ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ
МАМАДЫШСКОГО
МУНИЦИПАЛЬНОГО РАЙОНА
РЕСПУБЛИКИ ТАТАРСТАН
ул.М.Джалиля, д.23/33, г. Мамадыш,
Республика Татарстан, 422190

ТАТАРСТАН РЕСПУБЛИКАСЫНЫҢ
МАМАДЫШ МУНИЦИПАЛЬ
РАЙОНЫНЫҢ БАШКАРМА
КОМИТЕТЫ
М.Җәлил ур, 23/33 й., Мамадыш ш.,
Татарстан Республикасы, 422190

Тел.: (85563) 3-15-00, 3-31-00, факс 3-22-21, e-mail: mamadysh.ikrayona@tatar.ru, www.mamadysh.tatarstan.ru

Постановление **Карар**

№ 273 «30» 06 2023 ел

Мамадыш муниципаль районының җирле үзидарә органнарында файдаланыла торган программа, программа-аппарат чараларының куркынычсызлык дәрәҗәсен бәяләү регламентын раслау турында

Татарстан Республикасы Мамадыш муниципаль районы җирле үзидарә органнарында файдаланыла торган мәгълүмати системалардагы критик җитешсезлекләрне ачыклау, анализлау һәм бетерү буенча эшчәнлекне оештыру максатларында, Россия Федерациясенең техник һәм экспорт контроле буенча федераль хезмәте методик документлары нигезендә Татарстан Республикасы Мамадыш муниципаль районы Башкарма комитеты КАРАР БИРӘ:

1. Мамадыш муниципаль районының җирле үзидарә органнарында файдаланыла торган программа, программа-аппарат чараларының куркынычсызлык дәрәҗәсен бәяләү регламентын расларга (1 нче кушымта).

2. Әлеге карарны Татарстан Республикасы хокукый мәгълүматының рәсми порталында http://mamadysh.tatarstan.ru// адресы буенча һәм Мамадыш муниципаль районының рәсми сайтында бастырып чыгарырга.

3. Әлеге карарның үтәлешен контрольдә тотуны үз җаваплылыгымда калдырам.

Җитәкче вазифаларын башкаручы А.Х.Әгъләмов

0000011865

Татарстан Республикасы Мамадыш муниципаль районы Башкарма комитетының 30 06 2023 ел, № 273 карарына
1 нче кушымта

Мамадыш муниципаль районының җирле үзидарә органнарында файдаланыла торган программа, программа-аппарат чараларының куркынычсызлык дәрәҗәсен бәяләү регламенты

ЭЧТӘЛЕК

1. Гомуми нигезләмәләр 3
2. Программа, программа - аппарат чараларының куркынычсызлык дәрәҗәсен бәяләү тәртибе 4
3. Җитешсезлекләрне бетерүгә юнәлдерелгән мәгълүматны саклау буенча чаралар кабул итү 10

1. Гомуми нигезләмәләр

1.1. Программа, программа-аппарат чараларының куркынычсызлык дәрәҗәсен бәяләүнең әлеге методикасы (алга таба – Методика) Россия Федерациясе Президентының 2004 елның 16 августындагы 1085 номерлы Указы белән расланган техник һәм экспорт контроле буенча Федераль хезмәт турында нигезләмәнең 8 пунктының 4 пунктчасы нигезендә эшләнгән.

1.2. Методика мәгълүмати системаларның, мәгълүмати-телекоммуникация челтәрләренең программа, программа-аппарат чараларында, идарәнең автоматлаштырылган системаларында, шул исәптән мәгълүматларны эшкәртү үзәкләренең мәгълүмати-телекоммуникация инфраструктурасы базасында эшли торган (алга таба - мәгълүмат системалары) ачыкланган җитешсезлек дәрәҗәсен бәяләү тәртибен билгели.

1.3. Әлеге методика программа системаларының зәгыйфьлекләрен бетерү чараларын, программа-аппарат чараларының, шулай ук Россия ФСТЭК ның башка норматив хокукый актлары һәм методик документлары нигезендә дәүләт мәгълүмат системаларында булган мәгълүматны, Россия Федерациясенең мөһим мәгълүмати инфраструктурасы объектларының куркынычсызлыгын тәэмин итү таләпләрен кабул иткәндә мәгълүмат системаларының операторлары тарафыннан мәгълүматны яклау турында таләпләр нигезендә кулланылырга тиеш.

1.4. Сертификацияләнгән программа, программа-аппарат мәгълүматны яклау чараларында йомшак якларны бетерү өстенлекле тәртиптә тәэмин ителә һәм аларда эксплуатацион документация нигезендә, шулай ук әзерләүче рекомендацияләре белән гамәлгә ашырыла.

1.5. Регламентта «Мәгълүматны яклау. Төп терминнар һәм билгеләмәләр» ГОСТ Р 50922-2006, «Мәгълүматны яклау. Мәгълүмати системаларның җитешсезлекләре. Җитешсезлекләрне тасвирлау кагыйдәләре» ГОСТ Р 56545-2015, «Мәгълүматны яклау» Мәгълүмати системаларның җитешсезлекләре. Мәгълүмати системаларның җитешсезлекләрен классификацияләү» ГОСТ Р 56546-2015 мәгълүматны яклау һәм мәгълүмати иминлекне тәэмин итү өлкәсендә башка илкүләм стандартлар билгеләнгән терминнар һәм билгеләмәләре кулланыла.

ПРОГРАММА, ПРОГРАММА-АППАРАТ ЧАРАЛАРЫНЫҢ КУРКЫНЫЧСЫЗЛЫК ДӘРӘҖӘСЕН БӘЯЛӘҮ ТӘРТИБЕ

2.1. Куркынычларның критик дәрәҗәсе мәгълүмат системаларында җитешсезлекләрне анализлау нәтиҗәләре буенча программа, программа-аппарат чараларында ачыкланган җитешсезлеләрне бетерү кирәклеге турында мәгълүмат системаларының нигезле чишелешен кабул итү максатларында бәяләнә.

2.2. Куркыныч янауларның критиклыгын билгеләү өчен башлангыч мәгълүматлар булып түбәндәгеләр тора:

а) Россиянең ФСТЭК мәгълүмат иминлегенә куркыныч янаулар мәгълүматлары банкында булган программа тәэминаты, программа-аппарат чаралары куркынычсызлыгы базасы (bdu.fstec.ru), шулай ук билгеле куркынычлыклар турында мәгълүматлар булган башка чыганаклар;

б) мәгълүмати иминлек өлкәсендә программа белән тәэмин итүне, программа-аппарат чараларын һәм тикшеренүчеләрне эшләүчеләрнең рәсми мәгълүмат ресурслары;

в) инвентаризация нәтиҗәләре буенча алынган һәм (яисә) мәгълүмати системаларга документларда китерелгән мәгълүмати системаларның составы һәм архитектурасы турында белешмәләр;

г) оператор үткәргән мәгълүмат системаларының сакланышын тикшереп тору нәтиҗәләре.

Югарыда күрсәтелгән мәгълүматлар информацион системалар эшли торган эшчәнлек өлкәсендәге үзенчәлекләрне исәпкә алып аныкланырга яисә тулыландырырга мөмкин.

2.3. Программа, программа - аппарат чараларының куркынычсызлык дәрәҗәсен мәгълүматны саклау (мәгълүмати куркынычсызлык) буенча белгечләр бәяли.

2.4. Программа, программа - аппарат чараларының конкрет мәгълүмат системасына карата куркынычсызлык дәрәҗәсен бәяләү үз эченә ала:

1) куркынычлыкларга дучар булган программа, программа-аппарат чараларын билгеләү;

2) мәгълүмат системасында куркынычлыкларга дучар булган программа, программа-аппарат чараларын урнаштыру урынын билгеләү (мәсәлән, Система периметрында, системаның эчке сегментында, критик процессларны (бизнес-процессларны) һәм мәгълүмат системасының башка сегментларында);

1) мәгълүмат системасында программа, программа - аппарат чараларының куркынычсызлыгы дәрәҗәсен исәпләү (V).

Программа, программа - аппарат чараларының мәгълүмат системасындагы куркынычсызлык дәрәҗәсен исәпләү түбәндәге формула буенча башкарыла:

$$V = I_{cvss} \times I_{infr},$$

монда I_{cvss} – куркынычлылык дәрәҗәсен билгеләүче күрсәткеч;

I_{infr} – программа, программа-аппарат чараларының мәгълүмат системасы эшчәнлегенә йогынтысын характерлаучы күрсәткеч.

I_{cvss} күрсәткече common Vulnerability scoring system (Cvss) 3.0 яки 3.11.3.11 методикасы буенча конкрет мәгълүмат системасына карата база, вакыт һәм контекст метрикаларын исәпләү юлы белән билгеләнә.

Төп метрикалар мәгълүматның ачыклыгына, бөтенлегенә һәм конфиденциальлегенә тәэсир итүче, вакыт үтү белән үзгәрми торган һәм программа, программа-аппарат чараларының эшчәнлек мохитенә бәйле булмаган төп куркынычлык характеристикаларын чагылдыра. Төп метрикалар һөҗүм векторын, һөҗүмнең катлаулылыгын, өстенлекләр дәрәҗәсен, кулланучы белән аралашуны, конфиденциальлеккә, бөтенлеккә һәм ирешүчәнлеккә йогынты ясауны характерлаучы күрсәткечләрне үз эченә ала.

Вакыт метрикалары вакыт узу белән үзгәрә торган, әмма программа, программа-аппарат чараларының эшчәнлек мохитенә бәйле булмаган куркынычлык характеристикаларын чагылдыра. Вакытлы метрикалар эксплуатация чараларының, бетерү чараларының, куркынычсызлык турында мәгълүматка ышаныч дәрәҗәсен характерлаучы күрсәткечләрне үз эченә ала.

Контекст метрикалары программа, программа-аппарат чараларының эшчәнлек мохитенә бәйле булган куркынычлык характеристикаларын чагылдыра.

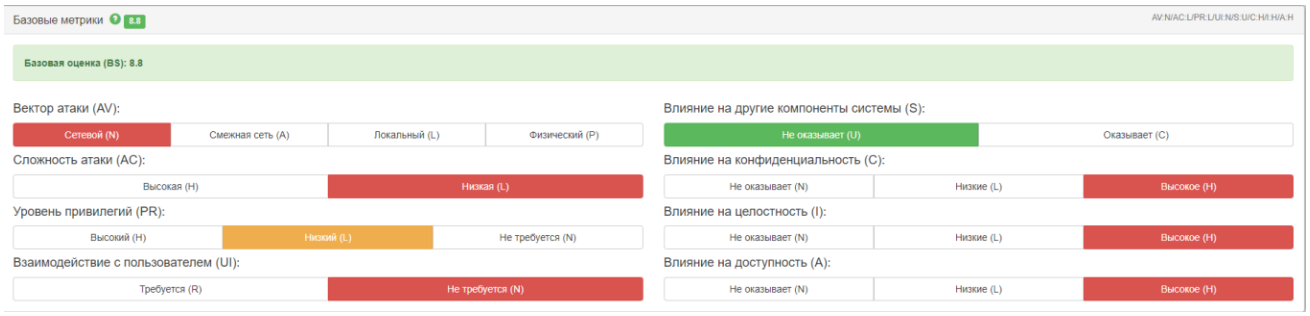
I_{cvss} күрсәткече Россиянең ФСТЭК мәгълүмат иминлегенә куркыныч янаулар банкында булган калькуляторны кулланып исәпләнә ала[2].

Калькуляторда конкрет система һәм челтәргә карата база, вакыт һәм контекст метрикаларын билгеләргә (дөресләргә) кирәк (рәсемнәр 1, 2, 3).

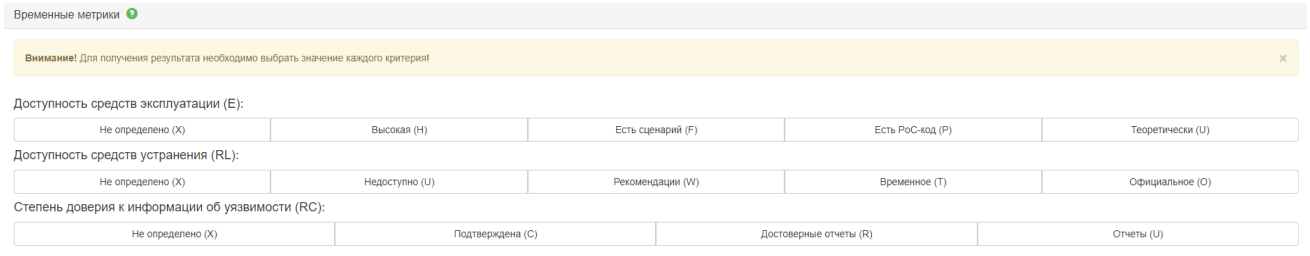
---

[1] https://www.first.org/cvss.

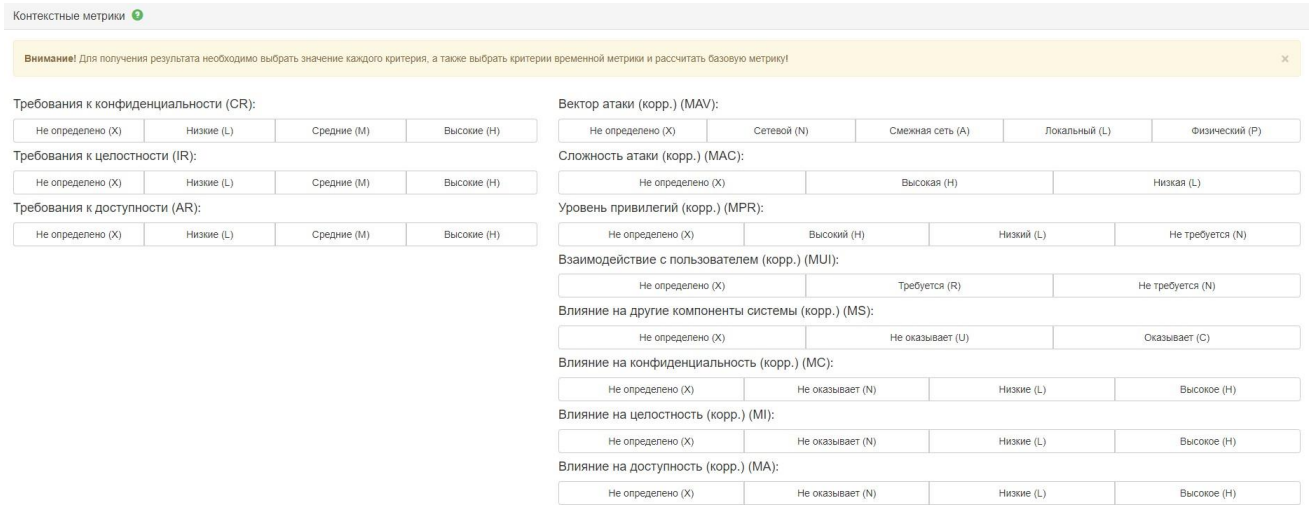
[2] https://bdu.fstec.ru/calc3, https://bdu.fstec.ru/calc31.



1 нче рәсем – Төп метрик җитешсезлекләрне исәпләү

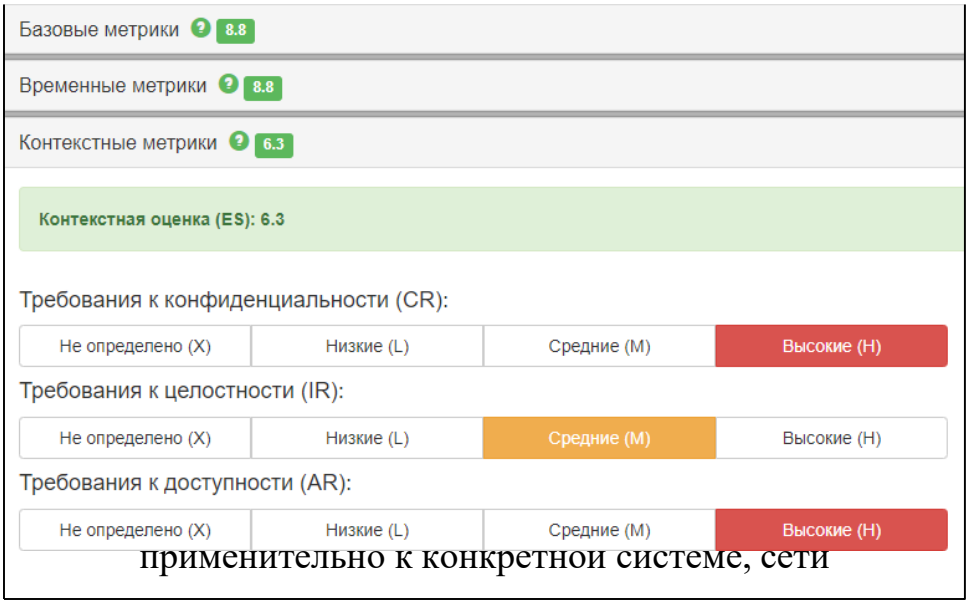


2 нче рәсем – җитешсезлекләрнең вакытлыча метригын исәпләү



3 нче рәсем – җитешсезлекләрнең контекст метрикасын исәпләү

Оператор тарафыннан калькуляторда төрле метрикалар бирелгәндә конкрет мәгълүмат системасына карата куркынычлык дәрәҗәсе автомат рәвештә исәпләнә һәм "контекст метрикалары" кырында күрсәтелә (4 нче рәсем).



применительно к конкретной системе, сети

I_{cvss} йомгаклау күрсәткече конкрет мәгълүмат системасына карата база, вакытлы һәм контекстлы метрик күрсәткечләренең җыелмасы белән билгеләнә.

2.4. I_{infr} күрсәткече түбәндәге формула буенча билгеләнә:

$$I_{infr} = k * K + l * L + p * P,$$ монда

K – куркынычка дучар булган мәгълүмати система компонентының тибын тасвирлаучы күрсәткеч;

L – мәгълүмат системасының куркынычлылык компонентлары (автоматлаштырылган эш урыннары, серверлар, телекоммуникация җиһазлары, мәгълүматны яклау чаралары һәм башка компонентлар) санын характерлаучы күрсәткеч;

P – зыянлы компонентның мәгълүмат системасы периметрының саклануына йогынтысын характерлаучы күрсәткеч;

k, l, p – күрсәткечләрнең үлчәү коэффициентлары.

Программа, программа-аппарат чараларының мәгълүмат системасына куркынычсызлыгын билгеләүче күрсәткечләрнең үлчәү коэффициентларын һәм бәяләрен исәпләү 1 нче таблицага ярашлы рәвештә үткәрелә.

Таблица 1

№ п/п	**күрсәткеч**	**Үлчәү**	**әһәмияте**	**бәяләү**	**нәтиҗә** ($k * Ki$, $l * Lj$, $p * Pm$)
1	Куркыныч янауга	0,4	Куркыныч янауга дучар булган	1	0,4

№ п/п	Показатель	Вес	Значение	Оценка	Итог ($k * Ki$, $l * Lj$, $p * Pm$)
	дучар булган мәгълүмати система компоненты тибы (К)		Критик процессларын (бизнес-процессларны), функцияләрне, вәкаләтләрне гамәлгә ашыруны тәэмин итүче мәгълүмат системасы компонентлары		
			Куркычка дучар булган серверлар	0,8	0,32
			куркыныч янауга дучар булган телекоммуникация җиһазлары, мәгълүмат тапшыру челтәрен идарә итү системасы	0,8	0,32
			куркыныч янауга дучар булган автоматлаштырылган эш урыннары	0,5	0,20
			куркыныч янауга дучар булган башка компонентлар	0,5	0,20
2	куркыныч янауга дучар булган телекоммуникация җиһазлары, мәгълүмат тапшыру	0,2	70% артык компонентларның гомуми санының компонентлары мәгълүмат системасында	1	0,2

	челтәрен идарә итү системасы, (автоматлаштырылган эш урыннары, телекоммуникация җиһазлары, мәгълүмат тапшыру челтәрен идарә итү системасы серверлары)		50-70% компонентларның гомуми санының компонентлары мәгълүмат системасында	0,8	0,16

№ п/п	күрсәткеч	Вес	әһәмияте	бәя	нәтиҗә ($k * Ki$, $l * Lj$, $p * Pm$)
	һәм башка компонентлар) (L)		мәгълүмат системасында компонентларның гомуми санының 10-50% компонентлары	0,6	0,12
			компонентлары мәгълүмат системасында компонентларның гомуми санының 10 % кимрәк	0,5	0,10
3	Система, челтәр периметрын саклауның нәтиҗәлелегенә йогынтысы (Р)	0,4	Интернет челтәреннән кулланыла торган куркыныч яный торган программа, программа-аппарат чарасы	1	0,4
			Интернет челтәреннән кулланылмый торган куркыныч яный торган программа, программа-аппарат чарасы	0,5	0,2

2.5. Хисап нәтиҗәләре буенча, конкрет мәгълүмат системасына карата куркынычлыкның критик дәрәҗәсе 2 нче таблицада күрсәтелгән кыйммәтләрне кабул итә.

Таблица 2

№ п/п	Куркынычсызлык балларының гомуми саны	Җитешсезлекләрнең критик дәрәҗәсен бәяләү
1	$7,0 \leq V \leq 10,0$	Критик
2	$4,5 \leq V < 7,0$	югары
3	$1,5 \leq V < 4,5$	уртача
4	$V < 1,5$	түбән

2. КУРКЫНЫЧ ЯНАУЛАРНЫ БЕТЕРҮГӘ ЮНӘЛДЕРЕЛГӘН МӘГЪЛҮМАТНЫ САКЛАУ ЧАРАЛАРЫН КҮРҮ

3.1. Программа, программа-аппарат чараларының куркынычсызлык дәрәҗәсенә бәйле рәвештә, конкрет мәгълүмат системасында оператор аларны бетерү кирәклеге турында Карар кабул итә.

3.2. Әлеге методикага ярашлы рәвештә критик дәрәҗә бирелгән программа, программа-аппарат чараларының куркынычсызлыгына карата аларны сәгатьләр дәвамында (24 сәгатькә кадәр) бетерү буенча чаралар күрергә киңәш ителә.

Әлеге методикага ярашлы рәвештә югары дәрәҗәдәге критиклык бирелгән программа, программа-аппарат чараларының куркынычсызлыгына карата аларны көн дәвамында (7 көнгә кадәр) бетерү буенча чаралар күрергә киңәш ителә.

Әлеге методикага ярашлы рәвештә уртача критиклык дәрәҗәсе бирелгән программа, программа-аппарат чараларының куркынычсызлыгына карата аларны бетерү буенча атналар дәвамында (4 атнага кадәр) чаралар күрергә киңәш ителә.

3.3.Программа, программа-аппарат чараларының куркынычсызлыгын программа тәэминатын яңарту, программа - аппарат чарасын урнаштыру яки мәгълүматны саклауның компенсацияләү оештыру һәм техник чараларын кабул итү юлы белән бетерү мөмкин.

3.4. Әгәр дә куркынычлыклар чит ил программа, программа-аппарат чараларында яки ачык чыганаклы программа тәэминатында булса, мондый программа тәэминаты, программа-аппарат чарасын яңартуны урнаштыру турында карар мәгълүмат системасы операторы тарафыннан программа, программа-аппарат чараларының куркынычсызлык яңартуларын сынау методикасына ярашлы рәвештә үткәрелә.

3.5. Программа, программа-аппарат чараларының яңартуларын алу, урнаштыру һәм сынау мөмкин булмаган очракта, мәгълүматны саклауның компенсация чаралары күрелә.

3.6. Мәгълүматны саклау буенча компенсация чараларын сайлау Оператор тарафыннан мәгълүмат системасының архитектурасын һәм үзенчәлекләрен, шулай ук программа, программа-аппарат чараларының куркынычсызлыгын эксплуатацияләү ысулларын исәпкә алып башкарыла.

Куркынычлыкларны эксплуатацияләү мөмкинлеген булдырмауга юнәлдерелгән компенсацияләү оештыру һәм техник чаралар булып түбәндәгеләр тора:

мәгълүмат системасының зәгыйфь компонентлары конфигурациясен үзгәртү, шул исәптән аларның функцияләренә керү ягыннан, аларның үтәлеше ачыкланган зәгыйфьлекләрне эксплуатацияләүгә ярдәм итә ала;

зәгыйфь программа, программа - аппарат чараларын куллану буенча чикләү яки аларны функцияләр режимына күчерү, аларга мөрәҗәгать итү ачыкланган зәгыйфьлекләрне куллану белән бәйле функцияләрне үтәүне чикләү (мәсәлән, зәгыйфь хезмәтләрне һәм челтәр протоколларын сүндерү);

мәгълүмат системасы компонентларын резервлау, шул исәптән серверларны, телекоммуникация җиһазларын һәм элемтә каналларын резервлау;

мәгълүмат системасында куркынычсызлык билгеләрен ачыклауны тәэмин итүче мәгълүматны саклау чаралары кагыйдәләрен хәл итүче имзаларны куллану;

мәгълүмати куркынычсызлык мониторингы һәм мәгълүмат системасында куркынычсызлык вакыйгаларын ачыклау.