УНИВЕРСИТЕТ ПО БИБЛИОТЕКОЗНАНИЕ И ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

КАТЕДРА „НАЦИОНАЛНА СИГУРНОСТ“

ДИПЛОМНА РАБОТА

на тема:

МОДЕЛ ЗА УПРАВЛЕНИЕ И ЗАЩИТА НА ИНФОРМАЦИЯТА В ИНФОРМАЦИОННИТЕ СИСТЕМИ И МРЕЖИ

Дипломант:
Константин Бойков Боев 255-ср
Информационна сигурност
Редовно обучение

Научен ръководител:.....
(доц. Н. Митев)

София
2018

Резюме

Боев, Константин. Модел за управление и защита на информацията в информационните системи и мрежи. Научен ръководител доц. Н. Митев. София 2018г., Катедра „Национална сигурност“. Факултет „Информационни науки“, УНИБИТ.

Брой страници – 57, брой източници – 5, брой фигури – 17.

Ключови думи: Защита, Информационна сигурност (ИС), Информационни технологии (ИТ), Информация, Сигурност, Управление, COBIT

Съдържание

Увод

В дипломната си работа съм акцентирал върху две основни неща – информацията, същност, управление и защита, и стандарта за информационна сигурност COBIT.

Избрах тази тема, защото исках по-подробно да се запозная със същността на моделите, какво включват, какви са целите им, какви рискове съществуват и най-вече тяхното приложение.

Според мен е особено важно и необходимо да се изгради една организационна култура със съответните етични норми, която да допринася за по-доброто разбиране вътре в организацията, за рисковете в нея и съответно да се прилагат определени стратегии за елиминирането на тези рискове или тяхното управление. Трябва да има пряка и обратна връзка между ръководител и служител. Първо, защото всеки трябва да знае своите задачи, но и да умеят да обменят информация за дейността, която е необходима за просперитета на организацията и постигане на нейните цели. Всяко управленско решение трябва да бъде разбрано от служителите на всички нива, с цел своевременно да изпълнят задълженията си и да отчитат постигнатите резултати.

Необходимостта от разработване на модели за управление на информацията се е породила именно от нуждите да се идентифицира риска, да се установят и приложат контролните дейности, да се направи оценка на ефективността на вътрешния контрол. Дава възможност на ръководството да наблюдава ключовите процеси, напредъка към постигане на целите и да се идентифицират тези области, където е необходима намеса.

Управлението на рисковете е изключително трудно. Причината за това е непрекъснатото развитие на технологиите. Ето защо е необходимо и се търсят хора с все по-голяма специализация, които непрекъснато да обогатяват знанията си, както и да се прилагат подходящи системи и механизми на управление.

Контролът трябва да осигури опазването на активите и информацията от различни рискове, от загубата им, като унищожаване, кражба, злоупотреба.

COBIT представлява набор от предписания и спомагателен инструментариум за ИТ управление, които са възприети в цял свят. Особено важна е ролята на одитора, който трябва да оцени адекватността и ефективността на системата за вътрешен контрол, обхващаща управлението на организацията, оперативната дейност и информационните системи. Задълбоченото познаване на основополагащите концепции, модели и рамки за управление на риска и вътрешния контрол, създадени през последните години е от съществено значение за компетентното осъществяване на дейността по вътрешен одит.

ГЛАВА I: ИНФОРМАЦИЯ И ИНФОРМАЦИОННА СИГУРНОСТ

1.1. Информация

Възможни са различни подходи при определяне на съдържанието на понятието „информация" тъй като терминът се използва в различен контекст в зависимост от конкретната предметна област. Първият предлага философска интерпретация на понятието като "едно от най-общите в науката, обозначаващо някакви сведения, съвкупност от някакви данни, знания и т.н." Трябва да се отбележи, че самото понятие "информация" предполага наличието най-малко на три обекта: източник на информация, потребител и преносна среда. Информацията не може да бъде предадена, приета и съхранявана в чист вид, неин носител се явява съобщението. Оттук следва, че понятието "информация" включва два основни елемента: сведение и съобщение[1].

Сведенията изпълняват няколко основни функции:

- познание на околния свят (гносеологическа), включваща формиране на представа за структурата на обкръжаващата среда, натрупване на знания за закономерностите на изменение на обектите в средата и протичащите в нея процеси; оценка на състоянието на тези процеси;
- социална комуникация (комуникативна), включваща формиране на представа за способите за удовлетворяване на базови и вторични потребности, формиране на представа за правилата за поведение в обществото, за

взаимодействие с другите хора, за нравствените ценности, формиране на личните скали на ценностите за материалните и духовни блага, допустимост на използване на определени методи и средства и т.н.;

- удовлетворяване на потребностите (прагматична), включваща целеполагане, т.е. формиране на оценка и избор на целите, достигането на които способства за удовлетворяване на базовите и вторичните потребности на човека, управление на дейностите по достигане на избраните цели.

Ценността на информацията, проявяваща се под формата на сведения, се определя от субективните задачи, за решението на които могат да бъдат използвани тези сведения, или за влиянието, което са оказали върху решаването на дадена задача. Това влияние може да се изразява в промяна на концептуалния модел на задачата, в изменение на приоритетите между възможните варианти на решения, в оценката на целесъобразността на решение на задачата въобще.

Информацията, получавана под формата на сведения, притежава редица свойства:

- идеалност - съществува само в съзнанието на личността и като следствие, е невъзможно да бъде възприета от органите на чувствата;
- субективност - зависимост на количеството и ценността на сведенията от информационния модел на субекта, получаващ тези сведения.
- информационна неунищожимост - невъзможност за унищожаване на сведенията от други сведения, получавани от личността;
- динамичност -възможност за изменение на ценността на наличните сведения и знания под въздействието на времето или на други постъпващи сведения;
- натрупване - възможност за практически неограничено натрупване на сведения в информационния модел на личността.

Способността за получаване, натрупване и използване на информацията под формата на сведения е отличителна характеристика на човека, но обемът и съдържанието на изпълняваните на база на тяхното използване функции съществено се различават.

Информационното пространство съдържа безкрайно количество потенциална информация, но тя трябва да бъде разменена между отправителя и получателя на основата на взаимно разбиране-това е базово условие, при липсата на което не съществува информация. Сведенията, които протичат по каналите за съобщения трябва да бъдат възприети и интерпретирани от получателя, при което той получава знание.

Понятието "съобщение" се определя като "кодиран еквивалент на събитието, фиксиран източник на информация, изразен с помощта на условни физически символи (азбука), образуващи определена подредена съвкупност". Съобщенията се използват преди всичко за предаване на сведения на други хора и съставляват същността на представителната страна на информацията, или нейната представителна форма. Информацията под формата на съобщение се проявява като реализация на способностите на човека да описва сведенията на някакъв език, представляващ съвкупност от лексика и граматика.

Отправителят, чрез формиране на съобщение селектира част от своя информационен модел, който иска да предаде, установява отношения между неговите елементи и известните му понятия. С помощта на езика и някаква азбука той осъществява кодиране на понятията, получавайки в резултат систематизиран набор от знаци, който може да бъде предаден на други хора, т.е. протича обективизация на съдържателната страна на информацията и съответстващите сведения стават достъпни за възприятие чрез органите на чувствата. Възприемайки съобщението, получателят установява отношения между съставляващите го набори от букви и знаци и известните му понятия, а след това - образи, усещания, оценки, асоциативни отношения, т.е. преобразува представителната форма на информацията в нейната съдържателна форма. Изхождайки от това, съобщението може да бъде представено като съвкупност от предаваните сведения и порядъка (алгоритъма) за тяхното кодиране в набор от знаци на съобщението и последващото му декодиране в сведения. Без алгоритъма на кодирането съобщението се превръща просто в набор от знаци.

Преобразуването на информацията от сведения в съобщения и обратно представлява същността на общия закон за разпространение на информацията.

Информацията във форма на съобщение притежава редица свойства, към които можем да отнесем:

- материалност - способност да въздейства на органите на чувствата;
- измеримост - възможност за количествена оценка на параметрите на съобщението (количеството на знаците, съставляващи съобщението);
- сложност - наличие на набор от знаци и алгоритми за тяхното кодиране и декодиране;
- проблемна ориентираност - съдържа сведения, отнасящи се към определена задача от човешката дейност.

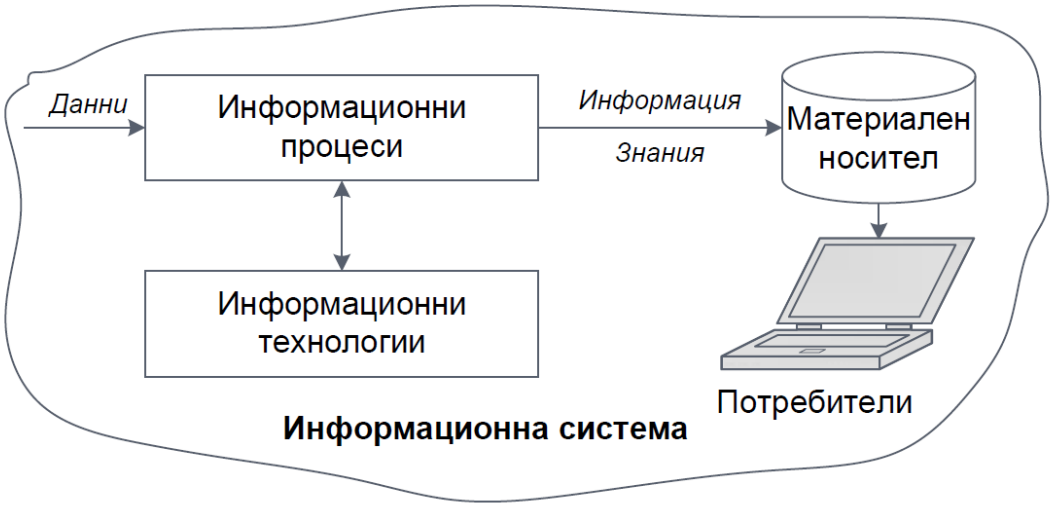
1.1.1. Информацията като ресурс

Вторият подход при определяне и оценка на ролята и значението на информацията в информационното общество е разглеждането ѝ като ресурс, позволяващ реализацията на социалните функции и осъществяване на икономическите дейности на организациите при постигане на техните цели.

Ресурс-запаси, източници, възможности, които осигуряват решаването на дадена задача. Ресурси се наричат елементите с икономически потенциал, с които разполага обществото и които, при необходимост, могат да бъдат използвани за постигане на конкретни цели на икономическото и социалното развитие. Управлението на всяка една организацията се състои в решаване на въпросите за привличане, разпределение и контрол над нейните ресурси.

Информацията се разглежда като един от видовете ресурси, използвани в обществената практика при реализацията на целевите програми, наред с останалите видове ресурси -работна сила, суровини и материали, оборудване и средства за производство, парични средства. Подобно на другите видове ресурси, информационните ресурси се явяват обект на покупко-продажба, на конкуренция, на политическа и икономическа експанзия.

Информационен ресурс: знания, формулирани от хората в тяхната история и фиксирани на материален носител. Тези знания са отчуждени от хората, които са ги създавали, натрупвали, анализирали, обобщавали и се ползват от цялото общество, материализирани във вид на документи, бази данни, бази знания, а също и във вид на произведения на изкуството, литературата и науката. Информационните ресурси отразяват естествени процеси и явления, фиксирани в резултат на научни изследвания и разработки или други видове целенаправени дейности в различни видове документи, концепции и решения, както и по-сложни модели на действителността.



Ресурс е цялата натрупана информация, в това число и недостоверната ("дефектна"), представена от съмнителни факти, неверни предположения, неефективни подходи, както и остаряла информация, несъпоставими данни, събрани по нестандартни методики, информация, загубила конкретност в резултат на субективни тълкувания в процеса на частни теоретични построения, преднамерена дезинформация, постъпила в информационните потоци. Без разкриване на недостоверната и остаряла информация, натрупвана в информационните ресурси се създават предпоставки за приемане на неефективни, в някои случаи и погрешни решения, нанасящи съществени вреди.

Основни характеристики на информационните ресурси:

- неизчерпаемост – с развитие на обществото и на ръста на потребност от знания, запасите на информационни ресурси не намаляват, а растат;
- нематериалност – осигурява сравнителна лекота при тяхното възпроизвеждане, предаване, разпространение в сравнение с други видове ресурси.

В зависимост от материалния носител, информационните ресурси се делят на пет основни класа:

- персонал, който притежава знания и квалификация;
- организационни единици -научни, производствени, управленски и други организации, разполагащи с кадрови, технически, производствени, финансови и др. възможности за решаване на определен кръг проблеми и задачи;
- документи от всякакъв вид и тяхната комплектация на всякакъв вид носители;
- материални обекти, създадени в процеса на производство, рецептури и технологии, стандартни образци, програмни продукти и т.н., явяващи се овеществен резултат от научната и производствена дейност на хората;
- научен инструментариум (в това число автоматизирани системи за научни изследвания, автоматизирани работни места, експертни системи и бази знания).

Информацията съществува в много форми - тя може да бъде напечатана или написана върху хартия, запомнена по електронен път, предадена по пощата, или с използване на електронни средства, или предадена по време на разговор. Каквато и форма да приеме информацията, тя винаги трябва да бъде адекватно защитена, за да се избегнат или намалят рисковете за нейното компрометиране, което позволява да се използват ефективно информационните ресурси и, в крайна сметка, да се осигури постигне на целите на организациите. От тази гледна, информационните ресурси се явяват икономическа категория и в съответствие с това притежават определени характеристики - цена, стойност,

разходи, печалба и т.н., което позволява да бъдат използвани като база за създаване на информационни продукти.

Информационен продукт - съвкупност от данни, събрани и обработени от производителя за разпространение във веществена или невеществена форма. Представлява особен вид стока, която не само има цена, изразяваща нейната конкретна полезност за конкретни потребители на пазара, но и която има всеобща полезност под формата на непосредствено натрупвано от човешката цивилизация знание.

Особености на информационния продукт:

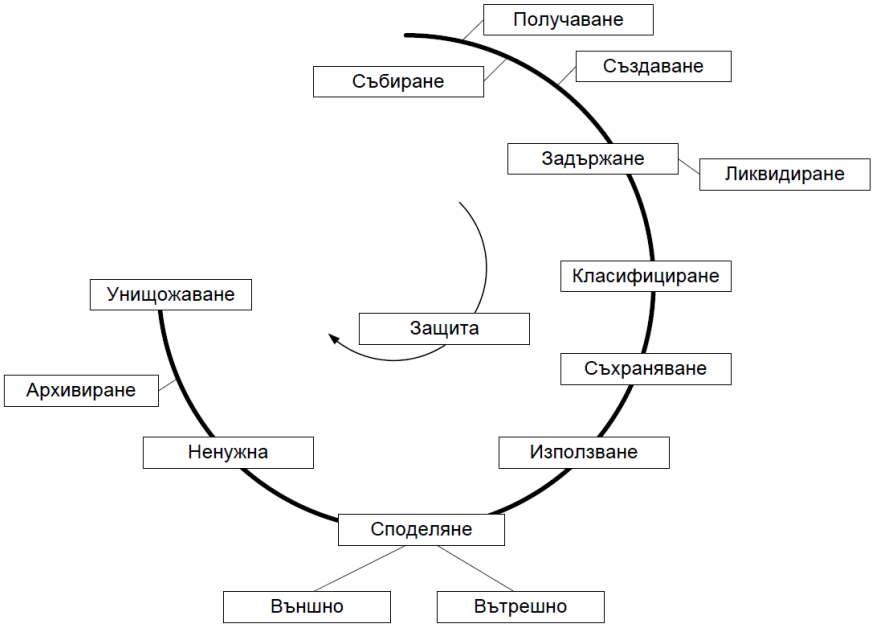
- Отразява информационния модел на производителя, в който е отразена на първо място неговата представа за съответната предметна област.
- Може да бъде използван многократно, като съхранява съдържащата се в него информация, независимо от броя на използването.
- Износва се във времето, т.е. съдържащата се в него информация губи своята актуалност.
- Потребителския интерфейс трябва да бъде съобразен с информационната култура на съответния потребител.
- Разходите за производство са значително по-големи от разходите за тиражиране.

Информационна услуга - предоставяне на потребителя, обработен за нуждите му информационен продукт. Превръщането на дейността по оказване на информационни услуги в основна човешка дейност води до формиране и развитие на глобален пазар на информационни продукти и услуги, който е основна характеристика на съвременното информационно общество. Вижда се, че границите между понятията информационен продукт и информационна услуга не са твърдо детерминирани, но като цяло, информационният продукт представлява фиксирана (документирана) информация, създадена и предназначена за удовлетворяване на определени потребности на потребителите, а информационните услуги са действията на субектите по осигуряване на ползвателите с информационни продукти. Това позволява един и същ информационен продукт да се използва като база за реализиране на цял спектър информационни услуги. Както всеки продукт, информацията има притежатели (собственици) и потребители, които се нуждаят от нея, защото притежава определени потребителски качества, благодарение на които удовлетворявана съответните потребности, нужди и изисквания на потребителите. Притежаването от информацията на необходимите качества, позволява на потребителите да постигнат допълнителен икономически или социален ефект при използване на информационните продукти за производствена или управленска дейност.

Информатизация - организационен социално-икономически и научно-технически процес по създаване на оптимални условия за реализация на правата по удовлетворяване на информационните потребности на гражданите, обществените организации и органите на държавната власт на основата на формиране и използване на информационни ресурси. Информатизацията се базира на националните информационни ресурси и се осигурява посредством информационни системи и телекомуникационни мрежи.

1.1.2. Жизнен цикъл на информацията

Управлението на информацията трябва да осигурява нейното ефективно производство и използване от организацията през целия ѝ жизнен цикъл. Реализацията на информационните процеси през отделните етапи има своята специфика и изисквания, като обединяващото е, че през всички стадии от жизнения цикъл на информацията тя се явява стратегически актив за организацията и трябва да бъде надеждно защитена[1].



Получаване. Информацията се получава по много пътища и в различна форма – електронна поща, извличане на съдържание от интернет, факс, обикновена поща, получена при срещи, семинари или конференции, публикации в медиите и открити източници на информация от организациите и държавните институции.

Събиране. Служителите на организацията събират информация от множество и разнообразни вътрешни (структурните единици на организацията, персонала) и външни (потребители, партньори, съизпълнители, доставчици и други заинтересовани лица) източници с цел предоставяне на информационни продукти и услуги.

Създаване. Организациите се нуждаят от създаване на записи на информацията (официални документи) за да могат да проследяват механизмите

да вземане на управленски решения, протичането на процесите по създаване, предлагане и реализация на продукти и услуги, с цел поддържане на общата (институционалната, корпоративната) памет.

Унищожаване или задържане. Един от най-критичните етапи при управление на жизнения цикъл на информацията, защото оценката за необходимостта и ценността на информацията за организацията зависи от множество вътрешни и външни фактори. В резултат на информатизацията, във всяка организация при реализацията на управленските и производствени процеси се създават и получават големи количества информация, която ако не бъде селектирана, оценена и сортирана, а ненужната унищожена, ще доведе до неефективно използване на ресурсите (човешки, материални, финансови и информационни) на организацията и ще затрудни нейното функциониране.

Класифициране (организиране). За всяка организация е важно да създаде и прилага система за организиране (класифициране) на информацията така, че тя, нейните структурни единици и служители, или други организации да могат бързо и лесно да я намират и използват, като същевременно се създава регламент за достъп и ползване на отделните категории информация.

Съхраняване. В организацията трябва да бъде създаден регламент с ясни правила за начините, процедурите и местата за съхраняване на информацията, в зависимост от формата и вида на носителя ѝ.

Използване. Необходимо е използването на информацията да се осъществява по начин, който максимално добре удовлетворява информационните потребности на организацията, позволява ѝ да създаде и предлага на други организации, партньори и потребители висококачествени информационни продукти и услуги, води до увеличаване на знанието, съхранявано от организацията.

Споделяне. Информацията най-често повишава ценността си за създателите, потребителите и за цялото общество, когато се споделя. Целенасоченото споделяне на информация чрез вътрешно и външно

разпространение в много случаи може да помогне на организациите да постигнат изпълнение на целите си.

Разпореждане. С течение на времето служителите в организациите обичайно установяват, че все по-рядко и по-малко се позовават на, и използват определени видове информация, обикновено защото губи своята актуалност.

Защита. Независимо от етапа от жизнения цикъл на информацията, тя трябва да бъде непрекъснато защитавана като стратегически актив за организацията, което е една от главните задачи мениджмънта на организацията, като се обръща внимание не само на класифицираната и персонална информация, за които съществуват законови изисквания за осигуряване на определени нива на сигурност, но и на всяка друга, която представлява актив с определена стойност за организацията. Защитата на информацията в информационните системи или мрежи е способността им да гарантират конфиденциалността, цялостността и достъпността на информацията в тях. В допълнение могат да бъдат включени и други способности, такива като гарантиране на автентичност, отчетност, безотказност и надеждност на информацията.

Конфиденциалност (секретност, поверителност) на информацията в информационните системи или мрежи е регулираща обществените отношения функция, с която се управлява достъпа до информацията и не се допуска нейното разкриване от потребител, който не е оторизиран за това. По отношение на информацията, това е качеството ѝ да бъде недостъпна или неоткриваема (тайна) за нямащите право на достъп индивиди, обекти, или процеси.

Цялостност на информацията в информационните системи или мрежи е функцията им, с която се поддържа интегритета на обработваната и съхранявана информация. Това означава, че обработката на информацията не я компрометира, или не допуска неоторизирани преднамерени (или случайни) промени в нея.

Достъпност на информацията в информационните системи или мрежи е функцията, с която се осигурява исканата от оторизираните лица информация, в указаното време и на нужното място, в желания вид, т.е. тези лица имат достъп винаги когато това е необходимо.

Организациите трябва да управляват информационните си ресурси и базираната на тях информация, така че да предоставят и поддържат ефективно и ефикасно услугите си, като по този начин осигуряват защита на стойността на инвестициите си по реализация и внедряване на информационните системи. Изповядването и прилагането на принципите и насоките на мениджмънта на информацията и информационните активи предполага наличие на прецизно планиране през целия ѝ жизнен цикъл.

1.2. Информационна сигурност

Информационна сигурност се нарича практиката на защита на информацията от неправомерен достъп, използване, разкриване, увреждане, промяна, преглед, запис или разрушаване. Терминът е достатъчно общ, за да бъде използван независимо от формата, която можа да имат данните (напр. електронна, физическа). Според определението на Европейската комисия информационната сигурност е защита на мрежите и информационните системи срещу човешки грешки, природни бедствия, технически неизправности или злонамерени атаки.

IT сигурността, наричана понякога компютърна сигурност, означава информационна сигурност, приложена към техниката (най-често под формата на компютърна система). При това компютър не се ограничава до персонален компютър, а е всяко устройство с централен процесор и компютърна памет. Това могат да са както самостоятелни, несвързани с други, прости устройства като калкулатори, така и свързани в телекомуникационна мрежа мобилни устройства като смартфони и таблети. Поради естеството и ценността на данните във всяко по-голямо предприятие има отдел по IT сигурност. Той отговаря за опазването

на компанията от злонамерени атаки, които се опитват да се доберат до критична чувствителна информация или да осъществят контрол върху вътрешни системи.

Осигуряването на сигурността на информацията започва още на етапа на проектиране и създаване на бъдещата информационна система. Това става със съставяне на спецификациите на необходимото оборудване и програмно обезпечение, като поръчителят на системата иска тя да осигурява определен набор от услуги, които са основни за нея. За да могат да функционират основните, има нужда да съществуват и се планират редица спомагателни услуги, като се анализират информационните потоци между тях, за да може да се контролира взаимната съвместимост. Когато описания етап е завършен, формирането на архитектурата на бъдещата система от съдържателна гледна точка може да се счита за готова и се пристъпва към разработване на мерките за сигурност. Главната цел на мерките, предприети на управленско ниво, е да се сформира програма за работа в организационната единица по отношение на приложение на ИТ и управление на информационната сигурност, да се осигури изпълнението като се отделят необходимите ресурси и се осъществява последващ контрол[2].

Информационната сигурност е такова състояние на организацията, в което се осигурява, поддържа и гарантира:

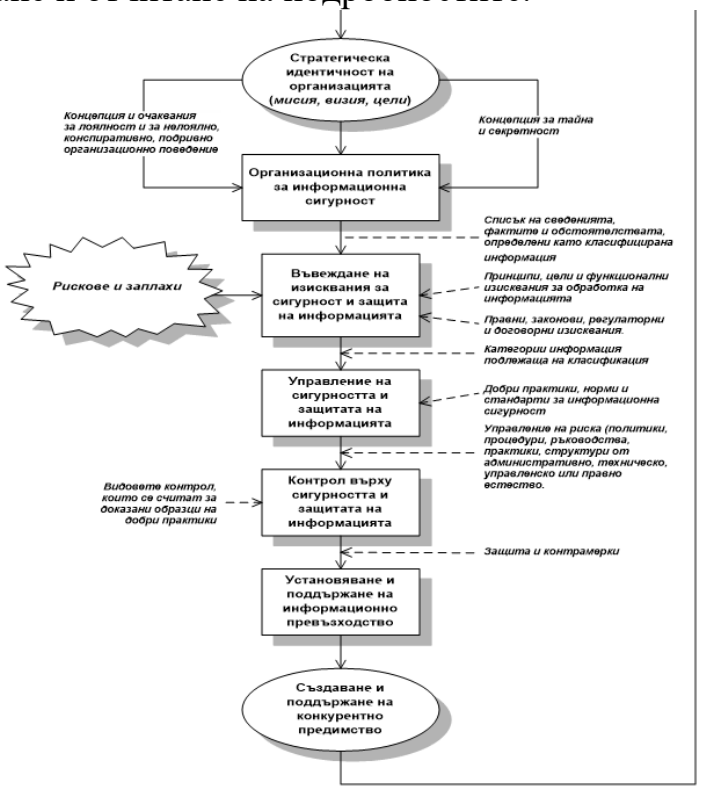
- непрекъснатост на работните процеси;
- минимизация на рисковете за организацията;
- максимизиране на възвръщаемостта на инвестициите;
- увеличаване на възможностите за успех на инициативите (начинанията).

1.2.1. Защо е необходима информационна сигурност?

Информацията и поддържащите процеси, системи и мрежи са важни активи на всяка организация. Определянето, оценката, постигането, поддържането и подобряването на сигурността на информацията са съществени за повишаването на конкурентоспособността, финансите, доходността, за

спазването на законите и поддържане на добрия имидж на организациите. Техните информационни системи и мрежи са изложени на заплахи за сигурността от голям брой източници, включващи неспазване на установените политики, правила и процедури за защита та информацията от страна на ръководството и на служителите, неправилна или небрежна употреба от страна на персонала и редица други заплахи за който ще говорим по-нататък.

Затова сигурността на информацията става все по-важна както за обществения, така и за частния сектор на икономиката и за защитата на критичните управленски информационни инфраструктури. В тези сектори, гарантирането на сигурността на информацията дава възможност да се избегнат или намалят рисковете, да осигури информационно превъзходство, да се експлоатират ефективно информационните активи и, в крайна сметка, да се постигне конкурентно предимство. Сигурността, която може да се постигне чрез технически средства е ограничена и трябва да бъде поддържана чрез съответното управление и установени процедури за реализация на информационните процеси. Определянето кои видове контрол трябва да се използват изисква грижливо планиране и отчитане на подробностите.



Съществуват три главни източника за определяне на изискванията за информационна сигурност:

- Първият е оценката на рисковете за организацията, получена чрез отчитане на нейната обща стратегия и цели. Чрез оценката на риска се определят заплахите за активите, оценява се уязвимостта към такива заплахи, вероятността от появата им и се оценява ефекта от потенциалното им въздействие.
- Вторият са правните, законови, регулаторни и договорни изисквания, на които трябва да отговаря дадена организация, нейните партньори, подизпълнители, доставчици на услуги и тяхната социално – културна среда.
- Третият източник е специален набор от принципи, цели и функционални изисквания за обработка на информацията, които организацията разработва за да поддържа дейността си.

Успешното гарантиране на сигурността на информацията в дадена организация зависи от следните критични фактори:

- отражението на спецификата на политиката за сигурност, нейните цели и дейности, върху целите на организацията;
- съвместимост между избраната концептуална рамка и подход за реализиране, поддържане, наблюдаване и подобряване на сигурността на информацията, от една страна и организационната култура, от друга;
- наличието на поддръжка и ангажимент за гарантирането на информационната сигурност на всички нива на управление;
- добро разбиране на изискванията за сигурност на информацията, оценката и управлението на риска;
- ефективен маркетинг на сигурността на информацията за постигане на обща осведоменост на всички ръководители, служители и трети страни;

•разпространение на ръководство (наръчник) за политиката за сигурност на информацията и актуалните стандарти между всички служители, ръководители и трети страни;

•осигуряване на достатъчността на финансирането на дейностите по управление на сигурността на информацията;

•осигуряването на съответната квалификация чрез обучение и образование;

•установяване на ефективен процес на управление на инцидентите със сигурността на информацията;

въвеждане на система за измерване, която се използва за оценка на ефективността на управлението на сигурността на информацията и за изработка на предложения за нейното подобряване.

1.3. Заплахи

Информационната защита е предотвратяването на загуба на данните при критични ситуации. Такива могат да включват, без ограничение: природни бедствия, повреда на компютри/сървъри, кражба или всеки друг случай, когато има риск от загуба на информацията. Тъй като в наши дни повечето от информацията се съхранява на компютри, за информационната защита най-често се грижат специалистите по IT сигурност. Един от най-честите методи за информационна защита е дублирането на информацията и съхраняването на резервни копия на различно място.

Заплахите за сигурността на информацията приемат най-различна форма. Някои от най-честите са софтуерни атаки, кражба на интелектуална собственост, кражба на самоличност, кражба на устройство или информация, саботаж и манипулиране на информацията. Повечето хора са изпитали някакъв вид софтуерна атака: вируси, червеи, фишинг и троянски коне са примери за такива атаки. Кражбата на интелектуална собственост е предмет на загриженост за много IT компании, като най-честа е кражбата на софтуер. При кражбата на самоличност атакуващият се опитва да получи достъп до лична информация, за

да се възползва от нея по злонамерен начин. Кражбата на устройства или информация е често срещана днес поради факта, че все повече информационни устройства са мобилни. Мобилните телефони са чест обект на кражба и са все по-желани с увеличаването на обема на съхраняваната информация. Саботажът може да приеме формата на повреждане на уебсайта на компанията в опит да се причинят вреди на потребителите. Манипулирането на информация се прави с цел да се изнудва собственика да заплати възстановяването на вярната информация или да получи обратно собствеността си.

Правителствата, военните, корпорациите, финансовите институции, болниците и частните компании натрупват голямо количество конфиденциална информация за своите поданици, служители, клиенти, продукти, изследвания и финансови операции. В наши дни по-голямата част от тази информация се събира, съхранява и обработва с помощта на компютри и се предава по компютърни мрежи на други компютри.

Информацията, през всички етапи на своя жизнен цикъл, е критически важен ресурс за всички предприятия. Съществуването и функционирането на всички видове съвременни предприятия са изключително зависими от информацията и динамично развиващите се ИТ.

1.3.1. Видове заплахи

1.3.1.1. Физическа сигурност на компютърните системи

- Кражба или неоторизиран физически достъп - сървъри и дискови масиви с чувствителна информация трябва да са в сигурни и охранявани помещения. Много по-лесно е да се извади информация от сървър при физически достъп до него.
- Природни стихии, технически сривове поради повреда или външни технически обстоятелства - съоръженията и компютърните системи трябва да бъдат добре подсигурени. Изграждат се противопожарни системи. Поддържат се подходящи условия – температура, вентилация, влажност. Обикновено за

критични информационни системи, при които временното нарушаване на наличността на информацията носи големи загуби за компанията, се изграждат огледални системи, но на достатъчно географско разстояние. По този начин компаниите се предпазват от природни и други бедствия и повреди на компютърните системи – пожар, наводнение, липса на ток и т.н.

1.3.1.2. Заплахи от собствения персонал

- Неволни технически грешки - една от най-сериозните заплахи за информационната сигурност са човешките грешки. Това е така, тъй като това е и най-често срещата причина за нарушаване на цялостта и наличността на информацията. Потребители и администратори допускат грешки, които водят до временна техническа неизправност на информационните системи, неволно инсталиране на вреден софтуер или загуба на информация.
- Други грешки и социално инженерство - невежи потребители често не осъзнават важността на информационната сигурност. Често те записват своите пароли за достъп на хартия или я споделят с колеги. Недоброжелатели се възползват от необучени потребители и се представят за технически персонал в опит да получат пароли или други конфиденциални технически детайли.
- Злонамерени служители - обикновено това е най-лесният начин за изнасяне на конфиденциална информация от компанията. Затова трябва да се спазва правилото за минимално възможен достъп до информация, който е достатъчен за работата на служителите. Въпреки това, такава заплаха съществува от технически персонал, ръководен персонал, служители по сигурността. Такива потребители често имат информация за технически детайли на информационните системи.

1.3.1.3. Злонамерени действия от външни лица

Съществуват различни категории хора, които се занимават с неоторизиран достъп. Целите им също са различни: индустриален шпионаж, нелоялна конкуренция, финансови облаги, отмъщение, вандализъм и др. При такива пробиви не винаги има разрушение на информация, а понякога компанията не разбира, че е изтекла информация.

- Хакери и кракери - в литературата се прави разлика между хакер, което означава високо квалифициран и добронамерен компютърен специалист и кракер - това е хакер, който използва своите способности с користна цел. Обикновено до неоторизиран достъп се стига след предварително проучване, социално инженерство и др. Чрез продължително следене се изгражда профил на системите за сигурност и нейните пропуски.
- Неоторизиран достъп чрез пароли - съществуват списъци с често използвани пароли. Недоброжелатели могат да използват тези списъци за да атакуват потребителски акаунти, които имат права и привилегии върху чувствителни информационни системи. Някои кракери използват програми, които генерират милиони възможни пароли в секунда. В някои случаи, при достатъчно кратки пароли се опитват всички възможни комбинации до намиране на правилната парола.

- Phishing - представлява мрежова заплаха, при която чрез достъп до мрежов ресурс се следи трафика, който минава през него. Това е опасно и често може да остане незабелязано. При някои по-стари системи дори потребителски пароли се предават в прост текст и чрез този метод лесно могат да бъдат записани от зложелатели.

1.3.1.4. Вреден софтуер

Съществуват различни видове вреден софтуер. Общото за него е, че обикновено се инсталира без знанието и съгласието на потребителя и има за цел да предостави или компрометира по някакъв начин информационната система.

- Шпионски софтуер (Spyware) - следят и записват информация за използването на компютъра. Следят се навиците на потребителите и спомагат за разучаването на хакери. Информацията се предава до определен получател.
- Логически бомби - стар тип зловреден софтуер. Обикновено не въздействат на системата по никакъв начин докато не се изпълни определено условие. След изпълнение са разрушителни.
- Троянски коне - инсталират се в допълнение към полезни програми и дават достъп до компютърната система на определени зложелатели. Определени хора могат да достъпват ресурси в заразената система избягвайки стандартните системи за сигурност. Могат да се изпълняват различни команди, да се прехвърлят файлове и друга информация, да се управлява компютърната система. За разлика от традиционните вируси, тези програми не заразяват други файлове.
- Червеи - тяхната основна цел е да се разпространяват в други системи чрез използване на достъпни мрежови връзки. Понякога се разпространява и чрез електронна поща. Може да носи и разпространява друг вреден софтуер.
- Вируси - представляват програми, които записват части от себе си в легитимни, полезни програми. Всяко тяхно копие след това може отново да се разпространява в други достъпни програми. Освен разпространението им, те обикновено имат и разрушително или друго вредно действие.

Затова днес, повече от всякога, предприятията и техните ръководители са задължени да:

- поддържат високо качество на информацията за приемане на управленски решения;

- създават стойност за бизнеса чрез реализация на инвестиции, свързани с ИТ, т.е. да постигат стратегическите цели и да получават изгоди от ефективното и иновативно използване на ИТ;
- усъвършенстват функционалния си модел чрез надеждно и рационално приложение на технологиите;
- гарантиране на приемливо равнище на ИТ рисковете;
- оптимизиране на разходите за ИТ услуги и технологии;
- поддържане на съответствие със законите, нормите, договорните задължения и политиките, свързани с приложение на ИТ. [3]

ГЛАВА II: МЕТОДИ ЗА УПРАВЛЕНИЕ И ЗАЩИТА НА ИНФОРМАЦИЯТА

2.1. Модели за създаване и поддържане на система за управление на информационната сигурност в организациите

В контекста на ИТ организацията управлението на риска се представя като интеграция на хора, процеси и инструменти, които заедно осигуряват ранно и непрекъснато идентифициране и обработка на рисковете в или за организацията. В крайна сметка управление то на риска има за цел да създаде и поддържа цялостна информационна система за рисковете, така че възможностите и целите за изпълнение да постигнат желания ефект.

2.1.1. ISO 9000

Серията стандарти ISO 9000, развити и публикувани от Международната стандартизационна организация (ISO), е първата широко приложима нормативна структура, която предлага указания, правила и препоръки за дефиниране, създаване, експлоатация и поддържане на системи за управление на организацията. По конкретно, стандартите разглеждат въпросите за внедряване на системи за управление на качеството от всякакъв тип организации, работещи в индустриите на производството и услугите. ISO 9000 се занимава с фундаментите на системата за управление на качеството (СУК),

включително основните принципи, на които е базирана фамилията стандарти, и също така дефинира изискванията, които трябва да изпълни организацията, за да може да внедри и поддържа СУК в съответствие със стандартите.

Въведените чрез серията стандарти ISO 9000 общи основни понятия и принципи за изграждане, внедряване и поддържане на системи за управление се прилагат при разработването и развитието на групите стандарти за управление в различни области на промишлеността и услугите, като например, ISO 20000 за системи за управление на ИТ и ISO 27000, отнасящ се за системи за управление на информационната сигурност. ISO 9000 въвежда процесният подход, въпреки че е за управление на качеството [2].

2.1.2. ISO/IEC 20000

ISO/IEC 20000 е първият международен стандарт за управление на ИТ услугите (IT Service Management - ITSM), чиято първоначална версия е разработена и предложена от ISO/IEC през 2005 г. Базира се на по-ранните модификации на BS 15000, който е създаден и развит от BSI[2].

Затова ISO/IEC 20000, подобно на своя предшественик BS 15000, се основава на разработената и съдържаща се в ITIL структура от нормативи, изисквания и препоръки, отразяваща обобщенията за добрите практики по осигуряване на оптимална ИТ инфраструктура и нейното управление, но освен това възприема и съвместява подходите и част компонентите на други свързани с ITSM структури, като MOF, itSMF, CMMI, както и на COBIT на ISACA, когато се разработват въпросите за одит и оценка на съответствието на организациите.

2.1.3. ITIL

ITIL (Библиотека на инфраструктурата на информационните технологии) е целесъобразно структурирана колекция от правила на мениджмънта на информационните технологии и специализирани методологически принципи, синтезирани от най-добрите практики.

ITIL дефинира процеси, дейности, функции, роли, отговорности и градивни елементи чрез приложение на модел, базиран на процесния подход, позволяващ осъществяването на перманентно наблюдение, контрол и управление на операциите. Библиотеката предлага обширни и подробни указания за внедряване, експлоатация, поддръжка и управление на информационните технологии и произведените с тях продукти и услуги. Те са дефинирани по начин, който ги прави приложими независимо от различните характеристики на производителите и сферата им на дейност, за да се гарантира ефективното и ефикасно използване на авангардните информационни технологии и да се оптимизират информационните процеси. Целта на ITIL е да събере огромния обем от знания и добри практики в различните сфери на дейност, отчитането на които прави възможно създаването на методология, чието приложение води до реализация на ефективно функционираща система за управление на информационните продукти и услуги.

За разлика от ITIL, в стандарта ISO 20000 само са маркирани най-важните етапи и цели, без отчитането на които е невъзможно да се говори за ефективна система за управление, затова структурата на работните процеси, представени в него не съответстват напълно на представените в ITIL. Стандартът използва и се базира на ITIL, но между тях има съществена разлика, тъй като ITIL остава сборник с добри практики, предлагащ подробна и детайлизирана структура на представените процеси за управление на информационните технологии, а ISO 20000 въвежда набор от изисквания за реализиране на системи за управление на качеството на услугите и дава проверяеми критерии за оценка на ефективността на това управление в ИТ организациите[2].

2.1.4. MOF

Ключовата стратегия за управление на услугите на Microsoft се изразява в предоставяне на решения за ефикасна и ефективна интеграция на хора, процеси и технологии, необходими на организациите, за да се възползват от предимствата на ИТ за осигуряване на качество при управление на услугите. Ръководството MOF на Microsoft предлага оптимизация на управлението при доставката на услуги чрез платформата на операционната система Windows, която осигурява ключова инфраструктура за посрещане на изискванията и за подпомагане на бизнеса при управление на услугите и работните процеси. Ръководството представлява поредица от документи с предписания, указания и препоръки, имащи за цел да помогнат на професионалистите в областта на ИТ за създаване и прилагане на надеждни и рентабилни услуги, отнасящи се за целия ИТ жизнен цикъл. MOF се базира на взаимосвързани дисциплини, опериращи с понятията управление, риск и съответствие (Governance, Risk, and Compliance - GRC) [2].

ИТ управлението се разглежда като дейност на висшия мениджмънт, част от функциите на който са да изясни кой взема решенията, да определи задълженията за дейностите и отговорностите за резултатите, както и методиката, по която ще се оценява очакваното изпълнение. По този начин, чрез MOF се цели да се помогне на организацията при създаване, опериране и поддържане на ИТ услуги, като същевременно се гарантира, че инвестициите в ИТ носят очакваните бизнес ползи и стойност при допустими нива на риска.

Прилагането на MOF може да помогне на организацията да създаде среда, където ИТ и бизнесът работят съвместно за постигане на функционално усъвършенстване и зрелост – MOF предлага проактивен модел, определящ процеси и стандартни процедури, съдействащи за повишаване на ефективността и ефикасността. Той дава на организациите един логически структуриран подход за вземане на решения по планиране, разгръщане и поддържане на ИТ услугите.

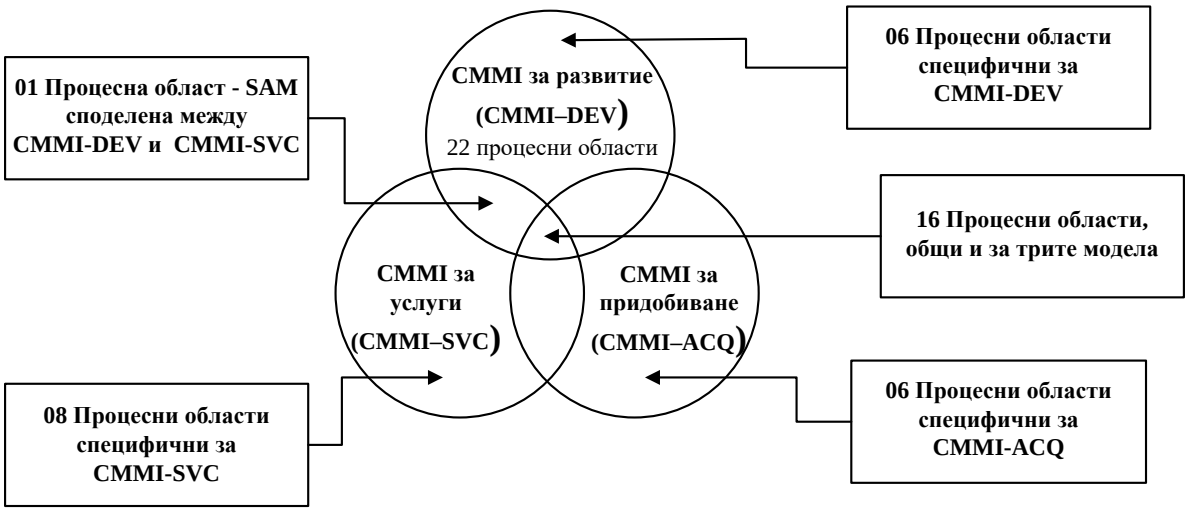
2.1.5. CMMI

CMMI е модел на процесна структура (рамка) за усъвършенстване на процесите, която е създадена чрез подбор и систематизация на колекция от най-добри практики в областта на мениджмънта на ИТ при постигане на бизнес целите на организацията. В настоящия момент този общ модел, който е приложим за пълния спектър от индустрии (софтуерно инженерство, производство, финанси, компютърен хардуер, отбрана, телекомуникации и т.н.) се състои от три интегрирани модела (подмодели), които могат да имат общи и отделни, собствени елементи, наречени процесни области.

CMMI първоначално е създаден за нуждите на софтуерния инженеринг, но с течение на годините силно се генерализира, придобива високо ниво на обобщеност и абстрактност, за да обхване и други области на дейност, отнасящи се за предоставяне на всякакъв вид услуги, както и за придобиване на продукти и услуги. В последните си версии, моделът не е специфично предназначен само за софтуерния инженеринг, за разлика от своя предшественик „софтуерния" CMM, и в момента представлява едно обобщение на концепциите за подобряване на управлението на процесите[2].

Трите интегрирани модела, представляващи компонентите на последната версия на CMMI са:

- CMMI за развитие (CMMI–DEV) – предназначен е за развитието на софтуерни продукти и услуги;
- CMMI за придобиване (CMMI– ACQ) – регламентира придобиването на продукти и услуги;
- CMMI за услуги (CMMI– SVC) – разглежда внедряването, управлението и доставката на услуги.



CMMI като цяло, и всеки от неговите три подмодела, е:

- процесно ориентиран подход, който осигурява на организациите базовите елементи за реализиране на ефективни процеси;
- може да бъде използван като ръководство за усъвършенстване по отношение на екип, проект, подразделение или цялата организация, или за формулиране на приоритетите и на структурирана съвкупност от цели за подобряване на процесите;
- предлага указания за осигуряване на качество на процесите, предоставя отправна точка за оценка на текущите процеси.

2.1.6. СУИС

Системата за управление на информационната сигурност (СУИС) представлява модел за създаване, внедряване, експлоатация, мониторинг, преглед, поддържане и подобряване на защитата на информационните активи на организацията, за да се осигури постигане на нейните бизнес цели, базирани на оценка на риска спрямо дефинирани нива на допустимия риск, определени от гледна точка на ефективно третиране и управление на риска. Успешното внедряване на СУИС може да се осъществи чрез анализ на изисквания за сигурност на информационните активи и прилагане на подходящи контроли и проверки, които да гарантират тяхната защита.

Като част от СУИС, рисковете асоциирани със информационните активи на организацията трябва да бъдат адресирани. Постигането на информационна сигурност изисква да бъде управляван риска, който обхваща видовете риск, асоциирани с физически, човешки и технологични заплахи, отнасящи се за всички форми на информация, използвани от организацията. Внедряването на СУИС е стратегическо решение за организацията, затова е необходимо тя да бъде старателно проектирана, интегрирана и актуализирана в съответствие с нуждите на организацията. Създаването и внедряването на СУИС зависи от целите на организацията, изискванията за сигурност, използваните бизнес процеси и от размера и структурата на организацията. При проектирането и експлоатацията на СУИС трябва да бъдат отразени интересите и изискванията по сигурността на информацията на всички заинтересовани страни на организацията, включително клиенти, доставчици, бизнес партньори, акционери и трети страни[2].

Възприемането и адаптирането на стандартите от фамилията СУИС се счита за все по-важно от организациите, тъй като демонстрира пред бизнес партньорите и други заинтересовани страни техните способности за последователно прилагане на широко известни и разпознаваеми принципи по сигурността на информацията. Внедряването на изискванията на стандартите позволява на организациите да управляват сигурността на своите информационни активи и да извършат подготовка за осъществяване на независима оценка за възможностите на тяхната СУИС да осигурява защита на информацията под всякаква форма – финансова информация, интелектуална собственост, данни за персонала и лични данни, информация, поверена им от техните потребители или от партньори.

2.1.7. ISO/IEC 27000

Серията предлага система от най-добри практики и препоръки за управление на сигурността на информацията, оценка на рисковете и въвеждане на контроли в контекста на цялостната СУИС, която е проектирана по начин, който я прави съвместима структурно и функционално със системите за управление, разработени и въведени с другите стандарти на ISO, като например за управление и гарантиране на качеството (QMS на серията ISO 9000) или за управление на ИТ (ITMS на серията ISO 20000).

Серията ISO 27000 е създадена съзнателно с максимално широк обхват както по отношение на качествените параметри и техническите условия и въпроси на сигурността на информацията, така и на обхванатите организации по тип, размери и сфера на дейност. Организациите от всякакъв вид са заинтересовани и насърчавани да прилагат стандарта цялостно или в отделни негови части, които смятат за подходящи и уместни в зависимост от своите нужди, при реализацията на указанията и предложенията за оценка на риска и на контрола за сигурността на информацията.

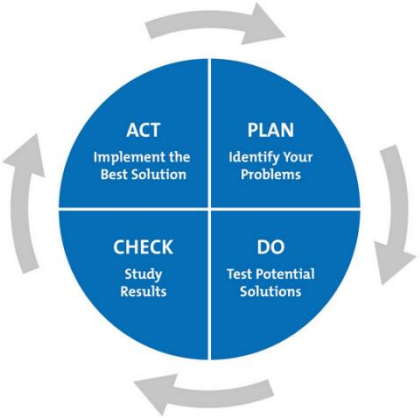
ISO/IEC 27000 регламентира изискванията за внедряване, управление, документиране и непрекъснато усъвършенстване на СУИС с приложение на подход, базиран на управление на риска за сигурността на информацията в организацията чрез установяването му в предварително определен диапазон на допустими стойности. По този начин дейностите по внедряване на системата СУИС се съсредоточават в посока идентифициране, анализ и оценка на рисковете и намаляването им до предварително зададено приемливо ниво, като за целта се използва съдържащата се в стандарта система от контролни точки за оценка на риска. Контролите покриват всички области, където сигурността на информацията може да бъде компрометирана и указват къде да се фокусират усилията на организацията при подготовката и приложението на подходящи политики и процедури за осъществяване на процесите.

Като цяло ISO/IEC 27000 следва модела на другите стандарти на ISO, осигуряващи дефиниции и речници, тъй като сигурността на информацията, както и повечето технически дисциплини, развива сложна терминологична структура[2].

2.1.8. PCDA

С понятието „процесен подход" се означава съвместното прилагане на система от процеси в организацията - идентифицирането и взаимодействието на тези процеси и тяхното управление. За да функционира ефективно, една организация трябва да идентифицира и управлява множество дейности. Всяка дейност използва ресурси и управление с цел да трансформира входящите елементи в резултати на изхода, което се разглежда като един процес. Много често резултатите от един процес служат за входящите елементи на следващ процес.

Подобно на другите стандарти на ISO, използващи процесния подход, серията ISO 27000 възприема и прилага процесния модел PDCA ("Plan-Do-Check-Act") за структуриране на включените в СУИС процеси. Предвид динамичния характер на информационната сигурност, концепцията на СУИС включва непрекъсната обратна връзка и подобряване на дейностите, което е базов принцип на подхода PDCA, като стремежът е да се следи динамиката и промените на заплахите и уязвимостите и въздействието на инцидентите върху сигурността на информацията.



Процесите, които влизат в отделните фази на модела PDCA:

1. Планиране (Plan) - въвеждане на СУИС: Създаване политика, цели, процеси и процедури за СУИС, отнасящи се до управление на риска и подобряване на сигурността на информацията за постигане на резултати в съответствие с общите политики и цели на организацията.

2. Реализация (Do) – внедряване и експлоатация на СУИС: Внедряване и задействане на СУИС политиката, контролите, процесите и процедурите.

3. Проверка *(Check)* – мониторинг и анализ на СУИС: Извършване на оценка, и където е приложимо, измерване на реализацията на процесите в съответствие със СУИС политиката и целите, докладване на резултатите на ръководството за анализ.

4. Усъвършенстване *(Act)* – поддръжка и развитие на СУИС: Предприемане на превантивни и коректив и действия, базирани на резултатите от вътрешния одит на СУИС, анализ на управлението и друга значима информация, за да се постигне непрекъснато подобрение на СУИС[2].

2.2. COBIT

COBIT (Control Objectives for Information and related Technology) е световно признат като система от инструменти, която мениджъри и специалисти от всякакъв тип организации могат да използват, за да гарантират, че тяхната базирана на ИТ информационна система им помага да решат стоящите пред тях задачи, да реализират намеренията си и да постигнат своите цели. [5]

COBIT 5 предлага цялостна методика, подпомагаща решаването на задачите по ръководството и управлението на ИТ в предприятието. По-просто казано, COBIT помага на предприятията да получат оптимална стойност от ИТ чрез поддържане на баланс между получените ползи и оптимизацията на рисковете и ресурсите. COBIT 5 дава възможност за ръководство и управление на ИТ в рамките на цялото предприятие, както в областите на функционалните отговорности на ИТ,

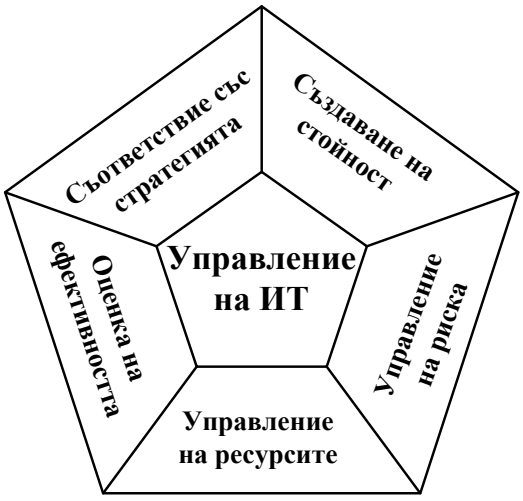
така и на бизнеса, като се отчитат потребностите от ИТ на вътрешните и външните заинтересовани страни.

Ръководството (governance) осигурява увереност за достигане на целите на предприятието чрез:

- балансиране на оценките за нуждите на заинтересованите страни, съществуващите условия и възможните варианти;
- задаване на направлението на развитието чрез приоритизация и приемане на решения;
- постоянен мониторинг за съответствие на фактическата производителност и степента на изпълнение на изискванията с приетите направления и цели на предприятието

Управлението (management) се заключава в планиране, създаване, изпълнение и наблюдение на дейностите, в съответствие с направленията, зададени от органите на ръководството, за постигане на целите на предприятието.

Прилагането на COBIT позволява на ръководството чрез оптимизиране на ИТ управлението да постигне реализация на бизнес целите на организацията в няколко основни (ключови) области (IT Governance Focus Areas - ITGFA)



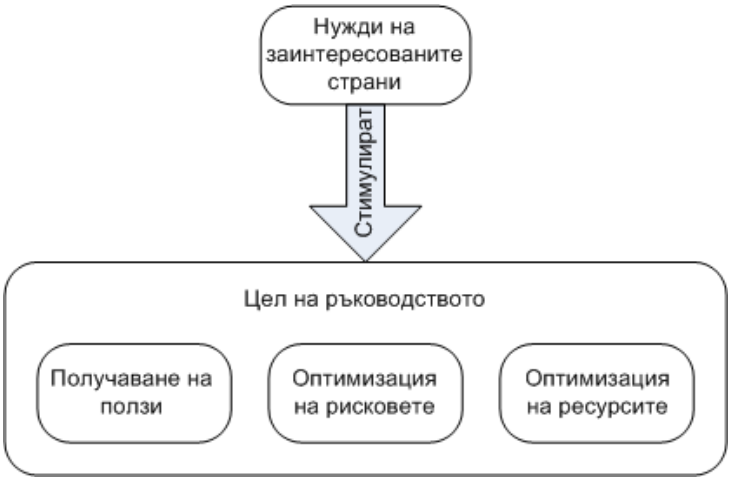
Целите, свързани с дейността на ИТ функциите са: подобряване изпълнението на дейността и управлението на разходите; по-бързо предоставяне на информационни услуги за потребителите; Подобряване на качеството на информационното обслужване, въвеждане на иновации; прозрачност в процеса на поемане на рискове и съответствие с рисковия профил на организацията; по-добро управление на риска от ИТ за бизнеса; съдействие за интеграция и стандартизация на бизнес процесите; задоволяване нуждите на потребителите и разширяване на техния брой.

2.2.1. Основни принципи на COBIT 5

COBIT 5 се базира на 5 принципа, които позволяват да се създаде ефективна методология за ръководство и управление на ИТ в предприятието, с цел оптимизиране на инвестициите в ИТ и получаване на ползи от заинтересованите страни[2]:

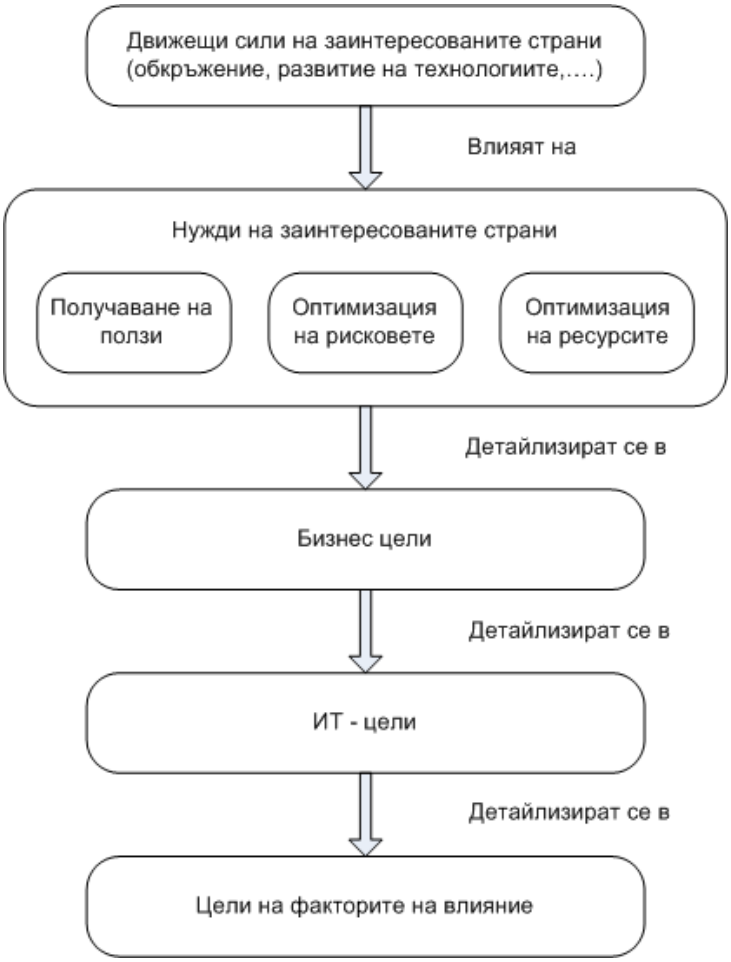
2.2.1.1. Принцип 1: Съответствие на нуждите на заинтересованите страни

Предприятията (публични или комерсиални) съществуват за да създават стойност за заинтересованите страни, което е и основна цел на ръководството. Създаването на стойност означава получаване на ползи при оптимизация на рисковете и на използване на ресурсите. Ползите могат да са различни: например на комерсиалните предприятия е важна финансовата полза, за обществените (държавните) – качеството на услугите, предлагани на населението. От резултатите на предприятието са заинтересовани множество страни, с различно разбиране за ”ползи”. При оценка на ползите, рисковете и ресурсите, ръководството трябва да отчита интересите на всички страни.



Каскада на целите на COBIT 5

Всяко предприятие работи в даден контекст, който се определя от външни фактори (пазар, отрасъл на икономиката, геополитика и т.н.) и вътрешни фактори (култура, организационна структура, склонност към риск и т.н.), като системата за ръководство и управление трябва да се настрои за отчитане на тези фактори. Каскадата на целите на COBIT 5 е механизъм за привеждане на нуждите на заинтересованите страни в конкретни, практични и гъвкави цели на предприятието, ИТ- цели и цели на факторите на влияние. Това позволява да се формулират и избират конкретни цели за всяко ниво и всяка област на ръководство, така че да се поддържат общите цели и нужди на заинтересованите страни чрез постигане на целите на предприятието с въвежданите ИТ решения и услуги.



Каскадата на целите на COBIT 5 минава през следните стъпки:

Стъпка 1: Движещите сили на заинтересованите страни влияят на техните потребности – на тези потребности влияят множество движещи сили, като изменение на стратегията, изменение на бизнес средата и/или законодателството, новите технологии.

Стъпка 2: Потребностите на заинтересованите страни се свързват с целите на бизнеса – разработени са на база измерванията чрез Системата за балансирани показатели (Balanced Scorecard) на Каплан и Нортън и представляват списък от най-широко приложимите цели, които може да определи за себе си предприятието.

Стъпка 3: Целите на предприятието се свързват с ИТ-целите – постигане на целите на предприятието изискват получаване на множество ИТ резултати, които се описват с ИТ целите. Под ИТ се разбират информационните и свързаните с

информацията технологии, а ИТ целите се структурират по измеренията (перспективите) на балансираните карти с ИТ показатели. COBIT 5 определя 17 ИТ-цели.

Стъпка 4: ИТ-целите се свързват с целите на факторите на влияние –фактори на влияние включват процеси, организационни структури и информация (те са част от 7-те фактора на влияние, разгледани подробно в 4-ия принцип на ръководството), като за всеки фактор се определя набор от конкретни цели, които се свързват с ИТ-целите.

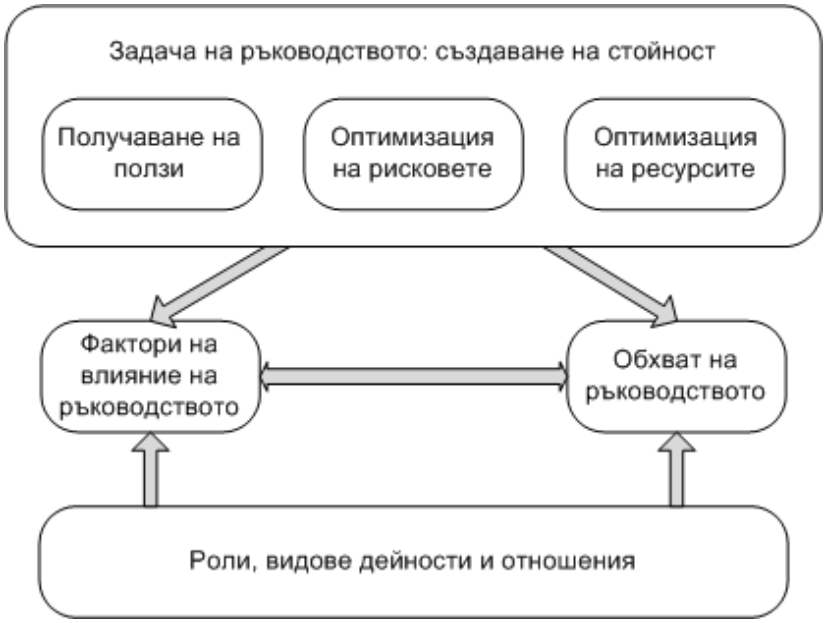
2.2.1.2. Принцип 2: Комплексен поглед на предприятието

Методологията на COBIT 5 разглежда предприятието комплексно, по цялата верига на създаване на стойност, включително ръководството и управлението на ИТ, което означава, че:

- разглежда ръководството на ИТ като част от ръководството на предприятието като цяло, поради което системата за ръководство на ИТ лесно се интегрира във всякаква система за ръководство;
- описва всички функции и процеси, необходими за ръководството и управлението на ИТ на предприятието, независимо от това, къде се обработва информацията. По този начин методологията на COBIT 5 може да опише всички вътрешни и външни ИТ услуги и свързаните с тях вътрешни и външни бизнес процеси.

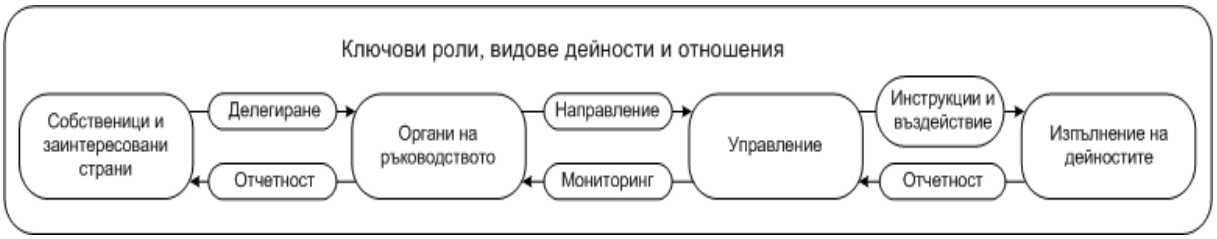
Методологията на COBIT 5 предлага цялостен и системен поглед върху ръководството и управлението на ИТ в предприятието, основан на набор от фактори на влияние. Факторите на влияние са универсални и приложими във всички етапи на създаване на стойност, което означава, че се отнасят към всички аспекти и *лица* (вътрешни и външни), имащи отношение към ръководството на ИТ в предприятието, включващи задълженията и дейностите им по осигуряване на ИТ функциите, а също така и на функционирането на бизнес подразделенията.

Подход към ръководството



Постигане на целта на ръководството на предприятието, създаване на стойност се осъществява с осигуряване на взаимодействието на трите елемента: получаване на ползи, оптимизация на рисковете и опцимизация на ресурсите. Фактори на влияние на ръководството. Това са организационните ресурси на ръководството, такива като методологии, принципи, структури, процеси и практически мерки, които се използват за насочване на дейността и достигане на целите. Факторите на влияние включват също и ресурсите на предприятието, например възможностите, предоставяни от услугите (ИТ инфраструктура, приложения и т.н.), персонал и информация. Недостатъчното количество ресурси може да повлияе на възможностите на предприятието да създава стойност. Обхват на ръководството. Ръководството може да се отнася както за цялото предприятие, така и за отделни подразделения, за материални или нематериални активи и т.н. Това означава, че на предприятието може да се гледа от различни гледни точки в зависимост от обекта на ръководство. Затова при прилагане на методиката на COBIT 5 трябва внимателно да се определя областта на ръководство. Роли, видове дейности, отношения. Последният елемент на ръководството е съвкупността от “Роли, видове дейности, отношения”. Тук се

определя кой и как е въвлечен в ръководството, какво точно влиза в неговите задължения, как се взаимодейства в рамките на системата на ръководство. COBIT 5 въвежда ясно разграничение на дейностите по ръководство и управление (под формата на домейни от процеси), регламентира взаимодействието помежду им и определя включените в тях роли.



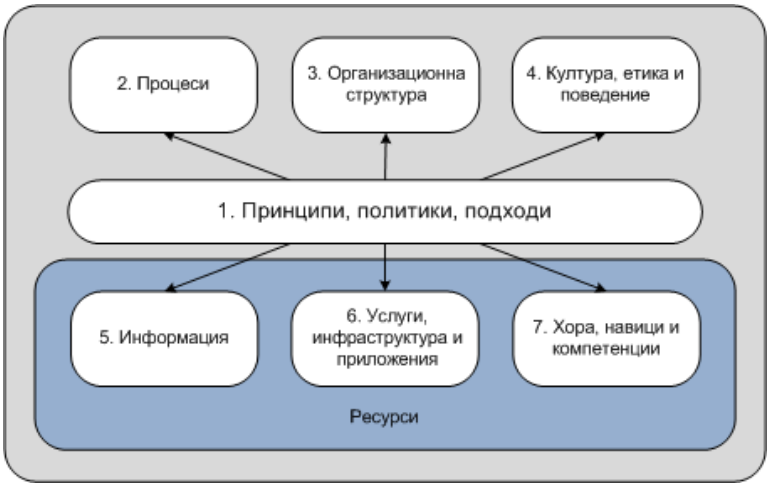
2.2.1.3. Принцип 3: Приложение на единна интегрирана методология

Методологията на COBIT 5 е цялостен подход, защото:

- съответства на най-новите стандарти и подходи, затова предприятията могат да използват COBIT 5 като интеграционна методология по ръководство и управление;
- описва предприятието като цяло, предоставяйки основа за интеграция на другите подходи, стандарти и практически методи.
- обединява знанията в различните подходи на ISACA. Методологията на COBIT 5 обединява разработените от ISACA в продължение на много години подходи и препоръки в помощ на предприятията, такива като COBIT, Val IT, Risk IT, BMIS, Board Briefing on IT Governance и ITAF.
- привежда съдържанието в съответствие с аналогични ръководства, норми и стандарти, такива като ITIL, TOGAF и стандартите на ISO.

2.2.1.4. Принцип 4: Осигуряване на холистичен подход

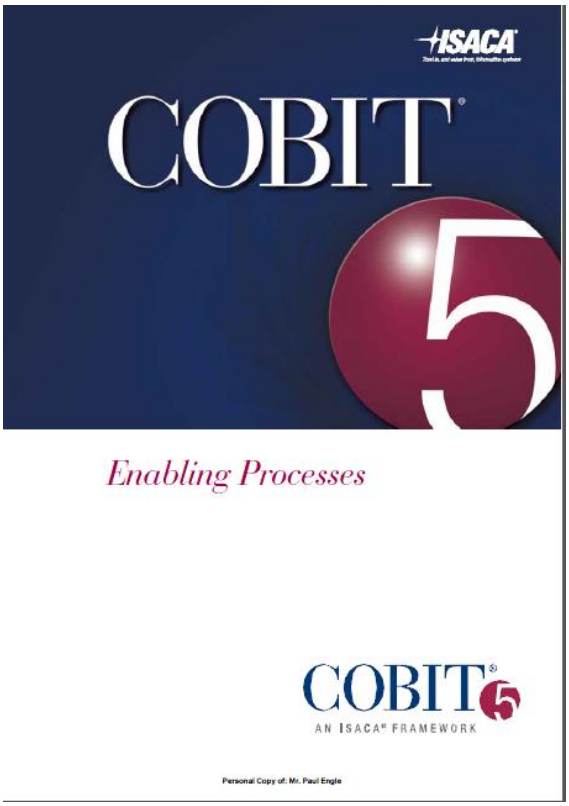
Фактори на влияние на COBIT 5



Факторите на влияние са елементи, които въздействат (по отделно и съвместно) на работоспособността на нещо. В случая – на работоспособността на ръководството и управлението на ИТ на предприятието. ИТ целите (от каскадата на целите) на предприятието определят задачите на различните фактори на влияние за тяхното постигане. Принципи, политики и подходи – осигурява транслация на желаното поведение в практически препоръки по оперативното управление на предприятието.

1. Принципите, политиките и подходите са инструмент за информиране за правилата, действащи в предприятието, така че целите на ръководството и ценностите на предприятието, определени от органите за ръководство и управление, да бъдат известни и осъзнати от всички заинтересовани лица. Принципите и политиките са механизми за комуникация, използвани за предаване на управляващи въздействия и инструкции от органите за ръководство и управление. Подходите към ръководството и управлението предоставят на органите за управление препоръки, структура, инструментариум и други способи за коректно управление на ИТ на предприятието.

2. Процеси – описват структуриран набор от практики и видове дейности, необходими за изпълнението на определени задачи и насочени към получаване на набор от резултати, осигуряващи постигането на ИТ целите. Процес – набор от практики, намиращи се под влиянието на корпоративните политики и процедури, получаващи на входа ресурси от различни източници (включително и други процеси), обработващи ги и формиращи резултати (изходи: продукти и услуги). Цел на процеса – това е "твърдение, в което се описва желания резултат от процеса. Резултатът може да е предмет, значително изменение на състояние или подобряване на възможностите на другите процеси". Целите на процесите (като един от факторите на влияние) влизат в каскадата на целите, т.е. процесите поддържат ИТ-целите, които от своя страна поддържат целите на предприятието.



В публикацията COBIT 5: Enabling Processes (Процесен модел) се съдържа еталонен модел на процесите, в който се описват с голяма детайлизация добрите практики за тяхната реализация и метриката, използвана за тяхната оценка. Нивата на детайлизация на процесите са: процесни практики, видове дейности и подробни видове дейности. Практиките са:

- списък от действия, насочени за получаване на полза, оптимизация на рисковете и оптимизация на използването на ресурсите;
- съответстват на общоприетите стандарти и добри практики
- универсални, поради което се нуждаят от адаптация за конкретната среда;
- описват ИТ и бизнес ролите, включени в процеса.

Видове дейности. В методологията на COBIT 5 това са основни действия, необходими за осъществяване на процеса. Те се определят като "препоръки за съблюдаване на практиките за управление, които водят до успешно ръководство и управление на ИТ на предприятието". Видовете дейности в COBIT 5 показват кое, защо и как да бъде внедрено, така че практиките на ръководство и управление да осигурят повишаване на производителността на ИТ и/или намаляване на риска от дадени ИТ решения или от предоставяни услуги. Подробни видове дейности. Видовете дейности може да са недостатъчни за постигане на ефективни и надеждни ИТ ръководство и управление, затова може да се развият нататък чрез приложение на съществуващите стандарти и сборници от добри практики, такива като стандарт ISO/IEC 20000, ITIL, PRINCE2 и др.

3. Организационна структура – най-важният елемент за приемане и изпълнение на решения в предприятието. Целта на фактора на влияние "Организационна структура" е точното делегиране на пълномощия и определяне на отговорности, определяне на принципите на работа и приложение на добрите практики. Организационната структура се прилага чрез ролите, тяхната дефиниция, взаимодействие и тяхното участие в изпълнението на практиките и дейностите на процесите като "отговорен" (Responsible), "утвърждаващ" (Accountable), "консултиращ" (Consulting) и "информиран" (Informed). Този RACI модел се въвежда с *COBIT 5: Enabling Processes* под формата на таблици (*RACI chart*) и показва участието на ролите и структурите, тяхното взаимодействие и отговорности при реализацията на практиките и дейностите на процесите.

Различните нива на участие са:

- Responsible – Кой изпълнява задачата? Отнася се за ролите с операционни функции, изпълняващи дейностите за постигане на търсения резултат.
- Accountable - Кой отчита успеха на задачата? Носи цялостна отговорност за изпълнение на задачата. Може да има по-високи и по-ниски нива на отчетност. Ролята може да има и операционни функции при изпълнение на задачата.
- Consulting – Кой осигурява входящите данни? За осигуряване на входящите данни получава информация от другите роли и външни партньори.
- Informed – Кой получава информация? Това са роли, които са информирани за постиженията по изпълнение на задачата.

4. Култура, етика и поведение - колективни и индивидуални модели на поведение на отделните хора и на цялото предприятие като съставляваща на успешното ръководство и управление. Към този фактор на влияние може да се отнесат аспектите:

- организационна етика, явяваща се следствие от ценностите на предприятието;
- лична етика, явяваща се следствие на персоналните ценности на служителя, зависещи от външни фактори, като националност, религия, социално-икономическо положение, личен опит и др.
- индивидуални модели на поведение, заедно определящи културата на предприятието. Никои модели на поведение са: склонност към риск; склонност към следване на политиките; отношение към негативните резултати и т.н.

5. Информация – ползва се повсеместно от всякакви организации и включва в себе си цялата информация (която може да е структурирана или неструктурирана, формализирана или неформализирана), произвеждана и използвана от предприятието. Информацията е фактор на влияние на ръководството, защото чрез нейното използване заинтересованите страни могат да осъществяват ръководството, да изпълняват определени роли и да си взаимодействат. Информацията служи за осъществяване на управлението и на

дейността на организацията, а на оперативно ниво често пъти информацията се явява главен резултат от дейността на организацията. За да има стойност за предприятието, информацията трябва да съответства на три аспекта за качество:
а) пряко качество – степен на съответствие на записаното значение на фактическото. Включва характеристиките:

- точност – степен на коректност и надеждност на информацията;
- обективност – степен на справедливост, непредубеденост и безпристрастност на информацията;
- достоверност – степен на истинност и довереност на информацията;
- репутация – степен на авторитетност на информацията.

б) контекстуално или репрезентативно качество – степен на приложимост на информацията за ползвателя. Включва характеристики, описващи качеството в контекста на използване :

- актуалност – степен на приложимост на информацията за решаване на конкретна задача;
- пълнота – степен на загуба на данни и достатъчна детайлност за изпълнение на задачата;
- новост – степен на актуалност на информацията;
- достатъчен обем информация – съответствие на обема на информацията на изпълняваната задача;
- удобство на представянето – компактност на представянето на информацията;
- еднообразие – универсалност на формата на представяне на информацията;
- интерпретируемост – достъпност на информацията на необходимите езици, в нужните символи и единици за измерване, наличие на ясни определения;
- ясност – удобство за възприемане на информацията;
- простота на използване – степен на простота на използване на информацията и използването ѝ за различни задачи.

в) качество на сигурност и достъп – степен на достъпно и лесно получаване на информацията.

- достъпност/своевременност – достъпност на информацията в нужния момент, бързина и удобство на достъпа;
- ограничение на достъпа – степен на защитеност на информацията от несанкциониран достъп.

6. Услуги, инфраструктура и приложения – фактор, включващ инфраструктура, технологии и приложения, предоставящи на предприятието инструменти за обработка на информацията и за предоставяне на услуги. Сервизни възможности – това са ресурси, такива като ИТ инфраструктура и приложения, които се използват за предоставяне на ИТ услуги. Моделът на сервизните възможности се базира на създаване и поддържане на необходимата архитектура. Добри практики за осигуряване на сервизни възможности – определяне на принципите на архитектурата. Те са препоръки към ръководството на високо ниво по отношение на внедряването и използването на ИТ ресурсите на предприятието. Примери за такива принципи са:

- Повторно използване. При проектиране и внедряване на целева и преходна архитектура трябва да се използват универсални компоненти.
- Да се купува или да се създава. Решенията трябва да се купуват само ако няма обосновани причини за отказ от разработване със собствени сили.
- Простота. Архитектурата на предприятието трябва да бъде проектирана и да се поддържа възможно най-проста, но да е съобразена и да отговаря на изискванията на предприятието.
- Гъвкавост. Архитектурата на предприятието трябва да бъде гъвкава, за да отговаря ефективно и рационално на променящите се бизнес нужди на предприятието.
- Откритост. В архитектурата трябва да се прилагат откритите отраслови стандарти. Предоставяне на заинтересованите страни на достъп до архитектурата

– модели, каталози, матрици, които описват архитектурата (например демонстрация на приложенията и как си взаимодействат).

7. Хора, навици, компетенции – необходими са за изпълнението на всички видове дейности, за приемането на правилни управленски решения и за изпълнение на коригиращи действия. Важен фактор на влияние върху изпълнението на ИТ и бизнес целите на предприятието. Образованието, квалификацията, техническите знания, опита, поведението и навиците за обработка на знания са необходими за успешно изпълнение на процесите и функционалните роли. Необходимо да има ясна представа за текущото ниво на компетенциите и навиците на сътрудниците и да се планират бъдещите нужди. Навиците и компетенциите трябва да се разработват (чрез обучение), да се придобиват (чрез подбор на нови кадри) и да се внедряват в организационната структура.

2.2.1.5. Принцип 5: Разделяне на ръководството от управлението

Методологията на COBIT 5 прокарва ясна граница между ръководство (Governance) и управление (Management). Тези две дисциплини включват различни дейности, изискват различни организационни структури и служат на различни цели. Според COBIT 5 разликата между ръководство и управление се заключава в следното:

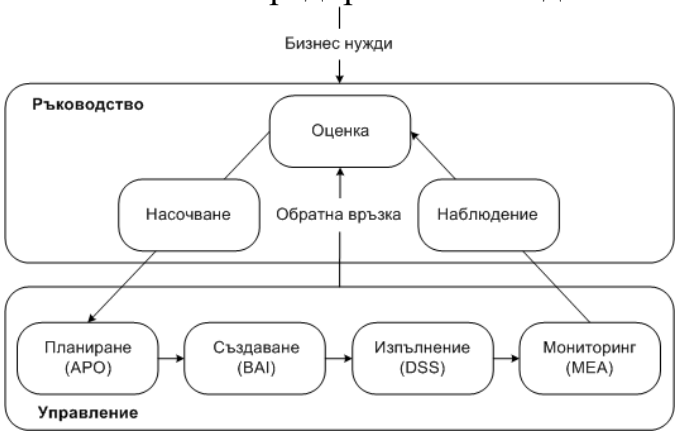
Ръководството (Governance) осигурява увереност за достигането на целите на предприятието по пътя на: балансирана оценка (Evaluate) на потребностите на заинтересованите страни, съществуващите условия и възможните варианти; определяне на направлението (Direction) на развитие чрез приоритизация и приемане на решения; постоянен мониторинг (Monitoring) за съответствие на фактическата продуктивност и степен на изпълнение на изискванията с приетите направление и цели на предприятието (EDM).

Управлението (Management) се отнася за планиране (Plan), създаване (Build), изпълнение (Run) и наблюдение (Monitor) на дейностите в съответствие

със зададените направления от органите на ръководството, за постигане на целите на предприятието (PBRM).

Модел на процесите на COBIT 5

Еталонният модел на процесите на COBIT 5 разделя всички процеси по ръководство и управление на ИТ на предприятието на два основни домейна:



1. Ръководство. Съдържа 5 процеса на ръководство със съответните практики и активности за оценка, насочване и наблюдение (Evaluate, Direct, Monitor - EDM).

2. Управление. Отнася се за областите на отговорност планиране, създаване, изпълнение, мониторинг (Plan, Build, Run, Monitor - PBRM), които показват комплексен поглед върху управлението на ИТ.

Домейнът “управление” се състои се от 4 домейна (поддомейни), всеки от които съдържа процеси, отнасящи се за различни области на отговорност по управлението:

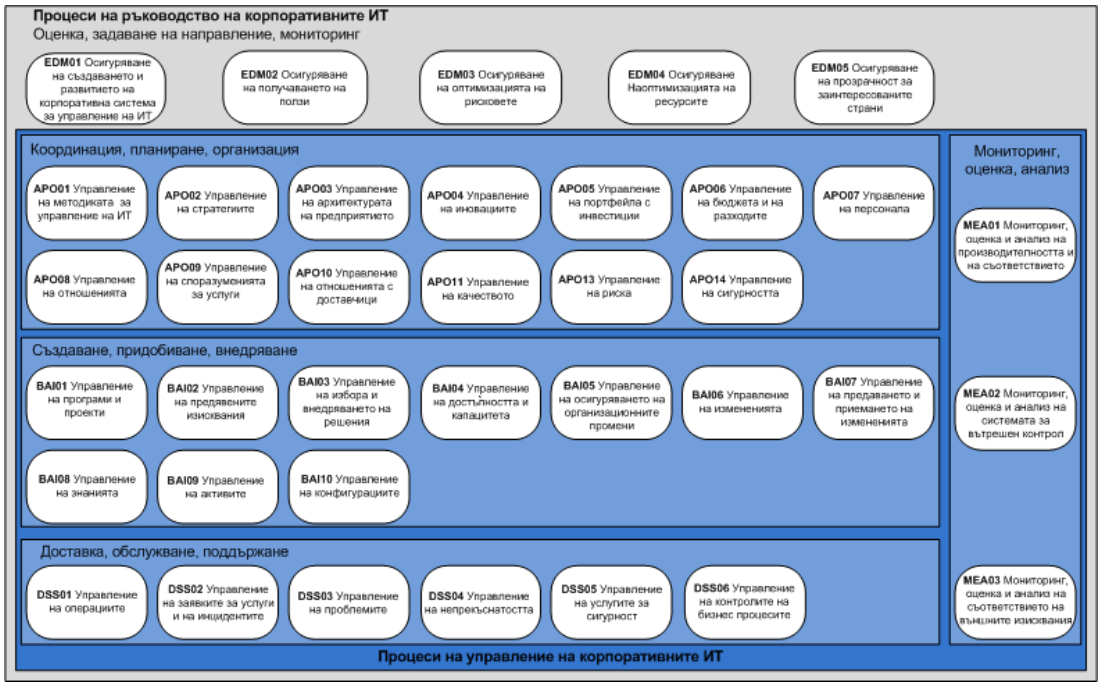
2.1. Координация, планиране, организация - Align, Plan, Organise (APO) – 13 процеса;

2.2. Създаване, придобиване, внедряване - Build, Acquire, Implement (BAI) - 10 процеса;

2.3. Доставка, обслужване, поддържане - Deliver, Service, Support (DSS) - 6 процеса;

2.4. Мониторинг, оценка, анализ - Monitor, Evaluate, Assess (MEA) - 3 процеса.

2.2.2. Модел на възможностите на процесите на COBIT 5



В пакета от продукти на COBIT 5 е включен модел за оценка на възможностите на процесите, базиран на ISO/IEC 15504. Моделът е предназначен за решаване на задачите по оценка на изпълнението и за усъвършенстване на процесите. Предлага способ за измерване на производителността на всеки един процес, както в домейна на ръководството на ИТ (EDM), така и в домейна на управлението на ИТ (PBRM) и позволява да се набелязват и формулират направления за усъвършенстване на процесите. Моделът включва шест нива на възможност на процесите, като всяко от тях (с изключение на ниво 0) е свързано със съответни атрибути (характеристики), които описват различието на всяко следващо ниво спрямо предходните нива:

0. Непълен процес. Такъв процес не е още внедрен или не съответства на предназначението си. На това ниво липсват доказателства за систематично достижение на целите от процеса, или такива доказателства са малко. Няма атрибути.

1. Осъществен процес. Процесът е внедрен и съответства на своето предназначение. Има един атрибут:

PA1.1 Производителност на процеса

2. Управляем процес. Осъществяваният процес от предишното ниво е управляем (т.е. планиран е, проследява се и се коригира). Създават се, контролират се и се поддържат работните продукти на процеса. Има два атрибута:

PA2.1. Управление на производителността

PA2.2. Управление на работните продукти

3. Установен процес. Управляемият процес от предишното ниво вече предоставя възможности за получаване на очаквани резултати. Има два атрибута:

PA3.1. Определение на процеса

PA3.2. Внедряване на процеса

4. Предсказуем процес. Установеният процес от предишното ниво вече предоставя възможности за получаване на резултати в условията на зададени ограничения. Има два атрибута:

PA4.1. Управление на процеса

PA4.2. Контрол на процеса

5. Оптимизиран процес. Предсказуемият процес от предишното ниво непрекъснато се усъвършенства, с цел постигане на текущите и бъдещите цели на предприятието. Има два атрибута:

PA5.1. Иновативност на процеса

PA5.2. Оптимизация на процеса

Процесът от ниво “0” не съответства на своето предназначение. Възможностите на ниво “1” означават, че като цяло е достигнат атрибута “производителност на процеса”, т.е. процесът се изпълнява и предприятието постига нужните му резултати. Постигането на това ниво в много случаи е достатъчно за предприятието. По-високите нива добавят нови атрибути към тези възможности, които повишават ефективността, надеждността и качеството при изпълнение на процесите. Например възможностите на процеса на ниво “3” изискват реализация на атрибутите на ниво “2” плюс своите атрибути, описание

(документиране) и контролирано внедряване на процеса по спецификациите. Всяко предприятие трябва да направи анализ (на база оценка на разходи, ползи, реализуемост и т.н.) и да избере своето целево ниво на възможностите.

2.2.3. Предимствата на COBIT 5

COBIT 5 се основава на модела на процеса, дефиниран по-рано в предишните издания на COBIT. Това е еволюционна промяна, която рационализира съществуващите процеси чрез комбиниране и пренасочване на практики на съществуващите процеси и включващи допълнителни процеси и практики за управление и управление на информационните технологии. Направени са значителни подобрения в системата от инструменти COBIT, за да бъде описан като модел за корпоративно управление на информационните технологии. За разлика от своя предшественик (COBIT 4.1) и ITIL v3, COBIT 5 обхваща всички три нива за управление на ИТ. Както COBIT 4.1, така и ITIL v3 са процесни модели, които описват ИТ практиките на оперативно ниво, осигуряващи полезен източник на добри практики. Независимо от това, нито COBIT 4.1, нито ITIL v3 не се занимават с управленските практики, необходими за нареждане и използват ИТ ресурсите ефективно и ефикасно, нито COBIT 4.1 или ITIL v3 описват процесите на корпоративно управление, които са от съществено значение за насочването и контрола на използването на ИТ. Подобренията на COBIT 5 включват преструктуриране на описанието на отделните процеси, идентифициране на действителните базови практики на всеки процес и описване на ключовите дейности на всяка основна практика. Най-съществената промяна в COBIT е реорганизацията на системата от инструменти от това да бъде модел на ИТ процес в система от инструменти за управление на ИТ с набор от управленски практики за ИТ, система за управление на непрекъснатото усъвършенстване на ИТ дейностите и процес на моделиране с базови практики. [4]

Заключение

С нарастващата зависимост на бизнеса от информационните технологии и уеб пространството нараства и интереса на хакерите към компрометиране чрез злонамерени действия. Причините са много и варират - от чисто удоволствие, през нужда за публично внимание и завършват с бизнес - финансово благополучие чрез измама или атака на конкуренцията.

Проблемът съществува и се задълбочава. Появяват се нови и по - сложни технологии, заедно с които се развиват разнообразни и креативни начини за компрометиране. Това налага усъвършенстване и постоянно развитие на технологиите за защита на информацията. Процесния модел PDCA е един от методите за усъвършенстване на процесите за защита на информацията. COBIT най-добре съответства на идеологията на PDCA и е световно признат стандарт за информационна сигурност и одит на риска.

COBIT е система от инструменти, която има за цел да управлява и ръководи ИТ и да подпомага ръководителите при определянето и постигането на бизнес и свързаните с ИТ цели. Системата от инструменти се счита за най-важната насока за управление на ИТ, която някога е била публикувана.

Моделът COBIT би подобрил управлението на наличните информационни ресурси и по този начин да съдейства за адекватното посрещане на правни и бизнес изисквания, както и за постигането на други цели. Това може да са задачи свързани с повишаване нивото на сигурност на информационната инфраструктура, с управление на данните в една или друга тяхна форма и по време на целия им жизнен цикъл, както и много други. По този начин организацията ще избегне опасностите от строго конфиденциална информация да бъде разгласена, данните да бъдат неточни или пък да не бъдат потвърдени, информацията да се получи от грешен потребител, да бъдат прекъснати информационните ресурси. Моделът трябва да се ползва от одитори и компании като начин за интегриране на технологиите с цел въвеждането на контролни функции и реализация на специфичните за бизнеса цели.

Според мен, COBIT е най-подходящ да се прилага от компании, най-вече за управление на риска. Прилагайки подходящата стратегия, рисковете се ограничават. За да бъдат удовлетворени нуждите на компанията, е необходимо информационните системи да предоставят пълни данни, качествен и лесен достъп до информацията, подобрено изпълнение на дейността, съгласувана отчетност и гъвкаво управление на ресурсите.

Източници

1. Денчев, Стоян, Семерджиев, Цветан. Концепция и политика за информационната сигурност.
2. Митев, Николай, Семерджиев, Цветан. Норми и стандарти за управление на информационните системи.
3. https://fisn.uni-plovdiv.bg/sandalski/zastita_na_FIS/Tema12.docx
4. http://itgovernance.com/changes%20in%20cobit5.pdf
5. https://en.wikipedia.org/wiki/COBIT