Механика Транспорт Комуникации

ISSN 1312-3823 (print)
ISSN 2367-6620 (online)
том 16, брой 2, 2018 г.
Научно списание **http://www.mtc-aj.com** **статия № 1700**

ДОБРИ ПРАКТИКИ ЗА УПРАВЛЕНИЕ НА РИСКА ПРИ ОСИГУРЯВАНЕТО НА ИНФОРМАЦИОННА СИГУРНОСТ

Мария Христова[1], Димитър Бахчеджиев[2]
mhristova@vtu.bg, dimitar.bahchedzhiev@intertek.com

[1]Висше транспортно училище „Тодор Каблешков“,
1574 София, бул. “Гео Милев” 158,
[2]Интертек ВА ЕООД
БЪЛГАРИЯ

Ключови думи: *информация, информационна сигурност, управление на риска, стандарти, система за управление на сигурността на информацията*

Резюме: *В съвременния взаимосвързан свят информацията и свързаните с нея процеси, системи, мрежи и персонал, участващ в нейната обработка, използване и защита, са активи, които са ценни за оцеляването на организациите и изискват защита срещу различни заплахи и опасности. Това е причината компютърната сигурност и информационната защита на компютърните системи и мрежи и използваната в тях информация да са основни елементи на информационната сигурност.*

Организациите трябва да изградят и поддържат компетентност и познания в сферата на информационната сигурност. Според авторите на настоящата работа в най-структуриран и цялостен вид това може да стане с помощта на адаптираните изисквания и практики, залегнали в световно утвърдените рамка и практики от серията международни стандарти по информационна сигурност ISO/ IEC 27000. В статията е представен процесът за управление на риска при осигуряване на сигурността на информацията. Разгледан е „методът на папийонката“ като особено полезен графичен метод за анализ на риска. Изследва се структурата от стандарти, изисквания, препоръки за създаване, развитие и поддържане за системите за управление на информационната сигурност. Анализирани са иновативни подходи за прилагане на мерките за контрол от приложение А на БДС EN ISO/IEC 27001:2017 и кодекса за добра практика за управление на риска при осигуряване сигурността на информацията.

ВЪВЕДЕНИЕ

В съвременното информационно общество социалните организации, независимо от сферата на дейността, типа и размера им, акумулират голямо количество чувствителна информация, в това число информация за служители, клиенти, продукти, разработки, финанси и т.н. Огромна част от тази информация (за повечето организации до 100%) се събира, обработва и съхранява в електронна форма. Информационните активи са обект както на преднамерени, така и на случайни заплахи, а свързаните с тях процеси, системи, мрежи и хора имат присъщи уязвимости. Примери за такива заплахи

са: измами, саботаж, вандализъм, пожар, наводнение и разбира се огромният брой хакерски атаки, които се реализират ежедневно.

Все повече компании прехвърлят част от нуждите си в областта на информационните технологии към доставчици на облачни услуги (cloud service), като създават хибридни инфраструктури, в които вътрешната им мрежа трябва да си взаимодейства безпроблемно и по сигурен начин със сървъри, собственост на трети страни. През последните години се наблюдава растяща кибер зависимост на световната общност, дефинирана от експерти в света на икономиката, политиката, науката и обществения живот. като сериозна тенденция в доклада на Световния икономически форум в Давос „Глобални рискове за 2018 година“ [1]. Посочва се, че пробивът в киберсигурността, както и кражбите и измамите с лични данни са сред първите пет най-сериозни глобални рискове пред човечеството през 2018 г. С всяка изминала година щетите от кибератаки върху световната икономика и държавните организации се увеличават, а операциите в интернет пространството са част от съвременните конфликти.

От друга страна измененията в процесите и системите на дейността или други външни промени могат да създадат нови рискове за сигурността на информацията. Новото законодателство, като например Европейският Регламент за защита на личните данни (GDPR), поставя организациите и фирмите под още по-силен натиск, с цел гарантиране сигурността на тяхната информация. Затова поради многообразието на начините, по които заплахите могат да навредят на организацията, винаги има рискове за сигурността на информацията. Информационна сигурност е защитата на информацията и информационните системи от неоторизиран достъп, използване, разкриване, промяна, прочитане, запис и унищожаване. Рискът за сигурността на информацията е възможността дадена заплаха да използва уязвимостите на актив или група активи и по този начин да причини вреда на организацията. Ефикасната сигурност на информацията намалява тези рискове чрез защитаване на организацията от заплахи и уязвимости и по този начин намалява въздействието върху активите им.

При дефинирането на информационната сигурност, международната общност гравитира около запазването на баланса между три основни компонента, а именно *поверителност, цялостност и наличност на информацията*, чрез прилагане на процес за управление на риска и създаване на увереност у заинтересуваните страни, че рисковете свързани с информационните активи се управляват по адекватен начин [13] [14].

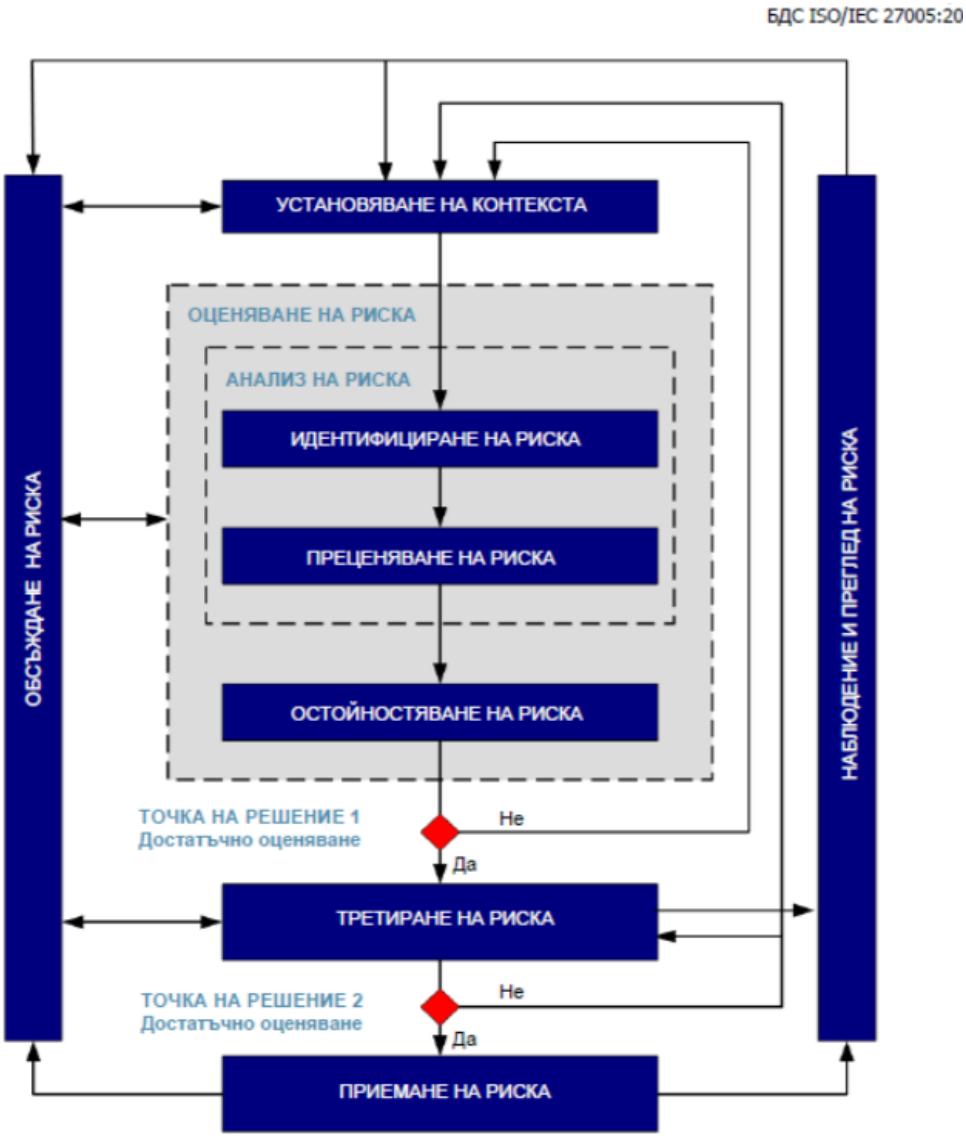
1. УПРАВЛЕНИЕ НА РИСКА ПРИ ОСИГУРЯВАНЕ СИГУРНОСТТА НА ИНФОРМАЦИЯТА

Важно място при осигуряване на информационната сигурност заемат процесите за управление на риска, тестването и оценката на мрежовата и информационна сигурност. Управлението на риска е процес по установяване на уязвимостите и заплахите, свързани с дадена организация и бизнес процесите, както и мерки за редуцирането на този риск до приемливи нива. Той е важна част от защитата на информацията. Процесът на управление на риска от страна на организациите е систематично прилагане на политика, процедури и практики за управление на дейностите за обмен на информация, за консултиране, за установяване на обстоятелствата, както и дейностите по идентифициране, анализ, преценяване (оценка), въздействие, наблюдение и преглед на риска. Това е ***Рамка за управление на риска за информационната сигурност.***

В различните литературни източници [2], [3], [7], [9] и стандарти [4], [5], [6], процесите по управление на риска се различават, но базовите елементи винаги са: идентификация на риска; анализ на риска, оценка на риска, разработване на мерки за

справяне с риска. Според международните стандарти ISO 31000:2018, IEC 31010:2009 и БДС ИСО?ИЕЦ 27005 управлението на риска обхваща следните етапи (Фиг. 1):

1. Установяване на контекста.
2. Идентифициране на рисковете.
3. Анализ на риска.
4. Измерване на риска.
5. Третиране на риска (разработване на мерки за справяне с риска).
6. Мониторинг и преглед.
7. Комуникация и консултация.



Фиг. 1 Процес на управление на риска за информационната сигурност

Каквито и елементи да се включват в процеса на управление на риска, крайната му цел винаги е да минимизира вероятността от сбъдване на нежелани събития и/или последиците от тях. В допълнение към това, отделните елементи са взаимосвързани, тъй като резултатът от един е вход за следващите.

Установяване на контекста. Като първа, необходима предпоставка за успешен и адекватен процес по управление на риска е установяването на контекста, в който функционира дадената организация, тъй като той е един от основните източници на риск. Определят се външните и вътрешните обстоятелства, които са свързани с

целите на организацията и които влияят на нейната способност да постигне желаните резултати от Системата за управление на сигурността на информацията (СУСИ/ ISMS). Това е рамката, в която ще се търсят рискове с цел тяхното управление. Дефинирането на тези обстоятелства се отнася за установяване на външния и вътрешния контекст на организацията, дефиниран в *БДС ISO 31000:2018 - Управление на риска. Принципи и указания* [4].

Следваща стъпка в постигането на съответствие с ISO 27001 (този стандарт ще бъде разгледан по-долу) или осигуряването на адекватна защита на информационната сигурност е определянето на обхвата на СУСИ. За да установи нейния обхват, организацията трябва да определи физическите и виртуалните граници и приложимостта на системата, като се вземат под внимание външните и вътрешните въпроси от организационния контекст и нуждите, очакванията и изискванията за заинтересованите страни, както и интерфейсите и зависимостите между процесите и дейностите, изпълнявани от организацията и тези, които се изпълняват от подизпълнители. Стандартът изисква организацията да документира и поддържа актуални обхвата и границите на системата за управление на информационната сигурност и да ги съхранява на хартиен или електронен носител, за да могат те да бъдат одитирани. Пълният анализ на контекста остава ангажимент на всяка организация, решила да внедри СУСИ. Крайни продукти от етапа са критериите за оценка и значимите външни и вътрешни фактори на средата.

Етапът **Идентифициране на риска** е процес по откриване, идентифициране и описване на съществуващи или потенциални рискови ситуации.

Анализ на риска. След приключване на етапа "идентификация" следва етап на анализ на рисковете спрямо утвърдената методология. При количествен подход към управлението на риска, стъпка „анализ" означава придаването на цифрови стойности за всеки един идентифициран риск по избраната скала. Най-често методологиите за управление на риска се състоят от два фактора, които се анализират (придава им се стойност), а именно „тежест" и „честота".

Процесът по анализ на риска включва: идентифициране и определяне на размера на несигурност; оценка на въздействието върху резултатите, които ни интересуват; изграждане на модел за анализ на риска, който изразява тези елементи в количествена форма. Впоследствие се изследва моделът, чрез симулация и анализ на чувствителността, както и вземане на решения за управление на риска; решения, които могат да ни помогнат рискът да се избегне, намали или да се справим с него по друг начин [7].

Известни са над 30 качествени и графични ***методи за анализ на риска*** [8]. Ето някои от тях:

1. Изследване на опасностите и работоспособността (HAZOP).
2. Анализ на опасностите и контрол на критичните точки (HACCP).
3. Структуриран анализ „Какво, ако?" (SWIFT).
4. Анализ на основните причини.
5. Анализ чрез дървото на отказите (Fault Tree Analysis).
6. Анализ чрез дървото на събитията (Event Tree Analysis).
7. Анализ на нивата на защита (LOPA).
8. Дърво на решенията.
9. Анализ "Причина-последствие" (Метод на папийонката).
10. Матрица на последствията/вероятностите.
11..Анализ на разходите и ползите.
12.. Многокритериален анализ на решенията (MCDA) и др.

Всеки от тези методи има своите предимства и недостатъци и се прилага за конкретни случаи. Особено полезен и използван метод е ***Методът на "папиойнката".*** Целта на този метод, известен още като „Възелът на папийонката".и Анализ "Причина-последствие" е да определи последователността от събития, които могат да доведат до неблагоприятни и нежелани последствия. Състои се в графична комбинация между методите "Дърво на отказите", "Дърво на събитията" и Диаграма на "бариерите" (мерките за безопасност), като комбинира анализа на причините (описани в „дърво на отказите") с анализ на последствията („дърво на събитията"). На фигура 2 е представена типична диаграма на метода на „папийонката".

Фиг. 2 Диаграма на „Метода на папийонката"

Методът на „папийонката" предполага, че е невъзможно да се осигури 100% защита на информационните активи при управлението на риска. Затова в средата на диаграмата е разположен неминуемият инцидент с информационен актив. Съвсем логично, отгоре е разположена проактивната превенция, или с други думи физическите и логическите бариери, с които организацията разполага, за да предотврати реализацията на подобно нежелано събитие. Така или иначе, инциденти с информационните активи възникват рано или късно, затова настоящият метод изисква да се развие и внедри долната част от папийонката, а именно:

- да има готовност за реакция, което ще способства за ограничаване и контрол на щетите;
- да има установен ред (процедури и структура) за анализ на коренните причини и разследване на инцидента.

Последната стъпка позволява да бъде затворен кръгът, да се установят пропуските в превантивната част на „папийонката" и да бъдат взети съответните мерки.

Изчертаването на “Дървото на отказите“ започва с веригата от основни събития отляво надясно (или отдолу нагоре). То се използва, за да илюстрира как тези основни събития или пораждащите ги събития могат да причинят едно “критично“ събитие (т.е. крайното събитие от “Дървото на отказите”). Дясната (горната) страна на „папийонката“ се чертае във формата на “Дърво на събитията”, показващо възможното развитие на критичното събитие в серия от алтернативни последици. Целта на индуктивния анализ “Дърво на събитията” е при наличие на подходящи данни за честотата на проявяване на критичното събитие, да се получи количествена оценка на вероятността за настъпване на определени последствия. Чрез изчисляване на вероятностите за всички иницииращи събития, може да се изчисли вероятността за възникване на всяко едно от последствията, като по този начин се опише нивото на риск за системата. Методът дава възможност и за вземане на най-правилно решение за това, какво подобрение трябва да се направи за предотвратяване на последствията и намаляване на риска.

Оценка на риска

Дейностите по идентификация, анализ и измерване на риска са представени в стандарта ISO 31000:2018 като елементи от общ процес на оценка на риска (Risk assessment). Някои от основните ползи от извършването на оценка на риска включват: разбиране на риска и неговото потенциално въздействие върху целите; предоставяне на информация за вземащите решения; идентифициране на важните участници в рисковете и слабите връзки в системите и организации (Оценка на уязвимостите - Vulnerability Assessment); Оценка на заплахите (Threat Assessment) - вероятността те да се случат, както и какво въздействие биха имали, ако настанат; сравняване на рисковете в алтернативни системи, технологии или подходи; съобщаване на рискове и несигурности; подпомагане при определянето на приоритети, допринасящи за предотвратяването на инциденти въз основа на разследване след инцидента; избор на различни форми на рисково третиране, отговарящи на регулаторните изисквания; оценка на рисковете за изхвърляне в края на жизнения цикъл и т.н.

Организациите използват оценката на риска, за да определят степента на потенциалната заплаха и рисковете, свързани с ИТ системите през целия им процес на създаване и използване (System Development Life Cycle - SDLC). Резултатът от този процес помага да се определят подходящи контроли за намаляване или отстраняване на риска през целия SDLC. Оценката на риска дава информация как целите на организацията могат да бъдат засегнати от идентифицираните опасности и оценените рискове, а също така и да дадат оценка за възможните последствия и вероятностите те да се реализират. Дава оценка за по-нататъшното управление на рисковете и намаляване на тяхното въздействие върху определените цели и резултати.

Това е най-критичният и един от най-трудните етапи от процеса на управление на риска поради трудността в оценяването на нематериалните последици и липсата на достатъчно данни за изследване. Крайната цел на оценката на риска е вземане на решение на кои рискове и как да се противодейства [8].

2. СТАНДАРТИ ЗА УПРАВЛЕНИЕ НА РИСКА ЗА ИНФОРМАЦИОННА СИГУРНОСТ

Принципите и общите насоки за управление на риска се определят от стандарти. Те могат да се използват от всички публични, частни или обществени предприятия, асоциации, групи или отделни личности. Могат да се прилагат през целия жизнен цикъл на организацията.

2.1 IEC/IEC 31010 Управление на риска – техники за оценка на риска е международен стандарт, предназначен да бъдат отразявани текущите *добри практики* в

областта на подбор и използване на техники за оценка на риска. Този стандарт се прилага заедно със стандарт ISO 31000:2009 Управление на риска – принципи и насоки). Посегателство върху марка и репутация на организация, кибер-престъпност, политически рискове и тероризъм са само някои от рисковете пред които частните и обществените организации все по-често са изправени. Новата версия на ISO 31000 „Управление на риска. Указания“, която бе публикувана през февруари 2018 г., има за цел да помогне на организациите да се справят именно с такъв вид проблеми.

2.2 Серия стандарти ISO/IEC 2700x за информационна сигурност

Организациите могат да постигнат сравнително добро ниво на защита на информационните си активи и устойчивост в своите операции, прилагайки световно утвърдените рамка и практики от серията международни стандарти по информационна сигурност ISO/ IEC 2700x [6]. Серията стандарти ISO/IEC 2700x съдържат най-добрите практики и препоръки за създаване, развитие и поддържане на СУСИ и предоставя модел за създаване, внедряване, функциониране, наблюдение, преглед, поддържане и подобряване на защитата на информационни активи. (фиг. 3).

Тези стандарти помагат на организациите да поддържат информационните си активи защитени чрез:

• идентификация на рисковете за стратегията и целите на организацията, като важен елемент от това е идентификацията на активите. Примери за активи могат да бъдат софтуерни приложения, процедури за поддръжка, оборудване и екипировка, съхранявана и архивирана информация, инструменти за развой, външно-предоставяни услуги, човешки ресурс, и дори репутация.

• наблюдение и управление на съответствието със законови, подзаконови, регулаторни и договорни изисквания, които организацията и нейни подизпълнители трябва да спазват, като: законодателство, свързано със защита на данните, лицензионни изисквания за използван софтуер, права за интелектуална собственост, използване на електронни подписи, унищожаване на различни носители на информация и др.

• наблюдение и управление на съществуващи принципи, цели и контрол при обработката на информация в установените процеси и процедури, например съществуващи права за достъп, ясно дефинирани отговорности на потребителите, администраторите и собствениците на информационните активи, прилагани политики при управление на паролите, „чисто бюро“, мобилни устройства и др.

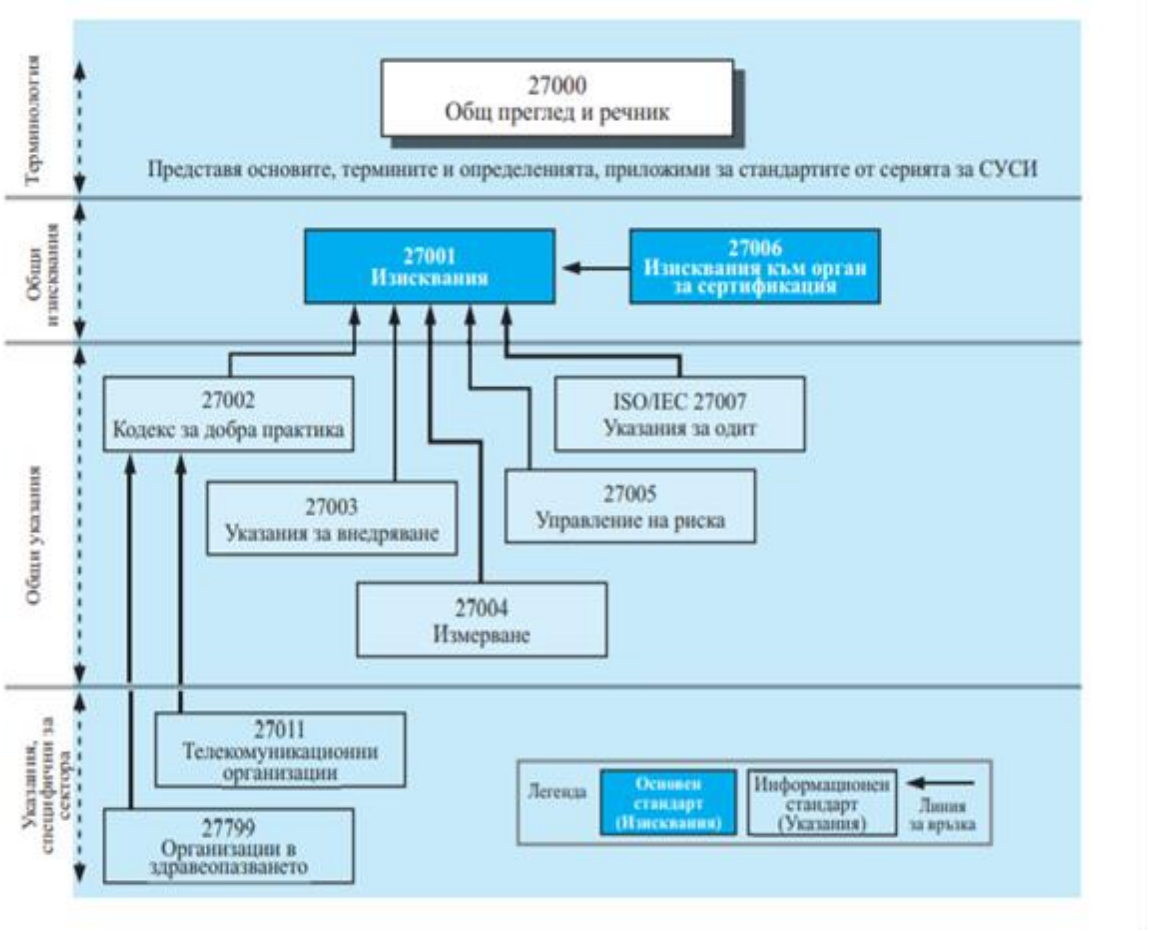
Към регламентиране дейностите и изискванията в тази насока са насочени международните стандарти:

• ISO/IEC 27001:2017 - Информационни технологии – Техники за сигурност – Системи за управление на информационната сигурност – Изисквания

• ISO/IEC 27002:2013 – Информационни технологии – Техники за сигурност – Практики за управление на информационна сигурност.

ISO 27001 [11] е стандарт, който предоставя доказана рамка за управление на сигурността на информацията, като използва интегриран набор от препоръчителни правила, процедури, документи и технологии под формата на система за управление на информационната сигурност. В допълнение към ISO 27001 е подготвен и възприет ISO/IEC 27001:2018, който се отнася за всички видове организации (например търговски предприятия, правителствени агенции и организации с идеална цел) и определя изискванията за създаване, внедряване, функциониране, наблюдение, преглед, поддържане и подобряване на документирана СУСИ с оглед на общия риск, свързан с дейността на организацията. Основни източници за идентификация на рискове и възможности са особеностите на организационния контекст по клаузи 4.1 и 4.2 в ISO 27001 и самите процеси в организацията. Организацията следва да оцени потенциалните последствия, които произтичат от осъществяване на рисковете,

идентифицирани в клауза 6.1.2 и да определи приоритети за въздействие върху тях (третиране), така, че те да бъдат управлявани и контролирани до свеждането им до приемливо ниво според приетите критерии за приемане на риска.



Фиг.4. Взаимовръзка между стандартите от серията за СУСИ

ISO 27002 – (Информационни технологии. Методи за сигурност. *Кодекс за добра практика за управление на сигурността на информацията).* Този международен стандарт дава указания и общи принципи за внедряване, поддържане и подобряване на управлението на сигурността на информацията в дадена организация. Стандартът съдържа списък с общоприети цели по контрола и най-добри практики за механизмите за контрол, които да бъдат използвани. Включва 11 точки, отнасящи се за контрол на риска и съдържащи общо 39 основни категории за сигурност. Международната общност е разработила ръководство с най-ефективните области и аспекти върху, които може да се влияе с цел подобряване на контрола. Това е указателен стандарт-ръководство БДС ISO 27002:2017. Сигурността на информацията се постига чрез внедряване на подходящ набор от механизми за контрол, включително политики, процеси, процедури, организационни структури и функции на софтуера и хардуера.

Актуалната версия на ISO 27002 съдържа 114 контроли, разработени в 35 основни категории в областта на информационните технологии, комуникации, здравния сектор, производството и т.н. Основните секции на стандарта са: структура, политиката на сигурност, организиране на информационна сигурност, управление на активи, контрол на достъпа, криптографията, операции за сигурност, комуникационна сигурност, управление на информационната сигурност при инциденти и други. Не всички от тези 114 контроли са задължителни - организацията може да избере кои контроли намира за приложими и след това да ги прилага. Например, контрол А.14.2.7

„Разработване на софтуер от външни страни“ може да бъде определен като неприложим, ако дадена фирма не възлага разработването на софтуер, а използва изцяло готови решения. Процесът по управление на риска, помага да се приоритизират управленските решения за внедряване механизмите за контрол, подбрани да защитават от идентифицирани и неидентифицирани рискове.

ISO/IEC 27005 На 20 август 2018 в допълнение към ISO/IEC 27001 е публикувана актуализирана версия на стандарта ISO/IEC 27005 - ISO/IEC 27005:2018 „Информационни технологии. Методи за сигурност. Управление на риска за сигурността на информацията“ [12]. ISO/IEC 27005 е актуализиран, за да отрази промените в новата версия на ISO/IEC 27001 и по този начин да гарантира, че ще отговори на съвременните изисквания на всички типове организации по най-добрия начин и че управлението на риска е съобразено с тяхната култура, бизнес цели и стратегии, особено в условията на променящите се пазарни условия и законови регулации.

ЗАКЛЮЧЕНИЕ

Управлението на риска за сигурността на информацията е непрекъснат процес, а не еднократен акт. Постоянно се появяват нови технологии, нови услуги, нови уязвимости, нови методи за атака и за защита. Необходими са нови подходи и добри практики. За окончателния им подбор в организациите е необходимо да се съобразят и техните характеристики и особености – същност, предимства и недостатъци.

Управлението на риска при осигуряване на информационната сигурност осигурява повишена конкурентоспособност, международно признание за компетентност, съответствие на фирмената практика към най-добрите световни практики и гарантирано спазване на законовите изисквания към информацията.

ЛИТЕРАТУРА

[1] The Global Risks Report 2018, World Economic Forum, https://www.weforum.org/reports/the-global-risks-report-2018

[2] Наръчник по киберсигурност, www.mtitc.government.bg/upload/docs/2015-11/MTITC_D4_NarachnikKiberSigurnost_n.pdf

[3] Стоев, Ст. Класификация на източници на риск за ИС, Юбилейна научна конференция “Предизвикателства пред информационните технологии в контекста на “Хоризонт 2020”. Свищов, 2016, с. 298-305.

[4] INTERNATIONAL STANDARD IEC/ISO 31000:2018, Risk management – Guidelines, https://www.iso.org/standard/65694.html

[5] IEC 31010, Risk management – Risk assessment techniques, www.iso.org/standard/51073.html

[6] ISO/IEC 27000 family - Information security management systems, https://www.iso.org/isoiec-27001-information-security.html

[7] Целков В., О. Исмаилов, Н. Стоянов, Управление на риска, тестване и оценка на мрежовата и информационна сигурност, DOI: 10.13140/RG.2.1.4766.4406, 2014

[8] Ценков Ю. Анализ на риска при проекти за развитие на въоръженията, автореферат на дисертационен труд за присъждане на научна степен доктор, 2014

[9] RISK ANALYSIS TUTORIAL - THE PROCES , https://www.solver.com/risk-analysis-process#Identify_and_Quantify_Uncertainty

[10] ISO/IEC 27000:2018 Information technology - Security techniques -Information security management systems -Overview and vocabulary

[11] БДС EN ISO/IEC 27001:2017 - Information technology - Security techniques - Information security management systems - Requirements

[12] ISO/IEC 27005:2018 - Information technology - Security techniques -Information security risk management (third edition), https://www.iso.org/standard/75281.html

[13] Република България, Национална стратегия за кибер сигурност „Кибер устойчива България 2020”

[14] НАРЕДБА за общите изисквания за мрежова и информационна сигурност, https://www.mtitc.government.bg/sites/default/files/naredba_za_obsite_iziskvaniq_za_mrejova_i_informacionna_sigurnost_zagl_izm_dv_br_5_ot_2017_g_v_sila_.pdf

GOOD RISK MANAGEMENT PRACTICES IN THE PROVISION OF INFORMATION SECURITY

Mariya Hristova[1], Dimitar Bahchedzhiev[2]
mhristova@vtu.bg, dimitar.bahchedzhiev@intertek.com

[1]Todor Kableshkov University of Tranport, 158 Geo Milev Str., 1574 Sofia,
[2]Intertek VA
BULGARIA

Key words: *information, information security, risk management, standards, information security management system.*

Abstract: *In today's interconnected world, information and processes, systems, networks, and staff involved in its processing, use and protection are assets that are valuable to the survival of organizations and require protection against various threats and dangers. This is why computer security and information protection of computer systems and networks and the information they use are key elements of information security.*

Organizations must build and maintain competence and knowledge in the field of information security. According to the authors of the present work, this can be done in the most structured and comprehensive way, with the help of the adapted requirements and practices, which are laid down in the internationally approved framework and practices of the international ISO / IEC 27000 series of information security standards. The article presents the management process of the risk of ensuring the security of information. The "bowl method" is considered as a particularly useful graphical method for risk analysis. It examines the structure of standards, requirements, recommendations for creation, development and maintenance of information security management systems. Innovative approaches for implementing the control measures of Annex A of BSS EN ISO / IEC 27001: 2017 and the Code of Practice for Risk Management in providing information security are analyzed.