

**ПРИМЕР !**

**ШАБЛОНИ  
ЗА  
ОЦЕНКА НА РИСКА КЪМ ИНФОРМАЦИОННИТЕ АКТИВИ**  
(Приложение към документ на СУУ – Метод за оценка на риска)

Разработените примерни шаблони са предназначени да подпомогнат дейностите:

- за оценка на риска към информационните активи от обхвата на СУУ;
- за определянето на тези заплахи (и съответните рискове за тяхната реализация), които влияят на **непрекъснатостта и наличността на съответната услуга** (в последствие се описва в документ на СУУ - **РИСКОВЕ КЪМ НЕПРЕКЪСНАТОСТТА И НАЛИЧНОСТТА НА УСЛУГА**)

Примерните шаблони са разработени в съответствие с процесите, описани в разработената **Методика за оценка на риска**.

**Шаблон № 1 “Оценка на риска за информационен актив”**

1. **Тип на информационния актив:** (напр. **хардуер** – от обхвата на СУУ, за една или повече услуги, подлежащи на управление).

2. **Описание на информационния актив:** (напр. **компютри** за развойна дейност - от обхвата на СУУ, за една или повече услуги)

3. **Идентификационен № на актива:** (съгласно поставения му идентификационен №, като информационен актив от обхвата на СУУ, в услуга, подлежаща на управление)

4. **Идентифицирани заплахи/уязвимости към/на информационния актив**

| № | Описание на заплахата | Описание на уязвимостта | Източник на заплахата | Мотивация на източника на заплахата* | Действия на източника на заплахата, за нейната реализация* |
|---|-----------------------|-------------------------|-----------------------|--------------------------------------|--|
| 1 |                       |                         |                       |                                      |  |
| 2 |                       |                         |                       |                                      |  |
| 3 |                       |                         |                       |                                      |  |
|   |                       |                         |                       |                                      |  |
| N |                       |                         |                       |                                      |  |

**\* Отнася се само за заплахи, чиито източник са хората**

***Забележка: На практика тази таблица се отнася за един или група активи от един и същи тип, от една или повече услуги и имащи общи уязвимости и съответно заплахи към тях. Всички следващи таблици се отнасят за същия актив / група активи от един тип, определени в т.1 – „Тип на информационния актив” и т.2 „Описание на информационния актив”.***

***Типовете на информационния актив могат да бъдат такива, каквито са описани в обхвата на СУУ – напр. хардуер, софтуер, персонал и т.н.***

### 5. Определяне на вероятността за реализация на идентифицирана заплата

| № | Описание на заплата (1) | Ниво на вероятност за реализация на заплата (2) | Коефициент на вероятността (3) | Времени период на вероятността (4) |
|---|-------------------------|---|--------------------------------|------------------------------------|
| 1 |                         |   |                                |                                    |
| 2 |                         |   |                                |                                    |
| 3 |                         |   |                                |                                    |
|   |                         |   |                                |                                    |
| N |                         |   |                                |                                    |

#### Забележки:

- (1) Както описанието в т. 4 от този шаблон;
- (2) Въвежда се качествена оценка - **високо, средно, ниско ниво**;
- (3) Въвежда се коефициент, съответен на качествената оценка – **1(за високо ниво), 0.5 (за средно ниво), 0.1 (за ниско ниво)**
- (4) Въвежда се времеви период, за който е отчетено нивото на вероятност за реализация на заплата – напр. 1 год.

**6. Определяне на неблагоприятното влияние при успешна реализация на заплаха чрез дадена уязвимост**

| № | Описание на заплаха<br>(1) | Описание на уязвимостта<br>(2) | Загуба на<br>конфиденц.<br>(3) | Загуба на<br>наличност<br>(3) | Загуба на<br>цялостност<br>(3) | Размер на<br>влиянието<br>(4) | Коефициент на<br>влиянието<br>(5) |
|---|----------------------------|--------------------------------|--------------------------------|-------------------------------|--------------------------------|-------------------------------|-----------------------------------|
| 1 |                            |                                |                                |                               |                                |                               |                                   |
| 3 |                            |                                |                                |                               |                                |                               |                                   |
| 3 |                            |                                |                                |                               |                                |                               |                                   |
|   |                            |                                |                                |                               |                                |                               |                                   |
|   |                            |                                |                                |                               |                                |                               |                                   |
| N |                            |                                |                                |                               |                                |                               |                                   |

**Забележки:**

- (1) Както описанието в т. 4 от този шаблон;
- (2) Както описанието в т. 4 от този шаблон;
- (3) Отбелязва се каква загуба (загуби) произтича за **информационния актив** – **да/не** за съответния тип загуба;
- (4) Въвежда се качествена оценка - **висок, среден, нисък** размер на влиянието;
- (5) Въвежда се коефициент, съответен на качествената оценка – **100 (за висок размер), 50 (за среден размер), 10 (за нисък размер)**

## 7. Определяне на нивата на риск към информационния актив

| № | Описание на заплахата<br>(1) | Описание на уязвимостта<br>(1) | Коефициент на вероятността на заплахата<br>(2) | Коефициент на влиянието<br>(3) | Коефициент на нивото на риск<br>(4) | Ниво на риска<br>(5) |
|---|------------------------------|--------------------------------|--|--------------------------------|-------------------------------------|----------------------|
| 1 |                              |                                |  |                                |                                     |                      |
| 2 |                              |                                |  |                                |                                     |                      |
| 3 |                              |                                |  |                                |                                     |                      |
|   |                              |                                |  |                                |                                     |                      |
|   |                              |                                |  |                                |                                     |                      |
| N |                              |                                |  |                                |                                     |                      |

### Забележки:

- (1) Както описанието в т. 4 от този шаблон;
- (2) Както е определено в т. 5 от този шаблон;
- (3) Както е определено в т. 6 от този шаблон;
- (4) Определя се чрез **умножаване на коефициентите за вероятност и влияние на заплахата**;
- (5) Въвежда се качествена оценка, в съответствие с получения коефициент на нивото на риска – **голям (от 50 до 100), среден (от 10 до 50) и малък (от 1 до 10)**

Получените стойности за нива на риска към информационния актив, за всяка двойка “заплаха – уязвимост” могат да се разпространят и за други активи (предварително дефинирани групи от информационни активи) от **същия тип**, имащи:

1. Еднаква или много близка степен на важност;
2. Еднакво или много близко по характеристики физическо обкръжение;
3. Еднакво или в непосредствена близост местоположение
4. Еднакви или много близки по функции и предназначение изградени защитни механизми.

За всеки информационен актив от обхвата на СУУ, който не може да бъде групиран по избраните общи признаци, всички стъпки (от 1 до 7) се изпълняват индивидуално.

**Шаблон № 2 “Регистър на идентифицираните рискове към информационните активи ”**

Обобщено представяне на нивата на риска към информационните активи от обхвата на СУУ – извършва се на база извършените оценки на отделните активи (групи от активи), съгласно стъпките по Шаблон № 1 “Оценка на риска за информационен актив”

| №    | Информационен актив - идентификационен № / описание | Заплаха | Уязвимост | Последствия – загуба на :<br>(1) | Вероятност на заплахата (коефициент) | Размер на влиянието (коефициент) | Ниво на риск (коефициент) |
|------|---|---------|-----------|----------------------------------|--------------------------------------|----------------------------------|---------------------------|
| 1    |   | 1.      | 1.        | 1.                               | 1.                                   | 1.                               | 1.                        |
|      |   | 2.      | 2.        | 2.                               | 2.                                   | 2.                               | 2.                        |
|      |   | M.      | M.        | M.                               | M.                                   | M.                               | M.                        |
| 2    |   | 1.      | 1.        | 1.                               | 1.                                   | 1.                               | 1.                        |
|      |   | 2.      | 2.        | 2.                               | 2.                                   | 2.                               | 2.                        |
|      |   | N.      | N.        | N.                               | N.                                   | N.                               | N.                        |
| .... |   |         |           |                                  |                                      |                                  |                           |
| .... |   |         |           |                                  |                                      |                                  |                           |
| .... |   |         |           |                                  |                                      |                                  |                           |
| .... |   |         |           |                                  |                                      |                                  |                           |

**Забележки:**

- (1) Въвежда се съгласно идентифицираните загуби в т. 6, Шаблон №1 – “**К**” за конфиденциалност, “**Н**” за наличност, “**Ц**” за цялостност;
- (2) В Регистъра трябва да фигурират всички активи от обхвата на СУУ, независимо, дали оценката на риска за тях е извършвана групово или индивидуално
- (3) **На базата на извършените оценки и анализ на риска, и на изискванията за непрекъснатост и наличност на услугите (описани в документ на СУУ - ИЗИСКВАНИЯ ЗА НЕПРЕКЪСНАТОСТ И НАЛИЧНОСТ НА УСЛУГА ) се определя, кои заплахи влияят на непрекъснатостта и наличността на съответната услуга (описва се в документ на СУУ - РИСКОВЕ КЪМ НЕПРЕКЪСНАТОСТТА И НАЛИЧНОСТТА НА УСЛУГА**

