Сумен жабдықтау және (немесе) су бұру саласындағы ақпараттық қауіпсіздікті қамтамасыз етуге арналған қағидаларды бекіту туралы

Қазақстан Республикасы Өнеркәсіп және құрылыс министрінің 2025 жылғы 16 қыркүйектегі № 370 бұйрығы. Қазақстан Республикасының Әділет министрлігінде 2025 жылғы 17 қыркүйекте № 36869 болып тіркелді

"Тұрғын үй қатынастары туралы" Қазақстан Республикасы Заңының 10-2-бабының 10-43) тармақшасына сәйкес БҰЙЫРАМЫН:

1. Қоса беріліп отырған Сумен жабдықтау және (немесе) су бұру саласындағы ақпараттық қауіпсіздікті қамтамасыз етуге арналған қағидалар бекітілсін.

2. Қазақстан Республикасы Өнеркәсіп және құрылыс министрлігінің Цифрлық трансформация департаменті заңнамада белгіленген тәртіппен:

1) осы бұйрықты Қазақстан Республикасының Әділет министрлігінде мемлекеттік тіркеу;

2) осы бұйрық ресми жарияланғаннан кейін оны Қазақстан Республикасы Өнеркәсіп және құрылыс министрлігінің интернет-ресурсында орналастыру.

3. Осы бұйрықтың орындалуын бақылау жетекшілік ететін Қазақстан Республикасының Өнеркәсіп және құрылыс вице-министріне жүктелсін.

Осы бұйрық алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі.

Қазақстан Республикасының
Өнеркәсіп және құрылыс министрі *Е. Нагаспаев*

"КЕЛІСІЛДІ"
Қазақстан Республикасының
Қаржы министрлігі

"КЕЛІСІЛДІ"
Қазақстан Республикасының
Ұлттық қауіпсіздік комитеті

"КЕЛІСІЛДІ"
Қазақстан Республикасының
Ұлттық экономика министрлігі

"КЕЛІСІЛДІ"
Қазақстан Республикасы Цифрлық даму,
инновациялар және аэроғарыш
өнеркәсібі министрлігі

"КЕЛІСІЛДІ"

Қазақстан Республикасының
энергетика министрлігі

Қазақстан Республикасының
Өнеркәсіп және
құрылыс министрінің
2025 жылғы 16 қыркүйектегі
№ 370 бұйрығымен
бекітілген

Сумен жабдықтау және (немесе) су бұру саласындағы ақпараттық қауіпсіздікті қамтамасыз етуге арналған қағидалар

1-тарау. Жалпы ережелер

1. Осы Сумен жабдықтау және (немесе) су бұру саласындағы ақпараттық қауіпсіздікті қамтамасыз етуге арналған қағидалар (бұдан әрі - Қағидалар) "Тұрғын үй қатынастары туралы" Қазақстан Республикасы Заңының 10-2-бабының 10-43) тармақшасына сәйкес әзірленді және сумен жабдықтау және (немесе) су бұру саласындағы ақпараттық коммуникациялық инфрақұрылымның аса маңызды объектілерінің ақпараттық қауіпсіздігін қамтамасыз етуге қойылатын талаптарды белгілейді.

2. Сумен жабдықтау және (немесе) су бұру саласындағы ақпараттық қауіпсіздіктің салалық орталығы (бұдан әрі - Салалық орталығы) сумен жабдықтау және (немесе) су бұру субъектілерінің технологиялық процестерінің негізі болып табылатын өнеркәсіптік басқару жүйелері болып табылады.

3. Сумен жабдықтау және (немесе) су бұру саласында ақпараттық қауіпсіздікті қамтамасыз ету мақсатында ақпараттық қауіпсіздік жөніндегі Салалық орталық жұмыс істейді, ол үйлестіру мен әдістемелік басшылықты, бірыңғай қорғалған ақпараттық кеңістікті құруды, сондай-ақ аса маңызды объектілердің ақпараттық қауіпсіздік қатерлеріне төзімділігін арттыруды жүзеге асырады.

4. Сумен жабдықтау және (немесе) су бұру саласында ақпараттық қауіпсіздікті қамтамасыз етудің мақсаттары мыналар болып табылады:

1) ақпараттық жүйелерде, соның ішінде интеграциялық шлюздерде, қолданбалы сервистерде, пайдаланушы интерфейстерінде және инфрақұрылымда өңделетін ақпараттың құпиялылығын, тұтастығын және қолжетімділігін қамтамасыз ету;

2) негізгі бизнес-процестердің үздіксіздігін қамтамасыз ету;

3) тәуекелдерді, қолжетімділікті, инциденттерді және қорғау шараларын орталықтандырылған басқаруды қоса алғанда, ақпараттық қауіпсіздікті басқаруға бірыңғай тәсілді қамтамасыз ету;

4) ақпараттық қауіпсіздік саласындағы заманауи қатерлер мен тәуекелдерге тиімді ден қою;

5) деректерді беру және өңдеу бөлігінде ақпараттық жүйелерді пайдалану, әзірлеу, сүйемелдеу және интеграциялау кезінде туындайтын тәуекелдерді барынша азайту;

6) ақпараттандыру саласындағы заңнама, нормативтік құқықтық актілер мен стандарттар талаптарының орындалуын қамтамасыз ету.

5. Сумен жабдықтау және (немесе) су бұру саласында ақпараттық қауіпсіздікті қамтамасыз етудің міндеттері мыналар болып табылады:

1) ақпараттық жүйелердің және олардың құрамдас бөліктерінің өмірлік циклі кезеңдерінің барлығында: жобалау, әзірлеу, тестілеу, пайдалануға енгізу, сүйемелдеу және пайдаланудан шығару барысында ақпараттық қауіпсіздік тәртібін енгізу;

2) қызметкерлердің аппараттық, бағдарламалық және ақпараттық ресурстарға қолжетімділігін шектеу;

3) ақпараттық жүйелерді пайдалану және интеграциялау барысында туындайтын ақпараттық қауіпсіздік тәуекелдерін тұрақты түрде айқындау, талдау, бағалау және басқару рәсімдерін енгізу;

4) ақпараттық қауіпсіздік саясатының талаптарын сақтау мен енгізілген ақпаратты қорғау шараларының тиімділігін бағалау мақсатында ішкі аудиттер жүргізу арқылы тұрақты тексерулерді жүзеге асыру;

5) информатизация саласындағы заңнама, нормативтік құқықтық актілер мен стандарттар талаптарының орындалуын қамтамасыз ету.

6. Салалық орталық өз қызметін жүзеге асыру барысында 2016 жылғы 20 желтоқсандағы № 832 Қазақстан Республикасы Үкіметінің қаулысымен бекітілген ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздік саласындағы бірыңғай талаптарды басшылыққа алады.

Салалық орталықтың ақпараттық қауіпсіздік жөніндегі бөлімшесі қажет болған жағдайда сумен жабдықтау және (немесе) су бұру субъектілерінен ақпараттық қауіпсіздік қатерлерін талдау мен бағалау үшін қажетті ақпаратты сұратуға, орындалуы міндетті әдістемелік құжаттарды әзірлеуге, ақпараттық-коммуникациялық жүйелердің қорғалу жағдайына тексеру жүргізуге, сондай-ақ анықталған бұзушылықтарды жою жөніндегі жоспарларды оларды орындау мерзімдерін көрсете отырып қалыптастыруға құқылы.

7. Осы Тәртіпте ақпараттандыру саласындағы заңнамада көзделген терминдер мен анықтамалар қолданылады.

2-тарау. Сумен жабдықтау және (немесе) су бұру саласындағы ақпараттық қауіпсіздікті қамтамасыз ету тәртібі

8. Ақпараттық қауіпсіздікті қамтамасыз ету мақсатында Салалық орталығы сумен жабдықтау және (немесе) су бұру саласындағы Салалық орталығына қосылған ұйымдардан деректерді жинауды жүзеге асыратын заманауи жүйелерді пайдалана отырып, ақпараттық қауіпсіздік қатерлеріне мониторинг жүргізеді.

9. Барлық келіп түсетін деректерде аномалиялық белсенділікті анықтау үшін машиналық оқыту әдістері мен мінез-құлықтық талдау қолданылады. Әсіресе технологиялық үдерістердің бұзылуына әкелуі мүмкін өнеркәсіптік басқару жүйелеріне бағытталған мақсатты шабуылдарды анықтауға ерекше назар аударылады.

10. Ақпараттық қауіпсіздік инциденттеріне жедел ден қою мақсатында Салалық орталығында қауіп-қатерлерді жіктеудің үш деңгейлі жүйесі қолданылады, оған мыналар жатады:

1) аса маңызды инциденттер – сумен жабдықтау және (немесе) су бұру объектілерінің тұрақты жұмысына тікелей қауіп төндіретін, анықталған сәттен бастап 1 сағат ішінде дереу ден қоюды талап ететін инциденттер;

2) жоғары тәуекелді инциденттер – анықталған сәттен бастап 4 сағат ішінде ден қоюды талап етеді;

3) төмен деңгейлі инциденттер – анықталған сәттен бастап 24 сағат ішінде ден қоюды көздейді.

11. Әрбір инцидент бойынша Салалық орталығының ден қою тобы инцидентті оқшаулау және оның салдарын жою бойынша жеке іс-шаралар жоспарын әзірлейді.

12. Сумен жабдықтау және (немесе) су бұру субъектілері өздерінің мониторинг жүйелерін Салалық орталығы платформасымен интеграциялауды қамтамасыз етеді, бұл ретте деректер Салалық орталығы регламентінде белгіленген форматтар мен көлемде ұсынылады.

13. Сумен жабдықтау және (немесе) су бұру ұйымдары ақпараттық қауіпсіздік қатерлерін өздері анықтаған жағдайда, белгіленген байланыс арналары арқылы деректерді қорғау хаттамаларын пайдалана отырып, дереу Салалық орталығын хабардар етеді.

14. Салалық орталығы (ақпараттық қауіпсіздік салалық орталығы) Қазақстан Республикасының Өнеркәсіп және құрылыс министрлігімен ақпараттық қауіпсіздік қатерлері туралы тұрақты есептер арқылы өзара әрекеттеседі, мемлекеттік бағдарламаларды әзірлеуге және нормативтік-құқықтық базаны жетілдіруге қатысады, сондай-ақ Ұлттық ақпараттық қауіпсіздік координациялық орталымен сертификатталған криптографиялық қорғау құралдарын пайдалана отырып, қорғалған байланыс арналары арқылы техникалық өзара әрекеттестікті жүзеге асырады.

15. Сумен жабдықтау және (немесе) су бұру субъектілерінен Салалық орталыққа келіп түсетін барлық деректер Қазақстан Республикасының ақпараттандыру саласындағы заңнамасының талаптарына сәйкес қорғалуға жатады.

16. Салалық орталық ақпаратты қорғаудың сертификатталған криптографиялық құралдарын, қолжетімділікті бақылау жүйелерін және өзге де ақпаратты қорғау құралдарын пайдаланады.

17. Сумен жабдықтау және (немесе) су бұрудың аса маңызды объектілері туралы, сондай-ақ олардың ақпараттық жүйелерінің осалдықтары жөніндегі ақпаратты қорғауға

ерекше талаптар қойылады. Мұндай ақпарат Салалық орталықтың ақпараттық жүйесінің арнайы бөлінген қорғалған сегменттерінде сақталады. Шектеулі қолжетімділігі бар ақпаратты үшінші тұлғаларға, оның ішінде халықаралық ұйымдарға беру тек уәкілетті мемлекеттік органдардың рұқсатымен жүзеге асырылады.