КУРС ЗА САМООБУЧЕНИЕ НА ТЕМА:

СИСТЕМА ЗА УПРАВЛЕНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ (СУИС)

“ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС, В СЪОТВЕТСТВИЕ С ИЗИСКВАНИЯТА НА ISO 27001 И ПРЕПОРЪКИТЕ НА ISO 27002”

Разработил курса: Пламен Каменов
Водещ одитор ISO 27001/ ISO 9001 / ISO 20000
e mail: infosecservicebg@gmail.com
август, 2018

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Съдържание на курса:

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 1 - Въведение

Всяка организация използва и зависи от информацията.

Различни рискове могат да въздействат неблагоприятно на сигурността (на нейните конфиденциалност, цялостност и достъпност) на тази информация.

Информационната сигурност се базира на управлението на риска, защото "тоталната" сигурност е непостижима задача за изпълнение.

Информационната сигурност не е ИТ проблем, тя е въпрос за решаване от бизнеса.

Рисковете се управляват чрез намаляване на вероятността за тяхната поява и/или чрез намаляване на последствията от тях към бизнеса.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 1 - Въведение

Целта на курса е да подпомогне държавните и частни организации при изграждането, поддръжката и развитието на техните Системи за управление на информационната сигурност (СУИС)

СУИС отразява дейностите (бизнеса) на организацията, нейните информационни активи, рисковете към тях, законовата рамка, изискванията на политиките за сигурност и способността,и готовността на организацията поема и понася рискове.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 1 - Въведение

Този курс е приложимо за три основни групи персонал:

- Ръководители, носещи отговорност за сигурността на информационните активи (управители, менажери, изпълнителни директори и др. ръководен състав);

- Персонал, който е отговорен за въвеждането, внедряването и/или наблюдението на управлението на риска към информационната сигурност в организацията;

- Персонал, който е отговорен за въвеждането, внедряването и/или поддръжката на информационната сигурност в организацията

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 1 - Въведение

Целите на курса са насочени към:

Повишаване на познанията за рисковете към сигурността на информационните активи и начините за противодействие.

Подпомагане на организациите при изграждането и внедряването на СУИС, в съответствие с изискванията на международните стандарти, чрез:

- предоставяне на цялостен подход и методология;

- предоставяне на начална база, за разработване на политики, процедури, инструкции, планове и др. документи по сигурността;

- предоставяне на базова информация за заплахите, уязвимостите и съответните контролни / защититни средства и / или механизми

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 1 - Въведение

Информацията в този курс може да бъде използвана за всеки етап от дадена дейност, функция, проект, продукт или актив, включващ информация, собственост на организацията и подлежаща на защита.

Като цяло, управлението на информационната сигурност е приложимо и за цялостни информационни системи. То може да бъде изпълнявано и за отделни системни компоненти или услуги, когато това е осъществимо и полезно за организацията

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 1 - Въведение

Широко възприето е, че технологията е само част от решенията за информационна сигурност.

Лошото прилагане и управление на технологията, и пренебрегването на човешкия фактор могат да повишат уязвимостта, а като следствие и рисковете към сигурността.

Необходимо е риска да бъде непрекъснато управляван, защото той се променя, а се появяват и нови рискове. Това означава, че трябва да се провеждат периодични прегледи за състоянието на рисковете към информационната сигурност, а също и такива (извън планираните периоди за преглед), когато имаме установени промени на обстоятелствата.

СУИС се занимава с всички тези въпроси.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 1 – Въведение

Този курс представя цялостен подход за управление на информационната сигурност, независим от големината, структурата и естеството на организацията (типа на нейния бизнес).

Разбира се, курса е ограничен, по отношение на заплахите към информационната сигурност, уязвимостите и защитите, защото те се променят и развиват непрекъснато.

Не всичко описано в курса е приложима за всякакви ситуации или за обстоятелства, специфични за дадена организация.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 1 – Въведение

Подхода, използван в курса, е да се представи цялостен процес за изграждане на СУИС, в съответствие с изискванията на ISO 27001 *Information technology – Security techniques –Information security management systems – Requirements*

В курса са описани процесите за управлението на риска и принципите на архитектурата за сигурност, с цел да улесни и подпомогне, а не да затрудни дейностите (бизнеса) на организацията.

На практика, курса допълва ISO 27002 *Information technology – Security techniques - Code of practice for information security management*, чрез описанието на допълнителни ред и правила за изпълнението на процесите за изграждане и внедряване на СУИС.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 1 – Въведение

Изграждането на СУИС, в съответствие с изискванията на ISO 27001 е ПРОЕКТ и изисква прилагането на методите, и техниките за управление на проекти (такива, каквито са възприети и прилагани в организацията за други проекти)

Този детайл е извън обхвата на курса.

Независимо от това, курса е структуриран в серия от логически свързани етапи и стъпки, съдържащи дейностите за планиране; изграждане и внедряване; наблюдение и контрол; подобряване и развитие на СУИС.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 1 – Въведение

Етапи и стъпки за изграждане на СУИС:

Дейност по Етап 1:
Рамка на СУИС

Резултати от Етап 1:
Документ за учредяване на СУИС
Политика за изграждане на СУИС
Обхват на СУИС
Критерии за оценка на риска
План на проекта за изграждане на СУИС

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 1 – Въведение

Етапи и стъпки за изграждане на СУИС:

Дейности по Етап 2:
Управление на риска

Стъпки по Етап 2:

Стъпка 1 – Финализиране на подхода
Стъпка 2 – Оценка на риска
Стъпка 3 – Възможни противодействия
Стъпка 4 – Избор на механизми за защита
Стъпка 5 – Одобрение от ръководството

Резултати от Етап 2:

Опис на информационните активи
Качествена / количествена оценка на риска
Оценка на възможните противодействия
План за противодействие на риска
Одобрен План за противодействие на риска

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 1 – Въведение

Етапи и Стъпки за изграждане на СУИС:

Дейности по Етап 3:
Внедряване в експлоатация

Резултат от Етап 3:
Внедрена СУИС

Дейности по Етап 4:
Наблюдение и подобрения

Резултат от Етап 4:
Подобрена СУИС

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 1 – Въведение

Основните три принципи, прилагани за информационната сигурност са:

1. **Управлението на риска към информационните активи е основата за избора и функционирането на защитите.**
2. **Защитите се внедряват и функционират , като елемент на СУИС, която е планирана и контролиране чрез ефикасен процес на управление.**
3. **Приложени защити, трябва да са пропорционални на риска към информационните активи.**

В допълнение към тези основни принципи, достъпа до информацията трябва да се определя от “необходимостта да се знае и възможно най-малко привилегии”

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Край на **Част 1 – Въведение**

За въпроси: Пламен Каменов
Водещ одитор ISO 27001/ ISO 9001 / ISO 20000
e mail: infosecservicebg@gmail.com

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 2 – Въведение в информационната сигурност

Всички форми на сигурност се определят от нуждите на бизнеса (организацията). Това означава, че сигурността трябва да отразява виждането и перспективата на бизнеса, и да допринася, а не да затруднява постигането на бизнес целите. Всичко това прави информационната сигурност въпрос на управление и ръководство, а не проблем на информационно – комуникационните технологии.

Единствено ръководството на бизнеса (организацията) притежава необходимите пълномощия, отговорности и виждане за:

- **Определянето на най-важните информационни активи и нивата на тяхната защита .**
- **Определяне приоритетите за инвестиране в информационната сигурност.**
- **Изграждането на организация, необходима за цялостна СУИС.**
- **Осигуряването на предпоставки за прилагане на изискванията на съществуващото законова уредба по информационната сигурност.**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 2 – Въведение в информационната сигурност

Управлението на риска е основа за управлението на информационната сигурност. Управлението на сигурността би трябвало да е неразделна част от общото управление на риска в организацията.

Информационната сигурност е само един аспект на сигурността.

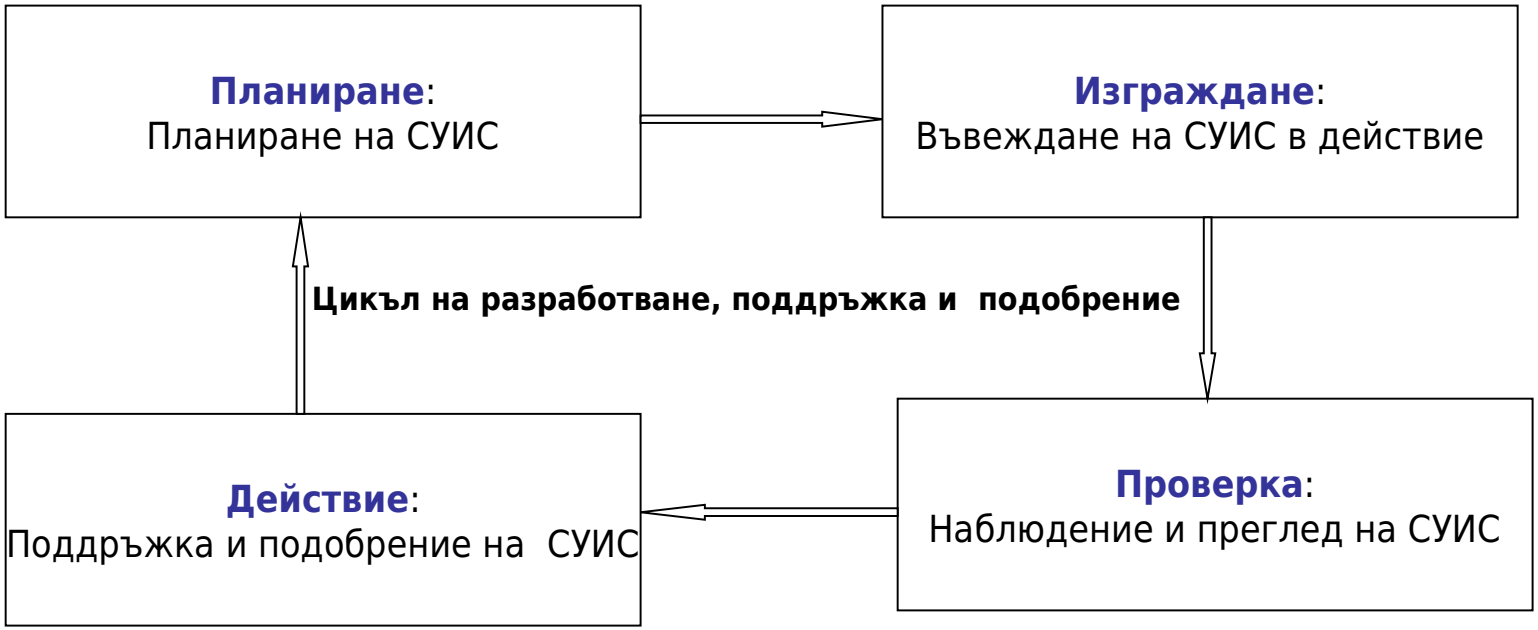
Постигането на необходимата и достатъчне информационната сигурност е цикличен управленски процес, изпълняван чрез СУИС.

Вътре в този процес, управлението на риска е непрекъснато и то се осъществява, чрез прилагане на съответните защити, с цел намаляване на вероятността и/или “смекчаване” на последствията от неприемливия риск.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 2 – Въведение в информационната сигурност

Цикъл на СУИС



ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 2 – Въведение в информационната сигурност – Базови принципи по сигурността

1. Осъзнаване – Служителите трябва да осъзнаят необходимостта от сигурност на информационните системи и мрежи, а също и какво могат те да направят да да подобрят сигурността

2. Отговорност – Всички служители са отговорни за сигурността на информационните системи и мрежите

3.Отговор – Служителите трябва да действат своевременно и организирано при превенцията, разкриването и ответните действия към инцидентите по сигурността

4. Етика – Служителите трябва да зачитат легитимните интереси на другите.

5. Демокрация – Сигурността на информационните системи и мрежите трябва да е съвместима с ценностите на демократичното общество.

6. Оценка на риска – Служителите трябва да провеждат оценка на риска.

7. Проектиране и внедряване на сигурността – Служителите трябва да внедряват сигурността, като съществен елемент на информационните системи и мрежите.

8. Управление на сигурността – Служителите трябва да възприемат всестранен подход към управлението на сигурността.

9. Преоценка – Служителите трябва да преглеждат и преоценяват сигурността на на информационните системи и мрежите, и съответно да извършат необходимите промени в политиките за сигурност, практиките, мерките и процедурите.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 2 – Въведение в информационната сигурност – Информационни активи

Информацията е актив, който има стойност за организацията или за някого извън нея, и затова тя трябва да бъде съответно защитавана.

Най-общо казано, информацията е основата, за извършване на дейностите от бизнеса / организациите.

Сигурната (благонадеждната) информация поддържа способностите на бизнеса, най-вече, чрез осигуряване на предпоставки за вземането на адекватни на ситуацията решения.

Концепцията за информационните активи изрично приема, че тези активи са необходими и много важни за постигането на целите на бизнеса / организацията.

В някои случаи събирането и обработката на информацията може да бъде цел на бизнеса. Някои информационни активи може да изглежда, че нямат директна стойност за бизнеса, независимо от това, те могат да имат стойност за определени лица, които нямат пълномощия за достъп / работа с тях.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 2 – Въведение в информационната сигурност – Информационни активи

Информацията може да бъде в различна форма. Тя може да бъде разпечатана, написана / нарисувана, електронно съхранявана, предавана по електронен начин или чрез обикновена поща, показвана чрез филми, изговорена при разговор или да съществува, като усещане.

Поради това, информационните активи включват:

- хартиени документи;

- електронни данни;

- системите (софтуер, хардуер и мрежи) чрез които, информацията се съхранява, обработва и комуникира;

- интелектуална информация (знания или усещане) придобито от дадено лице;

- физически устройства, от които може да се извлече информация за предназначение, компоненти, схеми и др.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 2 – Въведение в информационната сигурност – Система за управление на информационната сигурност (СУИС)

СУИС е система за изграждане, оперирane и непрекъснато осигуряване на адекватност на защитите, срещу заплахите към сигурността на информационните активи.

СУИС не въпрос само на технология или документация.

И двата компонента са необходими, но критично за СУИС е управляваното планиране и оперирane в съответствие с документирани процедури, и записване на всички решения и последващи действия.

СУИС зависи от хората, от техните знания и натренираност.

Хората са най-голямата сила (актив) на СУИС, но без необходимите знания, те са нейната най-голяма слабост и уязвимост !!

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 2 – Въведение в информационната сигурност – Система за управление на информационната сигурност (СУИС)

Информационната сигурност обикновено е постигана и проектирана / разработвана “от долу на горе”. По този начин тя отразява фокусирани решения и достъпни от много време технологии и решения. Това означава, че съществува тенденция информационната сигурност да бъде едно струпване на технологии по сигурността и решения за защити, без необходимата интеграция по-между им – това не е система.

Най общо казано, много трудно е това струпване на технологии и решения да бъде превърнато бързо в СУИС.

Това е възможно да се постигне единствено чрез изграждането на съответните системни процедури, съобразени с нуждите на бизнеса и рисковете към сигурността.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 2 – Въведение в информационната сигурност – Рискове и защити

Информационната сигурност е един от аспектите на сигурността на бизнеса, другите аспекти са физическата, персонална и индустриална сигурност, околната среда, а също и непрекъснатостта на бизнеса .

На риска към информационните активи се противодейства със защити. Те включват процедури, технологии (софтуер, хардуер, ИТ системи) и поведението на персонала. Защитите работят във взаимодействие и допълване, в единна система за защита.

ISO 27001 и ISO 27002 изискват процеса на управление на риска да бъде използван като база и основание за избор на защити за противодействие на риска.

Този курс и ISO 27001 не налагат възприемането и прилагането на точно определени технологии за защита и/или защити с конкретни характеристики и параметри.

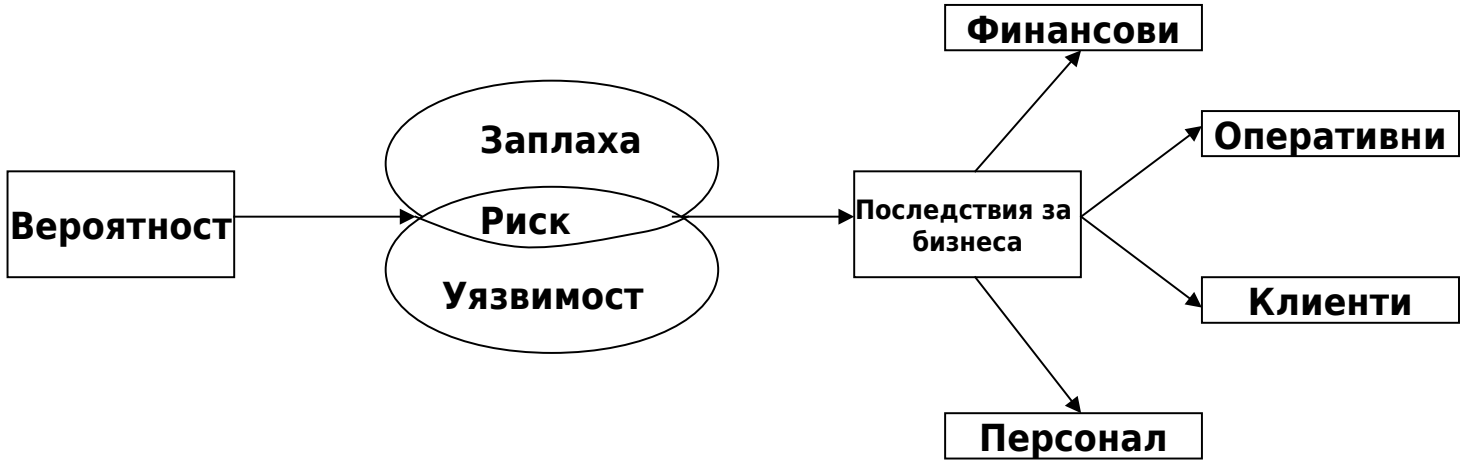
Избора на конкретните технологии и защити е въпрос на решение на ръководството на организацията и на въведените политики по сигурността.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 2 – Въведение в информационната сигурност – Рискове и защити

Управлението на риска е стратегически подход към информационната сигурност

Риска е комбинация от вероятността за поява на събитие по сигурността и последствията, свързани с тази поява. Събитие по сигурността възниква, когато дадена заплаха се реализира, чрез една или повече уязвимости.



ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 2 – Въведение в информационната сигурност – Рискове и защити

Управлението на риска е процес, който използва специализиран инструментариум и техники, в различните стадии на неговата реализация.

Този процес включва:

- **Определяне на контекста на управлението на риска.**
- **Разкриване на възможните рискове към информационните активи.**
- **Провеждане на оценка на риска, вкл. :**
  - **Анализ на риска**
  - **Остойностяване на риска**
- **Определяне и оценка на възможностите за противодействие**
- **Избор, планиране и внедряване на икономически, и финансово целесъобразни противодействия на риска.**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 2 – Въведение в информационната сигурност – Рискове и защити

Защитите противодействат (обработват) риска, чрез намаляване на вероятността от неговата поява или, чрез смекчаване на последствията от него.

Защитите трябва да докажат възвращаемост на направените инвестиции за тях. Сигурността, сама по себе си не е основание за вземане на решение за изразходване на средства.

Възвращаемостта обикновено са базира на избягването на загуби, които биха могли да се получат, ако съответните защити не са въведени.

Възможните загуби отразяват вероятността риска да се реализира и очакваната цена, ако това се случи (риска се реализира).

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 2 – Въведение в информационната сигурност – Рискове и защити

Необходимо е риска да се управлява непрекъснато, защото той се променя, а се появяват и нови рискова.

Това налага провеждането на периодични прегледи на риска, а също и такива, при възникване на промяна в обстоятелствата.

Необходимо е също, да се разбират разкритите заплахи и възможните последствия от тях.

Ефективното управление на риска налага прилагането на приоритети при неговата оценка.

Необходимо е да се прави преглед на рисковете на които се противодейства и на тези, останали без противодействие.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 2 – Въведение в информационната сигурност – Съответствие на СУИС с ISO 27001 и сертификация

Съответствие означава, прилагане на цикъла "планиране – изграждане – проверка – действие" и въвеждане на целите за защита и защитите в съответствие с Приложение А на ISO 27001, отчитайки нуждите на бизнеса и съответните приоритети.

Организациите се съобразяват със съществуваща и функционираща Система за управление на качеството, съответстваща на ISO 9000, като на практика това дава много добра база за изграждане на СУИС.

Сертификацията осигурява независима оценка и създава увереност на ръководството на бизнеса (организацията), че информационните активи са защитени, чрез прилагането на управляван процес.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 2 – Въведение в информационната сигурност – Съответствие на СУИС с ISO 27001 и сертификация

ISO 27001 определя над 100 възможни защити. Прилагат се само тези защити, които са приложими и необходими за бизнеса (организацията). В не малко случаи се налага да се добавят и допълнителни защити (извън списъка в Приложение А).

ISO 27002 описва подробно всички цели за защита и съответните защити (защитни механизми) от Приложение А на ISO 27001.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 2 – Въведение в информационната сигурност – Съответствие на СУИС с ISO 27001 и сертификация

Съгласно ISO 27002, повечето организации имат нужда от:

- **Политика за информационна сигурност;**
- **Възлагане на отговорности по информационната сигурност;**
- **Осъзнаване на информационната сигурност, обучение и тренировки;**
- **Сигурност на обработки те в приложенията;**
- **Управление на непрекъснатостта на бизнеса (дейностите);**
- **Управление на инцидентите по информационната сигурност и въвеждане на подобрения.**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 2 – Въведение в информационната сигурност – Съответствие на СУИС с ISO 27001 и сертификация

По принцип, сертификацията трябва да се провежда на цялата СУИС. Но при този процес трябва да се подходи прагматично и да се оценят необходимите финансови ресурси.

Например, сертифицирането на всеки локален офис може да е необосновано, още повече, ако там работят наследени приложения, които не са променяни, работят от дълго време без инциденти по сигурността. В този пример, риска към тези приложения може да бъде приемлив за бизнеса / организацията.

Обхвата на частта от СУИС, подлежаща на сертификация се описва в документа "Декларация за приложимост"

СУИС може да бъде съществено по-голяма от частта, подлежаща на сертифициране. В този смисъл, СУИС ще има собствена "Декларация за приложимост".

Несертифицираните елементи на СУИС (напр. локални офиси) могат да бъдат сертифицирани от вътрешни и/или външни одитори.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 2 – Въведение в информационната сигурност – Съответствие на СУИС с ISO 27001 и сертификация

Организациите, с изградена информационно – комуникационна инфраструктура, но предоставена и/или поддържана от външна организация не трябва да преотстъпват отговорностите си по информационната сигурност.

Преотстъпването най-често е свързано с управление на комуникациите и функционирането на ИТ, разработването на системи, поддръжката и понякога, контрола на достъпа.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 2 – Въведение в информационната сигурност – Архитектура за информационна сигурност

Системната архитектура е набор от правила и конвенции, които управляват проектирането, развитието и поддръжката на системите.

Архитектурата обслужва целите на системата, включително нуждите на бизнеса / организацията.

Архитектурата отразява и ограниченията, свързани с общото състояние на бизнеса, ресурсите, уменията и технологиите.

Архитектурата е средство за управление на сложността на системите и за прилагане на принципите на системния инженеринг, с цел постигане целите на бизнеса / организацията.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 2 – Въведение в информационната сигурност – Архитектура за информационна сигурност

Архитектурата за сигурност осигурява рамката от процедури, технологии и процеси.

Тя въвежда цялостен, икономически целесъобразен и сигурен подход за внедряване, използване и развитие на механизмите за защита.

Архитектурата за сигурност трябва да:

- **минимизира многообразието на технологиите;**
- **осигури цялостно функциониране по сигурността за всички информационни активи;**
- **интегрира защитите в единна система;**
- **раздели различните области и да управлява потоците от информация между тях;**
- **приложи логически свързани методи за сигурност, техники и конвенции.**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 2 – Въведение в информационната сигурност – Архитектура за информационна сигурност

Архитектурата за сигурност трябва да бъде декомпозирана по нива, като всяко ниво представя различна гледна точка за нея. Всяко ниво на архитектурата направлява нивата под него. Архитектурата за сигурност се разработва “отгоре - надолу”, като по ниските нива са с по-малка степен на абстрактност.

Пример – подход към архитектурата за сигурност

Поглед на бизнеса	**Контекстуална архитектура**
Поглед на архитекта	**Концептуална архитектура**
Поглед на проектанта	**Логическа архитектура**
Поглед на разработчика	**Физическа архитектура**
Поглед на внедрителя	**Архитектура на компонентите**
Поглед на потребителя	**Оперативна архитектура**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 2 – Въведение в информационната сигурност – Архитектура за информационна сигурност

Всяко ниво в модела на архитектурата за сигурност изисква отговор на въпросите:

Какво ? Защо ?

Как ? Кой ? Къде ? Кога ?

Този курс “привързва” етапите и стъпките за изграждане на СУИС към тези нива и въпроси.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Край на **Част 2 – Въведение в информационната сигурност**

За въпроси: Пламен Каменов
Водещ одитор ISO 27001/ ISO 9001 / ISO 20000
e mail: infosecservicebg@gmail.com

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 3 - Управление на информационната сигурност – Въведение

Загубата на конфиденциалност, цялостност и наличност на информацията, и съответните услуги, може да нанесе сериозен удар върху способността на бизнеса / организацията да постигне своите цели.

В този смисъл, защитата на информационните активи е много важна задача за изпълнение от бизнеса / организацията.

Подходящата защита на информационните активи, а като следствие и на целите на бизнеса, може да бъде постигната чрез:

- утвърждаването и прилагането на принципа, че управлението на информационната сигурност е въпрос за решаване от бизнеса;

- утвърждаването и прилагането на принципа, че управлението на информационната сигурност е неразделна част от управлението на риска;

- изграждането и внедряването на СУИС

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 3 - Управление на информационната сигурност – Въведение

Изграждането на ефективна система за информационна сигурност, по един ненатрапчив и дискретен начин не е лесна задача.

Скоростта на промените в технологиите и бизнеса превръщат управлението на информационната сигурност в динамична и предизвикателна дейност.

Доставянето на адекватни защити по сигурността много често е разглеждано, като вторичен елемент при осигуряването на функционалността на бизнеса.

Функционалност, която не води до бизнес способности, поради загуба на конфиденционалност, цялостност или наличност на информационните активи е несполучлива и ненужна инвестиция !

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 3 - Управление на информационната сигурност – Въведение

Собствениците на информационните активи (собствениците на бизнеса) носят отговорност за конфиденциалността, цялостта и наличността на информацията, при изпълнение на съответните бизнес операции.

ИТ звената могат да оперират с определени ИТ компоненти / системи и да осигуряват съответното обслужване по сигурността на бизнес звената.

Ако бизнес звената прехвърлят част от техните отговорности по сигурността към ИТ звената, то това прехвърляне трябва да включва и съответните ресурси и точни направления за работата им по сигурността.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 3 - Управление на информационната сигурност – Въведение

Бизнес звената не трябва никога да прехвърлят / преотстъпват всичките си отговорности по сигурността.

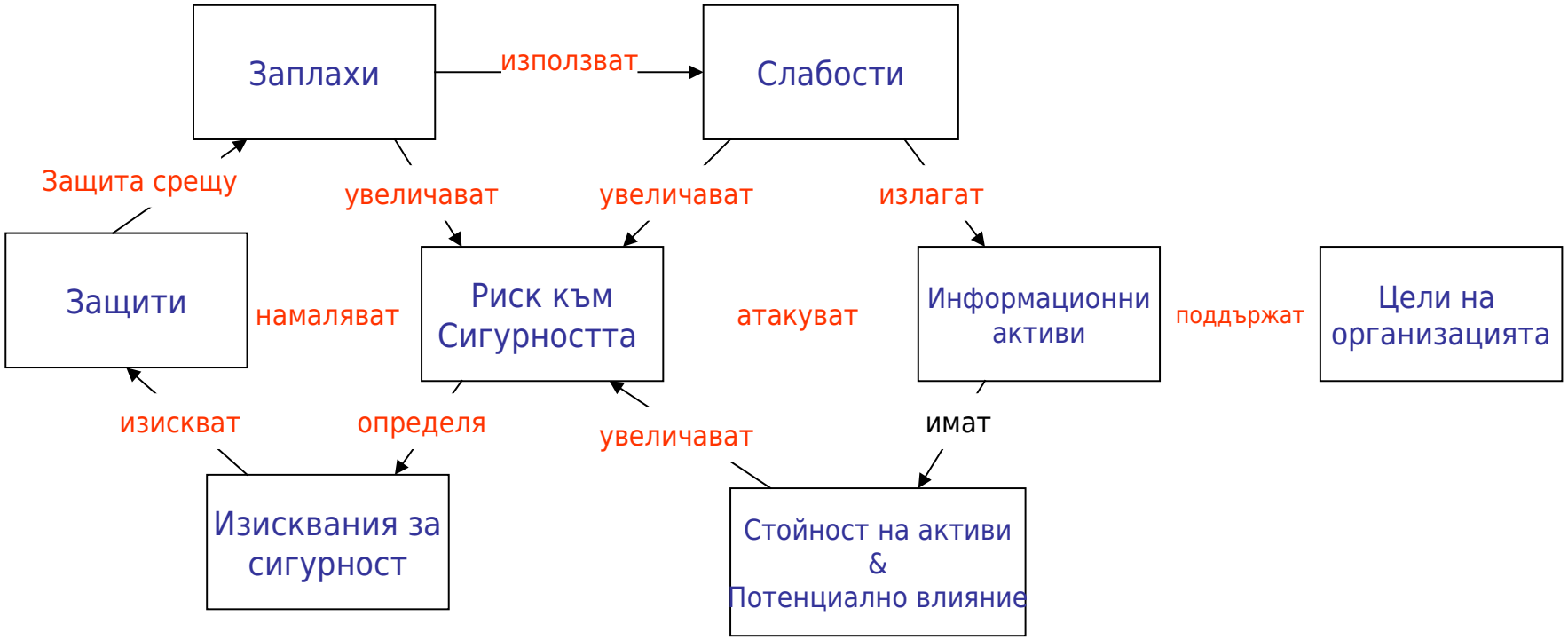
Бизнес звената са отговорни за постигане на необходимата и достатъчна степен на знания на техния персонал, за прилагане на съответните политики за сигурност.

Тези звена обикновено са отговорни, най-малкото за мерките за физическа сигурност и за някои от елементите за управление на непрекъснатостта на бизнеса.

Освен това, когато някои услуги по информационната сигурност се извършват от външна организация, отговорностите за сигурността на информационните активи е винаги в организацията, собственик на тези активи.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 3 - Управление на информационната сигурност – Компоненти на риска към информационната сигурност



Компоненти на риска към сигурността и връзките между тях

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 3 - Управление на информационната сигурност – Компоненти на риска към информационната сигурност

Информационни активи

Актив е всичко, което бизнеса е оценил за важно и/или е важно за някой, извън организацията. По тази причина, организацията трябва да защитава своите активи. Активите включват цялата информация и всичко, което я поддържа, и е необходимо за постигането на целите на бизнеса / организацията.

Примери за такива активи са:

- **информацията и данните**
- **хартиени документи**
- **оборудване и помещения**
- **информационни услуги**
- **персонала и техните знания, и опит**
- **визията, стойността, целите и репутацията на организацията**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 3 - Управление на информационната сигурност – Компоненти на риска към информационната сигурност

Стойност на информационните активи

Най-важните и стойностни информационни активи са тези, които са свързани със същинските и най-критични задължения, способности и цели на организацията. Тяхното разкриване и точно идентифициране на взаимната им свързаност определя най-високите приоритети на бизнеса, свързани със СУИС.

Стойността на информационните активи се представя от гледна точка на потенциалните последствия за бизнеса, възникващи при загубата на тяхната кофиденциалност, цялостност и/или наличност.

Потенциалните последствия включват директни и индиректни финансови загуби (непосредствени и последващи), загуба на приходи, невъзможност за изпълнение на задължения за предоставяне на услуги , загуба на репутация и др.

Индиректните последствия трябва да бъдат също отчетени.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 3 - Управление на информационната сигурност – Компоненти на риска към информационната сигурност

Заплахи

Заплахата е възможен източник на събитие, което може да навреди на бизнеса, чрез въздействие върху информационните активи и способностите, базирани на информацията.

Заплахите могат да имат различна природа – преднамерени и непреднамерени действия, извън или вътре в организацията, природни бедствия и много други.

Голямата част от заплахите се реализират чрез използване на съществуващи и разкрити слабости в информационните активи и поддържащата ги инфраструктура.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 3 - Управление на информационната сигурност – Компоненти на риска към информационната сигурност

Заплахи

Когато заплахата се реализира, произтичат последствия за бизнеса. Една реализирана заплаха, може да повлияе на различни информационни активи и да създаде различни по сила и обхват последствия, вкл. и да създаде нови слабости (уязвимости).

Тези ефекти подкопават в значителна степен бизнеса.

Най-общо казано, заплахата може да причини :

- **разрушаване на актив или способност**
- **кражба, премахване или загуба на активи или способност**
- **разкриване на актив**
- **незаконно използване на актив**
- **прекъсване на предоставянето на услуги**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 3 - Управление на информационната сигурност – Компоненти на риска към информационната сигурност

Заплахи

Някои заплахи могат да се появяват много пъти за час, други по един път на години. Честотата на поява на някои заплахи може да се определи от съществуващите записи във внедрените защити. За други заплахи, честотата на проява се определя от въведени средства за наблюдение и контрол, а в не малко случаи оценката се извършва на база експертно отсъждане.

Препоръчително е да се отчитат данните за честотата на поява на заплахата от различни източници и чак тогава да се определя вероятността.

Много приложимо е състоянието на вероятността за поява на дадена заплаха да се определя, като “най-вероятно”, “най-добър случай” и “най-лош случай”.

Този подход помага осмислянето на заплахите и е предпоставка за въвеждане на количествени методи за нейната оценка.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 3 - Управление на информационната сигурност – Компоненти на риска към информационната сигурност

Уязвимости

Уязвимостите са слабости, свързани с информационните активи или способностите на организацията. Те представляват състояние или набор от състояния, които създават предпоставки, дадена заплаха да въздейства на определен актив (и).

Уязвимост, която не може да бъде използвана от заплаха, или информационен актив, с неизвестна или само предполагаема уязвимост, не е риск към сигурността.

В някои случаи, малки уязвимости в различни системи могат да се обединят, ако тези системи са взаимно свързани.

Това налага провеждането на анализи за взаимната свързаност на уязвимостите, с цел разкриването на техния пълен ефект към информационната сигурност.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 3 - Управление на информационната сигурност – Компоненти на риска към информационната сигурност

Уязвимости

Обикновено уязвимостта е резултат от лоши процедури, персонал със слаби умения и/или дефектни технологии.

За да бъде дадена уязвимост експлоатирана, тя трябва да бъде позната или разкрита от заплахата (източника на заплахата)

От тук произтича важността на прилагането на принципа "необходимост да се знае", отчитайки информацията свързана със сигурността, и прилагането на този принцип към персонала и технологиите.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 3 - Управление на информационната сигурност – Компоненти на риска към информационната сигурност

Риск към сигурността

Риска към информационната сигурност е възможността, дадена заплаха да използва уязвимост на информацията, причинявайки загуба или вреда на информационен актив, и свързаните с него способности, задължения, и като следствие, и на бизнес целите, и дейностите.

Нивото на риска към сигурността се оценява на база комбинацията от вероятността от реализация на идентифицираната заплаха и, ако реализацията се е осъществила, от последствията към способностите на организацията и тяхната стойност.

Връзката между заплахите и последствията от тях е обикновено от типа “много към много”, като някои уязвимости позволяват други уязвимости да бъдат използвани от заплахите.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 3 - Управление на информационната сигурност – Компоненти на риска към информационната сигурност

Риск към сигурността

Анализа на риска, първоначално разглежда заплахите без да отчита съществуващите мерки за противодействие, приложени в организацията. Този подход дава възможност да се разкрият най-важните заплахи, а също и да се въведат приоритети за внедряване и поддръжка на подходящи защити.

След провеждането на първоначалния анализ, може да се извърши оценка на ефикасността на съществуващите защити и да се пристъпи към актуализация на на направения анализ на риска. По този начин се разкрива къде трябва да се извършат подобрения, като най-добре е тези подобрения е да се извършат в начина на опериране на съществуващите защити, а не в насока на постигане на техните теоретични възможности.

Идентифицирането на рискове, за които няма приложени защити, е предпоставка, че те и предвиденото за въвеждане противодействие към тях ще бъдат наблюдавани, и контролирани, в съответствие с изискванията за сигурност.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 3 - Управление на информационната сигурност – Компоненти на риска към информационната сигурност

Изисквания по сигурността

Изискванията за информационна сигурност отчитат, че:

- **ако риска към сигурността се осъществи, това ще предизвика неприемливи за бизнеса последствия;**
- **изискванията за сигурност в законите и договорите въздействат върху организацията, нейния бизнес, партньорите, котрагентите и предоставянето на услуги;**
- **политиките на организацията, нейните принципи, цели и изисквания поддържат нейните способности и стойност**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 3 - Управление на информационната сигурност – Компоненти на риска към информационната сигурност

Изисквания по сигурността

Основния източник за изискванията по сигурността са нуждите на бизнес отделите, които използва информационните активи за да осигурят собствени способности за постигане на поставените бизнес цели.

В този процес е необходимо посредничеството на ръководството, от гледна точка на отчитане на неговия поглед за рисковете към бизнеса.

Нуждите на бизнес отделите са обект на описание в политиките по сигурността, разработени и въведени от организацията.

В допълнение, някои от способностите на бизнес отделите произтичат от общата инфраструктура, осигурявана от ИТ отдела на организацията и / или от услуги, предоставяни от външни организации.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 3 - Управление на информационната сигурност – Компоненти на риска към информационната сигурност

Защити по сигурността

Защитите включват политики, процедури, поведение и технология. Всички те допринасят за защитата на информационните активи срещу заплахите, чрез намаляване на уязвимостта и вероятността от тяхната реализация, или чрез смекчаване на последствията от проявата на неприемливо за бизнеса събитие по сигурността.

Защитите се избират, внедряват и функционират в контекста на цялостната архитектура за сигурност.

Защитите могат да имат различни нива на сила (противодействие). Не съществува единен, възприет подход за дефиниране или измерване на тези нива.

Възможните подходи в това направление включват отчитането на предполагаемото ниво на компетентност на атаките към сигурността или намаляване на вероятността за успех на атаките, до предварително дефинирани приемливи нива.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 3 - Управление на информационната сигурност – Политики за сигурност

Политиката е израз на намеренията.

Разписаната политика е основното средство, чрез което ръководството на организацията осигурява управлението на ръководния, експертен и изпълнителски персонал.

Ефективните политики за сигурност осигуряват ясни направления и ангажираност, а също и създават конкретни функции и отговорности.

Политиката е част от ефективното управление и ръководене на организацията.

Политиките за информационна сигурност осигуряват административното управление и поддръжката, създават оперативните планове и процеси.

Политиките за информационна сигурност са контролна категория (механизъм за защита) в ISO 27001, които трябва да съществуват във всяка СУИС !

Тези политики създават и изискванията за поведение на персонала и последствията от тяхното нарушаване.

Не съществуват точни правила за определяне на съдържанието на политиките за сигурност.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 3 - Управление на информационната сигурност – Политики за сигурност

Терминът 'Политика за сигурност' е обширен и включва въпроси, които не са в обхвата на стандартното разбиране за политика.

Политиката за информационна сигурност включва три основни класа политики:

Политика за изпълнение (или Документ за учредяване на СУИС), подписана на най-високо ниво в организацията – определя ангажираността, целите на бизнеса, целите по сигурността и основните отговорности, свързани със СУИС.

Политика за СУИС – включва планове за управление, описващи детайлно рамката за изграждане и управление на СУИС, а също и принципите за избор и внедряване на защитите.

Оперативни политики – включват процедури, инструкции и планове за управление, внедряване и функциониране на защитите. Тези политики описват защитите, на база избраните противодействия на рисковете към сигурността. Те включват и технически "политики", описващи конфигурирането, настройката и функционирането на конкретните средства за защита.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 3 - Управление на информационната сигурност – Политики за сигурност

Оперативните политики трябва да бъдат съобразени с организацията – обикновено по-малките организации оперират, като цяло с по-малко формализъм от големите, което се отразява и в техните политики.

В допълнение, оперативните политики:

- **са предназначени за широка аудитория – потребители, ИТ персонал и ръководен състав;**
- **са много ясно обвързани с потребностите и целите на бизнеса;**
- **имат различни цели, ниво на детайлност, категоричност в направленията за действие;**
- **изискват прилагането на цикъла "планиране – изграждане – проверка – действие"**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 3 - Управление на информационната сигурност – Политики за сигурност

Когато се разработват различните политики за сигурност, много е важно те да бъдат логически свързани.

Това може да бъде постигнато, като се избягва разработването на голям брой политики, а също, като се приложи една цялостна структура за тях.

Например, Плана за управление на СУИС, осигурява изпълнението на Политиката за архитектурата за сигурност.

Трябва да се отчита и, че големите документи, описващи съответните политики, много рядко са удобни за употреба и прилагане.

Документите трябва да са разработени, отчитайки за кой са предназначени и съответно ясно да определят кой, какво, как, кога и къде трябва да върши.

Политики които са несъвместими с възприетата култура на работа в организацията, по принцип за обречени на провал !

От друга страна, добрите политики, тяхното прилагане и доразвиване са инструмент за повишаване на организационната култура на работа !

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 3 - Управление на информационната сигурност – Политики за сигурност

Ефективната Политика за СУИС трябва да бъде:

- **изпълнима от персонала на организацията, имащ ясно дефинирани отговорности и ред за действие;**
- **процедурно и технически приложима, и съдържаща санкции, когато настъпят нарушения;**
- **въвеждана в експлоатация, чрез процедури, технически и програмни механизми, базирани на документирани ръководства и инструкции;**

Не съществуват окончателно дефинирани, еднакви политики за СУИС, които да бъдат възприети и приложени от различните организации

Идеалния случай е, когато всяка организация разработва своите политики, отчитайки особеностите си, възприетия стил и култура на работа.

Най-добрия подход е да се документират съществуващите практики, след това те са се интегрират и подобрят, с цел постигане на задачите по сигурността

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 3 - Управление на информационната сигурност – Управление на конфигурациите

Всяка действаща СУИС трябва да прилага ефективно управление на конфигурациите. Управлението на конфигурациите в много случаи е изискване на самите защити.

Основните елементи на управлението на конфигурациите са:

- **официален план и процедури;**
- **идентифицирани обекти, подлежащи на управление на конфигурациите;**
- **ред за провеждане на управлението и контрола на промените;**
- **отчетност за статуса на конфигурациите;**
- **одит на конфигурациите**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 3 - Управление на информационната сигурност – Управление на конфигурациите

Механизма на процеса за управление на конфигурациите изисква:

- **Необходимостта от промяна да е ясно дефинирана и да е описана в официално Искане за промяна;**
- **Искането за промяна да е оценено, от гледна точка необходимостта от промяната;**
- **Официално упълномощено лице да реши, дали приема или отхвърля предложението за промяна;**
- **Ако предложението за промяна е прието официално, то промяната трябва да бъде приложена**

Обектите, подлежащи на конфигуриране могат да включват хардуер, софтуер, мрежи и документи от всякакъв тип.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 3 - Управление на информационната сигурност – Ангажираност на ръководството

Много важен фактор за информационната сигурност на всяка организация е реалната поддръжка и ангажираност на ръководството от всички нива на управление.

Това не гарантира успеха, но без него, неуспеха и гарантиран.

Направленията от ръководството на организацията и неговото ангажиране по въпросите на информационната сигурност е фактор за подобряване на културата на работа на персонала.

Ангажираността на ръководството помага и за сериозното възприемане на въпросите по информационната сигурност от целия персонал на организацията.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 3 - Управление на информационната сигурност – Ангажираност на ръководството

Ангажираността на ръководството към информационната сигурност се показва чрез:

- Ефективно и функциониращо ръководство, произтичащо и провеждано от най-високите нива на управление в организацията;

- Въведени в действие политики за сигурност;

- Разработените и прилагани управленски планове за СУИС, определящи в детайли организацията, отговорностите и задълженията;

- Създадена и внедрена в експлоатация СУИС;

- Планирано и осигурено ресурсно осигуряване по информационната сигурност;

- Налични и предоставени на ръководството доклади за функционирането на СУИС, база за подобряване и развитие на информационната сигурност, в съответствие с поставените цели.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 3 - Управление на информационната сигурност – Основни фактори за постигане на успех

В допълнение към ангажираността на ръководството, успешното внедряване на СУИС в организацията зависи и от други фактори:

- Политиките за сигурност и техните цели отразяват изискванията на бизнеса;
- Информационната сигурност е въпрос на бизнеса, тя не е проблем само на ИТ;
- Подхода и рамката за изграждане, внедряване и поддръжка на СУИС е в съответствие с организационната култура и засяга всички, имащи отношение към информационните активи на организацията;
- Рисковете към сигурността се оценяват реалистично;
- Осигурени ресурси за СУИС;
- Наличност и прилагане архитектура за сигурност на организацията;
- Ефективно въвеждане на въпросите по информационната сигурност на всички нива на управление и персонал;
- Обучение на целия персонал, по въпросите на информационната сигурност;
- Създаден и функциониращ процес за управление на инциденти по сигурността;
- Създаден и функциониращ процес за измерване на резултатите от функционирането на СУИС, оценка на нейната ефективност и подобряване на нейните компоненти

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 3 - Управление на информационната сигурност – Основни фактори за постигане на успех

Индикаторите за ефективна СУИС включват:

•Ръководството на организацията изисква и получава регулярно доклади по сигурността -функциониране на изградената СУИС и възникнали събития по сигурността;

•Информационната сигурност неизменно присъствува в дневния ред на ръководството, при оценката на рисковете към бизнеса.

•Нивата на рисковете към информационната сигурност се определят от ръководството и отразяват способността на организацията да приема и понася рискове;

•Ръководителите на бизнес отделите са отговорни за сигурността на информационните активи, осигуряващи функционирането на техния бизнес;

•Рисковете към информацията в основните бизнес процеси са разбрани, оценени и документирани;

•Носи се персонална отговорност за всяко извършено нарушение по сигурността , независимо дали нарушението е преднамерено или непреднамерено;

•Провеждане на регулярни прегледи на продуктите и услугите по информационната сигурност, въвеждани в организацията, с цел оценка на тяхното функциониране и ефективност ;

• Провеждане на регулярни прегледи по въведения в организацията

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

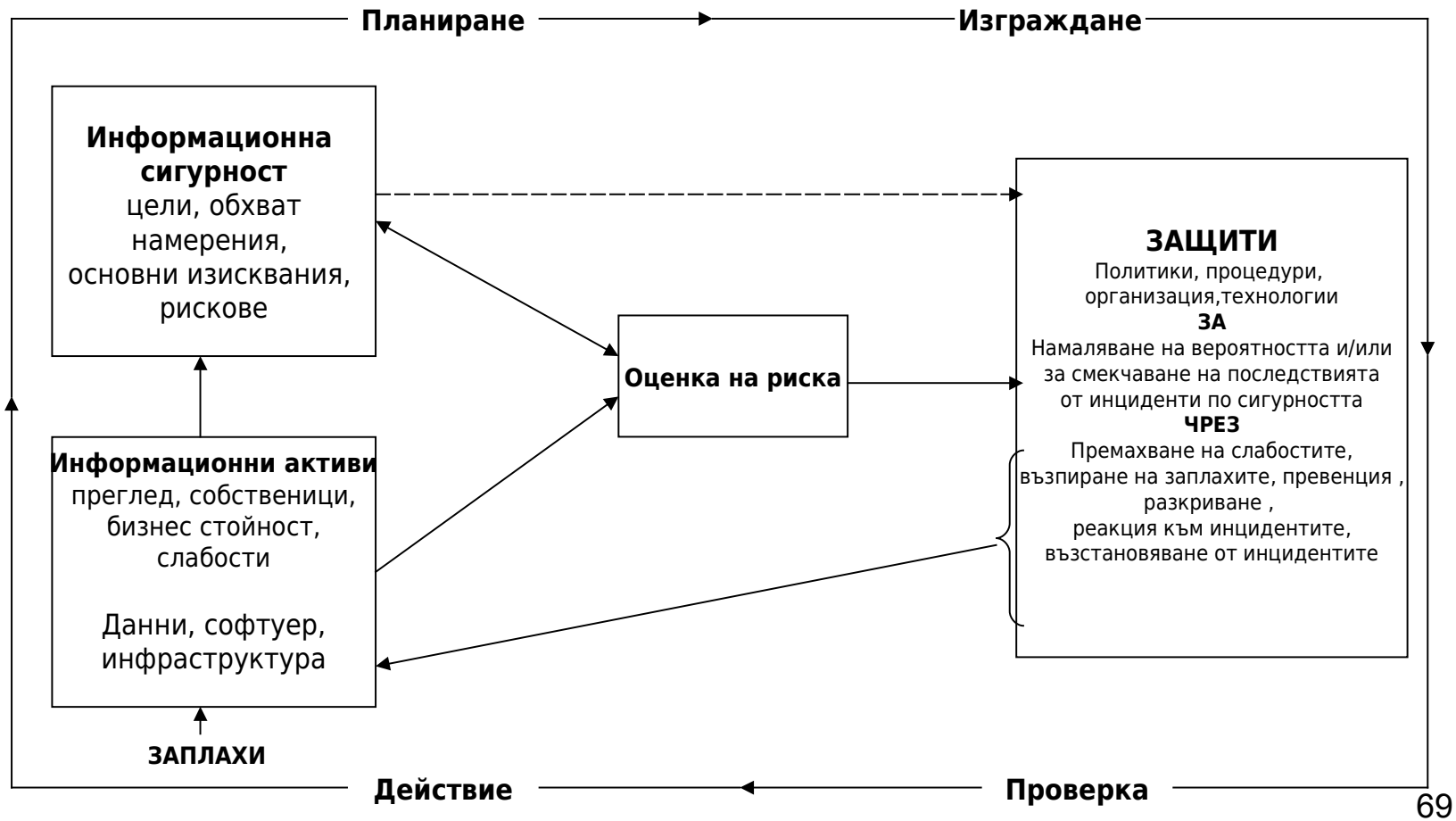
Край на **Част 3 - Управление на информационната сигурност**

За въпроси: Пламен Каменов
Водещ одитор ISO 27001/ ISO 9001 / ISO 20000
e mail: infosecservicebg@gmail.com

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 4: Етап 1 – Рамка на СУИС

Основна рамка на СУИС



ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 4: Етап 1 – Рамка на СУИС - Преглед

Планиране – Изграждане на политиките за сигурност, обектите, целите, процесите и процедурите, свързани с управлението на риска и подобряване на информационната сигурност, с цел постигането на резултати, заложени в политиката и целите на бизнеса / организацията.

За **стартирането** на етапа е необходимо:

- Ангажираност на ръководството за изграждане на СУИС
- Определени и налични ресурси за изпълнението на етапа

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 4: Етап 1 – Рамка на СУИС - Преглед

Изходите от този етап са:

- Съгласуван обхват на СУИС, включващ и определените основи информационни активи, тяхната бизнес стойност , обосновката за техния избор.
- Документ за учредяването на СУИС.
- Първоначален План за управление на СУИС, включващ и организационната структура по информационната сигурност
- Ръководство за управление на риска, необходимо за следващите етапи
- Съгласуван и одобрен План на проекта (за изграждане на СУИС) и определени ресурси за следващите етапи

Важно е, колкото се може по-рано да бъде създаден (приет) стандарт за документацията на СУИС, още повече, че това е стартовата точка за набиране на доказателства при сертифицирането на системата от съответните одитори

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 4: Етап 1 – Рамка на СУИС - Консултации, комуникация и поддръжка

Този етап изисква провеждането на интензивни консултации и комуникация с всички, имащи отношение към информационната сигурност.

Ръководството на бизнеса / организацията трябва да предостави ясни направления и да покаже своята ангажираност чрез официалното одобрение и съгласуване на документа за изграждане на СУИС.

Този документ трябва да бъде одобрен и подписан от Ръководител на организацията от най-високо ниво, а също и да бъде публикуван по начин, достъпен за запознаване от целия персонал на организацията.

Документа за изграждане на СУИС, трябва да бъде неразделна част от програмите за обучение на персонала по въпросите на информационната сигурност

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 4: Етап 1 – Рамка на СУИС - Консултации, комуникация и поддръжка

За провеждането на комуникациите с всички имащи отношение към информационната сигурност, трябва да се разработи и приложи План за комуникация.

Комуникациите трябва да са насочени към разкриването на специфични интереси и виждания по въпросите на информационната сигурност.

При всички случаи Плана за комуникация трябва да се осигури интензивен обмен на информация, мнения и предложения по въпросите на информационната сигурност.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 4: Етап 1 – Рамка на СУИС – Обхват на СУИС

Преди да започне анализа на риска и подготовката на политиките, обхвата на СУИС трябва ясно да бъде определен.

Обхвата определя рамката за останалите процеси за изграждане на СУИС, за които риска трябва да бъде управляван, а също и осигурява направленията за вземане на решения, информирането на организацията, и плановете за ресурсното осигуряване.

Точното и ясно дефиниране на границите на СУИС, позволява да се избегне извършването на дейности, които не са необходими, а също и да се подобри качеството на анализа на риска.

СУИС може да покрива цялата организация или част от нея, отделна системи и/или услуга.

Целта е СУИС да покрива всички части от организацията, в които проблемите по информационната сигурност могат да доведат до неприемливи последствия за бизнеса и организацията, като цяло.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 4: Етап 1 – Рамка на СУИС – Обхват на СУИС

Определянето на обхвата на СУИС изисква разбирането и познаването на:

- информационните активи на бизнеса / организацията
- бизнес способностите, зависещи от тези информационни активи
- стойността на информационните активи и тяхната важност за бизнеса

Постигането на тази задача, налага интензивен обмен на информация с всички, имащи отношение към информационната сигурност в организацията.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 4: Етап 1 – Рамка на СУИС – Обхват на СУИС

Определянето на обхвата на СУИС има за цел да изясни:

- Кои способности на организацията разчитат на конфиденциалността, цялостта и наличността на информацията, при вземането на решения ?
- Кои са въпросите, които трябва да се разгледат при оценката на рисковете към информационните активи?
- Коя информация трябва трябва да бъде защитаване?
- Какви критерии ще се прилагат при оценката на риска?
- Какви са изискванията за информационна сигурност в организацията?

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 4: Етап 1 – Рамка на СУИС – Обхват на СУИС

Основните компоненти при определянето на обхвата на СУИС са:

- определянето на външния контекст на риска;
- определяне на вътрешния контекст на риска;
- разработване критерии за оценка на риска;
- определяне на структура за управление на риска;
- определяне на най-важните информационни активи.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 4: Етап 1 – Рамка на СУИС – Рискове и критерии за тяхната оценка

Контекста на риска е важен елемент при определянето на обхвата на СУИС и при разработването на съответните политики на най-високо ниво. На този етап трябва да се разработят основното направление и указания за оценка на риска.

Определяне на външния контекст на риска

Този компонент отразява обкръжението в което функционира организацията. Организацията трябва да определи критичните елементи, които могат да поддържат или да намаляват нейните възможности за управление на рисковете към информационната сигурност.

Всяко решение, свързано с управлението на риска към информационната сигурност трябва да бъде в съответствие със състоянието на обществения сектор и обкръжението в което функционира организацията.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 4: Етап 1 – Рамка на СУИС – Рискове и критерии за тяхната оценка

Определяне на външния контекст на риска

Организацията трябва добре да познава и разбере:

- своите силни страни, слабости, възможности и заплахите към нея;

- своите външни партньори, отчитайки техните цели и разбирания по сигурността;

- финансовите, оперативните, политическите, социалните, културните и правните аспекти, свързани с нейното функциониране;

- конкуренцията и клиентите

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 4: Етап 1 – Рамка на СУИС – Рискове и критерии за тяхната оценка

Определяне на вътрешния контекст на риска

Този компонент изисква много добро познаване и разбиране на организацията – нейната структура, функции, способности, цели и стратегии за тяхното постигане.

Познаването на организацията облекчава и подпомага процеса за определяне, дали даден риск е приемлив или неприемлив, а също и формира базата за определяне на защитите на информационните активи.

Природата на информационните активи на организацията, тяхната “видима” и “невидима” стойност са част от организационния контекст на риска.

Много важен момент е и определянето на всички членове (персонал) на организацията, имащи отношение към информационната сигурност.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 4: Етап 1 – Рамка на СУИС – Рискове и критерии за тяхната оценка

Разработване на критерии за оценка на риска

С цел да се оцени риска, неговото влияние, последиците и избора на защити, трябва да се определят и използват количествени и/или качествени критерии.

Разглеждането на този въпрос се извършва в съответствие с нивото на риск, което организацията ще толерира. Степента на този толеранс ще се отрази в определенията, използвани в критериите за оценка на риска.

Критериите трябва да се разработят, но един път създадени и приети, те стават част от политиката за сигурност и подлежат на периодичен преглед и анализ. Много е важно, съответните критерии да бъдат определени още в началото на оценката на риска и в последствие да бъдат преглеждани чрез процесите за оценка на риска.

Критериите за оценка на риска могат и трябва да бъдат допълнително развивани и доуточняване, с цел постигане на адекватност с реалните рискове и техните нива.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 4: Етап 1 – Рамка на СУИС – Рискове и критерии за тяхната оценка

Разработване на критерии за оценка на риска

Критериите за оценка на риска включват:

- **Типовете последствия (оперативни, финансови, доставка на услуги, клиенти, репутация и др.)**
- **Определяне на вероятността и нивата (количествено и/или качествено)**
- **Определяне на последствията и нивата (количествено и/или качествено)**
- **Изчисляване на степените (произведение от вероятността и последствията)**
- **Приемливост, противодействие и приоритети на риска**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 4: Етап 1 – Рамка на СУИС – Рискове и критерии за тяхната оценка

Разработване на критерии за оценка на риска

Факторите, които влияят при разработването на критериите включват:

- **държавната политика;**
- **политиките и целите на организацията;**
- **очакванията на потребителите и всички, имащи отношение към в сигурността;**
- **правните изисквания;**
- **“ апетита” на организацията за приемане на риск и всички зони с нулева толерантност към нивото на риска**

Решенията, относно приемливото ниво на риска и последващите противодействия могат до се базират на оперативни, технически, финансови, правни, социални, хуманитарни или други критерии.

Много от рисковете имат различни по тип последствия. Повечето от рисковете имат последствия, свързани с финансите и репутацията на организацията.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 4: Етап 1 – Рамка на СУИС – Харта за СУИС

Подписаната на най-високо ниво в организацията Харта за СУИС излага бизнес целите, обхвата на СУИС, основните изисквания и отговорности за управление на информационната сигурност.

Хартата показва ангажимента на ръководството към целия персонал и всички останали, имащи отношение към бизнеса/дейностите и сигурността.

Тя може също да съдържа и описва:

- **контекста на рисковете, основните бизнес активи, стойности и способности;**
- **политиката за "собственост" на информационните активи;**
- **бизнес ориентирано ръководство за оценка на риска, включващо и финансови оценки;**
- **ръководство за приоритетите по сигурността и степените на защита;**
- **основата за обосновка на разходите по сигурността в термините на бизнеса**

На практика, Хартата за СУИС може да бъде / или е част от документа "Политика за СУИС"

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 4: Етап 1 – Рамка на СУИС – Политика за СУИС

Общата Политика за СУИС представлява план за управление и заедно с архитектурата за сигурност – ниво "Контекст" е основата за изграждане на СУИС

Тази политика е втората основна стъпка (след Хартата за СУИС) в процеса на изграждане на култура за сигурност, чиято цел е да убеди всеки един от персонала за необходимостта от сигурност, а също и да го запознае за неговата персонална роля и функции по сигурността.

Дейностите по подготвителното управление на риска са база за оперативните политики за сигурност, които от своя страна водят до по детайлно управление на риска и разработване на планове за информационна сигурност.

Ръководството на организацията решава за нивата на приемливия риск към бизнеса / дейностите, което от своя страна може да определи ресурсите, необходими за изграждането и внедряването на СУИС.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 4: Етап 1 – Рамка на СУИС – Политика за СУИС

Политиката за СУИС определя на най-високо ниво рамката за управление на риска. Разработването на тази политика изисква предварителното извършване на дейности по управление на риска:

- **определяне на контекста на риска, от гледна точка на бизнеса;**
- **отчитане на изискванията на бизнеса, правната уредба, регулациите и контрактите;**
- **определяне на подход за управление на риска и критерии за оценка на риска**

Политиката за СУИС трябва също да определи информационните активи, които подлежат на защита, подхода за управление на риска, целите по контрола и съответните защити, степента на изискваната сигурност.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 4: Етап 1 – Рамка на СУИС – Структура за управление на сигурността

Структурата за управление на сигурността трябва да бъде изградена, попълнена с персонал и да има ясно определени отговорности по сигурността.

Необходимо е да се планират взаимовръзките между отговорните за СУИС и тези за управлението на информацията, информационните системи, управлението на риска и физическата сигурност.

В Политиката за СУИС се определя организацията за управление на сигурността

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 4: Етап 1 – Рамка на СУИС – Структура за управление на сигурността

Отговорности и права

Отговорностите, правата и взаимовръзките на персонала (или контракторите) които изпълняват и проверяват работата, влияеща на управлението на информационната сигурност, трябва да бъдат дефинирани и документирани, особено за персонала, който трябва да има относителна организационна свобода, за да извършва едно или повече от следващите дейности:

- **установяване на областите в които риска към сигурността трябва да бъде управляван;**
- **започване на действия за предпазване или намаляване на рисковете;**
- **управление на последващите противодействия на риска, до постигане на нива на риск, приемливи за организацията;**
- **установяване и записване на всички проблеми, свързани с управлението на риска;**
- **започване, препоръчване или осигуряване на мерки за сигурност;**
- **проверка на внедрените мерки за сигурност;**
- **комуникации и консултации – вътрешни и външни – по сигурността**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 4: Етап 1 – Рамка на СУИС – Структура за управление на сигурността

Отговорности и права

Като правило, отговорността за сигурността на информацията остава в ръководството на организацията (напр. отговорност на Изпълнителния директор). Всички членове на ръководството споделят отговорностите по иницииране и контрол на внедряването на ефективна система за информационна сигурност в организацията.

Политиката за СУИС трябва да определи точно функционалните задължения, отговорности и права в организацията. Когато е необходимо, в това отношение Политиката за СУИС може да бъде допълнена с по - детайлни ръководства за определени системи, услуги и обекти.

Ограничените отговорности за отделни физически и информационни активи, и процеси по сигурността (напр. планиране то на непрекъсваемостта на бизнеса / дейностите) трябва да бъдат също много ясно определени и документирани.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 4: Етап 1 – Рамка на СУИС – Структура за управление на сигурността

Отговорности и права

За всеки информационен актив, трябва да има точно определен отговорник по сигурността. Този отговорник е ежедневно е отговорен за сигурността на съответния информационен актив.

Тази отговорност може да бъде делегирана и към отделен ръководител в организацията. Но, независимо от това, отговорника по сигурността на информационния актив остава отговорното лице, което може да определи, че всяка друга делегирана отговорност е била изпълнена коректно, в съответствие с изискванията за сигурност.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 4: Етап 1 – Рамка на СУИС – Структура за управление на сигурността

Отговорности и права

Задачите на структурата за управление на сигурността (вкл. до най-високо ниво на ръководство) обикновено включва:

- **управление на СУИС на организацията;**
- **наблюдение за възникнали промени в рисковете към информационната сигурност;**
- **осигуряване на съвети в областта на рисковете към информационната сигурност и мерките за контрол и противодействие;**
- **преглед и ревизия на политиките и плановете за информационна сигурност;**
- **наблюдение и прегледи на мерките за информационна сигурност;**
- **подпомагане на дейностите по управление на инциденти по информационната сигурност;**
- **събиране на информация от докладите по информационната сигурност**
- **подпомагане и поддръжка на програмата за обучение по сигурността**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 4: Етап 1 – Рамка на СУИС – Структура за управление на сигурността

Отговорности и права

Състава на Структурата за управление на сигурността зависи от големината на организацията и възможните рискове към нея. Основна роля в структурата има специално определен/назначен служител, отговорен за всички въпроси по информационната сигурност в цялата организация.

Служителя по информационната сигурност би трябвало да има достатъчно права и директен достъп до ръководството, в случаите, когато се изисква приемането на спешни мерки по сигурността.

Независимо от това, отговорностите за ресурсното осигуряване и внедряването на защити на информационните активи, обикновено остава в отделните ръководители на организацията.

При големи организации, за съгласуване изграждането на структурата е необходимо да се проведат интензивни комуникации и консултации с различни звена и техните ръководители.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 4: Етап 1 – Рамка на СУИС – Структура за управление на сигурността

Структура за оценка на риска към информационните активи

В зависимост от природата на рисковете и обхвата на тяхната оценка, структурата за оценка на риска може да бъде съставена от няколко елемента. Тези елементи трябва да осигурят логическата рамка за идентифициране и анализ на рисковете, като не допуска пренебрегването на съществени рискове към информационните активи на организацията.

Тази структура трябва да се базира на:

- **функциите и/или дейностите на организацията;**
- **типовете информационни активи на организацията;**
- **организационната структура;**
- **физическото местоположение на организацията;**
- **проектите, които изпълнява организацията**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 4: Етап 1 – Рамка на СУИС – Структура за управление на сигурността

Структура за оценка на риска към информационните активи

Структурата трябва да бъде подчинена на ръководството от най-високо ниво, за да може тя да има реалистичен поглед за функциите, дейностите, приоритетите и бизнес целите на организацията, а също и да се осигури подкрепата на ръководството при провеждането на нейните дейности.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 4: Етап 1 – Рамка на СУИС – Ресурсно осигуряване на СУИС

Осигуряването с персонал, занимаващ се с въпросите на информационната сигурност зависи от големината на организацията и нейните изисквания по сигурността.

Изграждането на СУИС се извършва като изпълнение на проект. Когато СУИС се изгради и внедри, това вече не е проект, това е система.

В големите организации обикновено се назначава обособен по сигурността персонал на пълно работно време. Разбира се, ръководството на организацията от всички нива участва с определен времеви ресурс в процесите на планиране (препланиране) проверка, контрол и развитие на СУИС.

Ръководството на организацията е отговорно за осигуряването на адекватни ресурси за изпълнението на Програмата за СУИС.

Ръководството на организацията трябва да осигури, че персонала работещ по сигурността има необходимите умения и знания за надеждно изпълнение на съответните функции и задачи.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Край на **Част 4: Етап 1 – Рамка на СУИС**

За въпроси: Пламен Каменов
Водещ одитор ISO 27001/ ISO 9001 / ISO 20000
e mail: infosecservicebg@gmail.com

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Общ преглед

Управлението на риска към информационната сигурност е систематично прилагане на политики за управление, процедури и практики към задачите за определяне на контекста, разкриването, анализирането, оценяването, противодействието и комуникирането на този риск.

Първите стъпки по управлението на риска се изпълняват в предишния етап, където се определя контекста на риска и са направени първите консултации с всички заинтересувани.

В този Етап 2, рисковете са разкрити и определени, оценени, и е планирано противодействието към тях.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Общ преглед

Входните данни за този етап са изходите от Етап 1.

Изходите от дейностите по Етап 2 са:

- **Съгласуван и одобрен План за противодействие на риска.**
- **Концептуалното и логическо ниво на Архитектурата за сигурност.**

Планирането на противодействието на риска към информационната сигурност е продукт (резултата) от Плана за СУИС на организацията и съответните процедури, инструкции и ръководства, а също и на изпълнението на процесите за управление на риска.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Консултации, комуникации и поддръжка

Консултациите и комуникациите се извършват през целия етап, с цел:

- **постигане на адекватност на СУИС с нуждите на бизнеса;**
- **събиране и обобщаване на опита и знанията по сигурността от всички заинтересовани;**
- **определяне на приоритетите за противодействие;**
- **развитие и прилагане на действия за запознаване с въпросите на сигурността на целия персонал;**
- **избягването на “изненади” за ръководството на организацията.**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Важност на документацията

Документирането на всяка стъпка в процеса на управление на риска към информацията е задължително, поради следните основни причини:

- **за доказване, че процеса се извършва коректно, съгласно приетата методика и подход в организацията;**
- **за осигуряване на аргументи и доказателства, относно предприетите решения, действия и обработки;**
- **за осигуряване на механизъм за търсене на отговорност;**
- **за подпомагане на провеждането на наблюдения и контрол по сигурността;**
- **за осигуряване на възможности за провеждане на одити по сигурността;**
- **за споделяне и обмен на информация.**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Важност на документацията

Обхвата и съдържанието на документацията зависи от нормативните изискания, стойността на усилията за нейното разработване и ползите за организацията от нея.

Организацията трябва да възприеме практически реализуем и икономически обоснован подход за документиране на процеса и резултатите от него.

Сертифицирането на СУИС, в съответствие с изискванията на ISO 27001 превръща документирането в много съществен процес.

В този смисъл документацията на процеса, трябва да бъде планирана, проектирана и да започне да се създава още със стартирането на процеса.

Плана за управление на СУИС би трябвало да осигури архитектурата на съпровождащата документация, ако не съществуват възприети ред и правила в това отношение в организацията.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Важност на документацията

Както за всяка друга документална система, организацията би трябвало да създаде и поддържа процедури за контрол на документите и за съответните отговорности с цел постигане на:

- **достъпност и наличност на текущите документи;**
- **периодичен преглед, обновяване и публикуване на текущите документи;**
- **сигурност, че старите версии на документите са ясно отменени, идентифицирани и запазени за последващо разглеждане при необходимост;**
- **прилагане на управление на конфигурациите на документите**

Организацията трябва да създаде и поддържа процедури за идентифициране, поддръжка, запазване и разполагане на записи, представляващи доказателства за изпълнение на изискванията на СУИС.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Важност на документацията

Всички документи и записи, свързани със съответните дейности, трябва да бъдат ясни, недвусмислени, да могат да бъдат идентифицирани и да създават възможност за проследимост.

Те трябва да бъдат съхранявани и поддържани по начин, защитаващ ги от преднамерено и/или случайно разрушаване, промяна и/или загуба.

Цялата документация свързана с действието на защитните механизми в СУИС, представлява информационен актив и трябва да се разпространява, спазвайки, най-малко, принципа “необходимо да се знае” !

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 1 – Определяне на подход за оценка на риска – Окончателно определяне на контекста на управлението на риска

Изходите от тази стъпка са :

- **План за изпълнението на Етап 2 “Управление на риска”.**
- **Определяне на информационните активи на организацията**

В Етап 1 са определени на първо ниво външния и вътрешен контекст на управлението на риска; обхвата на СУИС и основните критерии за управлението на риска.

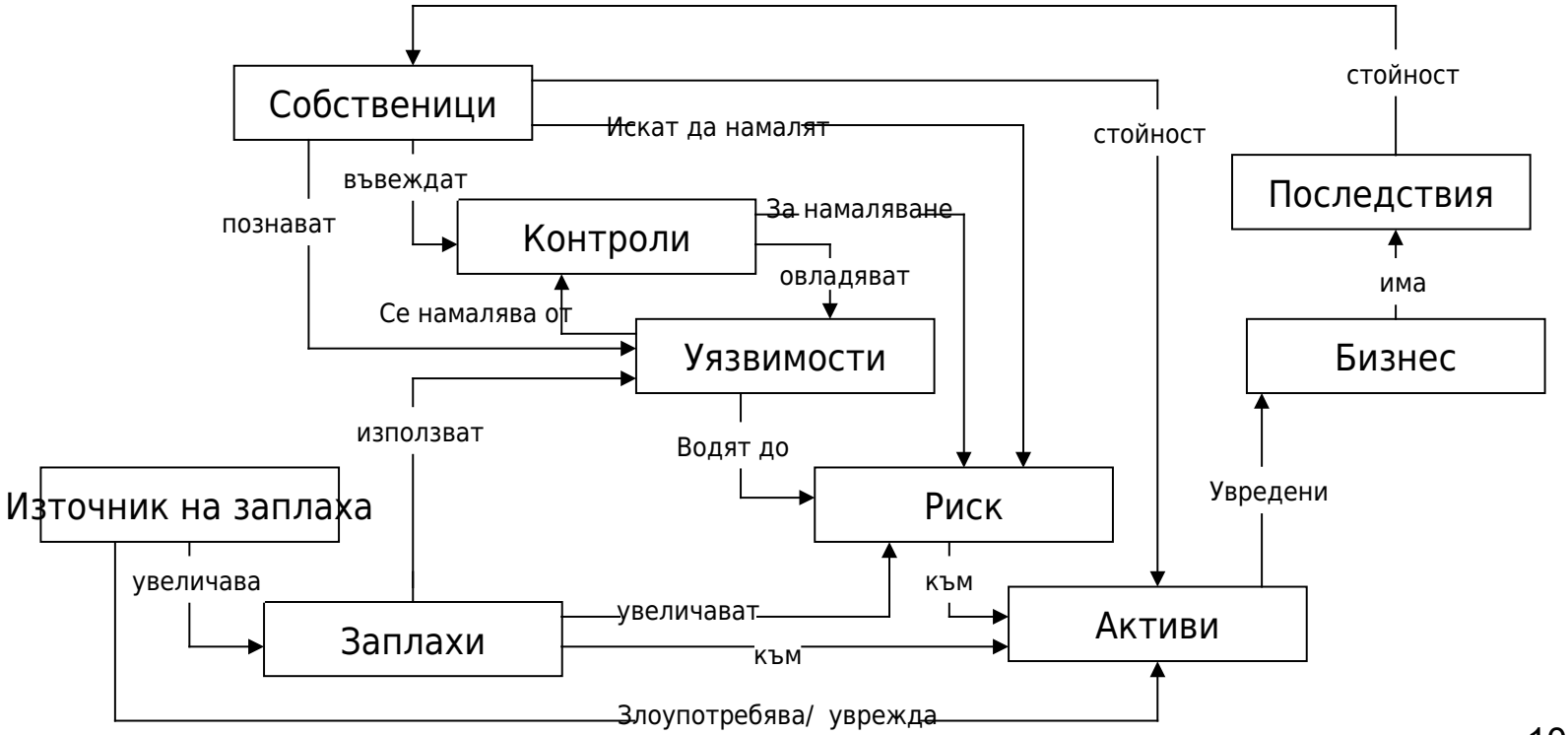
В Етап 2 се извършва окончателното определяне на контекста на управлението на риска.

На следващата фигура е показан основния контекст по сигурността на управлението на риска.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 1 – Определяне на подход за оценка на риска – Окончателно определяне на контекста на управлението на риска

Основен контекст по сигурността - взаимовръзки



ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 1 – Определяне на подход за оценка на риска – Определяне на информационните активи

Най – важните информационни активи са тези, осигуряващи дейностите на организацията, пряко свързани с постигането на нейните цели и задачи.

Информационните активи са част от системи или способности , използвани от организацията за постигане на нейните цели. Поради това, те трябва да бъдат защитавани, от гледна точка на сигурността. Информационните активи могат да бъдат идентифициране на база регистрите и архитектурата на организацията, а също и от плановете, свързани с информационните и комуникационни технологии.

При определянето на информационните активи, информацията трябва да се разглежда в по-широк смисъл, а не само в контекста на ИТ и свързаните с нея хардуер и софтуер.

Напълно приложимо е управлението на риска да бъде съобразено с различните типове информационни активи.

Всички информационни активи, определени в контекста на управление на риска, трябва да се идентифицират в необходимата детайлност. Това налага познаването на тяхната важност и приоритет за сигурността.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 1 – Определяне на подход за оценка на риска – Определяне на информационните активи

Списъка на определените на информационни активи включва следната информация :

- **идентификатор на актива;**
- **описание на актива;**
- **тип на актива;**
- **собственик на актива (отговорник по сигурността на актива)**
- **местоположение на актива**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 1 – Определяне на подход за оценка на риска – Класификация на информацията и означаване

Информацията се обозначава, като класифицирана, на база възприетите критерии за класификация от организацията.

На базата на тази класификация се вземат и решенията за необходимото и достатъчно ниво на защита на информацията.

Много е важно да се зачитат правилата за класификация на информацията, приложени от нейния създател (на информацията).

Степента на класификация на получената от външна организация информация не трябва да се променя, без изричното разрешение на организацията – подател и създател на информацията.

Не трябва да се “преиграва” с класифицирането на информацията, тъй-като това може да доведе до по-голяма стойност на защитите от стойността на възможните последствията при пробив на сигурността.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 2 - Провеждане на оценка на риска – Определяне на рисковете

Изхода от тази стъпка цялостно извършена оценка на риска.

Целта на Стъпка 2 е да определи, класифицира и да опиша всички рискови събития, уязвимостите и заплахите, които могат да имат ефект към информационните активи, определени в Стъпка 1.

При изпълнението на тази дейност могат да се използват и мненията на всички заинтересовани – от организацията и извън нея. Могат да се разработват и различни оперативни сценарии по сигурността. От голяма важност е разкриването и определянето на рисковете да се извърши без да се отчитат въведените и/или планирани за въвеждане защитни механизми.

Определянето на рисковете трябва да се извършва по утвърдена и документирана от организацията методика, като се включват и рисковете, извън контрола на организацията.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 2 - Провеждане на оценка на риска – Определяне на рисковете

Много често, рисковете, заплахите и уязвимостите имат ефект върху цялостта, конфиденциалността и наличността на информацията, не само по отделно, но и в различните им комбинации.

Вниманието трябва да се насочи към природата и източника на риск (заплаха). Трябва да се търси и намери отговор на въпросите:

- **Какво би могло да се случи?**
- **Как би могло да се случи?**
- **Защо би могло да се случи?**
- **Кой или какво ще бъде засегнато директно и/или индиректно?**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 2 - Провеждане на оценка на риска – Определяне на рисковете

Добрата практика определя риска в три основни състояния. Това би могло да се опише в табличен вид с три колони за информация – “източник”, “събитие” и “последствия”

Друг алтернативен начин на описание е : Реализирането на заплаха “……” чрез уязвимост “……”, създава риск, за възникване на събитие по сигурността “……” със следните последствия за бизнеса “……”

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 2 - Провеждане на оценка на риска – Анализ на риска

Анализа на риска определя вероятността за риск и последствията от него, като комбинацията от тях служи за оценка на цялостното ниво на риск.

Чрез този анализ се отделят приемливите за организацията малки рискове от тези, които не са приемливи, а също се осигуряват данни, необходими за противодействието на риска.

По време на този първоначален анализ, нивото на риска се определя, без да се отчитат внедрените в организацията защитни механизми. Игнорирането на внедрените защитни механизми спомага за идентифицирането на най-важните рискове, които впоследствие ще бъдат и наблюдавани като такива, дори при внедрени защитни механизми срещу тях.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 2 - Провеждане на оценка на риска – Анализ на риска

Анализ на риска може да бъде качествен, количествен или полу - количествен. В повечето случаи се използва качествен анализ, при който скалата на вероятностите, последствията и нивата на риска са точно и ясно определени. Използват се и полу-количествени методи, при които също се присвояват числа (обикновено между 0 и 1) към качествената скала.

Когато риска може да бъде представен в количествени измерения, би трябвало да се използват количествени методи за анализ. Основното правило, което трябва да се пазва е методът за анализ да бъде практически приложим и съобразен с нуждите на организацията. Количествените методи водят към използването на вероятностни методи за оценка на възвръщаемостта на инвестициите в сигурността.

Какъвто и метод да се използва, много важно е да се използват съгласувани определения. Когато се остойностява вероятността или последствията, те трябва да бъдат на ниво "най-вероятно", а не "най-добър" или "най-лош" случай. Когато оценяваме вероятностите, важно е да се определи времевия период за потенциалното възникване на дадено събитие, например вероятността за възникване на събитие XXXXX в рамките на период от 5 години.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 2 - Провеждане на оценка на риска – Анализ на риска

Вероятността и последствията се комбинират за определянето на цялостното “ниво на риска”. Нивата на риска не са абсолютни, те са различни за различните организации, имащи различни нива за приемливост на риска.

Съществуват много и различни източници, които могат да са полезни при оценката на последствията и вероятностите на риска. Те могат да включват:

- **Записи за извършени оценки на риска.**
- **Актуален опит при възникнали събития по сигурността**
- **Практики и опит в индустрията**
- **Изследвания и разработки**
- **Оценки на експерти и специалисти**
- **Статистически анализи и др.**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 2 - Провеждане на оценка на риска – Анализ на риска

Препоръчителен подход

Анализа на рисковете към сигурността на информационните активи може да отнеме много време. Един от най-ефективните подходи за анализ на риска е комбинирането на идентифицирането на риска, неговата оценка и противодействия.

Този комбиниран подход налага извършването на първоначален, на високо ниво анализ на риска към информационните активи, с цел разкриване на общите рискове, за които има ясно определени противодействия и практики (базови механизми за защита).

За другите типове специфични рискове е необходимо да се проведе допълнително детайлен анализ.

Този подход има предимство, изразяващо се в това, че вниманието се насочва към рискове, които не се разбират добре или не са много сериозни.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 2 - Провеждане на оценка на риска – Анализ на риска

Анализ на риска на високо ниво

Този компонент отчита бизнес стойността на информационните активи и рисковете, от гледна точка на бизнеса.

За да се определи необходимостта от допълнителен анализ трябва да се отчетат:

- **Бизнес целите, постигани чрез информационните активи;**
- **Степента на зависимост на способностите на организацията от информационните активи – от тяхната конфиденциалност, цялостност и наличност;**
- **Обема инвестиции в информационните активи – доставка, разработване, поддръжка, инфраструктура и др.**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 2 - Провеждане на оценка на риска – Анализ на риска

Анализ на риска на високо ниво

Ако бизнес целите, осигурявани от даден информационен актив са важни за бизнеса на организацията, средствата за възстановяване са големи или нивото на риска е високо, то тогава е необходимо провеждането на детайлен анализ на риска.

Всяко едно от по-горе посочените условия, може да бъде достатъчно за вземането на решения за детайлен анализ на риска.

Като правило, детайлния риск анализ, от който се определят възможните противодействия на заплахите, винаги е необходим, ако липсата на информационна сигурност може да доведе до вреди на организацията, нейните бизнес способности и / или активи.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 2 - Провеждане на оценка на риска – Анализ на риска

Анализ на риска на високо ниво – Остойностяване на информационните активи (и на възможните последствия)

За подпомагане на процеса на идентифициране на рисковете трябва да бъде постигнато необходимото разбиране за стойността и важността на информационните активи.

Всеки информационен активи или група от активи има различни изисквания за защита на неговите конфиденциалност, цялостност и наличност.

Организацията е длъжна да осигури степен на защита, съответстваща на стойността и важността на информационните активи, и на последствията от пробиви на сигурността спрямо тях.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 2 - Провеждане на оценка на риска – Анализ на риска

Анализ на риска на високо ниво – Остойностяване на информационните активи (и на възможните последствия)

Възможните последствия, предизвикани от пробиви по сигурността на информационните активи трябва да бъде структурирани по определени принципи и критерии. Един възможен подход за структуриране на последствията е показан по-долу. Това структуриране трябва да се прилага поотделно при нарушаването на конфиденциалността, цялостта и наличността:

Финансови	Оперативни	Клиенти и общество	Персонал
Загуба на приходи	Загуба на способности	Закъсняло обслужване	Морални загуби
Загуба на активи	Нарушения на нормативи	Зле настроени клиенти	Загуба на продуктивност
Задължения по договори	Прекъснати дейности	Загуба на репутация	Вреди / увреждания
Извънбюджетни плащания	Загуба на управление	Материални щети	

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 2 - Провеждане на оценка на риска – Анализ на риска

Анализ на риска на високо ниво – Остойностяване на информационните активи (и на възможните последствия)

Всички последствия могат да създадат и допълнителни финансови загуби, освен тези описани изрично, като такива.

Избягването на тези финансови загуби е сериозна полза за бизнеса / организацията.

Монетарната стойност, присвоена на информационен актив или група от активи трябва да бъде максималната сума от стойностите на някои или на всички възможни стойности, базирани на (например):

- **цената за придобиване, заместване, или възстановяване;**
- **наказанията и/или щетите произтичащи от нарушаване на нормативната уредба;**
- **потенциалните загуби на приходи**
- **потенциалните загуби от щети, произтичащи от разкриване, подмяна, промяна и/или унищожаване на информация**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 2 - Провеждане на оценка на риска – Анализ на риска

Анализ на риска на високо ниво – Остойностяване на информационните активи (и на възможните последствия)

Всичко казано до тук, по отношение остойностяването на информационните активи, показва съществуването на няколко, основни типове стойности за тях:

- **Монетарна стойност, обикновено свързана с материалните активи, и отразяваща стойностите за замяна, обезценяване и др.**
- **Скрита стойност, може да отразява усилията за създаване на информация или нейната пазарна стойност**
- **Стойност за конкуренцията - знания или интелектуална собственост в организацията, които имат висока стойност за други организации и/или лица, нямащи легитимни права за тяхното ползване**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 2 - Провеждане на оценка на риска – Анализ на риска

Анализ на риска на високо ниво – Остойностяване на информационните активи (и на възможните последствия)

Стойността на взаимно зависими активи може да бъде модифицирана, както следва:

- **ако стойността на зависимия актив (напр. данни) е по-малка или равна на стойността на основния актив (напр. софтуера, създаващ данните), то основния актив не променя своята стойност**
- **ако стойността на зависимия актив (напр. данни) е по-голяма от стойността на основния актив (напр. софтуера, създаващ данните), то основния увеличава своята стойност – съобразно степента на зависимост между двата актива, или му се присвоява стойността на зависимия актив**

При остойностяването на взаимно зависими активи, трябва да се отчита и техния брой, и разположение – напр. брой копия на софтуера, създаващ данните

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 2 - Провеждане на оценка на риска – Анализ на риска

Детайлен анализ на риска – Оценка на заплахите и уязвимостите

За информационните активи, за които се изисква провеждането на детайлен анализ на риска, се извършва и анализ на заплахите и уязвимостите.

Информационните активи са обект на много и различни по тип заплахи.

Заплахите могат да произтичат от вътрешен и/или външен за организацията източник.

Влиянието на инцидентите по сигурността могат да бъдат временни или постоянни.

Уязвимостите могат да бъдат във физическото обкръжение на информационните активи, процедурите, персонала, управлението и администрирането, хардуера, софтуера и комуникациите.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 2 - Провеждане на оценка на риска – Анализ на риска

Детайлен анализ на риска – Оценка на заплахите и уязвимостите

Вероятността дадена заплаха да се реализира трябва да се оценява за определен времеви период. Оценката на заплахите трябва да отчита и да е съобразена най-малко с:

- **източника на заплаха, неговата мотивация и ресурси;**
- **стойността на усилията за неупълномощен достъп;**
- **географския фактор (за заплахи, произтичащи от околната среда)**
- **честотата на поява на заплаха**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 2 - Провеждане на оценка на риска – Анализ на риска

Детайлен анализ на риска – Оценка на заплахите и уязвимостите

Примери за типични уязвимости :

- **незащитени комуникационни връзки ;**
- **процесите за автентикация на отдалечени потребители;**
- **необучени потребители;**
- **необучен персонал;**
- **лош подбор, използване и/или управление на пароли;**
- **лош контрол на достъпа (логически и/или физически);**
- **лошо конфигурирани защити;**
- **познати дефекти по сигурността на софтуерни продукти, които не са елиминирани;**
- **широко достъпна информация по информационната сигурност**
- **липса на back-up копия на информацията и/или софтуера**
- **разположение в регион, предразположен към наводнения и/или други природни бедствия**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 2 - Провеждане на оценка на риска – Анализ на риска

Детайлен анализ на риска – Оценка на заплахите и уязвимостите

Някои заплахи и уязвимости, могат да въздействат на повече от един информационен актив. Те могат да предизвикат и различни последствия, в зависимост от типа на засегнатите информационни активи.

За важните информационни активи, може да се наложи декомпозиране на риска, с цел пълното разбиране на степента на тяхното излагане на неприемливо въздействие.

Резултата от тази дейност е списък на заплахите и уязвимостите, свързани с информационните активи, вероятността за реализация на заплахите и последствията от тях.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 2 - Провеждане на оценка на риска – Оценяване на риска

При изпълнението на тази дейност се извършва сравнение на анализираните рискове с критериите за оценка на риска, разработени в Стъпка 1.

При оценяването на риска на тази стъпка, вече се отчитат ефикасността на съществуващите (въведените) защитни механизми и/или последствията за информационните активи, свързани със съответния риск.

За оценяването на въведените защитни механизми, от гледна точка на оперативната им ефикасност, могат да се използват различни методи – напр. инспекции по сигурността, техники за самооценка и др.)

Слабостите във въведените защитни механизми могат да бъдат следствие от лоши (или остарели) технологии и технически решения, неправилно управление и/или процедури, неадекватен модел на прилаганите бизнес процеси и др.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 2 - Провеждане на оценка на риска – Оценяване на риска

След като рисковете са оценени се създава приоритетен списък на рисковете, който отразява и влиянието на внедрените защитни механизми.

Целта на този приоритетен списък е да подпомогне процеса на определяне на приемливите и неприемливи рискове, в съответствие с избраните вече критерии.

Приоритетния списък на рисковете:

- **Осигурява общия поглед за основните нива на риска – с и без защитни механизми**
- **Насочва вниманието към текущите рискове с най-високо ниво**
- **Подпомага вземането на решения за незабавно противодействие или за разработването на планове за противодействие в дългосрочен период от време**
- **Определя рисковете, за които е необходимо специално наблюдение и контрол**
- **Улеснява определянето на необходимите ресурси за противодействие на рисковете**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 2 - Провеждане на оценка на риска – Оценяване на риска

Причините за приемане на риск включват:

- **Нивото на риска е толкова малко, че прилагането на противодействие с наличните ресурси е неуместно (нецелесъобразно).**
- **Липсва приложимо противодействие към риска – напр. риска и извън контрола на организацията.**
- **Цената за противодействие на риска надвишава ползите от неговото прилагане (това важи особено за ниските нива на риска).**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 2 - Провеждане на оценка на риска – Документация

Документацията, съпътстваща дейностите от тази стъпка включва:

- **Списък на идентифицираните рискове, вкл. източници и причини за всеки риск;**
- **Профил на информационните активи, вкл. степен на важност и възможни последствия за тях;**
- **Списък на заплахите и уязвимостите, свързани с информационните активи и заедно с вероятността и последствията от реализиране на заплаха за определен времеви интервал;**
- **Приоритетен списък на рисковете**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 3 - Определяне на възможностите за противодействие

Изхода от дейностите по тази стъпка е документ за противодействие на рисковете.

Организацията трябва да управлява рисковете и да защитава своите информационни активи ефикасно. Общо прието е разбирането, че по-голямата част от рисковете не могат да бъдат изцяло избягнати и винаги ще има остатъчен риск.

На рисковете, които са оценени, като неприемливи, задължително трябва да се противодейства, за да могат да достигнат нива на приемливост за организацията.

В не малко случаи, единствено възможно и/или практически приложимо е да се смекчат последствията от риска.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 3 - Определяне на възможностите за противодействие

Противодействието на риска може да включва всяка или комбинацията от следните възможности:

- **Избягване на риск – решение за неучастие в ситуация и/или дейност, която поставя информационните активи под риск.**
- **Намаляване на вероятността –внедряване на защитни механизми за възпиране или предотвратяване на заплахи и/или уязвимости, имащи ефект върху информационните активи**
- **Намаляване на последствията –внедряване на защитни механизми за смекчаване на влиянието на заплахите, чрез минимизиране излагането на информационните активи на заплахи.**
- **Споделяне на риска – напр. застраховане.**
- **Задържане на риска – организацията ще приеме всички или част от специфичните за нея рискове**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 3 - Определяне на възможностите за противодействие

Области за сигурност

Дадена област за сигурност се определя от еднакви и/или близки изисквания за сигурност и защитни механизми – напр. счетоводство, финанси, услуги за електронна поща и др..

Проблемите по сигурността в дадена област за сигурност не трябва по никакъв начин да оказват вредно въздействие върху сигурността от друга област за сигурност.

Всяка област за сигурност може да има собствен профил по сигурността, вкл. и за защитните механизми.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 3 - Определяне на възможностите за противодействие

Документация

Изхода от тази стъпка е Списък на възможностите за противодействие на разкритите и неприемливи рискове.

Политиката по сигурността, създадена на Етап1 би трябвало да бъде прегледана и актуализирана (при необходимост), с цел, постигането на ефикасно ръководство при избора на защитните механизми за противодействие на рисковете.

Остатъчния (приемлив) риск също трябва да бъде документиран за последващо съгласуване и приемане от организацията.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 4 - Оценка и избор на защити

Изхода от тази стъпка е разработен План за противодействие на риска

Защитите трябва да се подбират, отчитайки целите на организацията, архитектурата за сигурност, приоритетите и наличните ресурси.

Избраните защити за намаляване на на оценените рискове до приемливо за организацията ниво трябва да се идентифицират и избират на база оценка на съотношението стойност / ползи.

Основния принцип, който трябва да се спазва е, че стойността за внедряване и въвеждане в експлоатация на дадена защита (защитен механизъм) не трябва да надвишава стойността на последствията, ако тази защита е няма.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 4 - Оценка и избор на защити

Защитите трябва да се избират в съответствие с ISO 27002.

Този стандарт разделя защитите (защитните механизми) на 18 категории, показани и описани в Приложение А на ISO 27001:2014. (Приложение А е представено като отделен документ в материалите по курса)

Защитите се въвеждат в действие чрез оперативни политики (оперативни защити) и чрез технологии (технологични/технически/програмни защити)

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 4 - Оценка и избор на защити

При този процес, трябва да се отчитат внедрените и планираните за внедряване защити. Внедрените защити подлежат на проверка, относно тяхното ефикасно функциониране, ако това не е направено до този момент. Уязвимостите или излагането на заплахи показва къде е необходимо да се добавят нови защити и какви да бъдат те.

Основните въпроси, свързани с противодействието на риска, на които трябва да се отговори са:

- **Могат ли внедрените защити да бъдат подобрени, за да намалят риска до приемливо ниво?**
- **Необходими ли са нови защити или подмяна на съществуващи, за да се намали риска до приемливо ниво?**
- **Могат ли новите защити да подменят старите на приемлива цена?**
- **Финансово приемливи ли са защитите - дали тяхната цена (за целия жизнен цикъл) е по-малка от произведението на вероятността на риска и стойността на последствията, ако защитите липсват?**
- **Какви са необходимите ресурси – човешки, финансиране, оборудване и др.?**
- **Кой носи отговорност и има задължения за противодействието и управлението на риска?**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 4 - Оценка и избор на защити

Идентифицирането на функциите на защитите е важен момент. Много от защитите имат набор от функции и допринасят за постигането на две или повече цели за контрол. В много случаи е икономически целесъобразно да се подбират защити, които могат да изпълняват различни функции по сигурността:

Възпиране: Предотвратява или намалява вероятността от поява на нежелано събитие по сигурността

Отстраняване: Премахване на познати уязвимости и предотвратяване на създаването на нови

Предпазване: Защита на уязвимите или изложени на заплаха информационни активи от враждебни действия по сигурността

Разкриване: Идентифициране на появата на събития по сигурността и иницииране действието на различни защити – за предпазване, възстановяване и др.

Реагиране: Отговор и/или противодействие на събитие по сигурността, за минимизиране на неговото въздействие върху непрекъснатостта на бизнеса (процесите)

Възстановяване: Възстановяване на цялостта, наличността и конфиденциалността на информационните активи в тяхното желано / очаквано състояние

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 4 - Оценка и избор на защити

Базов подход

Базовия подход за противодействие на риска изисква създаването на минимален набор от защити, необходими за защита на цялата информация в организацията или за част от нея, от общите заплахи.

Защитите, определени по този подход, трябва да се сравнят с внедрените вече защити. Ако има защити, които липсват и са приложими, то те трябва да се внедрят.

При използването на този подход, една от първите стъпки е извършването на анализ и сравнение на внедрените защити и тези определени за внедряване от прилагането на подхода.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 4 - Оценка и избор на защити

Базов подход

Ползата от прилагането на базовия подход е значителното опростяване на оценката на риска.

Рисковете от използването на този подход са:

- възможно е да има неидентифицирани активи, специфични заплахи или уязвимости, които не могат да се обхвана от базовия подход

- подхода се прилага без много мисъл (като списък за проверка) и като заместител на процесите за управление на риска;

- решенията, базирани на този подход са обикновено необосновано скъпи и прекомерно “преоразмерени” спрямо реалните рискове;

Базови подход не трябва да се възприема от организацията, докато не се докаже, че той отговаря на нейния рисков профил – свързан с информационни активи, заплахи, уязвимости, последствия .

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 4 - Оценка и избор на защити

Оперативни и технически защити

Избора винаги трябва да балансира броя и вида на оперативните (не-технически) и технически защити

Оперативните защити са свързани с физическата и персонална сигурност, административните мерки, процедурите, поведението на персонала и др. Обикновено тези защити изискват да са привързани със съответните политики

Оперативните защити включват:

Физическа сигурност

Системи за контрол на достъпа до сгради и помещения, пожароизвестителни и противопожарни системи, охрана и др.

Персонална сигурност

Проучвания при постъпване на работа, наблюдение и контрол на поведението, проверки при напускане / преместване на работа, обучение по сигурността и др.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 4 - Оценка и избор на защити

Оперативни и технически защити

Процедурна сигурност

Процедурната сигурност обхваща оперативните процедури, разработването приложения, процедурите за приемане на разработки, за управление на инциденти по сигурността, за управление на промените, за непрекъснатост на бизнеса, за планиране при непредвидени случаи и/или за планиране на възстановяването и за управление при кризи.

Техническа сигурност

Техническата сигурност обхваща защитите на хардуера, софтуера и комуникациите, идентификацията и автентикацията, логическия контрол на достъп, записите по сигурността, автентикация на съобщенията, криптиране, цифрови подписи, наблюдение и контрол на мрежите, защитни стени (firewalls), анти-вирусен софтуер, разкриване и/или предотвратяване на проникванията и др.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 4 - Оценка и избор на защити

Оперативни и технически защити

Оценени по сигурността продукти и системи

Организацията трябва да придобива продукти и/или системи, които са проверени и оценени от независими експерти (организации). Това оценяване би трябвало да е извършено спрямо съответния профил за защита за продукта и/или системата, отчитайки и заплахите към тях. Оценените по този начин продукти и/или система създават увереност, че техните функционалности са в съответствие с изискванията.

Публикуваните и общодостъпни Общите критерии за оценка (Common Criteria) са предпочитана база за оценка, разбира се, оценените профил за защита и нив на сигурност на продуктите и/или системите, трябва да бъдат в съответствие с рисковете към съответната организация.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 4 - Оценка и избор на защити

Фактори, влияещи на избора на защити

Факторите, които трябва да се отчита при избора на защитите, подлежащи на внедряване (в допълнение към финансовите и икономически фактори), включват:

- **леснота на употреба;**
- **прозрачност за потребителите;**
- **близост на защитите до активите, които защитават;**
- **предлаганата помощ на потребителите, при изпълнение на действията;**
- **съвместимост и допълване с/на внедрените защити;**
- **интеграция с основните средства (инструментариум) за управление на сигурността;**
- **относителната / сравнителната устойчивост на защитите;**
- **профила за защита и оцененото ниво за осигуряване на сигурността;**
- **видовете функции, които изпълняват- възпиране, защита, разкриване, отговор/противодействие, възстановяване;**
- **възвръщане на разходите/инвестициите**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 4 - Оценка и избор на защити

Ограничения, които влияят на избора на защити

При избора, препоръчването и внедряването на защитите трябва да се отчетат различни видове ограничения.

Времеви ограничения

- **Внедряването на защитите се извършва в период, приемлив от ръководството на организацията**
- **Възможно ли е защитите да бъдат внедрени в периода на "живот" на системата**
- **Времето, определено от ръководството на организацията, предразполага да има активи, изложени на рискове по сигурността в този период**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 4 - Оценка и избор на защити

Ограничения, които влияят на избора на защити

Финансови ограничения

В организацията може да има конфликт между желанията и възможностите. Например, липсата на възможност за финансиране на всички оценени и избрани защити налага ръководството да вземе решение за частично и поетапно внедряване. В този случай, ръководството трябва да е готова да поеме всички разкрити и неосигурени със защити рискове, и последствията от тях. Ако ръководството не е подготвено да поеме тази отговорност, то е по-добре да се извърши препланират на бюджетните приоритети, в интерес на сигурността.

Технически ограничения

Техническите проблеми, като напр. съвместимост на софтуер или хардуер, могат лесно за бъдат избягнати, ако са отчетени тези въпроси при избора на защити.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 4 - Оценка и избор на защити

Ограничения, които влияят на избора на защити

Социологични ограничение

Социологичните ограничение или организационната култура при избора на защити може да бъде специфична за различните звена в организацията. Тези ограничения не могат и не трябва да бъдат игнорирани, защото много от защитите изискват активна поддръжка от персонала. Ако персонала няма необходимата организационна култура, много вероятно е усилията по избора на защитите да не бъдат продуктивни в степента, която се очаква от ръководството. Тази неблагоприятна ситуация може да се задълбочи, ако персонала не разбира необходимостта от въвеждането на мерките за информационна сигурност.

Ограничения от околната / обкръжаващата среда

Околната среда е важен ограничителен фактор и влияе при избора на защити – напр. липса на пространство, екстремни климатични условия и др.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 4 - Оценка и избор на защити

Ограничения, които влияят на избора на защити

Правни ограничения

Правните ограничени, включват:

- **Закони – напр. Закон за защита на класифицираната информация, Закон за електронното управление, Закон за личните данни и др.**
- **Нормативна уредба за безопасност на труда**
- **Нормативна уредба за интелектуалната собственост**
- **Нормативна уредба, свързана с националната сигурност**
- **Нормативна уредба, противопожарната безопасност**
- **Задължения по договори**

.Закон за защита на личните данни и др.

……

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 4 - Оценка и избор на защити

Ограничения, които влияят на избора на защити

Ограничения, произтичащи от хората, техните знания и умения

Някои защити изискват прилагането на специализирани умения за тяхното въвеждане и поддръжка (напр.криптография, TEMPEST и др.)

Възможно е защитите да не работят коректно, поради липсата на необходимите знания и умения в персонала, който ги инсталира, конфигурира и поддържа.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 4 - Оценка и избор на защити

Документация

Резултата от тази стъпка е разработен План за противодействие на риска. Когато този план бъде съгласуван и утвърден от ръководството, той се превръща в изпълнителна програма за управление на информационната сигурност.

Този План може да бъде използван за вход на проектни планове, свързани с внедряването на специфични системи за сигурност.

Плана за противодействие на риска се базира на Политиката за информационна сигурност, на резултатите от анализа на риска и отразява степента на приемливост на риска от ръководството на организацията.

Този План трябва да гарантира, че всички нови или променени защити са внедрени в пълно съответствие с установените приоритети по сигурността в краткосрочен, средносрочен и дългосрочен период от време.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 4 - Оценка и избор на защити

Документация

Плана за противодействие на риска би трябвало да включва:

- **целите по сигурността, в контекста на конфиденциалност, цялостност и наличност на информацията;**
- **обобщените резултати от оценката на риска;**
- **архитектурата за сигурност;**
- **списък на изискващите се защити, вкл. внедрени и планирани, оценка на тяхната ефективност и приоритет на внедряване;**
- **описание на приноса на защитите към процеса за управление на риска;**
- **профил за защита, позволяващ избор на оценени по сигурността продукти и/или системи;**
- **оценка на остатъчния риск, приет от организацията, след внедряването на защитите;**
- **план – график на дейностите за поддръжка и развитие на СУИС;**
- **оценка на стойността на новите защити за целия им жизнен цикъл и оценка на оперативните разходи за внедрените защити**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Стъпка 5 – Одобряване от Ръководството

Изхода от тази стъпка е съгласувания и одобрен от ръководството на организацията План за противодействие на риска.

Последната стъпка от този Етап 2 е да се получи и одобрение от ръководството на организацията за остатъчния риск и за програмата за въвеждане в действие на Плана за противодействие на риска.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 5: Етап 2 – Управление на риска – Подготовка на Декларация за приложимост

Когато е предвидено СУИС да бъде сертифицирано по ISO 27001, разработването на Декларация за приложимост е задължително. Разбира се, и без да е предвидена сертификация, тази Декларация е много полезна за СУИС.

Обикновено Декларацията се представя в таблична форма и отразява прилагането на защитни механизми (контроли), описани в Анекс А от ISO 27001. Декларацията също покрива и изискванията на части 4 до 7 на стандарта.

В Декларацията целите на контролите и защити се свързват с:

- **идентифицираните рискове;**
- **кратко описание защо защитите са приложими или неприложими,**
  - **когато избора за защити е комплексен или има значително влияние на риска, описанието е по-подробно**
  - **ясна обосновка, защо има изключени от внедряване защити от описаните в Приложение А от ISO 27001**
- **обобщено описание на всички противодействия, използвани от всяка приложима защита**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Край на **Част 5: Етап 2 – Управление на риска**

За въпроси: Пламен Каменов
Водещ одитор ISO 27001/ ISO 9001 / ISO 20000
e mail: infosecservicebg@gmail.com

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 6: Етап 3 – Внедряване на СУИС – Общ преглед

Първата задача от този Етап 3 е да започне въвеждането на избраните защити в съответствие с Плана за противодействие на риска.

При изпълнението на етапа се извършва:

- **Обучение на персонал за внедряване на защитите.**
- **Проектиране на процесите, разработване на оперативни политики, процедури и инструкции.**
- **Обучение на служителите/потребителите за запознаване и спазване на политиките, процедурите и инструкциите по сигурността.**
- **Придобиване на технологии (ако е необходимо), в съответствие с оперативните политики и съответните процедури по сигурността.**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 6: Етап 3 – Внедряване на СУИС – Изпълнение на Плана за противодействие на риска

Плана за противодействие на риска е разработен на база информацията и документите, създадени по времето на фаза Планиране на СУИС (всички дейности по етапите и стъпките, разгледани до тук)

Изпълнението на Плана трябва да включва оценка и измерване на неговата ефективност, в обхвата на целите на СУИС.

Изпълнението на Плана трябва да бъде управлявано и контролирано ежедневно. Особено внимание трябва да се обърне на придържането към оперативните политики и управлението на инцидентите по сигурността, които могат да се появят при внедряването на СУИС.

Задачите, свързани с изпълнението на Плана за изграждане на СУИС, би трябвало да бъдат определени с висок приоритет на осигуряване в административно, финансово и материално отношение.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 6: Етап 3 – Внедряване на СУИС – Въвеждане в действие

Въвеждането на СУИС в практическо действие налага ежедневно управление и контрол по изпълнението на оперативните политики по сигурността, а също и надлежно документиране на всички събития, решения и предприети действия, свързани със сигурността.

Обучение по информационна сигурност

Целта на програмата за обучение по информационната сигурност е да повиши знанията и уменията на персонала, а също и осъзнаването на важността на сигурността за бизнеса и за всеки отделен служител.

Програмата за обучение трябва да обхваща целия персонал (вкл.новопостъпващи) в организацията, като осигурява необходимите и достатъчни знания по сигурността, съобразени с различните типове персонал.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 6: Етап 3 – Внедряване на СУИС – Въвеждане в действие

Управление на инциденти

Не съществува система за информационна сигурност, която да работи перфектно през целия си жизнен цикъл. Някои от събитията, които възникват в системата могат да бъдат определени, като инциденти по сигурността, които с голяма степен на вероятност могат да нарушат изпълнението на бизнес процесите и да нанесат вреди на информационните активи. Тези събития трябва да се документират и анализират, с цел разкриване на тяхното въздействие, а също и за определяне на провеждането на коригиращи действия и/или промени по сигурността.

Необходимо е да се разработят и внедрят административни процедури, които да създадат ред и правила, осигуряващи своевременното и точно докладване на възникнали или възможни за възникване събития по сигурността. Тези процедури трябва да оказват и начина за провеждане на разследванията за инцидентите по сигурността и да отразяват политиката на организацията и/или държавата в това отношение.

Много важно е да си осигури запазване на доказателствата за възникналите събития по сигурността - това улеснява в значителна степен последващите разследвания.

Персонала трябва да е обучен “с кой, какво, как и кога” действа при възникване на инциденти по сигурността от различен характер

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Край на **Част 6: Етап 3 – Внедряване на СУИС**

За въпроси: Пламен Каменов
Водещ одитор ISO 27001/ ISO 9001 / ISO 20000
e mail: infosecservicebg@gmail.com

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 7: Етап 4 – Наблюдение и подобрение на СУИС – Общ преглед

Надеждното функциониране на СУИС изисква непрекъснато модифициране и подобряване.

Заплахите, бизнес дейностите, информационно - комуникационните системи и техните уязвимости непрекъснато се променят. Средствата, използвани от злонамерени лица, за активно разкриване на слабостите и недостатъците на системите непрекъснато се усъвършенстват и стават все по достъпни за употреба.

Необходимо е да се извършва анализ на инцидентите по сигурността, да се правят съответните изводи и да се вземат ефикасни решения за противодействие. Политиките, процедурите и инструкциите по сигурността, подлежат на периодични прегледи и актуализация.

СУИС, нейната документация и внедрени защитни механизми трябва да бъдат планирано одитирани и оценявани за ефикасност.

Наблюдението и контрола на изпълнението на политиките и процедурите по сигурността е отговорност на ръководството на организацията.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 7: Етап 4 – Наблюдение и подобрение на СУИС – Наблюдение и преглед

Целта на наблюдението и прегледите е да се оцени ефективността на СУИС, в рамките на нейния обхват и цели.

Чрез наблюдението се събират данни и информация, необходими за извършването на анализи по сигурността. Основните типове наблюдение и преглед са:

- **периодична верификация и валидация на СУИС, спрямо нейните цели и Плана за противодействие на риска;**
- **непрекъснато, оперативно наблюдение и преглед.**

Целите на верификацията и валидацията са свързани с доказването че:

- **защитите са подбрани правилно и съответстват на реалните рискове към информационните активи (валидация спрямо целите на защитите)**
- **защитите работят съгласно очакванията и са в съответствие с Плана за противодействие на риска (верификация спрямо този План и Политиките на СУИС)**

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 7: Етап 4 – Наблюдение и подобрение на СУИС – Наблюдение и преглед

Ефективното и ефикасно наблюдение изисква прилагането на метрики за наблюдение на функционирането и тенденциите за функциониране на а СУИС за нейния жизнен цикъл.

Има метрики, които се прилагат при наблюдението на техническото функциониране на системата, но независимо от това, необходимо е да се подготвят и бизнес ориентирани доклади за ръководството.

Метриките трябва да създават възможност за сравнение с предварително дефинирани цели (параметри) за постигане.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 7: Етап 4 – Наблюдение и подобрение на СУИС – Наблюдение и преглед

Валидация на СУИС

Валидацията отчита новите или променените заплахи, уязвимости и последствия. Тя отговаря на въпроса “Използва ли СУИС точните (необходимите и достатъчни) защити ?”

Това означава преглед на идентифицираните рискове, анализ и оценка, вкл. остатъчния и приемлив риск.

Верификация на СУИС

Верификацията се фокусира върху работата на СУИС и внедрените защити на информационните активи. При нея се извършва проверки на защитите от всякакъв тип и се извършва анализ на установените резултати.

Тя отговаря на въпроса “Работи ли СУИС както би трябвало ?”

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 7: Етап 4 – Наблюдение и подобрение на СУИС – Поддръжка и подобрения

Повечето защити изискват поддръжка за устойчивост и непрекъснатост на тяхното функциониране.

Поддръжка на СУИС, означава непрекъснато подобряване на СУИС.

Необходимостта от поддръжка и подобрения се обуславя от:

- **изводите от възникнали инциденти по сигурността;**
- **оперативното наблюдение, разкрило променени рискове, изискващи незабавни действия по сигурността;**
- **валидацията и верификацията на СУИС;**
- **развитието на технологиите и механизмите за защита, използване в СУИС**

Поддръжката изисква изпълнението на коректривни, превантивни и адаптивни мерки, за промени в СУИС.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 7: Етап 4 – Наблюдение и подобрение на СУИС – Поддръжка и подобрения

Определянето на влиянието на промените към функционирането на СУИС е много важна дейност, свързана с поддръжката на системата. От друга страна, някои малки промени могат да не изискват провеждането на детайлен анализ за тяхното влияние.

Много полезно е за всяка промяна в СУИС да се направи съпоставка между нейната стойност и очакваните ползи от нея. Това може да бъзе постигнато чрез разработването на различни бизнес случаи / сценарии, свързани с направените промени, отчитайки и техния жизнен цикъл.

Всички промени в СУИС, подлежат на документиране, управлявани от процедури за управление на конфигурациите. В много случаи,направените промени в СУИС, налагат промени и в програмата на организацията, свързана с провеждането на обучение на персонала по сигурността.

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Част 7: Етап 4 – Наблюдение и подобрение на СУИС – Консултации и комуникации

Извършването на дейностите по валидация и верификация, свързани с всички аспекти на СУИС, налагат провеждането на интензивни комуникации и консултации с всички участващи и заинтересовани от процесите по сигурността.

ЗАЩО ?.....

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Край на **Част 7: Етап 4 – Наблюдение и подобрение на СУИС**

и на курса за самообучение

За въпроси: Пламен Каменов
Водещ одитор ISO 27001/ ISO 9001 / ISO 20000
e mail: infosecservicebg@gmail.com

ПОДХОД И МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА СУИС

Допълнителни материали по курса:

1. **ISO 27000:2018 – Терминологичен речник по информационната сигурност и СУИС**
2. **ISO 27001:2014 – Система за управление на информационната сигурност (СУИС) – изисквания**

За въпроси: Пламен Каменов
Водещ одитор ISO 27001/ ISO 9001 / ISO 20000
e mail: infosecservicebg@gmail.com