**ПРИМЕР !**

# ОПИСАНИЕ И РЕЗУЛТАТИ ОТ ПРИЛАГАНЕТО НА

# МЕТОД ЗА ОЦЕНКА НА РИСКА

# КЪМ ИНФОРМАЦИОННАТА СИГУРНОСТ НА УСЛУГИТЕ

Методологията за оценка на риска , **в пълния си вид** включва изпълнението на **9 (девет)** основни стъпки, както следва:

- Стъпка 1 – Описание на обхвата на СУУ (**услуги и съответните за тях информационните активи)**, които осигуряват, напр. тяхното разработване, внедряване, поддръжка и развитие)
- Стъпка 2 – Идентифициране на заплахите към информационните активи;
- Стъпка 3 – Идентифициране на уязвимостите на информационните активи;
- Стъпка 4 – Анализ на защитните механизми – въведени и/или планирани за въвеждане;
- Стъпка 5 – Определяне на вероятностите за реализация на дадена заплаха;
- Стъпка 6 – Анализ на влиянието (последствията) от възможната реализациянададеназаплаха;
- Стъпка 7 – Определяне на риска към информационните активи;
- Стъпка 8 – Препоръки за въвеждане на нови / допълнителни защитни механизми;
- Стъпка 9 – Документация на процеса за оценка на риска

Обикновено тези стъпки се изпълняват при изграждането на **Системи за управление на информационната сигурност (СУИС).**

В случая, става въпрос за **информационна сигурност на ИТ услуги**, обект на **Система за управление на услугите (СУУ)**.

Изискванията за инфорамационна сигурност та ИТ услугите се основават на следните основни положения:

- ИТ услугите се реализират, поддържат и развиват най-общо казано, чрез хардуер, софтуер, данни / информация и обучен персонал – **активи на услугите;**
- Информационната сигурност на активите на услугите **влияе непосредствено на непрекъснатостта и/ или наличността** на услугите;
- Рисковете към информационнат сигурност на активите на услугите пораждат рискове към **непрекъснатостта и/ или наличността** на услугите;

- Прилагането на **адекватни на заплахите** защитни / контролни механизми за защита на информационната сигурност на активите на услугите, осигурява устойчивост в изпълнението на изискванията за непрекъснатост и наличност на услугите.

За оценката на риска **към информационната сигурност на услугите**, в конкретния случай, приложимата методология се изпълнява в следните стъпки:

- **Стъпка 1** – Описание на обхвата на СУУ (услуги и съответните за тях информационните активи), които осигуряват, напр. тяхното разработване, внедряване, поддръжка и развитие)
- **Стъпка 2** – Идентифициране на заплахите към информационните активи;
- **Стъпка 3** – Определяне на вероятностите за реализация на дадена заплаха;
- **Стъпка 4** – Определяне на влиянието (последствията) от възможната реализация на дадена заплаха;
- **Стъпка 5** – Определяне на риска към информационните активи;
- **Стъпка 6** – Документация на процеса за оценка на риска (чрез съответните документи от състава на СУУ)

## ИЗПЪЛНЕНИЕ НА СТЪПКИТЕ ЗА ОЦЕНКАТА НА РИСКА КЪМ ИНФОРМАЦИОННАТА СИГУРНОСТ НА УСЛУГИТЕ

**ИЗПЪЛНЕНИЕ НА СТЪПКА 1** - Описание на обхвата на СУУ (услуги и съответните за тях информационните активи), които осигуряват, напр. тяхното разработване, внедряване, поддръжка и развитие)

Тази стъпка се изпълнява, като за **всяка услуга от обхвата на СУУ** се описват **най-важните** активи, осигуряващи **функционирането** на съответната услуга (хардуер, софтуер, данни / информация, персонал и др., както е приложимо)

***Забележка:*** *Като* ***„най-важни”*** *се определят тези активи, които имат оределящо влияние в осигуряването на* ***изискванията за непрекъснатост и наличност*** *на съответната услуга.*

Резултатите от изпълнението на тази стъпка могат да се представят в табличен вид, както е показано в следващата таблица 1

Таблица 1

| Наименование на услугата | Тип актив: Хардуер (кратко описание) | Тип актив: Софтеур (кратко описание) | Тип актив: Данни / информация (кратко описание) | Тип актив: Персонал (кратко описание) |
|---|---|---|---|---|
| Услуга „-----„ | 1..... | 1..... | 1..... | 1..... |
| | 2..... | 2..... | 2..... | 2..... |
| | ..... | ..... | 3..... | ..... |

| | | | | |
|---|---|---|---|---|
| Услуга „-----„ | 1..... | 1..... | 1..... | 1..... |
| | 2..... | 2..... | 2..... | 2..... |

За конкретния случай е направено обобщението, че най-важните активи, от всички типове, осигуряващи функционирането на всички услуги са **едни и същи**, или ако са различни, то те са със **съпоставимо влияние** към услугите. Този подход ще облекчи прилагането на Методиката за оценка на риска, като на практика се работи с типове активи, представители на групи от конкретни активи **имащи съпоставимо влияние** към услугите. Този подход е напълно приемлив, отчитайки, че оценката на риска се извършва за пръв път и ще служи за база на последващи, по-детайлни оценки (за конкретни активи от конкретна услуга).

На практика, след направените обобщения Таблица 1 , за целта на конкретния **ПРИМЕР**, придобива следния вид (Таблица 1.1):

Таблица 1.1 (Обхват на СУУ по активи)

| **Наименование на услугата** | **Тип актив: Хардуер (кратко описание)** | **Тип актив: Софтеур (кратко описание)** | **Тип актив: Данни / информация (кратко описание)** | **Тип актив: Персонал (кратко описание)** |
|---|---|---|---|---|
| За всички услуги, обект на СУУ (напр. както са описани в Каталога на услугите) | 1.Компютри за разработване и поддръжка на софтуер за услугите | 1. Програмен инструментариум за проектиране на услугите и разработване софтуер за тях | 1.Споразумение за ниво на услугата (**SLA**) | 1.Отговорник за функционирането на услуга |
| | 2.Компютри, осигуряващи функционирането на услугите (сървери и др.) | 2.ИТ системи за управление на услуги | 2.Договори с клинеттите на услуги | 2.Проектант на услуга |

В случая, тази Таблица 1.1 **определя обхвата на СУУ по информационни активи (най-важните)**, осигуряващи функционирането на услугите. Тези активи (в Таблица 1.1) ще бъда обект на прилагане на Методиката за оценка на риска (в следващите стъпки).

**<u>ИЗПЪЛНЕНИЕ НА СТЪПКА 2</u>** - Идентифициране на заплахите към инфоинформационните активи

При нази стъпка се **определят заплахите към активите**, определени в Стъпка 1 – Таблица 1.1. Обект на разглеждане са тези заплахи, **за които се знае или се предполага с висока степен на вероятност, че съществуват уязвимости** в съответните активи, чрез които те могат да се реализират.

Резултата от работата по тази стъпка е **Списък на идентифицираните заплахи,** както следва:

## А. ЗАПЛАХИ, ПРОИЗТИЧАЩИ ОТ ОБКРЪЖАВАЩАТА СРЕДА

Тези заплахи включват **природни бедствия** и **други състояния на околната среда**. Резултатите от реализирането на тези заплахи са свързани със **загуба на наличност на данни / информацията** и могат да доведат, освен другото до **невъзможност или до силни затруднения** за изпълнение на важни за бизнеса задачи, **вкл. на предоставяни ИТ услуги, за дълъг период отвреме**;

В допълнение, тези заплахи могат да засегнат здравето и живота на персонала. Ако към тези заплахи се прибави и нарушена физическа сигурност, то резултатите могат да предизвикат **загуба и на конфиденциалност на информацията.**

Определните от този тип заплахи, които ще бъдат обект на Методиката за оценка на риска са:

- Пожар в работните и офис помещени на организацията (заплаха към активите от тип „**Хардуер**” и тип „**Персонал**”);
- Аварии в централното електрозахранване (заплаха към активите от тип „**Хардуер**”);

## Б. ПРЕДНАМЕРЕНИ ЗАПЛАХИ

Това са, заплахи, които могат да доведат до **преднамерено** разрушаване или манипулация на информационните активи.

**Основния източник и на такъв тип заплахи са хората** – напр. недоволни служители или контрагенти, консултанти, хакери, персонал за поддръжка и обслужване, потребители, доставчици, терористи, престъпници, разузнавачи и др.

Резултатите от реализацията на тези заплахи могат да доведат **до загуби на наличност, конфиденциалност и цялостност на информационните активи** и последствия за организацията, свързани, освен другото и с прекъсване изпълнението на договорирани задължения, **свързани с предоставянето на ИТ услуги.**

Определните от този тип заплахи, които ще бъдат обект на Методиката за оценка на риска са:

- Зловреден код – компютърни вируси от различен тип (заплаха към активите от тип „**Хардуер**”, „**Софтуер**” и „**Данни / информация**”);

- Злонамерена подмяна/промяна на данни, информация (заплаха към активите от тип „**Софтуер**” и „**Данни / информация**”);
- Социален инженеринг (заплаха към активите от тип „**Персонал**”, „**Софтуер**” и „**Данни / информация**”);
- Неупълномощен достъп до данни (заплаха към активите от тип „**Софтуер**” и „**Данни / информация**”);
- Неупълномощени промени на софтуер (заплаха към активите от тип „**Софтуер**”)

**В. СЛУЧАЙНИ (НЕПРЕДНАМЕРЕНИ) ЗАПЛАХИ**

Този тип заплахи, обикновено са свързани с **грешки и/или пропуски**. Грешките и пропуските, извършени от служителите на организацията са един от основните източници на проблеми с информационната сигурност.

В не малко случаи грешките могат да бъдат сериозна заплаха (напр. програмни грешки, водещи до “сриване” на система) или да създадат уязвимост (напр. оставен без наблюдение екран, съдържащ важна информация, може да бъде прочетена от лице, нямащо необходимост да е знае)

Този тип заплахи може да доведе, освен другото до **невъзможност за** изпълнение на задължения по договори за предоставяне на услуги.

Определните от този тип заплахи, които ще бъдат обект на Методиката за оценка на риска са:

- отпадане на комуникациите (заплаха към активите от тип „**Хардуер**” и „**Софтуер**”);
- грешки на персонала и потребителите (заплаха към активите от тип „**Хардуер**”, „**Софтуер**” и „**Данни / информация**”);
- грешки при програмиране (заплаха към активите от тип „**Софтуер**”);
- технически повреди (заплаха към активите от тип „**Хардуер**”);

В следващата Таблица 2, е представен Списъка на заплахите и съответните активи:

| № | ЗАПЛАХА | АКТИВ |
|---|---|---|
| **1** | Пожар в работните и офис помещени на организацията | хардуер, персонал |
| **2** | Аварии в централното електрозахранване | хардуер |
| **3** | Зловреден код – компютърни вируси от различен тип | хардуер, софтуер, данни / информация |
| **4** | Злонамерена подмяна/промяна на данни и информация | софтуер, данни / информация |
| **5** | Социален инженеринг | софтуер, данни / информация, персонал |
| **6** | Неупълномощен достъп до данни | софтуер, данни / информация |
| **7** | Неупълномощени промени на софтуер | софтуер |
| **8** | Отпадане на комуникациите | хардуер, софтуер |
| **9** | Грешки на персонала и потребителите | хардуер, софтуер, данни / информация |
| **10** | Грешки при програмиране | софтуер |
| **11** | Технически повреди | хардуер |

**ИЗПЪЛНЕНИЕ НА СТЪПКИ 3, 4 И 5** - Определяне на вероятностите за реализация на дадена заплаха; Определяне на влиянието (последствията) от възможната реализация на дадена заплаха; Определяне на риска към информационните активи;

Тези стъпки от Методиката за оценка на риска се изпълняват едновременно, както е показано в следващите таблици.

**I. <u>Идентифицирани заплахи към информационния актив тип „Хардуер” /</u> Компютри за разработване и поддръжка на софтуер за услугите / Ниво на вероятност за реализация на заплахата / Коефициент на вероятността**

| № | Описание на заплахата | Ниво на вероятност за реализация на заплахата (1) | Коефициент на вероятността (2) |
|---|---|---|---|
| 1 | Пожар в работните и офис помещени на организацията | **ниско** | **0.1** |
| 2 | Аварии в централното електрозахранване | **ниско** | **0.1** |
| 3 | Зловреден код – компютърни вируси от различен тип | **високо** | **1** |
| 4 | Отпадане на комуникациите | **ниско** | **0.1** |
| 5 | Грешки на персонала и потребителите | **средно** | **0.5** |
| 6 | Технически повреди | **средно** | **0.5** |

Забележки:

(1) Въвежда се качествена оценка - **високо, средно, ниско ниво**;
(2) Въвежда се коефициент, съответен на качествената оценка – **1 (за високо ниво), 0.5 (за средно ниво), 0.1 (за ниско ниво)**

**Определяне на неблагоприятното влияние при успешна реализация на заплахи към информационния актив тип „Хардуер” / Компютри за разработване и поддръжка на софтуер за услугите**

| № | Описание на заплахата | Размер на влиянието (1) | Коефициент на влиянието (2) |
|---|---|---|---|
| 1 | Пожар в работните и офис помещени на организацията | **висок** | **100** |
| 2 | Аварии в централното електрозахранване | **среден** | **50** |
| 3 | Зловреден код – компютърни вируси от различен тип | **висок** | **100** |
| 4 | Отпадане на комуникациите | **среден** | **50** |
| 5 | Грешки на персонала и потребителите | **среден** | **50** |
| 6 | Технически повреди | **среден** | **50** |

Забележки:

(1) Въвежда се качествена оценка - **висок, среден, нисък** размер на влиянието;
(2) Въвежда се коефициент, съответен на качествената оценка – **100 (за висок размер), 50 (за среден размер), 10 (за нисък размер**)

**Определяне на нивата на риск към информационния актив тип „Хардуер” / Компютри за разработване и поддръжка на софтуер за услугите**

| № | Описание на заплахата | Коефициент на вероятността на заплахата | Коефициент на влиянието | Коефициент на нивото на риск (1) | Ниво на риска (2) |
|---|---|---|---|---|---|
| 1 | Пожар в работните и офис помещени на организацията | 0.1 | 100 | 10 | малко |
| 2 | Аварии в централното електрозахранване | 0.1 | 50 | 5 | малко |
| 3 | **Зловреден код – компютърни вируси от различен тип** | 1 | 100 | 100 | голямо |
| 4 | Отпадане на комуникациите | 0.1 | 50 | 5 | малко |
| 5 | **Грешки на персонала и потребителите** | 0.5 | 50 | 25 | средно |
| 6 | **Технически повреди** | 0.5 | 50 | 25 | средно |

Забележки:

(1) Определя се чрез **умножаване на коефициентите за вероятност и влияние на заплахата**;

**(2)** Въвежда се качествената 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)**
Останалите данни в таблицата са определени в предишните таблици

Получените данни за нивата на риска към актив от тип „Хардуер” **/ Компютри за разработване и поддръжка на софтуер за услугите** могат да се считат за обективни и за актив **„Компютри, осигуряващи функционирането на услугите (сървери и др.)”,** тъй-като може да се приеме, че той е със съпоставима важност (или еднаква) за функционирането на услугите.

**II. Идентифицирани заплахи към информационния актив тип „Софтуер” / Програмен инструментариум за проектиране на услугите и разработване софтуер за тях / Ниво на вероятност за реализация на заплахата / Коефициент на вероятността**

| № | Описание на заплахата | Ниво на вероятност за реализация на заплахата (1) | Коефициент на вероятността (2) |
|---|---|---|---|
| 1 | Зловреден код – компютърни вируси от различен тип | **високо** | **1** |
| 2 | Злонамерена подмяна/промяна на данни и информация | **средно** | **0.5** |
| 3 | Социален инженеринг | **високо** | **1** |
| 4 | Неупълномощен достъп до данни | **средно** | **0.5** |
| 5 | Неупълномощени промени на софтуер | **средно** | **0.5** |
| 6 | Отпадане на комуникациите | **ниско** | **0.1** |
| 7 | Грешки на персонала и потребителите | **средно** | **0.5** |

| | | | |
|---|---|---|---|
| 8 | Грешки при програмиране | **средно** | **0.5** |

Забележки:

(1) Въвежда се качествена оценка - **високо, средно, ниско ниво**;
(2) Въвежда се коефициент, съответен на качествената оценка – **1 (за високо ниво), 0.5 (за средно ниво), 0.1 (за ниско ниво)**

**Определяне на неблагоприятното влияние при успешна реализация на заплахи към информационния актив тип „Софтуер” / Програмен инструментариум за проектиране на услугите и разработване софтуер за тях**

| № | Описание на заплахата | Размер на влиянието (1) | Коефициент на влиянието (2) |
|---|---|---|---|
| 1 | Зловреден код – компютърни вируси от различен тип | **висок** | **100** |
| 2 | Злонамерена подмяна/промяна на данни и информация | **висок** | **100** |
| 3 | Социален инженеринг | **висок** | **100** |
| 4 | Неупълномощен достъп до данни | **висок** | **100** |
| 5 | Неупълномощени промени на софтуер | **висок** | **100** |
| 6 | Отпадане на комуникациите | **среден** | **50** |
| 7 | Грешки на персонала и потребителите | **среден** | **50** |
| 8 | Грешки при програмиране | **висок** | **100** |

Забележки:

(1) Въвежда се качествена оценка - **висок, среден, нисък** размер на влиянието;

(2) Въвежда се коефициент, съответен на качествената оценка – **100 (за висок размер), 50 (за среден размер), 10 (за нисък размер**)

**Определяне на нивата на риск към информационния актив тип „Софтуер” / Програмен инструментариум за проектиране на услугите и разработване софтуер за тях**

| № | Описание на заплахата | Коефициент на вероятността на заплахата | Коефициент на влиянието | Коефициент на нивото на риск (1) | Ниво на риска (2) |
|---|---|---|---|---|---|
| 1 | Зловреден код – компютърни вируси от различен тип | **1** | **100** | **100** | **голямо** |
| 2 | Злонамерена подмяна/промяна на данни и информация | **0.5** | **100** | **50** | **голямо** |
| **3** | Социален инженеринг | **1** | **100** | **100** | **голямо** |
| 4 | Неупълномощен достъп до данни | **0.5** | **100** | **50** | **голямо** |
| **5** | Неупълномощени промени на софтуер | **0.5** | **100** | **50** | **голямо** |
| **6** | Отпадане на комуникациите | **0.1** | **50** | **25** | **средно** |
| **7** | Грешки на персонала и потребителите | **0.5** | **50** | **25** | **средно** |
| **8** | Грешки при програмиране | **0.5** | **100** | **50** | **голямо** |

Забележки:

(1) Определя се чрез **умножаване на коефициентите за вероятност и влияние на заплахата**;
(2)Въвежда се качествената 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)**
Останалите данни в таблицата са определени в предишните таблици

Получените данни за нивата на риска към актив от тип „Софтуер” **/ Програмен инструментариум за проектиране на услугите и разработване софтуер за тях** могат да се считат за обективни и за актив **„ИТ системи за управление на услуги”** тъй-като може да се приеме, че той е със съпоставима важност (или еднаква) за функционирането на услугите.

**III. Идентифицирани заплахи към информационния актив тип „Данни / информация” / Споразумение за ниво на услугата (SLA) / Ниво на вероятност за реализация на заплахата / Коефициент на вероятността**

| № | Описание на заплахата | Ниво на вероятност за реализация на заплахата (1) | Коефициент на вероятността (2) |
|---|---|---|---|
| 1 | Зловреден код – компютърни вируси от различен тип | **високо** | **1** |
| 2 | Злонамерена подмяна/промяна на данни и информация | **средно** | **0.5** |
| 3 | Социален инженеринг | **високо** | **1** |
| 4 | Неупълномощен достъп до данни | **средно** | **0.5** |
| 5 | Грешки на персонала и потребителите | **средно** | **0.5** |

Забележки:

(1) Въвежда се качествена оценка - **високо, средно, ниско ниво**;

(2) Въвежда се коефициент, съответен на качествената оценка – **1 (за високо ниво), 0.5 (за средно ниво), 0.1 (за ниско ниво**

**Определяне на неблагоприятното влияние при успешна реализация на заплахи към информационния актив тип „Данни / информация” / Споразумение за ниво на услугата (SLA)**

| № | Описание на заплахата | Размер на влиянието (1) | Коефициент на влиянието (2) |
|---|---|---|---|
| 1 | Зловреден код – компютърни вируси от различен тип | **висок** | **100** |
| 2 | Злонамерена подмяна/промяна на данни и информация | **висок** | **100** |
| 3 | Социален инженеринг | **висок** | **100** |
| 4 | Неупълномощен достъп до данни | **висок** | **100** |
| 5 | Грешки на персонала и потребителите | **среден** | **50** |

Забележки:

(1) Въвежда се качествена оценка - **висок, среден, нисък** размер на влиянието;
(2) Въвежда се коефициент, съответен на качествената оценка – **100 (за висок размер), 50 (за среден размер), 10 (за нисък размер**)

**Определяне на нивата на риск към информационния актив тип Данни / информация" / Споразумение за ниво на услугата (SLA)**

| № | Описание на заплахата | Коефициент на вероятността на заплахата | Коефициент на влиянието | Коефициент на нивото на риск (1) | Ниво на риска (2) |
|---|---|---|---|---|---|
| 1 | Зловреден код – компютърни вируси от различен тип | **1** | **100** | **100** | **голямо** |
| 2 | Злонамерена подмяна/промяна на данни и информация | **0.5** | **100** | **50** | **голямо** |
| **3** | Социален инженеринг | **1** | **100** | **100** | **голямо** |
| 4 | Неупълномощен достъп до данни | **0.5** | **100** | **50** | **голямо** |
| **5** | Грешки на персонала и потребителите | **0.5** | **50** | **50** | **голямо** |

Забележки:

(1) Определя се чрез **умножаване на коефициентите за вероятност и влияние на заплахата**;
(2)Въвежда се качествената 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)**
Останалите данни в таблицата са определени в предишните таблици

Получените данни за нивата на риска към актив от тип „Данни / информация" **/ Споразумение за ниво на услугата (SLA)** могат да се считат за обективни и за

актив **„Договори с клинеттите на услуги”** тъй-като може да се приеме, че той е със съпоставима важност (или еднаква) за функционирането на услугите.

**IV. Идентифицирани заплахи към информационния актив тип „Персонал ” / Отговорник за функционирането на услуга / Ниво на вероятност за реализация на заплахата / Коефициент на вероятността**

| № | Описание на заплахата | Ниво на вероятност за реализация на заплахата (1) | Коефициент на вероятността (2) |
|---|---|---|---|
| 1 | Пожар в работните и офис помещени на организацията | **ниско** | **0.1** |
| 2 | Социален инженеринг | **високо** | **1** |

Забележки:

(1) Въвежда се качествена оценка - **високо, средно, ниско ниво**;
(2) Въвежда се коефициент, съответен на качествената оценка – **1 (за високо ниво), 0.5 (за средно ниво), 0.1 (за ниско ниво)**

**Определяне на неблагоприятното влияние при успешна реализация на заплахи към информационния актив тип „Персонал ” / Отговорник за функционирането на услуга**

| № | Описание на заплахата | Размер на влиянието (1) | Коефициент на влиянието (2) |
|---|---|---|---|
| 1 | Пожар в работните и офис помещени на организацията | **среден** | **50** |
| 2 | Социален инженеринг | **висок** | **100** |

Забележки:

(1) Въвежда се качествена оценка - **висок, среден, нисък** размер на влиянието;
(2) Въвежда се коефициент, съответен на качествената оценка – **100 (за висок размер), 50 (за среден размер), 10 (за нисък размер**)

**Определяне на нивата на риск към информационния актив тип „Персонал ” / Отговорник за функционирането на услуга**

| № | Описание на заплахата | Коефициент на вероятността на заплахата | Коефициент на влиянието | Коефициент на нивото на риск (1) | Ниво на риска (2) |
|---|---|---|---|---|---|
| 1 | Пожар в работните и офис помещени на организацията | **0.1** | **50** | **5** | **малко** |
| 2 | Социален инженеринг | **1** | **100** | **100** | **голямо** |

Забележки:

(1) Определя се чрез **умножаване на коефициентите за вероятност и влияние на заплахата**;
(2)Въвежда се качествената 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)**
Останалите данни в таблицата са определени в предишните таблици

## ОБОБЩЕНО ПРЕДСТАВЯНЕ НА РЕЗУЛТАТИТЕ ОТ ПРИЛАГАНЕТО НА МЕТОДИКАТА ЗА ОЦЕНКА НА РИСКА

В следващата Таблица са представени заплахиге и съответните резултати за нивата на риска към отделните типове активи

| № | ЗАПЛАХА | Хардуер Ниво на риск | Софтуер Ниво на риск | Данни / информация Ниво на риск | Персонал Ниво на риск |
|---|---|---|---|---|---|
| 1 | Пожар в работните и офис помещени на организацията | малко | | | малко |
| 2 | Аварии в централното електрозахранване | малко | | | |
| 3 | Зловреден код – компютърни вируси от различен тип | голямо | голямо | голямо | |
| 4 | Злонамерена подмяна/промяна на данни и информация | | голямо | голямо | |
| 5 | Социален инженеринг | | голямо | голямо | голямо |
| 6 | Неупълномощен достъп до данни | | голямо | голямо | |
| 7 | Неупълномощени промени на софтуер | | голямо | | |
| 8 | Отпадане на комуникациите | малко | средно | | |
| 9 | Грешки на персонала и потребителите | средно | средно | голямо | |
| 10 | Грешки при програмиране | | голямо | | |
| 11 | Технически повреди | средно | | | |

От получените резултати от прилагането на Методиката за оценка на риска може да се направи извод, че основните заплахи, които имат **съществено влияние** (галямо ниво на риска) върху непрекъснатостта и/или наличността на услугите са:

**1. Зловреден код – компютърни вируси от различен тип**

**2. Злонамерена подмяна/промяна на данни и информация**

**3. Социален инженеринг**

**4. Неупълномощен достъп до данни**

**5. Неупълномощени промени на софтуер**

**6. Грешки при програмиране**

Останалите заплахи, имащи средно и малко ниво на риска, могат да бъдат приети, като **невлияещи съществено** върху непрекъснатостта и/или наличността на услугите.

**ИЗПЪЛНЕНИЕ НА СТЪПКА 6** - Документация на процеса за оценка на риска (чрез съответните документи от състава на СУУ)

При тази стъпка се подготвят **два документа** , произтичащи от резултатите при прилагането на Методиката за оценка на риска

1. Документ на СУУ (задължителен) - **РИСКОВЕ КЪМ НЕПРЕКЪСНАТОСТТА И НАЛИЧНОСТТА НА УСЛУГА**

Този документ, може да бъде представен в таблична форма, със съдържание **за конкретния случай**, както следва:

| № | Описание на разкрития, оценен и анализиран риск | Установено ниво на риска (голямо / средно / ниско ) | Риска влия или не вияе съществено на непрекъснатост и/или наличност на услугата |
|---|---|---|---|
| 1 | Риск от зловреден код – компютърни вируси от различен тип | **голямо** | влияе **съществено** на непрекъснатостта и наличност и на услугата |
| 2 | Риск от злонамерена подмяна/промяна на данни и информация | **голямо** | влияе **съществено** на непрекъснатостта и наличност и на услугата |
| 3 | Риск от социален инженеринг | **голямо** | влияе **съществено** на непрекъснатостта и наличност и на услугата |
| 4 | Риск от неупълномощен достъп до данни | **голямо** | влияе **съществено** на непрекъснатостта и наличност и на услугата |
| 5 | Риск от неупълномощени промени на софтуер | **голямо** | влияе на непрекъснатостта и наличност и на услугата |
| 6 | Риск от грешки при програмиране | **голямо** | влияе на непрекъснатостта и наличност и на услугата |

2. Документ – **ПЛАН ЗА ПРОТИВОДЕЙСТВИЕ НА РИСКА**

**Забележка:** Този документ е **важен планиращ документ** за Организацията, в действията и за противодействие на най-съществените разкрити рискове към непрекъснатостта и/или наличността на предоставяните услуге, обект на управление на СУУ. База за подготовката на този документо е документ **РИСКОВЕ КЪМ НЕПРЕКЪСНАТОСТТА И НАЛИЧНОСТТА НА УСЛУГА.**

Документа може да бъде представен таблично както следва:

| № | Описание на разкрития, оценен и анализиран риск | Планиран за въвеждане защитен механизъм | Необходими ресурси (човешки, материални, финансови, технологични) | Изпълнител (ръководител, състав на работна група) | Начална и крайна дата за въвеждане на защитния механизъм |
|---|---|---|---|---|---|
| 1 | **Риск от зловреден код – компютърни вируси от различен тип** | **Разработване и внедряване на ред и правила за избор и/или своевременното обновяване на антивиусен софтуер.** | | | |
| 2 | **Риск от злонамерена подмяна/промяна на данни и информация** | **Разработване и прилагане на Процедура за промяна на данни / информация - в документи, бази данни и т.н., както е приложимо** | | | |
| 3 | **Риск от социален инженеринг** | **Разработване и прилагане на Програма за обучение на персонала по въпросите на социалния инженеринг** | | | |
| 4 | **Риск от неупълномощен достъп до данни** | **Разработване и прилагане на Политика за контрол на достъпа до ресурсите на ИТ системите** | | | |
| 5 | **Риск от неупълномощени промени на софтуер** | **Разработване и прилагане на Политика за извършване на промени в софтуера, разработван в Организацията** | | | |
| 6 | **Риск от грешки при програмиране** | **Разработване и прилагане на Процедура за провеждане на тестове на софтуера, разработван в Организацията** | | | |

**Забележка**: Подбраните за въвеждане защитни механизми (в случай - административни), могат дабъдат допълнени и/или променени от Организацията с технологичин защитни механизми. З а избора на защитни механизми може да се използва съответния списък в **Приложение А** на **ISO 27001** (изпратено отделно)