберқауіптер жағдайында отын-энергетика кешені аса маңызды цифрлық объектілерінің орнықтылығын қамтамасыз ететін отын-энергетика кешенінің субъектілері үшін бірыңғай қорғалған цифрлық кеңістік құру болып табылады.

5. Заңның 5-бабы 6-4) тармақшасына сәйкес айқындалған отын-энергетика кешені қорғалған цифрлық кеңістігін қалыптастыру жөніндегі іс-шараларды ұйымдастыруды және үйлестіруді жүзеге асыратын заңды тұлға салалық орталық болып табылады.

6. Салалық орталық кибероқыс оқиғалар, қорғау жүйелерінің жұмыс параметрлері және киберқауіпсіздік аудиттерінің нәтижелері туралы деректерді қоса алғанда, киберқауіпсіздікке төнетін қатерлерді талдау үшін қажетті ақпаратты Отын-энергетика кешенінің субъектілерінен және киберқауіпсіздіктің жедел орталықтарынан сұратады және алады.

7. Салалық орталық киберқауіпсіздік шараларын ұйымдастыру кезінде Отын-энергетика кешенінің субъектілері ескеретін Отын-энергетика кешенінің субъектілерінің цифрлық жүйелерін қорғау жөніндегі әдістемелік ұсынымдарды, стандарттарды және регламенттерді әзірлейді. Салалық орталық Отын-энергетика кешенінің субъектілеріне жұмыста қолдану үшін Отын-энергетика кешені субъектілерінің цифрлық жүйелерін қорғау жөніндегі әдістемелік ұсынымдарды, стандарттарды және регламенттерді жолдайды, сондай-ақ оларды электр энергетикасы саласындағы уәкілетті органға мәлімет үшін жолдайды.

8. Салалық орталық мемлекеттік құпияларға жататын объектілерді қоспағанда, Отын-энергетика кешені субъектілерінің цифрлық жүйелерінің қорғалу жай-күйіне зерттеп-қарау жүргізеді.

9. Салалық орталық Отын-энергетика кешенінің субъектілерінің киберқауіпсіздігін зерттеп-қарау нәтижелері бойынша анықталған бұзушылықтарды бір ай ішінде орындау мерзімімен оларды жою жөнінде ұсынымдар жібереді. Отын-энергетика кешенінің объектілерінің тұрақты жұмысына қатер төндіретін сыни бұзушылықтар анықталған кезде Салалық орталық "Киберқауіпсіздік туралы" Қазақстан Республикасының Заңы 7–1-бабының 6) тармақшасына сәйкес киберқауіпсіздік қамтамасыз ету саласындағы уәкілетті органмен бекітілген "Мемлекеттік органдардың цифрландыру объектілерінің киберқауіпсіздігі оқиғаларына мониторинг жүргізу қағидаларына" сәйкес киберқауіпсіздікті қамтамасыз ету саласындағы уәкілетті органды хабардар етеді.

10. Салалық орталық киберқауіптердің мониторингін киберқауіпсіздіктің жедел орталықтарынан келіп түсетін киберқауіпсіздік оқиғалары туралы деректерді талдау арқылы жүзеге асырады.

Барлық келіп түскен деректер қалыптан тыс белсенділікті анықтау үшін мінез-құлықты талдау және машиналық оқыту әдістерді қолдана отырып талданады. Отын-энергетика кешенін басқарудың өнеркәсіптік жүйелеріне нысаналы шабуылдарды анықтауға ерекше назар аударылады.

11. Киберқауіпсіздіктің оқыс оқиғаларына ден қою үшін Салалық орталықта қауіптерді жіктеудің үш деңгейлі жүйесі жұмыс істейді, оның ішінде:

1) жедел ден қоюды талап ететін Отын-энергетика кешені объектілерінің тұрақты жұмысына тікелей қауіп төндіретін сыни оқыс оқиғалар – анықталған сәттен бастап 1 (бір) сағат ішінде;

2) жоғары қауіпті оқыс оқиғалар үшін ден қою мерзімі 4 (төрт) сағатқа дейінгі уақытты құрайды;

3) төмен деңгейдегі оқыс оқиғалар үшін ден қою мерзімі 24 (жиырма төрт) сағатқа дейінгі уақытты құрайды.

12. Әрбір жағдайда Салалық орталықтың ден қою тобы шабуылдың салдарларын оқшаулау және оларды жою жөніндегі жеке іс-шаралар жоспарын әзірлейді.

13. Отын-энергетика кешенінің субъектілері киберқауіпсіздік мониторингін жүзеге асыру үшін қажетті деректерді Салалық орталық регламентінде белгіленген форматтарда, көлемдерде және тәртіппен киберқауіпсіздіктің жедел орталықтарына беруді қамтамасыз етеді.

14. Отын-энергетика кешенінің субъектілері киберқауіпсіздік оқыс оқиғаларын өз бетінше анықтаған кезде Салалық орталықты оқыс оқиғаны анықтаған сәттен бастап 30 (отыз) минут ішінде хабардар етеді.

15. Салалық орталықтың электр энергетикасы саласындағы уәкілетті органмен өзара іс-қимылы мынадай форматтарда және мерзімдерде тұрақты ақпарат алмасу арқылы жүзеге асырылады:

1) киберқауіпсіздіктің барлық оқыс оқиғасы туралы хабарлама ден қою шараларын қабылдау үшін олар анықталған кезден бастап 1 (бір) сағат ішінде беріледі;

2) бұдан бұрын анықталған оқыс оқиғалардың мәртебесін (өңдеу) қоса алғанда, саланың киберқауіпсіздігінің ағымдағы жай-күйі туралы жедел мәліметтер күн сайын Астана қаласының уақыты бойынша сағат 10:00-ге дейін жіберіледі;

3) Астана қаласының уақыты бойынша әр жұма сайын сағат 18:00-ге дейін жіберілетін, кейіннен 3 (үш) жұмыс күні ішінде кері байланыспен саланың киберқауіпсіздігінің жай-күйі туралы апта сайынғы талдамалық есептер;

4) қабылданатын киберқауіпсіздік шараларының тиімділігін бағалай отырып, ай сайынғы есептер 10 (он) жұмыс күні ішінде жиынтық пікірді ала отырып, келесі айдың 5 (бесінші) күніне дейін ұсынылады.

16. Салалық орталық маңызды цифрлық инфрақұрылымды қорғау жөніндегі мемлекеттік бағдарламаларды әзірлеуге және оларды іске асыруға қатысады, Қазақстан

Республикасының отын-энергетика кешенінің киберқауіпсіздігі саласындағы заңнамасын жетілдіру жөнінде ұсыныстар енгізеді.

17. Салалық орталық "Киберқауіпсіздік туралы" Қазақстан Республикасы Заңының 9-бабына сәйкес Ұлттық киберқауіпсіздікті үйлестіру орталығымен тұрақты және жүйелі өзара іс-қимылды жүзеге асырады. Ұлттық киберқауіпсіздікті үйлестіру орталығымен техникалық өзара іс-қимыл ақпаратты криптографиялық қорғаудың сертификатталған құралдарын пайдалана отырып, қорғалған байланыс арналары арқылы жүзеге асырылады.

3-тарау. Ақпараттың құпиялылығын және оның қорғалуын қамтамасыз ету тәртібі

18. Салалық орталыққа отын-энергетика кешенінің субъектілерінен келіп түсетін барлық деректер Қазақстан Республикасы Үкіметімен бекітілген "Киберқауіпсіздік туралы" Қазақстан Республикасы Заңы 6-бабының 3) тармақшасына (бұдан әрі – Бірыңғай талаптар) сәйкес қорғалуға тиіс.

19. Салалық орталық сертификатталған криптографиялық ақпаратты қорғау құралдарын, қол жеткізуді басқару жүйелерін және техникалық қауіпсіздік құралдарын пайдаланады.

20. Отын-энергетика кешенінің аса маңызды цифрлық объектілері және олардың цифрлық жүйелерінің осалдықтары туралы ақпаратты қорғау мынадай талаптарды орындауға негізделеді:

1) Қазақстан Республикасы Үкіметінің 2022 жылғы 24 маусымдағы № 429 қаулысымен бекітілген "Мәліметтерді таратылуы шектелген қызметтік ақпаратқа жатқызу және онымен жұмыс істеу қағидаларында" белгіленген тәртіппен мәліметтерді таратылуы шектелген қызметтік ақпаратқа жатқызу;

2) Салалық орталықта ақпаратты өңдеу және сақтау Салалық орталық цифрлық жүйесінің арнайы бөлінген қорғалған сегменттерінде жүзеге асырылады.

21. Сегменттердің қауіпсіздігіне қойылатын талаптар ҚР СТ IEC 62443-3-3 " Коммуникациялық өнеркәсіптік желілер. Желі мен жүйенің қауіпсіздігі –3-3-бөлім. Жүйелік қауіпсіздік пен қауіпсіздік деңгейіне қойылатын талаптар" және Бірыңғай талаптармен" анықталады.

© 2012. Қазақстан Республикасы Әділет министрлігінің «Қазақстан Республикасының Заңнама және құқықтық ақпарат институты» ШЖҚ РМК