ОБЩИНА БАНИТЕ, ОБЛАСТ СМОЛЯН

ОБЩИНСКА АДМИНИСТРАЦИЯ

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

Версия:	01
Дата:	11.08.2020 г.
Одобрена от:	Милен Белчев – Кмет на община Баните
Класификация:	

I ОБЩИ ПОЛОЖЕНИЯ

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 № РД-234 от 11.08.2020г. на Кмета на община Баните.

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.

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.

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

- **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 използваеми;
- **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

1. 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).
2. Поддържа се списък с примерни заплахи в Риск-регистъра.

I. СОБСТВЕНИК НА РИСКА

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

II. ПРИЛОЖЕНИ МЕРКИ ЗА ЗАЩИТА

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

III. ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО

5. 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

IV. ОЦЕНКА НА ВЕРОЯТНОСТТА

6. 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%

V. ОЦЕНКА НА РИСКА. ПРИОРИТЕТ.

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

   Риск = Въздействие x Вероятност.

8. 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.

VI. НАМАЛЯВАНЕ НА РИСКА

9. Рисковете с Приоритет 1 и по преценка с Приоритет 2 се включват в Риск-регистъра, 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.
10. Остатъчните рискове се приемат от Кмета на Общинската администрация, като становището се документира със заповед.