

4. Тұрақты даму туралы есеп

- процестік тәсіл;
- ұйымдастырушылық және техникалық қорғаныс шараларын кешенді пайдалану;
- үздік тәжірибелерге ілесу;
- ақылға қонымды жеткіліктілік;
- хабардар болу және жеке жауапкершілік.

«Қазақтелеком» АҚ ақпараттық қауіпсіздікті қамтамасыз ету үшін жүйелі тәсілді қолданады. Маңызды аспектілердің бірі — деректердің Компания инфрақұрылымына түскен сәтінен бастап оларды мұрағаттауға немесе қайтарымсыз жоюға дейін барлық өмірлік цикл кезеңдерінде тәулік бойы бақылау.

Компанияда ақпараттық қауіпсіздікті қамтамасыз етудің халықаралық тәжірибелері қолданылады. Біздің ішкі жүйелеріміз ақпараттық ресурстарға қауіпсіз қашықтан қол жеткізу, интернетті қауіпсіз пайдалану, артықшылықты пайдаланушыларды бақылау (PAM), осалдықтар сканерлері, дерекқорларды қорғау және басқалары сияқты шешімдер арқылы қорғалған. Компания сыртқы да, ішкі қатерлерге де қарсы тұруға ұмтылады және ресурстармен жұмыс істеудің жаңа шешімдері мен әдістерін, оның ішінде Компанияда қажетті инфрақұрылым құру, білікті мамандарды оқыту, ақпараттық қауіпсіздіктің жедел орталығын қалыптастыру және ZeroTrust тұжырымдамасын енгізуді енгізеді.

Сондай-ақ Компанияда мемлекеттік киберқауіпсіздік жүйесіне ЕШДИ-ге ендірілу, Заттардың интернетінің қауіпсіздігі, Honeypot тұзақтарын пайдалану және машиналық оқыту (Machine Learning) технологиясы сияқты қауіпсіздіктің маңызды элементтері қолданылады. Сонымен қатар, Компания қызметкерлерін оқыту және олардың АҚ бойынша хабардарлығын арттыру тұрақты негізде жүргізіледі. Корпоративтік университет бағдарламасында қызметкерлерді ақпараттық қауіпсіздік саласындағы шараларды кешеніне стратегиялық мақсаттар, міндеттер мен негізгі талаптарды айқындау

мақсатында әзірленген «Қазақтелеком» АҚ-ның Ақпараттық қауіпсіздік саясатымен таныстыратын курс көзделген. Бұл шаралар ақпаратпен жауапты түрде жұмыс істеу мәдениетін қолдауға және адами фактор тәуекелдерін барынша азайтуға мүмкіндік береді.

Компанияда көрсетілетін сервистердің сенімділігіне, үздіксіздігіне және қауіпсіздігіне қойылатын талаптарды қоса алғанда, ИТ-қызметтерді басқару процестерінің бар екенін растайтын ISO 20000–1 «Қызметтер менеджменті жүйесі» стандартына сәйкестік сертификаты қолданылады.

2025 жылғы қазанда (28–29 қазан) «Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздік менеджменті жүйелері. Талаптар» ҚР СТ ISO/IEC 27001–2023 стандарты талаптарына сәйкестікке Корпоративтік бизнес дивизионының (Алматы қ. филиалы) инспекциялық аудиті жүргізілді. «Қазақстан сапа орталығы» ЖШС жүргізген аудит нәтижелері бойынша ақпараттық қауіпсіздік менеджменті жүйесінің белгіленген талаптарға сәйкестігі расталды.

2025 жылғы 31 қазанда ҚР СТ ISO/IEC 27001–2023 стандартына сәйкестік сертификаты берілді.

2026 жылға арналған жоспарлар:

Ақпараттық технологиялар дивизионы филиалында ақпараттық қауіпсіздік менеджменті жүйесін енгізуді аяқтау және сертификаттаудан өту, ISO/IEC 27001 стандартына сәйкестік сертификатын алу (жоспарланған мерзімі — 2026 жылғы наурыз).

4.4.5.2. Дербес деректерді қорғау

GRI 418-1

Компанияда Компания Басқарма Төрағасының 06.10.2023 ж. № 313 бұйрығымен бекітілген «Дербес деректерді қорғау саясаты» әзірленіп, енгізілген, онда клиенттердің, жеткізушілердің, іскерлік серіктестердің, қызметкерлердің және басқа да тұлғалардың дербес деректерін өңдеудің негізгі қағидаттары айқындалған, сондай-ақ дербес деректерді жинау, сақтау және өңдеу бойынша негізгі әрекеттер, сондай-ақ оларды қорғау бойынша шаралар айқындалған.

Қазақстан Республикасының 2025 жылғы 17 қарашадағы № 231-VIII «Қазақстан Республикасының кейбір заңнамалық актілеріне жасанды интеллект және цифрландыру мәселелері бойынша өзгерістер мен толықтырулар енгізу туралы» Заңы негізінде Қазақстан Республикасының «Дербес деректер және оларды қорғау туралы» Заңына өзгерістер енгізілді. Осыған байланысты Саясатқа мынадай бағыттар бойынша өзгерістер енгізілді:

- терминдер, қысқартулар мен анықтамалар тізбесін өзектендіру;
- дербес деректерді жинау мен өңдеуге келісімдер алу процесін жетілдіру;
- дербес деректерді жинау мен өңдеуге келісімдер алу тәртібіне тәсілдерді біріздендіру;
- дербес деректерді жинау мен өңдеуді жүзеге асыратын немесе оларға қол жеткізуге құқығы бар тұлғалар тізбесін бекіту тәртібін, сондай-ақ дербес деректерді өңдеуді ұйымдастыруға жауапты тұлғаны (тұлғаларды) тағайындау тәртібін енгізу;
- дербес деректерді бұғаттау мен сақтау процестерін жетілдіру;
- дербес деректерге қол жеткізуді ұсыну процестерін түзету.

Саясат дербес деректерді қорғау саласындағы негіз қалаушы құжат болып табылады, дербес деректерді қорғау саласындағы Компания өз қызметінде

басшылыққа алатын мақсаттарды, міндеттер мен қағидаттарды белгілейді. Дербес деректерді қорғаудың тиісті құжаттарын әзірлеу кезінде басшылық қызметін атқарады.

Дербес деректерді қорғауды қамтамасыз етудің негізгі қағидаттары:

- адам мен азаматтың конституциялық құқықтары мен бостандықтарын сақтау;
- дербес деректерді қорғауды қамтамасыз етудің заңдылығы;
- шектеулі қол жеткізудегі дербес деректер құпиялылығы;
- Компания басшылығының дербес деректерді қорғауды қамтамасыз ету процесіне тартылуы;
- бизнеске бағдарлану;
- процестік тәсіл;
- қорғау тәсілдерін, әдістерін және құралдарын кешенді пайдалану;
- үздік тәжірибелерге ілесу;
- ақылға қонымды жеткіліктілік;
- хабардар болу және жеке жауапкершілік.

Осы қағидаттарды іске асыру тиімділігін бағалау және құпиялылықты бұзу тәуекелдерін бақылау үшін «Қоғам абоненттерінің дербес деректерінің ағуына әкелген инциденттер саны» метрикасы қолданылады. Бұл көрсеткіш абоненттердің құпиялылыққа және дербес ақпаратты қорғауға деген құқығымен тікелей байланысты. Бұл көрсеткіш сыртқы мүдделі тараптардың мүдделерін көрсетеді және Компанияның ақпараттық қауіпсіздіктің жоғары деңгейін қамтамасыз етуге ұмтылысын көрсетеді.

Бұл метрика тәуекелдерді басқару жүйесінің бөлігі болып табылады және Ақпараттық технологиялар департаментінің Бас директорының Негізгі қызмет көрсеткіштеріне (ҚТК) енгізілген. Ол үшін мақсатты

4. Тұрақты даму туралы есеп

бағдар — 0% инциденттер белгіленген, бұл дербес деректер ағуына нөлдік төзбеушілік саясатына сәйкес келеді.

Бұған қосымша, Ақпараттық технологиялар департаменті Бас директорының ҚТК жүйесінде Компанияның ақпараттық қауіпсіздік пен клиенттік тәжірибе саласындағы тәуекелдерді басқару тәсілін көрсететін басқа да көрсеткіштер пайдаланылады, оның ішінде:

- Клиенттік адалдық индексі (Net Promoter Score, NPS);
- ZeroTrust ядросын қосымша жабдықтау бойынша іс-шараларды іске асыру;
- Уақтылы жойылған ақпараттық қауіпсіздік инциденттерінің үлесі;

4.4.5.3. Есепті кезеңдегі негізгі нәтижелер

2025 жылы Компанияда ақпараттық қауіпсіздік саласында корпоративтік ақпараттық жүйелерді, дербес деректерді, қызметтік ақпарат пен деректер беру желілерін қорғауды қамтамасыз ету үшін іс-шаралар кешені жүргізілді.

Ақпараттық қауіпсіздік қызметкерлерімен күдікті хаттарды алған кездегі пайдаланушылардың әрекеттері бойынша оқу-жаттығулары тұрақты негізде өткізіледі. 24/7 жұмыс істеу режимімен Ақпараттық қауіпсіздіктің жедел орталығының (АҚЖО) жұмысы үнемі жетілдіріліп отырады. Негізгі міндеттеріне мыналар кіреді:

- Компанияның корпоративтік периметрін қорғау;
- Ақпараттық қауіпсіздік (АҚ) оқиғаларын мониторингтеу;
- АҚ инциденттеріне әрекет ету;
- АҚ инциденттерін тергеу;
- Компанияның ақпараттық жүйелеріндегі осалдықтарды іздеу;
- Ақпараттық қауіпсіздік инциденттерін жою бойынша ұсынымдар беру;
- Ақпаратты қорғау құралдарын (АҚҚ) бақылау.

- Пайдаланушылар мүдделерін қорғауға және Компанияның сандық сервистеріне сенімді нығайтуға бағытталған басқа да метрикалар қолданылады.

Көрсетілген көрсеткіштерді мониторингтеу мен бақылау Компанияның ақпараттық қауіпсіздік жөніндегі ішкі регламенттері шеңберінде үнемі жүзеге асырылады.

2025 жылғы мамырда Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің Ақпараттық қауіпсіздік комитеті ақпараттық қауіпсіздік саласындағы заңнама талаптарының сақталуын тексеру жүргізді. Тексеру қорытындысы бойынша дербес деректерді қорғау бөлігінде бұзушылықтар анықталған жоқ.

2025 жылы Компанияның ZeroTrust моделіне көшуінің үшінші кезеңі іске асырылды, бірқатар бағдарламалық-аппараттық ақпаратты қорғау құралдары (АҚҚ) енгізілді, бұл Компанияның корпоративтік инфрақұрылымының бар қорғанысын күшейтуге мүмкіндік берді.

Клиенттер құпиялылығын бұзуға қатысты алынған негізделген шағымдардың жалпы саны нөлге тең. Оның ішінде:

- Сыртқы тұлғалардан және негізделген ұйымдардан алынған шағымдар — 0;
- Бақылаушы органдардан алынған шағымдар — 0;
- Анықталған клиенттер деректерінің ағуы, ұрлануы немесе жоғалуы — 0.

Бұл көрсеткіштер есепті кезеңде клиенттер құпиялылығын бұзуға байланысты тіркелген инциденттердің болмауын куәландырады.

Корпоративтік АҚЖО жұмысының нәтижелері:

Клиенттер ресурстарына жасалған шамамен **9 000 DDoS-шабуыл** (шыңы 400 Гбит/сек астам), жалпы трафигі 1 230 Тбит астам тойтарылды.

Шамамен **80 тұзақ** (Honeypot — компанияның ақпараттық жүйелерін/ресурстарын толығымен имитациялайтын) өрістетілді, олар компанияның корпоративтік желісі ішінде **50 408-ден астам** зиянды сұрауды анықтауға мүмкіндік берді.

Антивирустық шешіммен зиянды белсенділік пен күдікті нысандарды анықтаудың **шамамен 260 000 жағдайы** анықталды.

Веб-қосымшалар мен БҚ осалдықтарын сканерлеумен Компанияның 98,8 мың активтерінде шамамен **60,9 мың белсенді осалдық** анықталды; жауапты әкімшілермен 55,6 мыңнан астам осалдық (жалпы санның 61,66%-ы) жойылды.

SIEM жүйесінің жұмыс істеуі шеңберінде **567 лог көзінен** деректерді орталықтанған қабылдау мен корреляциялау жүзеге асырылады, бұл компанияның корпоративтік желісі ішінде **4 873-тен астам сын-қатер** және жоғары тәуекелді оқиғаны анықтауға және өңдеуге мүмкіндік берді.

WAF көмегімен Интернет-ресурстарға **шамамен 27,3 млн веб-сұрау** тіркелді. Олардың ішінде 1,75 млн зиянды әрекет табысты тойтарылды.

РАМ артықшылықты пайдаланушыларды бақылау жүйесінің көмегімен **305-тен астам артықшылықты пайдаланушы** (ақпараттық жүйелер әкімшілері, сыртқы пайдаланушылар және мердігерлер) корпоративтік ақпараттық жүйелердің терминалдық серверлерінің 420-дан астам ІР-мекенжайларына қол жеткізуге ие.

DLP жүйесімен шамамен **1,5 млн оқиға** тіркелді. Негізгі белсенділік USB, File Share және Clipboard арналарына тиесілі болды.

Алаяқтыққа қарсы күрес бөлімімен ФРОД бірге шетелде орналасқан фрод-трафик көздерін анықтау бойынша жұмыс жүргізіледі, **7 млн-нан астам** алаяқтық қоңырау бұғатталды.

4.4.5.4. Қызметкерлерді ақпараттық қауіпсіздік мәселелері бойынша хабардар ету және оқыту

GRI 418-1

Компанияда деректердің құпиялылығын, тұтастығы мен қолжетімділігін қамтамасыз етуге бағытталған қызметкерлердің ақпараттық қауіпсіздік саласындағы хабардарлығын арттырудың жүйелі бағдарламасы іске асырылуда.

Ақпараттық қауіпсіздік мәселелері бойынша ақпараттық материалдар қызметкерлерге электрондық құжат айналымы жүйесі арқылы тұрақты түрде жіберіледі. Компанияның ақпараттық қауіпсіздік саласындағы құжаттарын қоса алғанда, барлық ұйымдастырушылық-өкімдік құжаттар Сапа тобымен танысу фактісін міндетті тіркеумен қызметкерлердің назарына жеткізіледі.

Талаптарды түсіну мен меңгеру деңгейін тексеру үшін кейіннен тестілеумен ақпараттық қауіпсіздік және дербес деректерді қорғау мәселелері бойынша оқу тренингтері өткізіледі. Есепті жылы Ақпараттық технологиялар департаменті (АТД) типтік инциденттерді талдауға және ақпараттық ресурстармен жұмыс істеу кезіндегі қауіпсіз мінез-құлық дағдыларын қалыптастыруға бағытталған презентациялық материалдар мен практикаға бағдарланған кейстерді пайдаланумен қызметкерлерді оқытудың қосымша форматын бастамалады. Әлеуметтік инженерлік шабуылдарға тұрақтылықты бағалау мақсатында фишингтік оқу-жаттығулар ұйымдастырылады: қызметкерлерге салынымдары бар имитациялық фишингтік хаттар жіберіледі, хаттарды ашу, салынымдарды ашу мен нысандарды толтыру фактілері тіркеледі, ал нәтижелер қосымша түсіндіру жұмысын жүргізу үшін пайдаланылады.

Ақпараттық қауіпсіздік әкімшілік деңгейде де — әр қызметкер Компанияның ақпараттық қауіпсіздік

саласындағы регламенттері, қағидалары, саясаттарының талаптарымен танысуға және орындауға міндетті, техникалық және физикалық деңгейде де — компанияда әртүрлі аппараттық-бағдарламалық кешендер, ақпаратты криптографиялық қорғау құралдары және басқалары пайдаланылады — қамтамасыз етіледі.

Сонымен қатар, АҚ дивизионының мамандары ақпараттық қауіпсіздік, киберқауіпсіздік, АҚ тәуекелдері мен қатерлері бойынша біліктілікті арттырудың әртүрлі курстарынан тұрақты түрде өтеді. Деректерді заңсыз пайдалану тәуекелі едәуір жоғары клиенттермен жұмыс істеу мен персоналмен жұмыс істеу бөлімшелерінің қызметкерлеріне гигиена деңгейін арттыру бойынша жалпы оқыту/тестілеу жүргізіледі.

77-кесте. Компанияның ұзақ мерзімді құн жасауына әсер ететін маңызды тақырып бойынша көрсеткіштер

Көрсеткіш	2025 жылға арналған мақсат	2025 жылғы нәтиже
Абоненттердің дербес деректерінің ағуына әкелген инциденттер саны	0 инцидент	0 инцидент A
Уақтылы жойылған АҚ инциденттерінің үлесі	100%	100%
Осалдықтарды анықтау мен жою	Сын-қатер мен жоғары тәуекелді осалдықтарды уақтылы жою	60,9 мың осалдық анықталды 55,6 мыңы жойылды
Деректерді қорғау мен фрод-трафикке қарсы күрес	Алаяқтық трафикті анықтау мен бұғаттау	шамамен 9 000 DDoS-шабуыл тойтарылды 1 230 Тбиттен астам DDoS-трафик 7 млн-нан астам алаяқтық қоңырау бұғатталды

«Қоғам абоненттерінің дербес деректерінің ағуына әкелген инциденттер саны» және «Уақтылы жойылған АҚ инциденттерінің үлесі» метрикаларын қоса алғанда, ақпараттық қауіпсіздік пен деректерді қорғау саласындағы көрсеткіштер Ақпараттық қауіпсіздік жөніндегі Басқарушы директор мен Ақпараттық қауіпсіздік қызметінің Басшысының ҚТК-не енгізілген. ҚТК орындау Компанияның ішкі құжаттарында белгіленген тәртіпте олардың сыйақыларының ауыспалы бөлігінде ескеріледі.