Бекітемін
«Әбілқас Сағынов атындағы Қараганды техникалық университеті» КеАҚ
Басқарма Төрағасы – Ректоры
_____ Сагинтаева С.С.
Басқарманың «14» қаңтар 2026 ж.
№ 23 шешімі

ІШКІ НОРМАТИВТІК ҚҰЖАТ

АҚПАРАТТЫ ӨҢДЕУ ҚҰРАЛДАРЫМЕН БАЙЛАНЫСТЫ АКТИВТЕРДІҢ ҮЗДІКСІЗ ЖҰМЫСЫН ҚАМТАМАСЫЗ ЕТУ ЖӘНЕ ЖҰМЫСҚА ҚАБІЛЕТТІЛІГІН ҚАЛПЫНА КЕЛТІРУ ЖӨНІНДЕГІ ІС-ШАРАЛАР ЖОСПАРЫ

ІНҚ ІІ-08-2026

Әзірлеген: Ақпараттық қауіпсіздік жөніндегі инженер
Д.К. Читян _____

Қарағанды

Құжатты рұқсатсыз көшіруге тыйым салынады

Мазмұны

1 Қолдану саласы 3
2 Нормативтік сілтемелер 3
3 Терминдер, анықтамалар және қысқартулар 3
4 Жауапкершілік және өкілеттіктер 4
5 Жалпы қағидалар 4
6 Активтерді сыни тұрғыдан жіктеу 5
7 Үздіксіз жұмысты қамтамасыз ету жөніндегі іс-шаралар 6
8 Резервтік көшірме жүйесі 8
9 Оқиғалар мен бұзылуға әрекет ету 9
10 Жекелеген жүйелердің істен шығуы кезіндегі әрекеттер 10
11 Мониторинг 11
12 Жоспарды тестілеу 12
13 Келісу, бекіту және қолданысқа енгізу 12
14 Сақтау 13
15 Қайта қарау және өзектендіру тәртібі 13

Құжатты рұқсатсыз көшіруге тыйым салынады

1 Қолдану саласы

1.1 Осы Ақпаратты өңдеу құралдарымен байланысты активтердің үздіксіз жұмысын қамтамасыз ету және жұмысқа қабілеттілігін қалпына келтіру жөніндегі іс-шаралар жоспары «Әбілқас Сағынов атындағы Қарағанды техникалық университеті» КеАҚ-та қолданылады.

1.2 Жоспардың талаптары Университеттің барлық ақпараттық активтеріне, АТ-инфрақұрылымына, сервистеріне, деректері мен процестеріне, сондай-ақ АТ-ресурстарын пайдалануға, сүйемелдеуге және қолжетімділігін қамтамасыз етуге қатысатын барлық қызметкерлер мен құрылымдық бөлімшелерге қолданылады.

1.3 Жоспар Ақпараттық технологиялар департаментінің қызметкерлері, ақпараттық қауіпсіздік жөніндегі инженерлер, ақпараттық жүйелердің әкімшілері, сондай-ақ АТ-ресурстарын пайдаланушылар өздерінің өкілеттіктері мен міндеттеріне қатысты бөлігінде орындауы үшін міндетті болып табылады.

2 Нормативтік сілтемелер

2.1 Ережені әзірлеу кезінде мына нормативтік құжаттар пайдаланылды:

1) «Ақпараттандыру туралы» Қазақстан Республикасының 2015 жылғы 24 қарашадағы № 418-V Заңы.

2) ҚР СТ ИСО/МЭК 27002-2023 «Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару шаралары».

3) ҚР СТ ИСО/МЭК 27001-2023 «Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар».

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

2.2 Ереже Университеттің ішкі нормативтік құжаты болып табылады және Университеттің Ақпараттық қауіпсіздік саясатына сәйкес келеді.

3 Терминдер, анықтамалар және қысқартулар

1) Актив – ақпаратты өңдеуге, сақтауға немесе беруге қатысатын жабдық, бағдарламалық қамтамасыз ету, сервис, дерекқор, ақпарат тасымалдаушы немесе процесс.

2) Активтің сыни сипаты — Университеттің жұмыс істеуі үшін активтің маңыздылығының және оның істен шығуы салдарының деңгейінің көрсеткіші.

Құжатты рұқсатсыз көшіруге тыйым салынады

3) Қызметтің үздіксіздігі (Business Continuity) — оқиғаларға, іркілістерге және авариялarға қарамастан Университет инфрақұрылымының негізгі процестердің орындалуын қамтамасыз ету қабілеті.

4) Авариядан кейін қалпына келтіру (Disaster Recovery, DR) — істен шыққаннан кейін жүйені жұмысқа жарамды күйге қайтару жөніндегі іс-шаралар кешені.

5) Резервтеу – негізгі жүйе істен шыққан кезде жұмысты қамтамасыз ететін қайталанатын компоненттер құру.

6) Резервтік көшіру – деректерді сақтау және кейіннен қалпына келтіру мақсатында олардың көшірмелерін жасау процесі.

7) Ақпараттық қауіпсіздік оқиғасы – ақпараттың құпиялылығын, тұтастығын немесе қолжетімділігін бұзатын немесе бұзуға қабілетті оқиға.

8) АТД — Университеттің ақпараттық технологиялар департаменті.

9) RTO (Recovery Time Objective) — сервисті қалпына келтірудің рұқсат етілген ең ұзақ уақыты.

10) RPO (Recovery Point Objective) — қалпына келтіру кезінде мүмкін болатын деректердің барынша шектеулі жоғалуы (уақыт бойынша).

4 Жауапкершілік және өкілеттіктер

4.1 Жоспардың іске асырылуына жалпы басшылық жасау, бұзылу кезіндегі іс-қимылдарды үйлестіру және ресурстарды бөлуді АТД директоры жүзеге асырады.

4.2 Ақпараттық қауіпсіздік инженері оқиғалардың себептерін талдауға, тәуекелдерді бағалауға, қорғау шараларының орындалуын бақылауға және қалпына келтіру шараларына қатысуға жауап береді.

4.3 Жүйелік, желілік әкімшілер және дерекқор әкімшілері сервистерді сүйемелдеуді, резервтеуді, мониторингті, ақауларды жоюды және жүйелердің жұмысын қалпына келтіруді қамтамасыз етеді.

4.4 Құрылымдық бөлімшелердің басшылары АТ активтері үшін жауапты тұлғаларды тағайындауды және оқиғалар кезінде АТД-мен өзара іс-қимылды қамтамасыз етеді.

4.5 АТ-ресурстарын пайдаланушылар ақаулар туралы уақтылы хабарлауға және белгіленген пайдалану ережелерін сақтауға міндетті.

5 Жалпы қағидалар

5.1 Осы Жоспар үздіксіз жұмысты қамтамасыз ету және Университеттің АТ активтерін қалпына келтіру бойынша ұйымдастырушылық және техникалық шараларды айқындайды.

5.2 Іс-шараларды жоспарлау тәуекелдерді талдауға, активтерді сыни тұрғыдан жіктеуге, резервтеу, резервтік көшіру, мониторинг және қалпына келтіруді тестілеу тетіктерін енгізуге негізделген.

5.3 Жоспар Университеттің ішкі нормативтік құжаты болып табылады және ақпараттық қауіпсіздіктің сәтсіздіктеріне, апаттарына және оқиғаларына әрекет ету кезінде негізгі регламент ретінде пайдаланылады.

5.4 Жоспардың талаптары Университеттің АТ-инфрақұрылымын жобалау, жаңғырту және пайдалану кезінде ескеріледі.

6 Активтерді сыни тұрғыдан жіктеу

6.1 Университеттің барлық активтері ітен шығудың салдарына байланысты сыни деңгейлер бойынша жіктеледі.

6.2 3 – класс – Сыни активтер

6.2.1 Істен шығу Университеттің негізгі процестерін (білім беру, әкімшілік, қаржылық) тоқтатуға әкеледі.

6.2.2 Сыни активтер:

1) Active Directory;
2) Корпоративтік электрондық пошта;
3) Интернетке кіру;
4) Электрондық құжат айналымы жүйесі;
5) Виртуалдандыру серверлері;
6) DNS, DHCP серверлері;
7) бейнебақылау жүйесі, КББЖ;
8) бухгалтерлік және кадрлық жүйелер;
9) сақтық көшірмелер үшін СХД / NAS.

6.3 **2-класс – Маңызды активтер**

6.3.1 Істен шығу жекелеген процестерге әсер етеді, бірақ Университет қызметін толығымен бұғаттамайды.

6.3.2 Маңызды активтер:

1) қашықтықтан оқыту сервистері;
2) білім беру порталдары;
3) электрондық кітапхана;
4) факультеттердің Жергілікті веб-ресурстары;
5) қызметкерлерді қолдау сервистері.

6.4 **1-класс – Сыни емес активтер**

6.4.1 Істен шығу шектеулі әсер етеді және негізгі қызметке кедергі келтірмейді.

6.4.2 Сыни емес активтер:

1) ақпараттық панельдер;
2) бөлімшелердің жергілікті серверлері;

3) сыни ресурстарға қол жеткізусіз жекелеген АЖО.

7 Үздіксіз жұмысты қамтамасыз ету жөніндегі іс-шаралар

7.1 Ұйымдастыру іс-шаралары

7.1.1 АТ-активтерінің өзекті тізілімі. Жабдықты, бағдарламалық жасақтаманы, шоттарды, желілік инфрақұрылымды, қызметтерді және ақпараттық жүйелерді қамтитын құрылымдық активтер тізіліміне қолдау көрсетіледі. Әрбір актив үшін сыни, меншік иесі, орналасқан жері, сүйемелдеу жауапкершілігі, басқа активтерге тәуелділік және өзгерістер тарихы жазылады.

7.1.2 Архитектура және процестерді құжаттау. Желінің физикалық және логикалық архитектурасының схемасына, виртуалдандыру ортасының топологиясына, қызметтердің өзара әрекеттесу схемаларына, қауіп модельдеріне, резервтік схемаларға және ақауларға төзімділікке қолдау көрсетіледі. Құжаттама АТ-инфрақұрылымы өзгерген сайын өзектендіріледі.

7.1.3 Сыни процестерді сәйкестендіру. Университеттің білім беру, әкімшілік және қаржылық қызметі үшін маңызды процестер анықталады. Әр процесс үшін тәуелді қызметтер, RTO және RPO жазылады. Ақпарат қалпына келтіру сценарийлерін әзірлеу кезінде қолданылады.

7.1.4 АТ-тәуекелдерін үнемі бағалау. Операциялық тәуекелдерді талдаудың жыл сайынғы рәсімі жүргізіледі: сәтсіздік ықтималдығын бағалау, осалдықтарды анықтау, университет қызметіне әсерін талдау. Нәтижелер есепте жазылады және қорғау шараларын өзектендіру үшін қолданылады.

7.1.5 Қызметкерлерді оқыту. АТД қызметкерлері ден қою рәсімдері, резервтік көшіру жүйесімен жұмыс істеу, апат кезіндегі іс-қимылдар және резервтік ресурстарға ауысу ережелері бойынша нұсқаулықтан өтеді. Пайдаланушылар ақаулар мен пайдалану ережелерін сақтау бойынша нұсқаулар алады.

7.1.6 Қол жетімділікті шектеу. Жабдыққа, конфигурацияларға, деректер мен қызметтерге ең аз қажетті қол жетімділік анықталады. RBAC саясаты жүзеге асырылады, кіру журналдары жүргізіледі, екі факторлы аутентификация қолданылады.

7.1.7 Өзгерістерді бақылау (Change Management). Инфрақұрылымдағы барлық өзгерістер жүйелердің қолжетімділігіне әсері бағаланатын ресми келісу рәсімінен өтеді. Өзгерістерді енгізу регламенттік терезелерге кері қайтару мүмкіндігімен орындалады.

7.1.8 Жеткізушілер мен мердігерлерді басқару. Байланыс қызметтерін, сервистік келісімшарттарды және БҚ жеткізушілері SLA, реакция уақыты, техникалық қолдау сапасы бойынша бағаланады. Шарттарға қол жетімділік талаптары мен тоқтап қалу жауапкершілігі кіреді.

7.2 Техникалық іс-шаралар

7.2.1 Маңызды қызметтер мен инфрақұрылымдық компоненттерді резервтеу

1) Серверлік жабдық. Кластерленген шешімдер (Failover Cluster, VMware HA) аппараттық ақаулар болған жағдайда тоқтап қалу уақытын азайту үшін қолданылады. AD функциялары әртүрлі физикалық сайттарға немесе серверлерге бөлінген бірнеше домендік контроллерлерге орналастырылады.

2) Деректер қоймалары. СХД 5/6/10 деңгейіндегі RAID массивтерін пайдаланады. Көлемді шағылыстыру, сақтық көшірмелерді сақтауға арналған резервтік NAS, мұрағат деректері үшін бөлек сегмент ұйымдастырылған.

3) Желілік жабдық. Негізгі бағдарлауыштар мен қосқыштар қайталанады. VRRP/HSRP механизмдері, LACP, резервтік Uplink арналары қолданылады. Маңызды инфрақұрылым бірнеше тәуелсіз қуат желілері арқылы қосылған.

7.2.2 Ақпараттық жүйелерді резервтеу. Сыни қызметтер контейнерлеу, виртуалдау немесе жоғары қолжетімділік қызметтері технологияларын пайдалана отырып орналастырылады:

— резервтік дерекқорлары (қағытпалау, Always On, Master/Slave);

— қосымшалар кластерлері;

— айналандыру LDAP/AD;

— веб-сервистерді және олардың конфигурацияларын қайталау.

7.2.3 Бағдарламалық жасақтаманы уақтылы жаңарту. ОЖ және қолданба жаңартуларын басқарудың орталықтандырылған жүйесі іске асырылуда. Тек тексерілген және тексерілген жаңартулар орнатылады. Есеп нұсқаларды басқару жүйесі және жаңартуларды орындау журналы арқылы жүзеге асырылады.

7.2.4 Инфрақұрылымның жағдайын үздіксіз мониторингтеу. Мониторинг автоматтандырылған жүйелермен жүзеге асырылады (Zabbix, FortiGate, Windows Server). Мыналар бақыланады:

— CPU, RAM, дискілерді жүктеу, жабдықтың температурасы;

— желілік трафик, кідірістер, бағдарлау;

— VPN туннельдері мен байланыс арналарының жағдайы;

— DNS/DHCP сұраулар, авторландырудың бұзылуы;

— қауіпсіздік журналдары, AD уақиғасы, рұқсатсыз кіру әрекеттері;

— виртуалды машиналардың жұмысқа қабілеттілігі;

— резервтік көшірме жасау (сәттілік, қателер).

7.2.5 Қауіпсіздікті қорғау және бақылау жүйесі. Инфрақұрылымда мыналар қолданылады:

— кәсіпорын класындағы вирусқа қарсы шешімдер;

— ағып кетуді бақылау үшін DLP;

— OSI деңгейлері бойынша сүзілген желіаралық FortiGate брандмауэрі;

— желіні сегменттеу (VLAN, ACL);

— орталықтандырылған логингтеу және оқиғалардың өзара байланысы (SIEM болған кезде).

7.2.6 Инфрақұрылымды физикалық қорғау. . Серверлік үй-жайларда:

- климатты бақылау;

- жүктеме мониторингімен үздіксіз қуат және ҮҚК;
- жабық тірек немесе шектеулі бөлме;
- бейнебақылау және келулерді тіркеу;
- түтін, температура және су тасқыны датчиктері іске асырылады.

7.2.7Тұрақтылықты арттыру үшін пайдалану рәсімдері:

1) Жабдықтың жағдайын жоспарлы тексеру.

2) қуат көзінің температурасы мен қуатын бақылау.

3) белсенді емес қызметтерді немесе уақытша контейнерлерді үнемі қайта жүктеу.

4) резервтік көшірмесі бар желілік конфигурацияларды жаңарту.

5) файлдық жүйелердің тұтастығын тексеру.

6) резервтік ресурстарға ауысуды тестілеу.

7.3 Тоқтап қалудың алдын алу шаралары

7.3.1 Шамадан тыс жүктемені болжау үшін өнімділік трендтерін талдау.

7.3.2 Қызмет ету мерзімінің соңына жететіп қалған жабдықты ауыстыру бойынша профилактикалық жұмыстар.

7.3.3 ДСЖ жүктемесін бақылау және массивті уақтылы кеңейту.

7.3.4 Біртұтас істен шығу нүктесін болдырмау үшін желілік құрылымды оңтайландыру.

7.3.5 Сыни сервистер үшін QoS және Traffic Shaping саясаттарын қолдану.

8 Резервтік көшірме жүйесі

8.1 Резервтік көшірме жүйесі ақаулар, пайдаланушы қателері, аппараттық ақаулар және АҚ оқиғаларынан кейін деректердің сақталуын қамтамасыз етудің және АТ-қызметтерін кепілдендірілген қалпына келтірудің негізгі құрамдас бөлігі болып табылады.

8.2 Резервтік көшірме мамандандырылған бағдарламалық қамтамасыз етуді және арнайы инфрақұрылымды (NAS, жеке резервтік серверлер, қорғалған желілік сегменттер) пайдалана отырып, АТД басқаруымен орталықтандырылған түрде орындалады.

8.3 «3–2–1» принципі қолданылады:

— деректердің кемінде 3 көшірмесі;

— кем дегенде 2 түрлі тасымалдаушы немесе сақтау түрлері;

— негізгі контурдан тыс немесе жеке сегментте кемінде 1 көшірме.

8.4 Көшіру негізгі қызметтердің жұмысына айтарлықтай әсер етпестен жүзеге асырылады (дедупликаттау, инкременталды бэкаптар, VSS, VM суреттері қолданылады).

8.5 Резервтік көшірме түрлері:

1) Күнделікті қосымша көшірмелер

Өзгерістерді тіркеуге және деректер көлемін азайтуға мүмкіндік береді. Басталу уақыты – түнгі терезе (01:00-05:00).

2) Апта сайынғы толық көшірмелер

Жүйелік файлдарды, конфигурацияларды және пайдаланушы деректерін қоса, деректердің толық суреті.

3) Ай сайынғы мұрағаттық көшірмелер

Ұзақ мерзімді көшірмелер арнайы қоймада сақталады және ұзақ уақыт ішінде деректерді қалпына келтіруге арналған.

4) Арнайы сақтық көшірмелер

- бағдарламалық жасақтаманы жаңартпас бұрын;
- конфигурацияларды өзгертпес бұрын;
- сервистерді немесе инфрақұрылымдық жұмыстарды ауыстырар алдында.

8.6 Көшірмелер қол жетімділігі шектеулі арнайы NAS-та (мысалы, Synology) сақталады.

8.7 Мұрағаттық көшірмелер үшін сырттан ең аз қолжетімділігі бар жеке желілік сегмент қолданылады.

8.8 Криптовирустардан қорғау үшін маңызды көшірмелерді офлайн тасымалдаушыларға тасымалдауға болады.

8.9 Қоймаға кірудің қатаң шектеулі әкімшілер тізімі бар.

8.10 Құпия деректердің барлық көшірмелері шифрланады. Көшірудің сәтті журналдары қолданылады. Модификациядан қорғау жүзеге асырылады (WORM, immutable snapshots).

8.11 Тоқсанына кемінде бір рет сыни сервистерді тестілік қалпына келтіру орындалады. Нәтижелер жазылады: қалпына келтіру жылдамдығы, деректердің тұтастығы, конфигурациялардың дұрыстығы. Қате болған жағдайда жоспарға түзетулер енгізіледі.

9 Оқиғалар мен бұзылуға әрекет ету

9.1 Оқиғаларға жауап беру деректердің жоғалуын және тоқтап қалу уақытын азайтуды, сондай-ақ бұзылу салдарының таралуын болдырмауды қамтамасыз етеді.

9.2 Барлық бұзушылықтар туралы хабарламалар, пайдаланушылардың өтініштері және мониторинг оқиғалары АТД оқиғалар журналында тіркеледі. Оқиға уақыты, сипаттамасы, зардап шеккен қызметтер, сыни деңгей және тартылған қызметкерлер жазылады.

9.3 Оқиға түрі техногендік ақаулық, желілік оқиға, АҚ оқиғасы, пайдаланушының қателігі немесе жабдықтың істен шығуы ретінде жіктеледі.

9.4 Актив класы (1-3) және Университет қызметіне ықтимал әсер анықталады.

9.5 Сыни оқиға болған жағдайда кеңейтілген әрекет ету тобы құрылады.

9.6 әрекет ету тобының әрекеттері:

1) бастапқы диагностика (ping, tracert, журналдарды қарау, қызметтердің қолжетімділігін тексеру).

2) тәуелділікті талдау: желілік қызметтер (DNS, DHCP), ДБ, виртуалдандыру.

3) каскадты істен шығудың алдын алу үшін ақаулы сегментті оқшаулау.

4) жүктемені резервтік ресурстарға ауыстыру (серверлер, арналар, АШТ).

5) егер деректерді қалпына келтіру қажет болса-қажетті резервтік көшірмені жүктеу.

6) қалпына келтіруді растау: функционалдылықты тексеру, журналдарды тексеру.

9.7 оқиға аяқталғаннан кейін себептерді, тоқтау уақытын және қайталанудың алдын алу бойынша ұсыныстарды талдай отырып есеп ресімделеді. Оқиға барлық тәуелді қызметтер тұрақтандырылғаннан кейін ғана жабық болып саналады, қажет болған жағдайда жоспар жаңартылады.

10 Жекелеген жүйелердің істен шығуы кезіндегі әрекеттер

10.1 Серверлер немесе виртуалды инфрақұрылым компоненттері істен шыққан кезде НА немесе кластерлік механизмдерді пайдалана отырып, резервтік серверге автоматты немесе қолмен ауысу орындалады. Физикалық түйін апатқа ұшыраған жағдайда виртуалды машина басқа қол жетімді серверде іске қосылады. Қажет болса, қалпына келтіру виртуалды машинаның сақтық көшірмесінен немесе толық сақтық көшірмеден жасалады. Егер қалпына келтіру мүмкін болмаса, бекітілген үлгіден (gold image) жаңа виртуалды машинаны орналастыру жүзеге асырылады.

10.2 Желілік жабдық істен шыққан кезде резервтік коммутаторға немесе маршрутизаторға ауысу жүзеге асырылады. Балама маршруттар болған кезде резервтік маршруттау схемасы қолданылады. Аппараттық конфигурация резервтік көшірме файлынан қалпына келтіріледі. Толық істен шыққан жағдайда ақаулы құрылғыны жедел ауыстыру орындалады.

10.3 Жеке диск зақымдалған кезде raid қалпына келтіру механизмі автоматты түрде іске қосылады. Қажет болған жағдайда резервтік қоймаға ауысу жүргізіледі. Сыни қате болған жағдайда деректердің тұтастығын кейіннен міндетті түрде тексере отырып, мұрағаттық резервтік көшірмеден деректерді қалпына келтіру орындалады.

10.4 Электр қуаты жоғалған кезде үздіксіз қуат көздеріне лезде ауысу орындалады. Кезекші қызметші оқиға туралы автоматты түрде хабарлама алады. Электр желісі ұзақ уақыт болмаған кезде ҮҚК заряд деңгейін бақылау және сыни емес сервистерді кезең-кезеңімен ажырату жүзеге асырылады. Резервтік генератор болған жағдайда ол жұмысқа енгізіледі.

Құжатты рұқсатсыз көшіруге тыйым салынады

10.5 Деректер тұтастығының бұзылуын анықтаған кезде бағдарламалық жасақтама қателерін, аппараттық ақауларды немесе пайдаланушылардың әрекеттерін қоса алғанда, мәселенің көзін анықтау үшін журналдар мен журналдарға талдау жасалады. Себебін анықтағаннан кейін деректер ең өзекті дұрыс сақтық көшірмеден қалпына келтіріледі және ақаулы инфрақұрылым сегменті оқшауланады**.**

10.6 Ақпараттық қауіпсіздік оқиғалары кезінде жұқтырған немесе бұзылған жүйелерді дереу оқшаулау орындалады. Күдікті процестер тоқтатылады, тиісті есепті жазбалар бұғатталады. Барлық жүйелер вирусқа қарсытық және EDR көмегімен тексеріледі. Деректер сақтық көшірмелерден қалпына келтіріледі, содан кейін жаңартуларды, көп факторлы аутентификацияны және желіні сегментациялауды қоса алғанда, қосымша қорғау шаралары енгізіледі.

11 Мониторинг

11.1 Мониторинг сыни сервистердің қолжетімділігін қолдауға, сәтсіздіктер мен деградацияны ерте анықтауға, инциденттерге жедел ден қоюға, резервтік көшірмелердің орындалуын бақылауға, сондай-ақ АТ-инфрақұрылымын талдау және дамыту үшін деректер жинауға бағытталған.

11.2 Виртуалды машиналардың жүктемесін, температурасын және қолжетімділігін бақылайтын серверлер мен виртуалды инфрақұрылым мониторингке жатады. Желілік жабдықтар мен байланыс арналарының күйі, соның ішінде өткізу қабілеттілігі, кідірістер және vpn жұмысы бақыланады. Деректерді сақтау жүйелері мен NAS, дискілердің күйі мен RAID және өнімділік бақыланады. Бақылау аймағына AD, DNS/DHCP, пошта жүйелері, порталдар мен дерекқорлар, ақпараттық қауіпсіздік жүйелері және сақтық көшірме процестері сияқты маңызды қызметтер кіреді.

11.3 Мониторинг үшін Zabbix жүктемені, қолжетімділікті және триггерлерді бақылау үшін, Windows Server қызметтері мен оқиғалар журналдарын бақылау құралдары, Fortinet трафикті талдау құралдары, IPS және VPN, Kaspersky Security Center, NAS/Synology кіріктірілген бақылау құралдары және журналдарды орталықтандырылған жинау үшін қолданылады.

11.4 Шамадан тыс жүктемелер, RAID істен шығуы, қызметтердің тоқтауы немесе VPN істен шығуы сияқты маңызды жағдайлар туындаған кезде автоматты хабарламалар жасалады. Ескертулер жауапты мамандарға жіберіледі. Реакцияның басталу уақыты маңызды активтер үшін 5 минутқа дейін және маңызды жүйелер үшін 30 минутқа дейін.

11.5 Күн сайын негізгі қызметтердің жай-күйі, қоймалардың толтырылуы және желілік қателердің болуы тексеріледі. Апта сайын жүктеме талдауы және ДСЖ және виртуалдандыру жұмысын бақылау жүргізіледі. Ай сайын қауіпсіздік журналдарын тексеру және сақтық көшірменің дұрыстығын талдау жүргізіледі.

Құжатты рұқсатсыз көшіруге тыйым салынады

11.6 Ай сайын сервистердің қолжетімділігі, оқиғалар саны, қалпына келтіру уақыты және жүктеме динамикасы бойынша есептер қалыптастырылады. Есептер жоспарды түзету және инфрақұрылымды жаңартуды жоспарлау үшін қолданылады.

12 Жоспарды тестілеу

12.1 Кешенді жыл сайынғы тестілеу негізгі сервистердің істен шығуын модельдеуді, резервтік серверлерге ауысуды тексеруді, деректер базасын қалпына келтіру тестін, желінің немесе ДСЖ ақауларын имитациялау кезінде сыни жүйелердің қолжетімділігін бақылауды, сондай-ақ ақпараттық қауіпсіздік инциденттерін имитациялауды және персоналдың іс-әрекеттерін бағалауды қамтиды. Файлдарды, каталогтарды, виртуалды машиналар мен дерекқорларды қалпына келтіру мүмкіндігін тексере отырып, деректерді қалпына келтіру тестілеуі тоқсан сайын жүргізіледі. Жоспардан тыс тестілеу инфрақұрылымдағы Елеулі өзгерістерден кейін, соның ішінде гипервизорды жаңарту, жаңа жабдықты енгізу немесе желілік архитектураны өзгерту арқылы жүзеге асырылады.

12.2 Барлық сынақтар пайдаланушыларға ең аз әсер ете отырып, регламенттік уақытта жүргізіледі. Нәтижелер тестілеу журналында жазылады. Сәйкессіздіктер анықталған кезде түзету шаралары 30 күнге дейінгі мерзімде орындалады. Тестілеу нәтижелері резервтік көшірменің тиімділігі мен инфрақұрылымның тұрақтылығын бағалау үшін қолданылады.

13 Келісу, бекіту және қолданысқа енгізу

13.1 Осы Жоспар қызметі АТ-активтерді пайдалануға, сүйемелдеуге және олардың қолжетімділігін қамтамасыз етуге байланысты Университеттің құрылымдық бөлімшелерінің басшыларымен келісуге жатады.

13.2 Жоспарды келісу қажет лауазымды тұлғалар мен құрылымдық бөлімшелердің тізбесін құжатты әзірлеуші оның мазмұнын, қолданылу саласын және қозғалатын активтердің сыни деңгейін ескере отырып айқындайды.

13.3 Жоспар жобасын қарау мерзімі оны алған сәттен бастап бес жұмыс күнінен аспауға тиіс. Ескертулер мен ұсыныстар дәлелді және нақты нысанда ұсынылады.

13.4 Ескертулер болмаған кезде не олар есепке алынғаннан кейін Жоспарға келісуші тұлғалар қол қояды және атқарушы органға Басқармаға бекітуге беріледі.

Құжатты рұқсатсыз көшіруге тыйым салынады

13.5 Жоспардың қолданысқа енгізілген күні оның бекітілген күні болып есептеледі. Бекітілген сәттен бастап жоспар оны орындау үшін міндетті болып табылады.

13.6 Жоспардың жаңа редакциясын бекіту немесе өзгерістер енгізу кезінде алдыңғы нұсқасы күшін жояды және жарамсыз деп есептеледі.

14 Сақтау

14.1 Бекітілген Жоспардың түпнұсқасы Университеттің Ақпараттық қауіпсіздік қызметінде сақталады.

14.2 Жоспардың электрондық нұсқасы уәкілетті құрылымдық бөлімшелер мен қызметкерлер үшін шектеулі қолжетімділікті қамтамасыз ете отырып, университеттің корпоративтік ақпараттық ресурстарында орналастырылады.

14.3 Университет қызметкерлерін осы Жоспармен таныстыру ішкі нормативтік құжаттар үшін белгіленген тәртіппен танысу парағын ресімдеумен жүзеге асырылады.

14.4 Көшірмелерді есепке алу, рұқсатсыз пайдаланудың алдын алу және бөлімшелерде Жоспардың сақталуына олардың басшылары жауапты болады.

15 Қайта қарау және өзектендіру тәртібі

15.1 Осы Жоспарды қайта қарауды Ақпараттық технологиялар департаменті Ақпараттық қауіпсіздік қызметімен бірлесіп кемінде екі жылда бір рет жүзеге асырады және оның ережелерін АТ-инфрақұрылымының ағымдағы жай-күйіне, тәуекелдер деңгейіне және ақпараттық қауіпсіздікті басқару жүйесінің талаптарына сәйкес келтіруге бағытталған.

15.2 Жоспарды жоспардан тыс өзектендіру АТ-инфрақұрылымының архитектурасы немесе сыни активтердің құрамы өзгерген кезде, Қазақстан Республикасы заңнамасының және ақпараттық қауіпсіздік және қызметтің үздіксіздігін қамтамасыз ету саласындағы нормативтік құжаттардың талаптары өзгерген кезде, жаңа ақпараттық жүйелерді енгізу немесе қолданыстағы шешімдерді елеулі жаңғырту кезінде, сондай-ақ Жоспарды тестілеу, ішкі аудиттер, оқиғаларды немесе нақты оқиғаларды талдау нәтижелері бойынша сәйкессіздіктер анықталған кезде жүргізіледі.

15.3 Осы Жоспарға өзгерістер мен толықтырулар жаңа редакция не жекелеген өкімдік құжат түрінде ресімделеді және осы Жоспарды бекіту үшін белгіленген тәртіппен бекітіледі.

Құжатты рұқсатсыз көшіруге тыйым салынады

Ф.01-2022

Келісу парағы

Лауазымы	Аты-жөні	Күні	Қолы
Басқарма мүшесі – Цифрландыру жөніндегі проректор	Амиров А.Ж.	9.12.25	
Заң қызметінің басшысы	Аязбаева Г.С.	9.12.25	
Software-орталығының басшысы	Штефан К.Б.	9.12.25	

Ф.02-2022

Танысу парағы

Лауазымы	Аты-жөні	Күні	Қолы

Құжатты рұқсатсыз көшіруге тыйым салынады