



Община Джебел , област Кърджали

ул. "Еделвайс" № 19, тел.: +3593632/20-51, e-mail: kmet_dj@abv.bg

ЗАПОВЕД

№ 1919
Град Джебел 31.12.2020 година

На основание чл. 44, ал. 2 от ЗМСМА и чл. 7, ал. 1-4 от Наредбата за минималните изисквания за мрежова и информационна сигурност

УТВЪРЖДАВАМ:

Методика за анализ и оценка на риска за сигурността на информационните и комуникационните системи на Община Джебел.

Настоящата заповед да се публикува на сайта на община Джебел, ведно с Методика за анализ и оценка на риска за сигурността на информационните и комуникационните системи на Община Джебел..

Контрол по изпълнението възлагам на Хайрие Мехмед – Секретар на община Джебел.

НЕДЖМИ АЛИ
КМЕТ НА ОБЩИНА ДЖЕБЕЛ



/ХМ



Община Джебел , област Кърджали

ул. "Еделвайс" № 19, тел.: +3593632/20-51, e-mail: kmet dj@abv.bg

Методика за анализ и оценка на риска за сигурността на информационните и комуникационните системи на Община Джебел

Версия:	01
Дата:	31.12.2020 г.
Одобрена от:	Неджми Али Кмет на община Джебел
Класификация:	

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Настоящата методика е разработена на основание чл.7, ал.1-4 от „НАРЕДБА за минималните изисквания за мрежова и информационна сигурност“ и е утвърдена със заповед № 1919 от 31.12.2020 г. на Кмета на община Джебел.

Чл. 2. По своята същност управлението на риска представлява съвкупност от процеси за идентифициране на потенциалните заплахи към носителите на информация и активите, участващи в предоставянето на електронни услуги, анализ и оценка на рисковете, породени от тези заплахи.

Чл. 3. Целта на процеса за управление на риска е да се минимизират загубите от потенциални нежелани събития, настъпили в резултат от реализиране на заплахи към сигурността на мрежите и информационните системи, които биха засегнали конфиденциалността, интегритета и достъпността на информацията, създавана, обработвана, предавана и унищожавана чрез тях.

Чл. 4. Методиката има за цел да даде общ подход при анализа и оценката на риска за сигурността на информационните и комуникационните системи, предоставяни от различните администрации, с цел получаване на съизмерими, относително обективни и повтарящи се резултати чрез:

- регламентиране на дейностите и тяхната последователност при анализа и оценката на риска за електронните услуги;
- определяне на критериите;
- определяне на приоритетите на риска.

II. ТЕРМИНИ И ДЕФИНИЦИИ

Чл. 5. При изготвяне на анализ и оценка на риска за сигурността на информационните и комуникационните системи на Община Джебел, използваните термини имат следното значение:

- **Информационна сигурност** – запазване на цялостност, наличност и поверителност;
- **Цялостност** – информацията и активите да са цели, пълни и с вярно съдържание;
- **Наличност** – информацията и активите да са достъпни и използвани;
- **Поверителност** – предоставяне на информация и активи само на оторизирани служители и лица;
- **Риск** – ефект на неопределеност. Възможността дадена заплаха да използва дадена уязвимост на актив и по този начин да причини вреда на организацията
- **Остатъчен риск** - рискът, който остава след въздействието върху първоначално оценения риск

- **Заплаха** – потенциална причина за нежелан инцидент, който може да навреди на система или организация
- **Вероятност** – възможността дадена заплаха да се осъществи
- **Третиране на риска** – третиране на въздействие, уязвимост, вероятност
- **Третиране на степента на заплаха / въздействие** – внедряване на мерки и контроли за намаляване на ефекта от заплахата върху актива (при реализирана заплаха);
- **Третиране на вероятността** - внедряване на мерки и контроли, които оказват влияние върху външната(околната) среда на актива;
- **Информационен актив** – информация свързана с дейността на организацията, носителите на тази информация, средствата за обработка на информацията, физическото място в което се обработва и съхранява;
- **Отговорник на актива** – служител, който работи с него, съхранява или му е зачислен персонално;
- **Собственик на риска** – служител, който взема решения за управлението и приемането на риска;
- **Собственик на процес** – служител който отговаря за бизнес процес;

III. ИДЕНТИФИКАЦИЯ НА ЗАПЛАХИТЕ

Чл. 6. Вземайки под внимание външните и вътрешни фактори, които биха повлияли на дейността на Общинската администрация, всеки началник на отдел определя и описва потенциалните заплахи свързани с информационната сигурност в отделен прозорец на Риск-регистъра (електронна таблица).

Чл. 7. Поддържа се списък с примерни заплахи в Риск-регистъра (**Приложение 1**)

Чл. 8. Всеки началник на отдел е собственик на риска свързан с дейностите в неговото структурно звено и използваните от него активи.

Чл. 9. Собствениците на рискове описват в Риск-регистъра всички приложени мерки за защита имащи отношение към съответните заплахи.

IV. ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО

Чл. 10. Собственикът на риска определя въздействието по скалата и документира оценката в Риск-регистъра.

Стойност	Материални и нематериални щети, които заплахата ще причини, ако се реализира
5	Катастрофални щети свързани с репутация, финанси и отпадане на всички услуги

4	Големи щети свързани с репутация, финанси и отпадане на голяма част от услугите
3	Значителни щети свързани с финанси и отпадане на част от услугите
2	Малки щети свързани с финанси и затруднено използване на услугите
1	Незначителни щети свързани със затруднено използване на услугите

V. ОЦЕНКА НА ВЕРОЯТНОСТТА

Чл.11. Собственикът на риска определя вероятността по скалата и документира оценката в Риск-регистъра.

Стойност	Честота
5	Реализирането на заплахата в рамките на 1 година е над 70%
4	Реализирането на заплахата в рамките на 1 година е от 50% до 70%
3	Реализирането на заплахата в рамките на 1 година е от 30% до 50%
2	Реализирането на заплахата в рамките на 1 година е от 10% до 30%
1	Реализирането на заплахата в рамките на 1 година е под 10%

VI. ОЦЕНКА НА РИСКА. ПРИОРИТЕТ.

Чл. 12. Собствениците на рискове оценяват риска в Риск-регистъра по формулата:

Риск = Въздействие x Вероятност.

Чл. 13. След оценката на риска приоритизирането на риска се разделя на три нива, като приемливото ниво е до 6.

ПРИОРИТЕТИ	ВЕРОЯТНОСТ				
ВЪЗДЕЙСТВИЕ	1	2	3	4	5
	2	4	6	8	10
	3	6	9	12	15
	4	8	12	16	20
	5	10	15	20	25

- Рисковете в диапазона 1 - 6 се определят като приемливи, с **ПРИОРИТЕТ 3** и не се изисква да се предприемат мерки за намаляване на риска.
- Рисковете в диапазона 8 – 12 се определят с **ПРИОРИТЕТ 2** и се прави анализ на възможните мерки, които биха могли да се предприемат за смекчаването им, и се преценява дали разходът на ресурси за прилагането им е пропорционален на

щетите от реализиране на заплахата. В случай че щетите са повече от разходите, се определят отговорно лице и срок за прилагане на тези мерки.

- Рисковете в диапазона 15 – 25 се приемат с **ПРИОРИТЕТ 1** и затова незабавно се планират мерки, които биха намалили риска от реализиране на конкретната заплаха, и се определят отговорници и срокове за прилагането им.

VII. НАМАЛЯВАНЕ НА РИСКА

Чл. 14. Рисковете с Приоритет 1 и по преценка с Приоритет 2 се включват в Рискрегистъра, където собствениците на рисковете планират нови мерки за намаляване на риска, определят съответните ресурси и срокове за внедряване им, след което оценяват остатъчния риск по гореописаната формула, отчитайки на кой от двата компонента (вероятност и въздействие) ще повлияе за намаляване.

Чл. 15. Остатъчните рискове се приемат от Кмета на Общинската администрация, като становището се документира със заповед.

Приложение №1

Към Методика за анализ и оценка на риска за мрежовата и информационна сигурност, на община Джебел

Заповед № 1919 31.12.2020 год.

№ по ред	Информационен актив	Заплаха/нежелани събития	Приложени мерки за защита	Оценка на въздействието (от 1 до 5)	Оценка на вероятността (от 1 до 5)	Оценка на риска Приоритет на риска (от 1 до 3)	Планирани мерки за смекчаване на риска (за приоритет 3 и 2)	Необходими ресурси	Отговорник за прилагане на планираните мерки	Срок за прилагане на планираните мерки

ВЕРОЯТНИ ЗАПЛАХИ

- Влошаване на средствата за съхраняване
- Грешки при техническото обслужване
- Грешки при предаването
- Електромагнитна радиация
- Зловреден програмен код
- Злоупотреба с ресурси
- Използване на неразрешени програми и данни
- Кражба маскиране на потребителска идентификация (нелегално проникване)

- Неоторизиран достъп до компютри, данни, услуги и приложения
- Неоторизиран достъп до средствата за съхраняване
- Неправилна (погрешна) маршрутизация/ пренасочване на съобщения
- Отричане (доказуемост)
- Повреда на комуникационното оборудване и услугите
- Подслушване
- Пожар, наводнение
- Потребителска грешка
- Администраторска грешка
- Прекъсване/повреда на захранването (електричество и климатизация)
- Претоварване на трафика
- Природни бедствия
- Кибератака
- Софтуерни проблеми
- Техническа повреда (мрежа, системен хардуер)