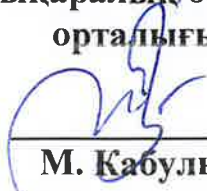


«БЕКІТЕМІН»
Басқарма төрағасының м.а.
«Халықаралық бағдарламалар
орталығы» АҚ


М. Кабульдинов
« » 2026 ж.

ТЕХНИКАЛЫҚ ЕРЕКШЕЛІК

сатып алынатын

**«Диагностикалау/сараптама/талдау/сынақтар/тестілеу/тексеріп қарау
жөніндегі қызметтер. Ақпараттандыру объектілерін ақпараттық
қауіпсіздік талаптарына сәйкестікке келтіру» қызметтерінің
(«е-Болашақ» КАЖ цифрлық объектісін киберқауіпсіздік талаптарына
сәйкестікке сынақтарға дайындау)**

Параметр	Мәні
Тапсырыс беруші	«Халықаралық бағдарламалар орталығы» акционерлік қоғамы, БСН 050440007456, Қазақстан, Астана қ., Есіл ауданы, Сығанақ к-сі, 70 ғимарат.
Қызметтің атауы (ТЖҚ ЕНА бойынша)	Диагностикалау/сараптама/талдау/сынақтар/тестілеу/тексеріп қарау жөніндегі қызметтер
Қызметтің сипаттамасы (ТЖҚ ЕНА бойынша)	Ақпараттандыру объектілерін ақпараттық қауіпсіздік талаптарына сәйкестікке келтіру
ТЖҚ ЕНА коды	712019.000.000009
Қосымша сипаттама	«Киберқауіпсіздік туралы» Қазақстан Республикасы Заңының 49-бабына сәйкес аккредиттелген сынақ зертханасы жүргізетін киберқауіпсіздік талаптарына сәйкестікке сынақтарға «е-Болашақ» КАЖ цифрлық объектісін (бұдан әрі — Жүйе) дайындау
Өлшем бірлігі / саны	Бір қызмет / 1
Сатып алу тәсілі	Ашық конкурс (мемлекеттік сатып алу веб-порталы goszakup.gov.kz)
Қызмет көрсету орны	Қазақстан, Астана қ., Есіл ауданы, Сығанақ к-сі, 70 ғимарат. Қызметтердің жекелеген түрлері (қашықтан талдау, сканерлеу, консультациялар) Тапсырыс берушімен келісу бойынша қашықтан көрсетілуі мүмкін
Қызмет көрсету мерзімі	Шарт жасалған күннен бастап 2026 жылғы 20 желтоқсанға дейін
Төлем шарттары	көрсетілген қызметтер актісі негізінде қызметтер іс жүзінде көрсетілгені бойынша

Осы құжатта «е-Болашақ» КАЖ цифрлық объектісін (бұдан әрі — Жүйе, сынақ объектісі) киберқауіпсіздік талаптарына сәйкестікке сынақтарға дайындау жөніндегі қызметтердің мазмұнын, көлемін, көрсету шарттарын және нәтижелеріне қойылатын талаптарды айқындайтын техникалық ерекшелік берілген.

орындалған түзетулерді тексеру және ресми сынақтар үшін құжаттар жиынтығын дайындау болып табылады. Ресми сынақтарды Тапсырыс беруші бөлек ұйымдастырады және оларға ақы төлейді. Ресми сынақтарды жүргізетін ұйым Қазақстан Республикасының заңнамасына және қолданылатын Сынақ қағидаларына сәйкес айқындалады.

1.1. Терминдер

Термин	Анықтама
Тапсырыс беруші	«Халықаралық бағдарламалар орталығы» акционерлік қоғамы - Жүйенің меншік иесі (иеленушісі)
Әлеуетті өнім беруші	Мемлекеттік сатып алу туралы шарт жасасуға үміткер кәсіпкерлік қызметті жүзеге асыратын жеке тұлға, заңды тұлға (егер Қазақстан Республикасының заңдарында өзгеше белгіленбесе, мемлекеттік мекемені қоспағанда), заңды тұлғалардың уақытша бірлестігі (консорциум)
Жүйе (сынақ объектісі)	«е-Болашақ» КФАЖ цифрлық объектісі, оның жұмыс істеуін қамтамасыз ететін қолданбалы БҚ, дерекқорларды, виртуалдандыру ортасын, серверлік және желілік жабдықты қоса алғанда
Киберқауіпсіздік (КҚ)	Цифрлық объектілердің құпиялылығының, тұтастығының немесе қолжетімділігінің бұзылуынан қорғалу жай-күйі. 2026 жылға дейін қабылданған НҚА мен стандарттарда «ақпараттық қауіпсіздік» (АҚ) термині қолданылады; осы техникалық ерекшеліктің мақсаттары үшін терминдер баламалы
Сынақтар	Цифрлық объектіні «Киберқауіпсіздік туралы» ҚР Заңының 49-бабына және Сынақ әдістемесі мен қағидаларына сәйкес КҚ талаптарына сәйкестікке сынау
Зертхана	Сынақтарды жүргізетін аккредиттелген сынақ зертханасы (мемлекеттік техникалық қызмет)
Бірыңғай талаптар	ҚР Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысымен бекітілген Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптар
Сынақ әдістемесі мен қағидалары	2019 жылғы 3 маусымдағы № 111/НҚ бұйрықпен бекітілген «Цифрлық үкіметтің» цифрлық объектілері мен аса маңызды цифрлық объектілерін киберқауіпсіздік талаптарына сәйкестікке сынақтар жүргізу әдістемесі мен қағидалары
Мониторинг қағидалары	2018 жылғы 28 наурыздағы № 52/НҚ бұйрықпен бекітілген «Цифрлық үкіметтің» цифрлық объектілері мен аса маңызды цифрлық объектілерінің киберқауіпсіздігін қамтамасыз етуге мониторинг жүргізу қағидалары
Сәйкессіздік	Жүйенің, оның конфигурациясының, құжаттамасының немесе процестерінің жай-күйінің 3-бөлімде көрсетілген НҚА мен стандарттардың талаптарынан ауытқуы
Осалдық	КҚ-ны бұзу үшін пайдаланылуы мүмкін БҚ-ның, конфигурацияның немесе архитектураның кемшілігі
Соңғы нүкте	Тапсырыс берушінің EDR жүйесінің агенті орнатылатын жұмыс станциясы немесе сервері
Статикалық талдау құралы	Әлеуетті өнім беруші Жүйенің бастапқы кодын талдау үшін қолданатын SAST класындағы бағдарламалық құрал (6.14-тармақ)

1.2. Қысқартулар

Қысқарту	Толық жазылуы
БСН	Бизнес-сәйкестендіру нөмірі
ТЖҚ БНА	Тауарлардың, жұмыстардың және көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы
АҚ	Ақпараттық қауіпсіздік (2026 жылға дейін қабылданған НҚА мен стандарттардың термині; «Киберқауіпсіздік» қараңыз)
КҚ	Киберқауіпсіздік
ЖАЭ	Желіаралық экран
ДМ	Бағдарламалық қамтамасыз етудің декларацияланбаған мүмкіндіктері
НҚА	Нормативтік құқықтық акт
ОЖ	Операциялық жүйе
СБД	ҚР СТ ISO/IEC 15408-3-2017 бойынша сенімнің бағалау деңгейі
АҚЖО	Ақпараттық қауіпсіздікті қамтамасыз етудің жедел орталығы (киберқауіпсіздіктің жедел орталығы)
БҚ	Бағдарламалық қамтамасыз ету
ҚР	Қазақстан Республикасы
АҚКҚ	Ақпаратты қорғау құралдары
ҚР СТ	Қазақстан Республикасының ұлттық стандарты
ДБЖ	Дерекқорларды басқару жүйесі
API, REST API	Қолданбалы бағдарламалау интерфейсі (Application Programming Interface); REST API — REST архитектуралық стилі бойынша құрылған бағдарламалық интерфейс
CI/CD	Үздіксіз интеграция және жеткізу (Continuous Integration / Continuous Delivery)
CVE	Common Vulnerabilities and Exposures — жалпыға белгілі осалдықтардың тізілімі
CVSS	Common Vulnerability Scoring System — осалдықтардың сындарлылығын бағалау жүйесі (3.1 немесе одан кейінгі нұсқасы қолданылады)
CWE, CWE/SANS	Common Weakness Enumeration — БҚ кемшіліктерінің жіктемесі; CWE/SANS Top 25 — БҚ-ның аса қауіпті кемшіліктерінің тізбесі
EDR	Endpoint Detection and Response — соңғы нүктелердегі қатерлерді анықтау және оларға ден қою жүйесі
EXE, DLL	Windows ОЖ-ның орындалатын файлдары мен динамикалық кітапханалары
HIPAA	Health Insurance Portability and Accountability Act — медициналық деректерді қорғау стандарты (АҚШ); статикалық талдау құралының есептілік үлгілерінің бірі ретінде пайдаланылады
HIPS	Host Intrusion Prevention System — хост деңгейінде басып кірулердің алдын алу жүйесі
HTTP/HTTPS, POP3/POP3S, SMTP, IMAP/IMAPS, SMB, RPC, RDP, SSL	Желілік хаттамалар: гипермәтінді беру (оның ішінде қорғалған), электрондық поштаны қабылдау және жіберу, файлдарға қол жеткізу, процедураларды қашықтан шақыру, қашықтағы жұмыс үстелі, қорғалған көлік деңгейі хаттамалары
IDS	Intrusion Detection System — басып кірулерді анықтау жүйесі

Қысқарту	Толық жазылуы
JAR, WAR, EAR, AAR, APK, IPA, APP	Java/Scala, Android, iOS және macOS компиляцияланған қосымшаларының пакеттер (архивтер) форматтары
MITRE ATT&CK	MITRE корпорациясы жүргізетін қаскүнемдердің тактикалары мен техникалары туралы білім базасы
OWASP Top 10, OWASP Mobile Top 10, OWASP MASVS	OWASP жобасының веб- және мобильді қосымшалар қауіпсіздігінің аса сыни тәуекелдерінің тізбелері және мобильді қосымшалар қауіпсіздігін верификациялау стандарты
PCI DSS	Payment Card Industry Data Security Standard — төлем карталары индустриясының деректер қауіпсіздігі стандарты
SARIF	Static Analysis Results Interchange Format — статикалық талдау нәтижелерімен алмасу форматы
SAST	Static Application Security Testing — қосымшалардың бастапқы кодының қорғалуын статикалық талдау
SIEM	Security Information and Event Management — қауіпсіздік оқиғалары мен ақпаратын басқару жүйесі
SOAR	Security Orchestration, Automation and Response — инциденттерді оркестрлеу, автоматтандыру және оларға ден қою жүйесі
UEFI	Unified Extensible Firmware Interface — компьютердің кіріктірілген БҚ (жүктеуіші) интерфейсі
URL	Uniform Resource Locator — Интернет желісіндегі ресурс мекенжайы
VDI	Virtual Desktop Infrastructure — виртуалды жұмыс үстелдерінің инфрақұрылымы
WMI	Windows Management Instrumentation — Windows ОЖ басқару құралдары
Git, SVN	Бастапқы код нұсқаларын бақылау жүйелері
CSV, HTML, PDF, XML, YAML	Файл форматтары: үтірмен бөлінген мәндер; гипермәтіндік белгілеу тілі; тасымалданатын құжат форматы; кеңейтілетін белгілеу тілі; деректерді сериялау форматы

2. Қызмет көрсету мақсаты

Қызмет көрсету мақсаты — Жүйені Қазақстан Республикасының нормативтік құқықтық актілерінде және Қазақстан Республикасының аумағында қолданылатын стандарттарда белгіленген киберқауіпсіздік талаптарына сәйкес келтіру және Жүйені Зертханада сынақтардан табысты өтуге дайындау.

Мақсатқа қол жеткізу үшін Әлеуетті өнім беруші Жүйенің техникалық құжаттама, КҚ саласындағы нормативтік құқықтық актілер мен стандарттар талаптарына сәйкестігін бағалау, сәйкессіздіктер мен осалдықтарды анықтау, оларды Тапсырыс берушінің (Жүйе әзірлеушісінің) күшімен жоюды сүйемелдеу және Зертханаға ұсыну үшін құжаттар мен мәліметтер жиынтығын дайындау жөніндегі талдамалық, консультациялық және аспаптық жұмыстар кешенін орындайды.

3. Нормативтік құқықтық актілер және стандарттар

3.1. Қызметтер мынадай нормативтік құқықтық актілер мен стандарттарға (қызметтер көрсетілген күнгі қолданыстағы редакцияларында) сәйкес көрсетіледі:

3.1.1. Қазақстан Республикасының 2026 жылғы 9 қаңтардағы № 255-VIII Цифрлық кодексі;

3.1.2. «Киберқауіпсіздік туралы» Қазақстан Республикасының 2015 жылғы 24 қарашадағы № 418-V Заңы (оның ішінде 49 «Киберқауіпсіздік талаптарына сәйкестікке

сынақтар», 50 «Киберқауіпсіздік аудиті» баптары, 9 «Цифрлық объектілерді қорғау» тарауы);

3.1.3. «Дербес деректер және оларды қорғау туралы» Қазақстан Республикасының 2013 жылғы 21 мамырдағы № 94-V Заңы;

3.1.4. «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы» Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысы;

3.1.5. Қазақстан Республикасы Цифрлық даму, қорғаныс және аэроғарыш өнеркәсібі министрінің 2019 жылғы 3 маусымдағы № 111/НҚ ««Цифрлық үкіметтің» цифрлық объектілері мен аса маңызды цифрлық объектілерін киберқауіпсіздік талаптарына сәйкестікке сынақтар жүргізу әдістемесі мен қағидаларын бекіту туралы» бұйрығы;

3.1.6. Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі министрінің 2018 жылғы 28 наурыздағы № 52/НҚ ««Цифрлық үкіметтің» цифрлық объектілері мен аса маңызды цифрлық объектілерінің киберқауіпсіздігін қамтамасыз етуге мониторинг жүргізу қағидаларын бекіту туралы» бұйрығы;

3.1.7. ҚР СТ ISO/IEC 27001-2023 «Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздік менеджменті жүйелері. Талаптар»;

3.1.8. ҚР СТ ISO/IEC 27002-2023 «Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару құралдары»;

3.1.9. ҚР СТ ISO/IEC 27005-2022 (ақпараттық қауіпсіздік тәуекелдерінің менеджменті);

3.1.10. ҚР СТ ISO/IEC 15408-1-2017, ҚР СТ ISO/IEC 15408-2-2017, ҚР СТ ISO/IEC 15408-3-2017 «Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық технологиялар қауіпсіздігін бағалау критерийлері» (1–3-бөліктер);

3.1.11. ҚР СТ 2199-2012 (веб-қосымшалардың қауіпсіздігіне қойылатын талаптар);

3.1.12. Жүйенің санатын, мақсатын, өңделетін деректердің құрамын және пайдалану шарттарын ескере отырып, оған тікелей қолданылатын Қазақстан Республикасы заңнамасының өзге де міндетті талаптары. Әлеуетті өнім беруші сәйкестік матрицасында нақты нормативтік құқықтық актіні, талаптың тармағын және оны қолдану негізін көрсетеді. Қосымша ерікті стандарттар Тапсырыс берушімен келісу бойынша қолданылады.

4. Қызметтер көрсету объектісі

4.1. Қызметтер көрсету объектісі — «цифрлық үкімет» объектілеріне жататын және мемлекеттік ақпараттық жүйелермен және өзге де цифрлық объектілермен интеграцияланатын, меншік иесі (иеленушісі) Тапсырыс беруші болып табылатын, Тапсырыс берушінің Сығанақ к-сі, 70-ғимарат мекенжайындағы меншікті серверлік үй-жайында және QazTech деректерді өңдеу орталығында орналастырылған «Халықаралық бағдарламалар орталығы» АҚ-ның «е-Болашақ» көпфункционалды ақпараттық жүйесі (бұдан әрі — «е-Болашақ» КФАЖ).

4.2. Қызметтер Жүйеге толық құрамда — қолданбалы бағдарламалық қамтамасыз етуге, дерекқорларға, виртуалдандыру ортасына, серверлік және желілік жабдыққа, ақпаратты қорғау құралдарына, әкімшілердің автоматтандырылған жұмыс орындарына және Жүйенің жұмыс істеуін қамтамасыз ететін барлық өзге де компоненттерге — олардың санына қарамастан көрсетіледі. Серверлердің, виртуалды машиналардың, желілік құрылғылардың және өзге де компоненттердің саны қызметтердің көлемі мен құнын өзгертуге негіз болып табылмайды.

4.3. Жүйе компоненттерінің нақты құрамын Әлеуетті өнім беруші 1-кезеңде (5-бөлім) Тапсырыс беруші ұсынатын құжатта мен мәліметтер негізінде нақтылайды және ол зерттеп-қарау туралы есепте (7-бөлім) тіркеледі.

5. Қызметтер көрсетудің құрамы мен кезеңдері

5.1. Қызметтер көрсету мынадай кезеңдерге бөлінеді:

№	Кезең	Мазмұны	Нәтиже (есептік құжаттар)
1	Жүйе инфрақұрылымының КҚ-ын талдау (зерттеп-қарау)	Бастапқы деректерді жинау, архитектураны, конфигурацияларды, журналдауды, физикалық қорғауды талдау, аспаптық сканерлеу, жүктемелік тестілеу, бастапқы кодты талдау (6.1, 6.3, 6.5, 6.7, 6.9, 6.10, 6.13, 6.14-тармақтар)	Зерттеп-қарау туралы есеп; сканерлеу, жүктемелік тестілеу және бастапқы кодты талдау бойынша есептер
2	Сәйкессіздіктерді анықтау және ұсынымдар беру	Зерттеп-қарау нәтижелерін 3-бөлімнің талаптарымен салыстыру, басымдықтарын белгілей отырып және жою жөніндегі ұсынымдармен сәйкессіздіктер мен осалдықтардың тізбесін қалыптастыру (6.2, 6.4, 6.6, 6.8, 6.15-тармақтар)	Сәйкессіздіктер тізбесі және оларды жою жөніндегі іс-шаралар жоспары
3	Сәйкессіздіктерді жоюды консультациялық сүйемелдеу	Сәйкессіздіктерді жою кезінде Тапсырыс беруші мен Жүйе әзірлеушісіне консультация беру, бақылау (қайталама) тексерулері, Зертханаға ұсыну үшін құжаттар жиынтығын дайындау (6.11, 6.12, 6.16, 6.17-тармақтар)	Қайталама тексерулер бойынша есептер; Жүйенің сынақтарға дайындығы туралы қорытынды есеп
4	Тапсырыс беруші персоналының хабардарлығын арттыру	6.2, 6.4, 6.6, 6.8, 6.11, 6.15, 6.17-тармақтарды орындау барысында Жүйе әкімшілеріне және Тапсырыс берушінің КҚ-ға жауапты тұлғаларына анықталған сәйкессіздіктер, қолданылған қорғау шаралары және сынақтарға дайындалу тәртібі бойынша консультация беру және нұсқама жүргізу	Консультациялар хаттамалары (тиісті тармақтар бойынша есептерде тіркеледі)

5.2. Кезеңдердің күнтізбелік мерзімдері қызметтер көрсетудің жоспар-кестесімен айқындалады, оны Әлеуетті өнім беруші шарт жасалған күннен бастап 10 жұмыс күні ішінде Тапсырыс берушіге келісуге ұсынады. Егер бұл жұмыстардың логикасына қайшы келмесе, кезеңдер қатар орындалуы мүмкін.

6. Қызметтердің толық сипаттамасы

Әлеуетті өнім беруші қызметтер көрсету шеңберінде мыналарды орындауға тиіс:

6.1. Қолданбалы бағдарламалық қамтамасыз етудің, дерекқордың (Жүйе әзірлеушісімен бірлесіп), виртуалдандыру ортасының және серверлік жабдықтың операциялық жүйелерінің функционалының қауіпсіздігін Бірыңғай талаптарға және ҚР СТ ISO/IEC 27002-2023-ке сәйкестігіне талдау, оның ішінде: есептік жазбаларды және қол жеткізу құқықтарын басқару, парольдік саясат және көпфакторлы аутентификация,

жаңартуларды басқару, пайдаланылмайтын қызметтер мен порттарды өшіру, компоненттердің өзара іс-қимыл арналарын қорғау, резервтік көшіру конфигурациясы.

6.2. Қолданбалы бағдарламалық қамтамасыз етуді, дерекқорды (Жүйе әзірлеушісімен бірлесіп), виртуалдандыру ортасын және серверлік жабдықтың операциялық жүйелерін КҚ жөніндегі талаптарға сәйкес баптау (қорғалуын күшейту) бойынша анықталған әрбір сәйкессіздік бойынша жазбаша ұсынымдар бере отырып консультация беру.

6.3. Қолданбалы бағдарламалық қамтамасыз етудің, дерекқордың (Жүйе әзірлеушісімен бірлесіп), виртуалдандыру ортасының және серверлік жабдықтың операциялық жүйелерінің оқиғаларын журналдауды талдау: тіркелетін оқиғалардың құрамы, толықтығы, сақтау мерзімдері, журналдарды өзгертуден қорғау, уақытты синхрондау.

6.4. Қолданбалы бағдарламалық қамтамасыз етудің, дерекқордың, виртуалдандыру ортасының және серверлік жабдықтың операциялық жүйелерінің оқиғаларын журналдауды Мониторинг қағидаларына және Бірыңғай талаптарға сәйкес, оның ішінде оқиғаларды КҚ-ны қамтамасыз ету мониторингі жүйесіне беруге қойылатын талаптарды қоса алғанда, баптау бойынша консультация беру.

6.5. Желілік жабдықтың (желіаралық экрандар, маршрутизаторлар, коммутаторлар, қашықтан қол жеткізу құралдары) конфигурациясын талдау: желіні сегменттеу, трафикті сүзгілеу қағидалары, басқару интерфейстерін қорғау, пайдаланылатын хаттамалар, есептік жазбалар.

6.6. Желілік жабдықты Бірыңғай талаптарға сәйкес баптау бойынша жазбаша ұсынымдар бере отырып консультация беру.

6.7. Желілік жабдық оқиғаларын журналдауды талдау.

6.8. Желілік жабдық оқиғаларын журналдауды Мониторинг қағидаларына және Бірыңғай талаптарға сәйкес баптау бойынша консультация беру.

6.9. Серверлік үй-жайдың физикалық қорғалуын (Әлеуетті өнім берушінің Жүйе орналасқан жерге баруы) Бірыңғай талаптарға сәйкестігіне тексеру: қол жеткізуді бақылау және есепке алу, күзет және өрт дабылы, өрт сөндіру, климаттық жабдық, үздіксіз электрмен қоректендіру, жабдықты орналастыру, келушілер журналдарын жүргізу; нәтижелері бойынша — сәйкессіздіктер тізбесі және оларды жою жөніндегі ұсынымдар көрсетілген есеп.

6.10. Жүйенің серверлерін, желілік жабдығын және веб-қосымшасын аудит режимінде (Тапсырыс беруші ұсынған есептік жазбаларды пайдалана отырып) және енуге тестілеу режимінде (есептік жазбаларсыз, сыртқы және ішкі периметрден) осалдықтар базасы өзекті қорғалуды талдау құралын пайдалана отырып, осалдықтардың болуына аспаптық сканерлеу, сондай-ақ келісілген шекараларда қолмен енуге тестілеу. Анықталған осалдықтар CVSS 3.1 немесе одан жаңа нұсқасына сәйкес сындылық деңгейі бойынша жіктеледі; әрбір осалдық бойынша жою жөніндегі ұсынымдар беріледі. Сканерлеу Тапсырыс берушімен келісілген уақыт аралықтарында жүргізіледі.

6.11. Серверлерді, желілік жабдықты және веб-қосымшаны сканерлеу нәтижелері бойынша анықталған осалдықтарды жоюды Тапсырыс берушімен (Жүйе әзірлеушісімен) бірлесіп пысықтау: жою тәсілдері бойынша консультация беру, қолданылған шараларды тексеру.

6.12. Осалдықтар жойылғаннан кейін аудит және енуге тестілеу режимдерінде осалдықтардың болуына қайталама аспаптық сканерлеу. Аяқтау өлшемшарты: сындылығы сыни және жоғары деңгейдегі осалдықтардың болмауы (CVSS базалық бағасы 7,0 және одан жоғары). Бұғаттаушы сәйкессіздіктер үшін «дайын емес» мәртебесін және қажетті әрекеттер тізбесін көздеу.

6.13. Тапсырыс берушімен келісілген әдістеме бойынша (сценарийлер, бір мезгілдегі пайдаланушылар саны, сұраныстар қарқындылығы, бақыланатын көрсеткіштер: жауап беру уақыты, қателер үлесі, ресурстарды пайдалану) ең жоғары жүктемені айқындау үшін

Жүйені жүктемелік тестілеу, оңтайландыру жөніндегі ұсынымдар беру; ұсынымдар іске асырылғаннан кейін — нәтижелерді салыстыра отырып, қайталама жүктемелік тестілеу.

6.14. Жүйенің бастапқы кодын осалдықтардың және декларацияланбаған мүмкіндіктердің (ДМ) болуына статикалық талдау құралымен (SAST) талдау, нәтижелерді жіктей отырып (CWE, OWASP Top 10) және жою жөніндегі ұсынымдар бере отырып; анықталған кемшіліктер жойылғаннан кейін — нәтижелерді салыстыра отырып қайталама талдау. Бастапқы кодты Тапсырыс беруші (Жүйе әзірлеушісі) ұсынады. Талдауды Әлеуетті өнім беруші өз алаңында меншікті статикалық талдау құралын пайдалана отырып — талдау құралын Тапсырыс берушінің инфрақұрылымында өрістетпей және оған лицензияларды Тапсырыс берушіге бермей орындайды; нәтижесі 6.14.5-тармаққа және 7-бөлімге сәйкес ресімделген сканерлеу туралы есеп (бастапқы және қайталама) болып табылады. Әлеуетті өнім беруші қолданатын статикалық талдау құралы 6.14.1–6.14.10-тармақтардың талаптарына сәйкес келуге тиіс.

Әлеуетті өнім беруші 6.14-тармақты орындау кезінде қолданатын бастапқы кодты статикалық талдау құралы мынадай ең төменгі талаптарға сәйкес келуге тиіс:

6.14.1. Жалпы функционалдық талаптар: бағдарламалық қамтамасыз етуді бастапқы код бойынша КҚ талаптарына сәйкестігіне талдау; бастапқы кодтар және жөндеу ақпараты болмаған кезде байт-код (бинарлық код) бойынша статикалық талдау әдісімен талдау; декларацияланбаған мүмкіндіктерді (ДМ) іздеу; талдау нәтижелері бойынша пайдаланылуын ақпаратты қорғау құралдарын (АҚК) баптау арқылы болдырмауға болатын осалдықтар мен ДМ үшін АҚК-ны баптау жөніндегі ұсынымдар беру.

6.14.2. Талдау әдістері: осалдықтар мен ДМ-ді іздеу кемінде мынадай статикалық талдау әдістерін қолдана отырып жүзеге асырылуға тиіс: үлгілер бойынша талдау; басқару ағынын талдау; taint-талдау (деректер ағындарын талдау); синонимдерді талдау; тұрақтыларды тарату. Әдістер бастапқы (байт-) код трансляцияланатын ішкі ұсынымға қолданылады.

6.14.3. Бастапқы код бойынша талдау: бағдарламалау тілдерін қолдау: Java, JavaScript, TypeScript, PHP, Python, C#, Go, PL/SQL, T-SQL, HTML5, SQL, Bash, PowerShell, XML, YAML; тілдерді автоматты түрде тани отырып, көптілді жобаларды талдау; құрастыру құралдарымен интеграция.

6.14.4. Жүйеде бастапқы коды қолжетімсіз компоненттер болған кезде бинарлық (байт-) код бойынша талдау: 6.14.2-тармақтың әдістерін қолдана отырып, Java/Scala (JAR, WAR, EAR, AAR), C/C++ (DLL, EXE), Android (APK), Apple iOS (IPA), Apple macOS (APP) тілдерінен трансляциялау арқылы алынған байт-кодты талдау.

6.14.5. Нәтижелер және есептілік: орыс және ағылшын тілдерінде CSV, HTML, PDF және SARIF форматтарында есептер қалыптастыру; PCI DSS, OWASP Top 10, OWASP Mobile Top 10, HIPAA, CWE/SANS, OWASP MASVS стандарттары мен жіктемелеріне сәйкестік туралы есептер; әрбір осалдық және ДМ бойынша — сипаттамасы, сындылық дәрежесі, кодтағы орны (оның ішінде бастапқы код болмаған кезде), қауіптілігін және пайдаланудың ықтимал тәсілдерін түсіндіру, түзету жөніндегі ұсынымдар, сыртқы дереккөздерге және жіктемеге сілтемелер; сканерлеу тарихы және жобаны сканерлеу нәтижелерін салыстыру (қайталама талдау нәтижелері бойынша кемшіліктердің жойылғанын растау үшін); қосымшаның қауіпсіздік метрикаларын есептеу және сындылық дәрежесі бойынша жиынтық статистика; есеп құрамын баптау (қосымшалар мен осалдық санаттарын таңдау).

6.14.6. Интерфейс және рөлдер: ақпаратқа бірыңғай қол жеткізу нүктесі; орыс және ағылшын тілдеріндегі интерфейс; функцияларды кемінде «әкімші», «қауіпсіздік офицері», «әзірлеуші», «басшы» пайдаланушылар санаттары үшін рөлдік ажырату; талдау үшін қосымшаны жүктеу және репозиторий мен әзірлеу тармағына жолды көрсету; әкімші интерфейсінде пайдаланушыларды және олардың құқықтарын басқару. Тапсырыс берушінің сұрауы бойынша Әлеуетті өнім беруші талдау нәтижелерін құрал интерфейсінде (оның ішінде қашықтан) көрсетеді.

6.14.7. Интеграция: талданатын кодты нұсқаларды басқару жүйелерінен (Git, SVN) және мұрағат түрінде жүктеуді қолдау; үздіксіз интеграция сервистерімен (CI/CD) және қателерді қадағалау жүйелерімен интеграцияны қолдау; ашық API болуы. Осы қызметтер шеңберінде Жүйені әзірлеушінің инфрақұрылымымен интеграция орындалмайды.

6.14.8. Талдау құралының қауіпсіздігі: әкімші баптайтын құқықтарға сәйкес иерархия деңгейлері бойынша қол жеткізуді ажырату; пайдаланушы мен әкімші функцияларына тек жеке тіркелгі деректері бойынша қол жеткізу; парольдерді шифрланған (хештелген) түрде сақтау; тіркелгі деректерін енгізудің қате әрекеттерінің санын бапталатын шекпен шектеу; парольді тұрақты ауыстыруға және оның қолданылу мерзіміне қойылатын бапталатын талаптар; пайдаланушы белсенді болмаған кезде сеансты автоматты түрде аяқтау; пайдаланушылар мен әкімшілер әрекеттерін толық журналдау.

6.14.9. Бастапқы кодты орналастыру және онымен жұмыс істеу: талдау құралы Әлеуетті өнім берушінің Қазақстан Республикасы аумағындағы алаңында орналастырылады және Тапсырыс берушінің инфрақұрылымында өрістетілмейді; Жүйенің бастапқы коды Тапсырыс берушімен (Жүйені әзірлеушімен) Әлеуетті өнім берушіге қорғалған арна арқылы не қабылдау-беру актісі бойынша жеткізгіште беріледі, Әлеуетті өнім берушінің оқшауланған ортасында сақталады, үшінші тұлғаларға берілмейді және Қазақстан Республикасынан тыс жерлердегі бұлттық сервистерге жүктелмейді; қызметтер көрсету аяқталғаннан кейін Әлеуетті өнім берушідегі бастапқы кодтың көшірмелері 8.4-тармақта белгіленген тәртіппен жазбаша растаумен жойылады.

6.14.10. Пайдалану заңдылығын растау: Әлеуетті өнім беруші статикалық талдау құралын заңды негізде (лицензия, жазылым немесе пайдаланудың өзге құқығы) қолданады. Әлеуетті өнім беруші конкурстық өтінімнің құрамында статикалық талдау құралының өндірушісінен (құқық иеленушісінен) Тапсырыс берушінің атына ресімделген, лоттың (сатып алудың) атауы мен нөмірі, талдау құралының атауы мен нұсқасы, сондай-ақ Әлеуетті өнім берушінің Тапсырыс берушіге қызметтер көрсету кезінде оны пайдалану құқығын растау көрсетілген авторизациялық хатты қоса беруге тиіс. Хаттың мәтіні шет тілінде болған жағдайда хат нотариалды куәландырылуға және қазақ немесе орыс тілдеріне аударылуға тиіс.

6.15. Тапсырыс берушінің КҚ жөніндегі қолданыстағы техникалық құжаттамасын (КҚ саясаты, Бірыңғай талаптарда көзделген қағидалар мен регламенттер, Жүйеге арналған құжаттама) толықтығына, 3-бөлімнің талаптарына және Зертхана сұрататын құжаттар тізбесіне сәйкестігіне талдау; оны өзектендіру бойынша консультациялар және жетіспейтін құжаттардың жобаларын дайындау.

6.16. Әлеуетті өнім беруші Тапсырыс берушінің ресми сұрауы бойынша Тапсырыс берушінің инфрақұрылымын соңғы нүктелердегі қатерлерді анықтау және оларға ден қою жүйесімен (EDR) (бұдан әрі — EDR жүйесі) кемінде 25 (жиырма бес) лицензия (қорғалатын соңғы нүктелердегі — жұмыс станциялары мен серверлердегі EDR агенттері) көлемінде, лицензиялардың қолданылу мерзімі кемінде 2026 жылғы 31 желтоқсанға дейін болатындай етіп жарақтандыруға тиіс. EDR жүйесі 6.16.1–6.16.10-тармақтардың талаптарына сәйкес келетін орталықтандырылған басқару құралдарын, жұмыс станциялары мен серверлерді қорғау компоненттерін және анықтау және ден қою модулін қамтуға тиіс. Серверлік компоненттер Тапсырыс берушінің инфрақұрылымында өрістетіледі (жергілікті орналастыру). Осы тармақ бойынша қызметтер көлеміне мыналар кіреді: EDR жүйесін пайдалану құқықтарын (лицензияларды) беру; серверлік компоненттерді орнату және баптау; Тапсырыс берушінің соңғы нүктелерінде агенттерді өрістету; қорғау саясаттары мен анықтау қағидаларын базалық баптау; Тапсырыс берушінің әкімшілеріне жүйені пайдалану бойынша нұсқама беру; лицензиялардың қолданылу мерзімі ішінде өндірушінің техникалық қолдауы.

6.16-тармақ бойынша жеткізілетін EDR жүйесі мынадай ең төменгі талаптарға сәйкес келуге тиіс:

6.16.1. Жалпы талаптар: барлық компоненттердің интерфейсі, оның ішінде басқару консолі, контекстік анықтама және пайдалану құжаттамасы (оның ішінде орнатуды, баптауды және пайдалануды сипаттайтын әкімші нұсқаулығы) — орыс және ағылшын тілдерінде; өндірушінің телефон және электрондық пошта арқылы орыс тіліндегі техникалық қолдауы, қажет болған жағдайда — Тапсырыс берушіге барумен; өндірушінің веб-сайтында техникалық қолдау бөлімі мен білім қорының болуы.

6.16.2. Орталықтандырылған басқару консолі: бүкіл инфрақұрылымның қорғалуын сертификатпен қорғалған қосылым арқылы бірыңғай веб-интерфейстен басқару; басты және бағынышты басқару серверлерінің иерархиясы; Windows, Linux және macOS басқаруындағы соңғы нүктелердің жабдықтары мен бағдарламалық қамтамасыз етуін түгендеу; агенттерді, қорғау компоненттерін және бөгде БҚ-ны қашықтан орнату және жою, алдын ала орнатылған конфигурациясы бар орнату пакеттерін қалыптастыру (оның ішінде оқшауланған желілер үшін); саясаттар мен тапсырмаларды автоматты түрде тағайындайтын статикалық және динамикалық топтар, компьютерлер, пайдаланушылар және топтар құрылымын Active Directory-ден импорттау; экспорттау және импорттау мүмкіндігі бар кірістірілген және пайдаланушылық саясаттар; әкімшілер құқықтарын рөлдік ажырату, Active Directory топтары арқылы аутентификация, әкімшілерді екі факторлы аутентификациялау; барлық әрекеттер мен конфигурация өзгерістерінің аудит журналы; мониторинг тақтасы және электрондық поштаға кесте бойынша жіберілетін бапталатын есептер (PDF, CSV); syslog және REST API арқылы SIEM-мен интеграция; Интернетке қол жеткізу мүмкіндігі жоқ желілер үшін жаңартулардың жергілікті айнасы; өзін-өзі қорғау тетіктері, автоматты жаңартуы және командалық жолдан басқаруы бар тәуелсіз басқару агенті; VDI орталарын қолдау; ОЖ өндірушілерінің қолдау өмірлік циклінде тұрған Windows, Linux және macOS өзекті нұсқаларын қолдау.

6.16.3. Жұмыс станцияларын қорғау: вирустардан, трояндық, тыңшылық және жарнамалық бағдарламалардан, фишингтен, ықтимал қажетсіз және қауіпті бағдарламалардан, руткиттерден нақты уақыт режимінде, сұрау бойынша және кесте бойынша қорғау, оның ішінде ОЖ іске қосылған кезде сканерлеу, жүктеу секторларын және UEFI-ді, тізілім мен WMI-ді, жедел жадты сканерлеу; сигнатуралық талдауды, эвристиканы және машиналық оқытуды үйлестіру; эксплойттардан қорғау, бопсалаушы бағдарламалардан мінез-құлықтық қорғау, пайдаланушылық қағидалары бар хостта басып кіруді болдырмау жүйесі (HIPS), өндірушінің бұлттық базасында процестердің беделін тексеру; сыртқы құрылғыларды түрі, өндірушісі, моделі және сериялық нөмірі бойынша домен пайдаланушылары мен топтарына және уақыт аралықтарына байланыстыра отырып бақылау; пошта трафигін (POP3/POP3S, SMTP, IMAP/IMAPS) және тіркемелерді тексеру; SSL-сертификаттарды бақылай отырып, фишингтік ресурстарды, ботнет серверлерін және басқарушы серверлерді бұғаттай отырып, URL тізімдерімен HTTP/HTTPS-трафикті тексеру; желі профильдері, желілік шабуылдарды анықтау модулі (IDS) және CVE көрсетілген желілік хаттамалардың (SMB, RPC, RDP) осалдықтарын пайдаланудан қорғауы бар дербес брандмауэр; домен пайдаланушылары мен топтары үшін санаттар бойынша веб-бақылау; базаларды тәулігіне кемінде 24 рет жергілікті айнадан және резервтік көздерден кері қайтару мүмкіндігімен жаңарту; баптауларды парольмен қорғау; қашықтан орнату; Windows 10/11 және кең таралған Linux дистрибутивтерін қолдау.

6.16.4. Серверлерді қорғау: тиісті ерекшеліктерді құра отырып, сервер рөлдерін автоматты түрде анықтау; жұмыс станцияларындағыдай (6.16.3-тармақ) анықтау тетіктерімен нақты уақыт режимінде, сұрау бойынша және кесте бойынша қорғау, оның ішінде эксплойттардан және бопсалаушы бағдарламалардан қорғау, HIPS, UEFI мен жедел жадты сканерлеу; Нурер-V виртуалды машиналарын агенттер орнатпай сканерлеу; сыртқы құрылғыларды бақылау; пошта және веб-трафикті тексеру; домен және жұмыс тобы кластерлерінде жұмыс істеу; сканерлеу ағындарының санын баптау; терминалдық

серверлер үшін графикалық интерфейссіз режим; параметрлерді өзгертуден және жоюдан парольмен қорғау; қашықтан орнату; Windows Server 2016–2025 және кең таралған серверлік Linux дистрибутивтерін (Red Hat Enterprise Linux, Ubuntu, Debian, SUSE Linux Enterprise Server, Oracle Linux, Rocky/Alma Linux) қолдау.

6.16.5. Анықтау және ден қою модулі (EDR) — анықтау: EDR серверімен басқарылатын коннектор (агент) арқылы соңғы нүктелерден телеметрияны деректерді жергілікті сақтай отырып жинау; тек сигнатуралық анықтау негізінде ғана емес, қағидалар (әдепкі қағидалар жиынтығы және XML-де өңделетін меншікті қағидалар) негізінде аномальды мінез-құлықты анықтау; ескертулерді сыни деңгейі бойынша автоматты түрде жіктеу, басымдық беру және топтастыру (түрі, компьютер, қағида, процесс, файл бойынша); жиынтық ақпараты (уақыт, компьютер, пайдаланушы, процесті бастамашылаған орындалатын файл), оқиға сипаттамасы, ықтимал себептері, тәуекелдері мен ұсынымдары бар анықтау карточкасы; MITRE ATT&CK техникаларымен салыстыру; түпкі себептерді талдау және файлдық жүйе, тізілім, желілік қосылымдар және URL өзгерістерін егжей-тегжейлі көрсететін процестердің толық ағашы; орындалатын файлдар (EXE/DLL) мен скрипттерді сыни деңгейі бойынша автоматты түрде жіктеу; мақсатты шабуылдарды анықтау үшін беделі, таралуы, цифрлық қолтаңбасы және мінез-құлқы бойынша сүзгілер; соңғы нүктелердегі барлық орындалатын файлдар мен скрипттерді түгендеу; іздеу тапсырмаларын сақтай отырып, бүкіл телеметрия базасы бойынша кез келген параметрлер (оның ішінде командалық жол фрагменттері) бойынша іздеу; аномальды оқиғалар мониторингінің тақтасы.

6.16.6. Анықтау және ден қою модулі (EDR) — ден қою: барлық соңғы нүктелерде орындалатын файлдарды бақылау сомасы бойынша бұғаттау, қара және ақ тізімдер, егжей-тегжейлі ерекшеліктер (бақылау сомасы, жол, цифрлық қолтаңба); файлдарды қашықтан жою және карантинге орналастыру; бір рет басу арқылы бұзылған құрылғыны желіден оқшаулау және оқшаулаудан шығару; қашықтан қайта жүктеу және өшіру; тереңдетілген сканерлеуді іске қосу; ОЖ күйінің суретін жасау (процестер, желілік қосылымдар, тізілім, жоспарлағыш, пайдаланушылар және артықшылықтар, сыни файлдар); талдау үшін соңғы нүктелерден күдікті файлдар мен скрипттерді жүктеп алу және оларды консольден сыртқы бедел сервистерінде тексеру; сүзгілеу үшін объектілерге тегтер тағайындау; SIEM, SOAR және тапсырмаларды өңдеу жүйелерімен интеграцияға арналған бағдарламалық интерфейс (API); әкімшілерді екі факторлы аутентификациялау; коннектордың Windows 10/11, кең таралған Linux дистрибутивтерін және macOS қолдауы.

6.16.7. Бұлттағы кеңейтілген талдау (жеткізілетін лицензиялар құрамында болған жағдайда): күдікті файлдарды жұмыс станциялары мен серверлерден машиналық оқытуды қолдана отырып талдау үшін өндірушінің бұлттық құмсалғышына автоматты және қолмен жіберу; бастапқы талдау нәтижелері бойынша (бірнеше секундтан 6 минутқа дейін) және ұзақ бақылау кезінде нөлдік күн қатерлерін бұғаттау; үлгілерді жіберу мен сақтаудың бапталатын саясаттары; талдау нәтижелері туралы есептер.

6.16.8. Сенімнің бағалау деңгейі: EDR жүйесінің бағдарламалық өнімі ҚР СТ ISO/IEC 15408-3-2017 «Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық технологиялар қауіпсіздігін бағалау критерийлері. 3-бөлім. Қорғауды қамтамасыз етуге қойылатын талаптар» бойынша 4-тен төмен емес сенімнің бағалау деңгейіне (СБД) ие болуға тиіс. Тапсырыс беруші Әлеуетті өнім берушіден сұрау салынған күннен бастап 3 (үш) жұмыс күні ішінде бағдарламалық өнімнің ҚР СТ ISO/IEC 15408-3-2017 талаптарына сәйкестік сертификатын (сәйкестікті растайтын құжатты) 4-тен төмен емес сенімнің бағалау деңгейін көрсете отырып талап етуге құқылы.

6.16.9. Әлеуетті өнім беруші конкурстық өтінімнің құрамында EDR жүйесі өндірушісінің (құқық иеленушісінің) Тапсырыс берушінің атына ресімделген, бағдарламалық өнімнің атауы мен нұсқасы, лицензиялардың саны мен қолданылу мерзімі көрсетілген, сондай-ақ Әлеуетті өнім берушінің Қазақстан Республикасының аумағында пайдалану құқықтарын беруге (лицензияларды жеткізуге) және техникалық қолдау

көрсетуге құқығы расталған авторизациялық хатын қоса беруге тиіс. Хаттың мәтіні шет тілінде болған жағдайда хат нотариат куәландырған және қазақ немесе орыс тілдеріне аударылған болуға тиіс;

6.16.10. Берілетін құжаттар: өрістету нәтижелері бойынша Әлеуетті өнім беруші Тапсырыс берушіге лицензиялардың саны мен қолданылу мерзімі көрсетілген лицензиялық құжаттарды (белсендіру кілттерін/сертификаттарын), пайдалану құжаттамасын және қорғалған соңғы нүктелердің тізбесі көрсетілген EDR жүйесін орнату және баптау актісін береді.

6.17. Сынақтарға дайындық мәселелері бойынша мемлекеттік органдармен, Зертханамен және Жүйені әзірлеушімен хат алмасуды жүргізу кезінде Тапсырыс берушіге жәрдем көрсету, оның ішінде Тапсырыс берушінің Зертханаға кейіннен ұсынуы үшін Сынақ әдістемесі мен қағидаларына сәйкес сынақтар жүргізуге арналған өтінімнің және қоса берілетін құжаттар топтамасының жобаларын дайындау.

7. Нәтижелерге және есептік құжаттарға қойылатын талаптар

7.1. Қызметтер көрсету нәтижелері бойынша Әлеуетті өнім беруші Тапсырыс берушіге мынадай есептік құжаттарды ұсынады:

№	Құжат	Мазмұнына қойылатын талаптар / мерзімі
1	Қызметтер көрсетудің жоспар-кестесі	Кезеңдер, мерзімдер, жауаптылар, Тапсырыс берушіден қажетті деректер мен қолжетімділіктердің тізбесі. Шарт жасалған күннен бастап 10 жұмыс күні ішінде
2	Жүйенің КҚ зерттеп-қарау туралы есеп	Архитектураның және зерттеп-қарау периметрінің сипаттамасы; 6.1, 6.3, 6.5, 6.7, 6.9-тармақтар бойынша талдау нәтижелері; 3-бөлімнің талаптарына сәйкестікті бағалау
3	Сәйкессіздіктердің тізбесі және оларды жою жөніндегі іс-шаралар жоспары	Әрбір сәйкессіздік: сипаттамасы, НҚА/стандарт талабына сілтеме, сыншылдық деңгейі, ұсыным, жауапты тарап, болжамды мерзімі
4	Осалдықтарға сканерлеу бойынша есептер (бастапқы және қайталама)	Периметр, режимдер, CVSS бағалауы бар осалдықтардың тізбесі, ұсынымдар; бастапқы және қайталама сканерлеу нәтижелерін салыстыру; сканерлеу құралынан экспорт
5	Жүктемелік тестілеу бойынша есептер (бастапқы және қайталама)	Әдістеме, сценарийлер, алынған көрсеткіштер, анықталған ең жоғары жүктеме, ұсынымдар, нәтижелерді салыстыру
6	Бастапқы кодты сканерлеу туралы есептер (бастапқы және қайталама)	Периметр (модульдердің тізбесі, кодтың тармағы/нұсқасы, берілген архивтердің бақылау сомалары), талдау құралы және оның нұсқасы, жіктелуі мен сыншылдық дәрежесі көрсетілген анықталған осалдықтар мен ДМ, жою жөніндегі ұсынымдар, бастапқы және қайталама сканерлеу нәтижелерін салыстыру; талдау құралынан PDF және SARIF/CSV форматындағы түсірілім
7	Серверлік үй-жайдың физикалық қорғалуын тексеру туралы есеп	6.9-тармақ бойынша тексеру нәтижелері, Тапсырыс берушімен келісу бойынша фототіркеу, сәйкессіздіктер мен ұсынымдар
8	КҚ жөніндегі құжаттама бойынша қорытынды	Қолда бар және жетіспейтін құжаттардың тізбесі, ескертулер, өзектендіру жөніндегі ұсынымдар, құжаттардың жобалары

№	Құжат	Мазмұнына қойылатын талаптар / мерзімі
9	EDR жүйесі бойынша құжаттар (Тапсырыс берушінің сұрауы бойынша жаратқандырған кезде, 6.16-тармақ)	Лицензиялардың саны мен қолданылу мерзімі көрсетілген лицензиялық құжаттар (белсендіру кілттері/сертификаттары); пайдалану құжаттамасы; қорғалған соңғы нүктелердің тізбесі көрсетілген орнату және баптау актісі (6.16.10-тармақ); Тапсырыс берушінің сұрауы бойынша — СБД 4-тен төмен емес ҚР СТ ISO/IEC 15408-3-2017 сәйкестік сертификаты және өндірушінің авторизациялық хаты (6.16.8, 6.16.9-тармақтар)
10	Жүйенің сынақтарға дайындығы туралы қорытынды есеп	Жиынтық нәтижелер, сәйкессіздіктерді жою мәртебесі, қабылданған тәуекелдердің тізбесі, Зертханаға ұсынуға арналған құжаттар топтамасы

7.2. Есептік құжаттар орыс тілінде немесе Тапсырыс берушінің талабы бойынша қазақ тілінде электрондық түрде (PDF форматында және өңделетін форматта) және Тапсырыс берушінің талабы бойынша қағаз жеткізгіште 1 (бір) данада ұсынылады. Осалдықтар мен конфигурациялар туралы мәліметтерді қамтитын есептік құжаттар қорғалған арналар арқылы не жеткізгіште қолхат арқылы беріледі.

8. Қызметтер көрсету шарттары

8.1. Тапсырыс беруші жоспар-кестемен келісілген мерзімдерде Әлеуетті өнім берушіге: Жүйеге арналған техникалық құжаттаманы, желі схемаларын, компоненттердің тізбесін, жұмыстарды орындау үшін қажетті есептік жазбалар мен қолжетімділіктерді, Тапсырыс беруші өкілінің сүйемелдеуімен серверлік үй-жайға кіруді, сондай-ақ Тапсырыс беруші мен Жүйені әзірлеуші тарапынан байланыс тұлғаларын ұсынады.

8.2. Жүйенің қолжетімділігіне әсер етуі мүмкін жұмыстар (аспаптық сканерлеу, жүктемелік тестілеу) тек Тапсырыс берушімен келісілген уақыт терезелерінде, жазбаша хабарламадан кейін және Тапсырыс берушіде Жүйенің өзекті резервтік көшірмесі болған жағдайда орындалады. Жүктемелік тестілеу тестілік стендте / өнеркәсіптік ортада ең жоғары жүктеме сағаттарынан тыс уақытта жүргізіледі.

8.3. Жұмыстарды жүргізу кезінде деструктивті әсер ететін осалдықтарды пайдалануға, Тапсырыс берушінің деректерін өзгертуге немесе жоюға, Тапсырыс берушімен келіспей Жүйенің конфигурациясына өзгерістер енгізуге жол берілмейді. Барлық өзгерістерді Әлеуетті өнім берушінің ұсынымдары негізінде Тапсырыс беруші (Жүйені әзірлеуші) не Тапсырыс берушінің жазбаша тапсырмасы бойынша Әлеуетті өнім беруші орындайды.

8.4. Әлеуетті өнім беруші Қазақстан Республикасының заңнамасына сәйкес қызметтер көрсету барысында алынған барлық ақпараттың, оның ішінде осалдықтар, конфигурациялар туралы мәліметтер мен дербес деректердің құпиялылығын қамтамасыз етеді; жұмыстар басталғанға дейін тараптар жария етпеу туралы келісімге қол қояды. Қызметтер көрсету нәтижелері Тапсырыс берушінің меншігі болып табылады; қызметтер көрсету аяқталғаннан кейін Әлеуетті өнім беруші жұмыстар барысында алынған Тапсырыс беруші деректерінің көшірмелерін растаумен жояды.

8.5. Әлеуетті өнім беруші пайдаланатын қорғалуды талдау, жүктемелік тестілеу және бастапқы кодты талдау құралдары заңды негізде (лицензиялық не еркін таратылатын) қолданылуға, осалдықтардың/қағидалардың өзекті базаларына ие болуға және есептерді электрондық түрде қалыптастыруды қамтамасыз етуге тиіс. Бастапқы кодты статикалық талдау құралына қойылатын талаптар және оны пайдаланудың заңдылығын растау тәртібі 6.14.1–6.14.10-тармақтарда белгіленген.

8.6. Қызметтерді Әлеуетті өнім берушінің білікті персоналы көрсетеді. Әлеуетті өнім берушіге қойылатын біліктілік және өзге де талаптар конкурстық құжаттамамен белгіленеді.

8.7. Тараптардың өзара іс-қимылы тағайындалған жауапты өкілдер арқылы жүзеге асырылады; жұмыс мәселелері кеңестердің хаттамаларымен немесе ресми хат алмасумен (оның ішінде электрондық пошта арқылы) тіркеледі.

9. Қызметтерді тапсыру-қабылдау тәртібі

9.1. Қызметтерді тапсыру-қабылдау қызметтер көрсету тұтастай аяқталғаннан кейін ұсынылған есептік құжаттар (7-бөлім) және Қазақстан Республикасының мемлекеттік сатып алу туралы заңнамасында белгіленген тәртіппен ресімделетін көрсетілген қызметтер актісі негізінде жүзеге асырылады.

9.2. Әлеуетті өнім беруші ескертулерді оларды алған күннен бастап 10 (он) жұмыс күні ішінде жояды.

9.3. Қызметтер 7-бөлімнің талаптарына сәйкес келетін есептік құжаттардың толық топтамасы ұсынылған және 6.12, 6.13 және 6.14-тармақтарда белгіленген өлшемшарттар орындалған кезде тиісінше көрсетілген болып есептеледі.

10. Қызметтер көрсету мерзімі мен орны

10.1. Қызметтер көрсету мерзімі: шарт жасалған күннен бастап 2026 жылғы 20 желтоқсанға дейін.

10.2. Қызметтер көрсету орны: Қазақстан, Астана қ., Есіл ауданы, Сығанақ к-сі, 70-ғимарат. Қатысуды талап ететін жұмыстар (физикалық қорғалуды тексеру, персоналды оқыту, қашықтан қолжетімділіксіз Тапсырыс беруші желісіндегі жұмыстар) Жүйе (Тапсырыс беруші) орналасқан жерде орындалады; қалған жұмыстар Тапсырыс берушімен келісу бойынша қашықтан орындалуы мүмкін.

11. Қызметтер көрсету нәтижелері бойынша Әлеуетті өнім берушінің міндеттемелері

11.1. Әлеуетті өнім беруші қызметтер көрсету мерзімі шегінде анықталған сәйкессіздіктерді жою мәселелері бойынша Тапсырыс берушіні консультациялық сүйемелдеуді, оның ішінде олардың жойылуын қайта тексеруді қамтамасыз етеді.

11.2. Әлеуетті өнім беруші есептік құжаттардың толықтығы мен дұрыстығы және берілген ұсынымдардың негізділігі үшін жауапты болады. Тапсырыс берушінің көрсетілген қызметтер актісіне қол қойылғаннан кейін 30 (отыз) күнтізбелік күн ішінде анықталған есептік құжаттарға ескертулерін Әлеуетті өнім беруші қосымша ақысыз жояды.

11.3. Әлеуетті өнім берушінің міндеттемелері Жүйенің сынақтарға дайындығы туралы қорытынды есеп (7-бөлімнің 10-тармағы) бойынша көрсетілген қызметтер актісіне қол қойылған сәттен бастап толық көлемде орындалған болып есептеледі. Әлеуетті өнім беруші Тапсырыс берушінің (Жүйені әзірлеушінің) берілген ұсынымдарды жоймауы, қызметтер көрсету аяқталғаннан кейін Жүйенің құрамының немесе конфигурациясының өзгеруі, сондай-ақ Әлеуетті өнім берушіге ұсынылған деректер мен қолжетімділіктердің толық болмауы салдарынан туындаған сәйкессіздіктер үшін жауапты болмайды.

11.4. Әлеуетті өнім берушінің кепілдік міндеттемелері

Егер осы техникалық ерекшеліктің 10.1-тармағында белгіленген қызметтер көрсету мерзімі аяқталғанға дейін осы техникалық ерекшелікте көзделген жекелеген іс-шаралар Тапсырыс берушіге байланысты емес себептер бойынша, оның ішінде анықталған сәйкессіздіктерді, осалдықтарды жою, Жүйені пысықтау, қайта тексерулер, сканерлеулер мен тестілеулер жүргізу қажеттілігіне байланысты аяқталмаған жағдайда, Әлеуетті өнім беруші кепілдік міндеттемелер шеңберінде 2027 жылғы 1 қарашаны қоса алғанға дейін Тапсырыс берушіден қосымша ақы алмай оларды одан әрі сүйемелдеуді және орындауды қамтамасыз етеді.

11.5. Кепілдік міндеттемелер анықталған сәйкессіздіктер мен осалдықтарды жоюды консультациялық сүйемелдеуге, осы техникалық ерекшелікте көзделген қайта тексерулерді, сканерлеулер мен тестілеулерді жүргізуге, Әлеуетті өнім беруші бұрын

дайындаған есептік материалдарды өзектендіруге, сондай-ақ көрсетілген қызметтердің нәтижелеріне қатысты ескертулерді жоюға қолданылады.

11.6. Көрсетілген іс-шараларды кепілдік кезеңі ішінде орындауды Әлеуетті өнім беруші жасалған шарт бойынша қызметтердің құны есебінен жүзеге асырады және ол шарт құнының ұлғаюына, қосымша шарт жасасуға не Тапсырыс берушіде өзге де қаржылық міндеттемелердің туындауына әкеп соқпайды.
