ACCESS
Велико Търново, 2022

Информационна сигурност. Стандарти от серията ISO 27000 – перспективи и проблеми

Пламен Цветанов Павлов

МОНОГРАФИЯ

ПЛАМЕН ЦВЕТАНОВ ПАВЛОВ

ИНФОРМАЦИОННА СИГУРНОСТ. СТАНДАРТИ ОТ СЕРИЯТА ISO 27000 – ПЕРСПЕКТИВИ И ПРОБЛЕМИ

МОНОГРАФИЯ

Велико Търново, 2022

РЕЦЕНЗЕНТИ:

проф. д-р Миглена Петрова Темелкова-Бакалова, Висше училище по телекомуникации и пощи – София, Република България

проф. д-р Димитър Дамянов Дамяновски, Технически университет – София, Република България

ISBN 978-619-91511-9-8

Отпечатано с готов оригинал-макет на автора.

Монографията е посветена на проблема за управлението на информационната сигурност в съответствие с ускорената дигитализация на икономиката в света и в Република България. Анализирани са проблемите при управлението на информационната сигурност в организациите и трудностите, срещани от техния мениджмънт.

Основното изложение включва аргументиране на тезата, че ефективното управление на информационната сигурност трябва да бъде базирано върху принципите и изискванията на международни стандарти от серията ISO 27 000. Последователно са описания изискванията, методите за разработване на документацията, внедряването и последващото сертифициране според изискванията на стандарта ISO 27 001:2013. Представени са принципите и методите за интегриране на ISO 27 001:2013 с ISO 9001:2015.

Монографичният труд „Информационна сигурност. Стандарти от серията ISO 27000 – перспективи и проблеми" може да е полезен както за научни изследователи, докторанти и студенти в областта на информационната безопасност, така и за широк кръг мениджъри на компании и ръководители на организации от различни сектори на икономисата.

Павлов, Пл. (2022) *Информационна сигурност. Стандарти от серията ISO 27000 – перспективи и проблеми*. / редактор. - Демирова, С., ACCESS Press Publishing house, Велико Търново, България. 188 с.

Pavlov, Pl. (2022). *Information security. ISO 27000 series standards – perspectives and issues*. - Demirova, S., ACCESS Press Publishing house, Veliko Tarnovo, Bulgaria. 188 p.

ISBN 978-619-91511-9-8

https://doi.org/10.46656/book.2022.Plamen_Pavlov

5000 Veliko Tarnovo, Bulgaria
E-mail:office@access-bg.org
http://www.access-bg.org

СЪДЪРЖАНИЕ

ВЪВЕДЕНИЕ

Съвременното общество се основава на информацията, във всички нейни аспекти. Масовото използване на компютърната и комуникационната техника дава възможност информацията да бъде събирана, обработвана, предавана и съхранявана в огромни обеми. Съвременната икономика все по-често се асоциира с разпространението на информационни продукти и услуги и все по-рядко с добивната и обработващата промишлености. Съвременната икономика се характеризира с използването на компютърна техника и на телекомуникационни системи. Това налага разработването и прилагането на икономически ефективни методи и решения в информационната сфера. Информационното общество възникна на базата изключителното развитие на информационните и компютърните технологии (ИКТ) и глобалната информационна мрежа Интернет. Това предоставя принципиално нови възможности за международен бизнес и за информационен обмен. Формира се глобално информационно пространство (Георгиев & Георгиева, 2015, стр. 11).

Прогресът в съвременните ИКТ доведе до повишаване на уязвимостта на обществото и до заплахи за информационната сигурност, както на обществото като цяло, така и на организацията в частност.

1. Информационна безопасност и сигурност

Информационна сигурност представлява: „Защитата на информацията и информационните системи от неоторизиран достъп, използване, разкриване, нарушаване, модифициране или унищожаване с цел осигуряване на поверителност, целостта и достъпността (National Institute of Standards and Technology. U.S. Department of Commerce (Editor: Kissel, R.) , 2019, p. 94).

Защита на информацията и информационните системи от неразрешен достъп, използване, разкриване, прекъсване, модификация или унищожаване, за да се осигури:

1) целостта, което означава предпазване от неправомерно изменение или унищожаване на информация и включва осигуряване на автентичност на информацията;

2) поверителност/конфиденциалност, което означава запазване на разрешени ограничения за достъп и разкриване, включително средства за защита на личната неприкосновеност и поверителна информация; и

3) достъпност, което означава осигуряване на навременен и надежден достъп и използване на информация.

„Информационната сигурност е защита на информацията и поддържащата инфраструктура от случайни или умишлени влияния от естествен или изкуствен характер, способни да нанесат вреда за собствениците или потребителите на информация и поддържаща инфраструктура. Информационната сигурност не се ограничава само до защита на информацията (б.а. – буквален превод, не сме съгласни, но така го казва авторът). Субектът на информационните отношения може да понесе (да понесе загуби) не само от неоторизиран достъп, но и от срив в системата, който е причинил прекъсване на обслужването на клиентите. Освен това за много отворени организации (например образователни) действителната

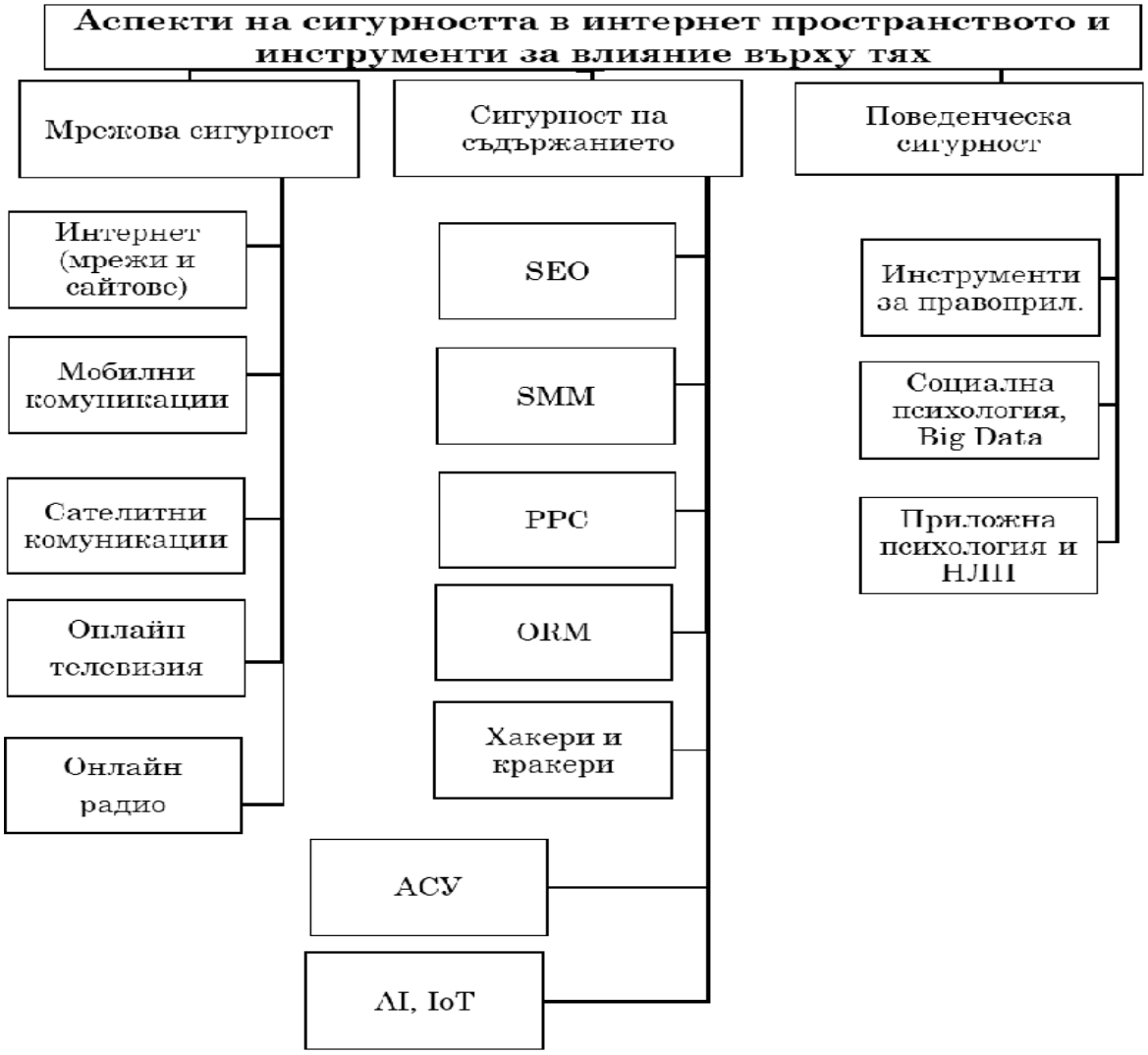
защита на информацията не е на първо място.“ (Andress, 2014, p. 240) „Под информационна сигурност се разбира такова състояние на информацията, което изключва възможността за преглед, промяна или унищожаване на информация от лица, които нямат право на това, както и изтичане на информация поради съпътстващо електромагнитно излъчване и смущения, специални устройства за прихващане (унищожаване) по време на предаване между обекти на компютърна технология“ (Andress, 2014, p. 240).

Информационната сигурност(безопасност) се проявява в:

- защитеността на информационната система, която е разработена, внедрена и осигурява развитие на организацията в интерес на заинтересованите страни;
- състоянието на информационната инфраструктура, което дава възможност наличната информация да бъде използвана изключително по нейното предназначение и това да не оказва отрицателно въздействие върху дейността;
- състоянието информацията, което предотвратява или значително затруднява нарушаването на нейната конфиденциалност, цялостност и достъпност;
- състоянието на структурата за управление на компанията, която включва системи за събиране, съхраняване и обработване на информацията за повишаване на ефективността на управлението.
- състоянието на финансовите информационни бази от данни на мрежите на банковите институции, системите за обмен на финансова информация (Димитров, 2018).

2. Аспекти на информационната сигурност и мерки за повишаването ѝ

Информационната сигурност обхваща няколко аспекта:



SEO – оптимизация за търсещи машини, SMM -управление на социалните медии, PPC – платена реклама, ORM – управление на онлайн репутацията, AI– изкуствен интелект, IoT– интернет на нещата, НЛП-невролингвистичното програмиране, Big Data.

Фиг. 1. Аспекти на информационната сфера (Аспекти на информационната сигурност и методи за нейното осигуряване., n.d.)

Физическият аспект представлява сферата в която са разположени физическите елементи на информационните системи. Това са мрежите,

технологиите за тяхното осъществяване и телекомуникационните системи за предаване на информацията. Информацията представлява електронни сигнали разпространявани от физически устройства(предаватели и приемници), които са обединени в компютърни системи, информационни мрежи, телевизионни и радио мрежи, сателитни и наземни устройства и др. (Аспекти на информационната сигурност и методи за нейното осигуряване., n.d.). Основните процеси са предаване/приемане на електронни данни, обработване и съхраняване на тези данни във физически устройства. Физическият аспект се състои и зависи от високотехнологични устойства и инструменти.

Мрежовата сигурност се явява физически аспект на информационната сигурност. Тя е предназначена да осигурява поверителността, цялостността, достъпността и проверката за автентичност на мрежите. Главната й задача е да гарантира поверителността на мрежовия трафик (например, чрез прилагане на различни криптографски методи, които не позволяват неговото подслушване, eavesdropping), да запазва на неговата достоверност (от фалшифициране на обменяните данни или на техния изпращач), да контролира съдържанието на трафика за да може да осъществява противодействие на разпространяването на вредителски съдържание, както и да осигури достъпност на мрежовите ресурси и др. В различни ситуации се налага да се обърне по-сериозно внимание на сигурността на физическите компютърни системи. Тогава този аспект се нарича **компютърна сигурност.**

Информационният аспект засяга тази част, в която информацията се създава, обработва се и се споделя във вид на **съдържание**. Тези, които изпращат информацията или я получават са в състояние много лесно да променят съдържанието й и по този начин да влияят върху вземането на управленските решения от мениджърите. Този вид информация ние всички ползваме като потребители или създатели на уебсайтове, като споделяме

текстове, видео, аудио съобщения в социалните мрежи или ползваме информацията в тях и др. Този аспект на информационната сигурност се определя като **„*сигурност на съдържанието*“.** При него се използват инструменти и технологии за промяна на съдържанието. Те се изразяват в *оптимизиране на сайтовете в помощ на SEO - машините за търсене, SMM - управление на социални медии, PPC - контекстна и платена реклама, управление на онлайн репутацията и* други дейности изискващи експертни знания.

Автоматизираните информационни системи (АИС), Интернет на нещата (IoT) и изкуственият интелект (AI) могат да бъдат причислени и към физическия аспект, както и към информационния аспект.

Поведенческият аспект на информационната сигурност намира място в човешкия ум свързан с възможността му да познава, приема и обработва информацията на и колективното поведение на хората. Тук информацията е важна не като сигнал или съдържание, а като причина за практически човешки действия (Аспекти на информационната сигурност и методи за нейното осигуряване., n.d.). Поведенческият аспект съдържа нематериални неща изразяващи се в лидерско поведение, морал, колективен дух на екипите, ниво на квалификацията и др. Инструментите включват *нормативни и психосоциалните техники, социална и приложна, психология и невролингвистично програмиране*, които могат да въздействат върху поведението и комуникационните процеси протичащи в социалните групи или върху отделните индивиди. Това може да бъде дефинирано **„*поведенческата сигурност*“**. Към нея може да бъде отнесен и анализа на голям обем от данни (Big Data), които подпомагат изследванията в областта на социалните науки.

В следствие на трите аспекта се формират и три вида мерки за налагане на информационната сигурност.

Мерки за налагане на информационната сигурност

Физическите мерки се явяват част от информационната сигурност на организацията и включват в себе си мониторинг и контрол върху на работната среда (Аспекти на информационната сигурност и методи за нейното осигуряване., n.d.). Когато се извършва оценка на физическата уязвимост на информационната система трябва да се отчетат четирите основни области: сгради, компютърни устройства, мрежи, софтуер, документи, архиви и оборудване. Пример за такива мерки: заграждания и жива охрана, видео наблюдение, контрол на достъпа, системи за противопожарна охрана. Предназначението на физическа сигурност е предотвратява нерегламентиран физически достъп до корпоративните хардуер и софтуер. Да осигури оптимални физически и температурни условия, защита от пожар или други вредни влияния. Контролът на достъпа може да се изгради на базата на използване биометрия (разчитане на отпечатъци на пръсти, на изображения на ириса, на ретината, на глас), карти за физически достъп, охранители, секретни ключалки, използване на CCVT-камери, аларми и сензори за движение. Противопожарната система за осигуряване на информационната безопасност трябва да притежава три възможности за регистриране на възникването на пожар: термално(чрез топлинен сензор), засичане на дим и пламък. Физическата сигурност трябва да съдържа и мерки и методи за защита от прихващане на предаваните данни - пряко наблюдение, прихващане през интернет и електромагнитно прихващане (EMR).

Таблица 1. Защитени зони

(Аспекти на информационната сигурност и методи за нейното осигуряване., n.d.)

Периметър на физическа сигурност	Защита с физически прегради-бариери, четци на карти, охрана
Контрол на физическия достъп	Да не се допускат неоторизирани лица
Защитени офиси, стаи и устройства	Физическа защита
Защита от външни заплахи и заплахи от околната среда	Пожар, наводнение, земетресение, взрив, граждански вълнения и др.
Работа в защитени зони	Физическа защита и указания
Публичен достъп, зони за доставки и зареждане	Изолиране на точките на достъп

Информацията и средствата за обработка на информация трябва да бъдат защитени чрез разработване на дефинирани зони за сигурност. Освен това самото оборудване също трябва да е защитено от аварии със средства за пожар, кабелната мрежа да е защитена от подслушване и повреда, да е подсигурена поддръжката на оборудването, което не трябва да се изнася или унищожава без разрешение.

Техническите мерки включват използването на специализиран софтуер, контрол на достъпа до информационните ресурси и до компютърните системи. Примери: потребителски имена, пароли, антивирусен софтуер, защитни стени, контрол на достъпа до фолдър или файл, криптиране и други.

Важно значение като технически контрол имат ограничените права при използването на компютърната система. Чрез ограничаване на индивидуалните права на потребителя до конкретна програма или до системен процес се предоставят само тези минимални права, които са му необходими за изпълнението на конкретната задача. Пример за нарушаването на този принцип е когато на компютъра, на който

изпълняваме ежедневните си задачи, да притежаваме администраторски права.

Административни (правни, организационно-технически, икономически и процедурни) мерки. Тези мерки включват нормативно дефинирани политики, процедури, стандарти и инструкции. В тях са определени процедурите, които трябва да спазва персонала в ежедневната си работа. Нормативната база и регулации също са някакъв вид административни мерки. Административните мерки се явяват базата, върху която са изградени техническите и физическите мерки - контрол върху системата за ИС, управление на критичните за безопасността приложения и комуникационната инфраструктура.

Фиг. 2 Осигуряване на информационната сигурност

(Туджаров, 2009)

- Правните методи се изразяват в създаване, приемане (от институциите) и въвеждане в практиката на юридически нормативни актове

(законови и подзаконови), които регламентират отношенията в информационната сфера.

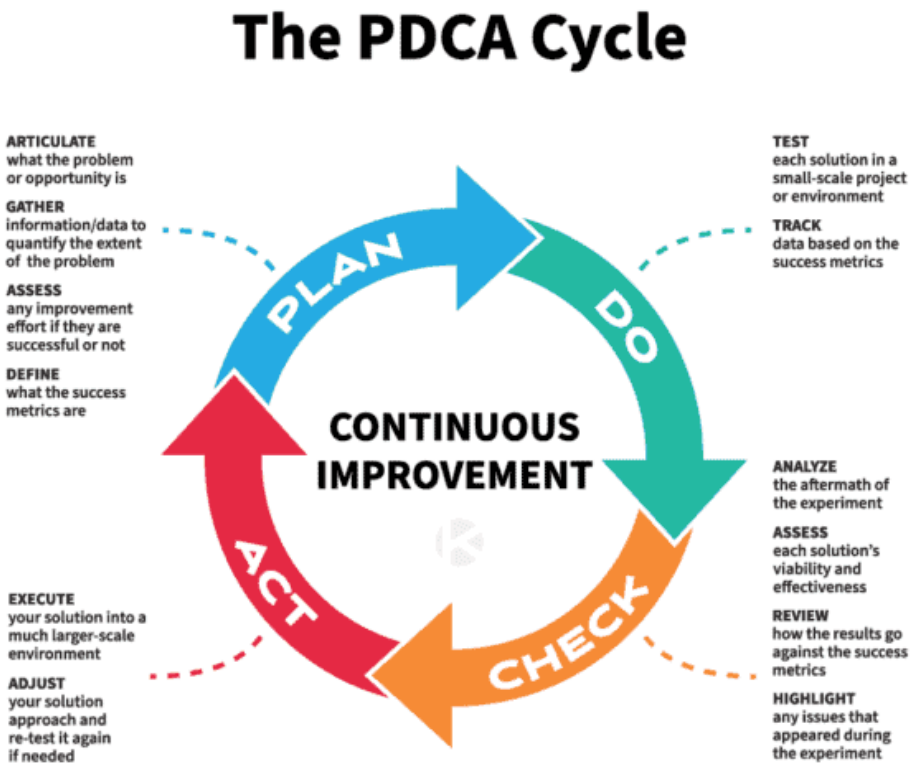
- Организационно-техническите методи за гарантиране на информационна сигурност се изразяват в създаване и усъвършенстване на организационните действия чрез лицензиране на дейността на организациите.
- Икономическите методи за информационна сигурност изискват разработване на специални програми и определяне на начина, по който те ще бъдат финансиран.

3. Управление на информационната безопасност

Управлението на информационната безопасност се състои в стриктно изпълнение на всички регламентирани процедури за осигуряване на ИБ, в координиране и регулиране на различните процедури, в контрол върху тяхното правилно и ефективно изпълнение.

Стандартът определя два основни принципа за управление.

1. Процесен подход при управлението на информационната безопасност. Процесният подход включва съвкупност от взаимосвързани операции и действия. Той акцентира вниманието на служителите върху постигането на поставените цели, върху наличните ресурси и придобиване на липсващите, върху разходите направени за постигане на тези цели.
2. Използване на модела PDCA като основа при разработването и изпълнението на всички процедури за управление на информационната безопасност. „Моделът Шухарт-Деминг“ (PDCA-моделът - Планиране, Изпълнение, Проверка и Действие) се базира на тези четири етапа, които трябва последователно да се изпълняват за всеки един от процесите.



Фиг. 3 Цикъл на проектиране на СУИБ

ПЛАНИРАНЕ: Установяване на СУИБ

Тази фаза на ISO 27001 помага на организацията да установи обхвата на целите и контролите на СУИБ. Клауза 4.2 от стандарта ISO 27001 определя контекста на организацията. Във фазата на планиране е необходимо да бъдат анализирани външните и вътрешните проблеми на организацията. Идентифицирането на тези проблеми помага на организация да внедри процедури в СУИБ в съответствие с ISO 27001, които да елиминират тези проблеми. Външните проблеми за организацията се описват в списък от заплахи - юридически, икономически и политически. Вътрешните проблеми включват организационна структура, организационна култура, ценности, ИКТ инфраструктура, налични ресурси и др.

ИЗПЪЛНЕНИЕ: Прилагане на СУИБ

Това е фазата, по време на която организацията внедрява и използва политиката, контролите, процесите и процедурите на системата за управление на информационната сигурност. Организацията извършва оценка на рисковете и оценява причините за тяхното възникване във всяка от структурите. Организацията изготвя система от процедури, посочващи рисковете и тяхното обработване. Те трябва да гарантират, че документите описващи процедурата и политиката са достъпни и адекватно защитени, разпространени и съхранени в СУИБ. Документите, които имат външен произход, трябва да покриват обхвата на СУИБ съответстваща на 27001.

ПРОВЕРКА: Мониторинг и преглед на СУИБ

Тази фаза обхваща мониторинг, измерване, анализ, проверки и оценка на изпълнението на процедурите и дейностите в рамките на организацията. Ефективността на процесите трябва да бъде оценена, от отговорните лица, спрямо политиките, целите и практическия опит в документирана процедура, установена на по-ранната фаза. Отговорните лица трябва да представят резултатите на висшето ръководство и предложат план за прилагане на резултатите от тези политики. Това е най-ефективният начин да бъдат идентифицирани проблемите, да им бъде въздействано, да бъдат елиминирани и е ако е необходимо, да бъдат преразгледани и усъвършенствани.

ДЕЙСТВИЕ: Актуализиране и усъвършенстване на СУИБ

Организацията трябва да предприеме коригиращи и превантивни действия въз основа на проведения вътрешен одит на СУИБ и резултатите от Прегледа на ръководството. Може да бъде назначен главен информационен директор (CIO) който да отговаря за наблюдението и измерването на информационната сигурност в организацията. CIO трябва да предприеме действия по всяка констатация, която е свързана с нарушаване на информационната сигурност. Постоянното подобряване е неразделна

част от ISO 27001. Стандартът изисква организациите да се усъвършенстват непрекъснато за да елиминират допълнителни заплахи.

По този начин за всяка процедура се определят ясни правила за нейното изпълнение, необходимите за това ресурс, график за нейното изпълнения, процедурите за нейното контролиране, критериите за оценка на нейната ефективност. При изпълнението на всяка процедура последователно и непрекъснато се следват тези етапи: планиране на процедурата, внедряване на процедурата, проверка на правилността и ефективността от изпълнението на процедурата, въвеждане на необходимите изменения в процеса на изпълнението на процедурата. Периодически е необходимо отново да бъдат преразгледани целите и задачите при изпълнението на процедурата – отново изпълнение на етапите на модела PDCA.

Основният проблем се изразява в сложността при оценяването на ефективността на процедурите включени в СУИБ. Затова е необходимо за всяка процедура да бъдат дефинирани съответните критерии, по които да бъде оценявана ефективността й. Такива критерии трябва да бъдат разработени за цялата СУИБ като цяло.

За критерии за оценка на ефективността на СУИБ могат да бъдат приети, например, промяна в броя на инцидентите свързани с информационната безопасност, промяната в квалификацията на потребителите и др.

4. Исторически аспекти на стандарта ISO 27001.

Стандарт ISO/IEC 27001 може да бъде определен като най-концептуален и комплексен. Неговото съществуване започва с публикуваните от Центъра за компютърна безопасност на Департамента за търговия и индустрии на Великобритания препоръки DTI CCSC User's Code of Practice. Този документ е бил разработен на базата на приетата от компанията Royal Dutch Shell (днес Shell) политика за информационна безопасност. Документът представлявал набор(списък) от ключови мерки за осигуряване на информационната безопасност, които задължително трябвало да бъдат изпълнявани при работа с корпоративните мейнфрейми (от англ. mainframe) с голям универсален високопроизводителен и отказоустойчив сървър с голям обем оперативна и външна памет, предназначен за използване в критически важни системи (англ. mission-critical). През 1993 година документът е бил доразработен и публикуван от Британския институт по стандарти (British Standards Institute, BSI) под името Code of Practice for Information Security Management. През следващите години този документ се доработва и развива от BSI и като резултат през 1995 година е издаден британският национален стандарт BS 7799:1995. Той съдържа актуализиран набор(списък) от препоръчителни за използване в организациите мерки за защита на информацията. За съжаление изборът на най-оптималните за конкретната организация мерки за защита на информацията все пак оставал извън рамките на този стандарт. За да може да бъде решен този проблем през 1998 година BSI разработва допълнение към стандарта BS 7799 Part 2:1998. Именно той може да бъде считан за пряк предшественик на стандарта ISO/IEC 27001.

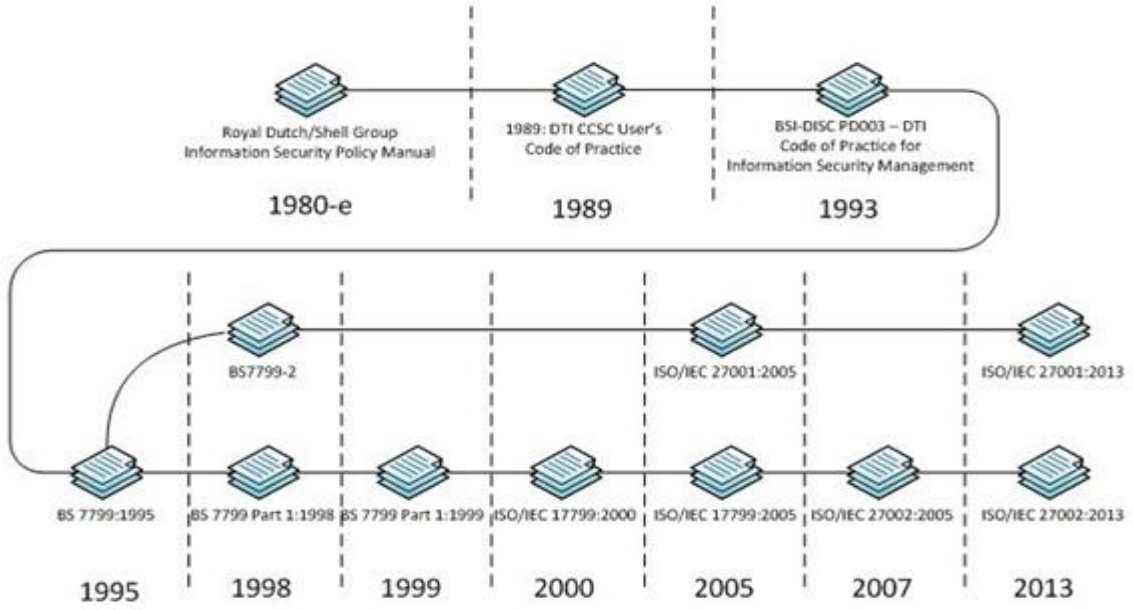
Като едно от най-важните събития свързано с историята за развитието на стандартите BS 7799 може да бъде отбелязано тяхното признаване от страна на Международната организация по стандартизация (International

Organization for Standardization, ISO) и Международната електротехническа комисия (International Electrotechnical Commission, IEC).

През 2000 година техническият комитет, който е създаден и съществува под егидата на тези две организации, прие стандарта ISO/IEC 17799:2000, който се явява развитие на стандарта BS7799-1.

През 2005 година през тази процедура премина стандартът BS 7799 Part 2:1998, и получи идентификация ISO/IEC 27001. От този момент нататък всички международни стандарти, свързани с мениджмънта на информационната безопасност, създавани под патронажа на ISO/IEC, са неразделна част от серията 270xx.

През 2007 година актуализираната версия на стандарта ISO/IEC 17799:2000 получи идентификация ISO/IEC 27002. Създалата се разлика във времето между публикуването на стандартите ISO/IEC 27001 и ISO/IEC 27002 беше отстранена през 2013 година, когато обновените версии и на двата стандарта бяха публикувани едновременно (Фиг. 4).



Фиг. 4 Хронология на развитието на стандарта ISO/IEC 27001

Към настоящия момент серията 27xxx включва в себе си повече от 30 стандарта свързани с различните направления на системата на управление на информационната безопасност (СУИБ), започва с нивото на стратегическото управление и контрола на СУИБ и завършва с техническите препоръки свързани с използването на отделните организационни и технически мерки за защита на информацията. Всички тези стандарти могат да бъдат класифицирани в няколко групи (Фиг. 5).

Термини и описание	*ISO/IEC 27000*
Базови изисквания	*ISO/IEC 27001* *ISO/IEC 27002*
Алгоритъм за внедряване на СУИБ	*ISO/IEC 27003*

Ръководство за основните процеси на СУИБ	*ISO/IEC 27004* *ISO/IEC 27005* *ISO/IEC 27007* *ISO/IEC TR 27008*
Корпоративно управление на ИБ	*ISO/IEC 27014* *ISO/IEC TR 27016*
Специфични области на дейността	*ISO/IEC 27009* *ISO/IEC 27010* *ISO/IEC TR 27011* *ISO/IEC TR 27015* *ISO/IEC TR 27019* *ISO/IEC 27018* *ISO/IEC TR 27799*
Ръководство за мерки за защита	*ISO/IEC 2703x* *ISO/IEC 2704x* *ISO/IEC 2705x*
Интеграция с други стандарти	*ISO/IEC 27013* *ISO/IEC 27031*
Кибер-безопасност	*ISO/IEC 27103*
Миграция между версиите на базовите изисквания на стандарта	*ISO/IEC 27023*

Изисквания към специалистите	*ISO/IEC 27006* *ISO/IEC 27021*

Фиг. 5 Групиране на стандартите от серията 27 xxx

Базовите стандарти ISO/IEC 27001 и ISO/IEC 27002 в течение на времето са били допълнени със следните документи:

1. Стандартът ISO/IEC 27000, описва терминологията и общия подход на цялата серия от стандарти;
2. Стандартът ISO/IEC 27003 включва указания за реда при внедряването на СУИБ;

➢ стандартите по отделните процеси на СУИБ: измерването на ефективността, риск-мениджмънта, одит;

➢ стандартите по направленията на стратегическото управление на информационната безопасност и икономическите резултати на СУИБ;

➢ стандартите свързани с особеностите на СУИБ в специфичните области на дейностите: телекомуникационните услуги, финансовите операции, обработването на персоналните данни в облачните услуги, енергийните комплекси, обществата за информационен обмен, организациите в областта на здравеопазването;

➢ детайлни изисквания към предприеманите марки за защита на информацията, в това число по управлението на инцидентите, мрежовата безопасност;

➢ ръководства за интегриране на СУИБ със системите за IT-мениджмънта (ISO 20000) и системите за осигуряване на непрекъснатостта на дейността (включително ISO 22301);

➢ ръководство за осигуряване на кибербезопасността в съответствие с общите подходи и прилаганите практики в СУИБ;

3. стандартите ISO/IEC 27006 и ISO/IEC 27021, които описват изискванията към експертите и одиторите на СУИБ.

Стандартите от серията постепенно се превеждат на български езикк и издават Българския институт по стандартизация.

В колекцията от стандарти „ISO/IEC 27000 - Системи за управление на сигурността на информацията“ са включени международните стандарти, които са основополагащи за внедряването на изключително важната за всяка организация, независимо от големината й, система за управление. С поредната актуализация от м. декември 2021 г. се включва изданието на БДС ISO/IEC 27005:2018 на български език.

Така колекцията включва официалните издания на следните стандарти:

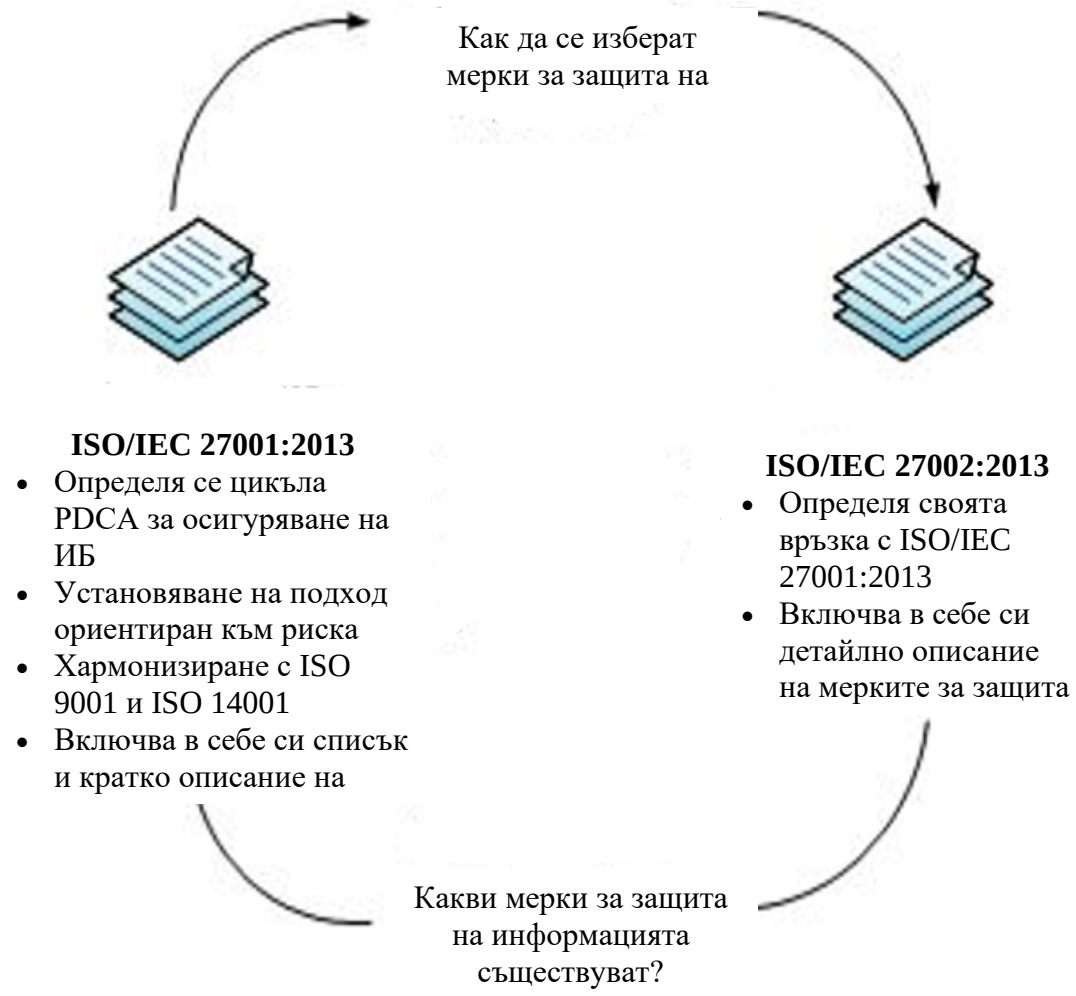
- БДС EN ISO/IEC 27000:2020 Информационни технологии. Методи а сигурност. Системи за управление на сигурността на информацията. Общ преглед и речник (ISO/IEC 27000:2018) (на английски език)
- БДС EN ISO/IEC 27000:2017 Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Общ преглед и речник (ISO/IEC 27000:2016) (на български език) (отменен).
- БДС EN ISO/IEC 27001:2017 Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Изисквания (ISO/IEC 27001:2013, вкл. Cor.1:2014 и Cor.2:2015) (на български език).
- БДС EN ISO/IEC 27002:2017 Информационни технологии. Методи за сигурност. Кодекс за добра практика за управление на сигурността на информацията (ISO/IEC 27002:2013, вкл. Cor.1:2014 и Cor.2:2015) (на български език).
- БДС ISO/IEC 27003:2020 Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията.

Указания (ISO/IEC 27003:2017) (на английски език).
- БДС ISO/IEC 27003:2011 Информационни технологии. Методи за сигурност. Указания за внедряване на системи за управление на сигурността на информацията (на български език) (отменен).
- БДС ISO/IEC 27004:2017 Информационни технологии. Методи за сигурност. Управление на сигурността на информацията. Наблюдение, измерване, анализ и оценяване (ISO/IEC 27004:2016) (на български език).
- БДС ISO/IEC 27005:2018 Информационни технологии. Методи за сигурност. Управление на риска за сигурността на информацията (ISO/IEC 27005:2018) (на български език).
- БДС ISO/IEC 20000-1:2018 Информационни технологии. Управление на услуги. Част 1: Изисквания относно системата за управление на услуги (ISO/IEC 20000-1:2018) (на български език).
- БДС ISO/IEC 27013:2015 Информационни технологии. Методи за сигурност. Указания за съвместно внедряване на ISO/IEC 27001 и ISO/IEC 20000-1 (на български език).
- БДС EN ISO/IEC 27701:2021 Методи за сигурност. Допълнение към ISO/IEC 27001 и ISO/IEC 27002 за управление на неприкосновеността на информацията. Изисквания и указания (ISO/IEC 27701:2019) (на български език).

5. Подходи на ISO 27001 за осигуряване на информационната безопасност.

Подходът при управлението на информационната безопасност се дефинира от два взаимосвързани стандарти: ISO/IEC 27001 и ISO/IEC 27002 (Фиг. 6). Основната роля тук заема стандартът 27001, който съдържа препоръки към управлението на информационната безопасност в организацията на базата на повсеместно използвания в корпоративната

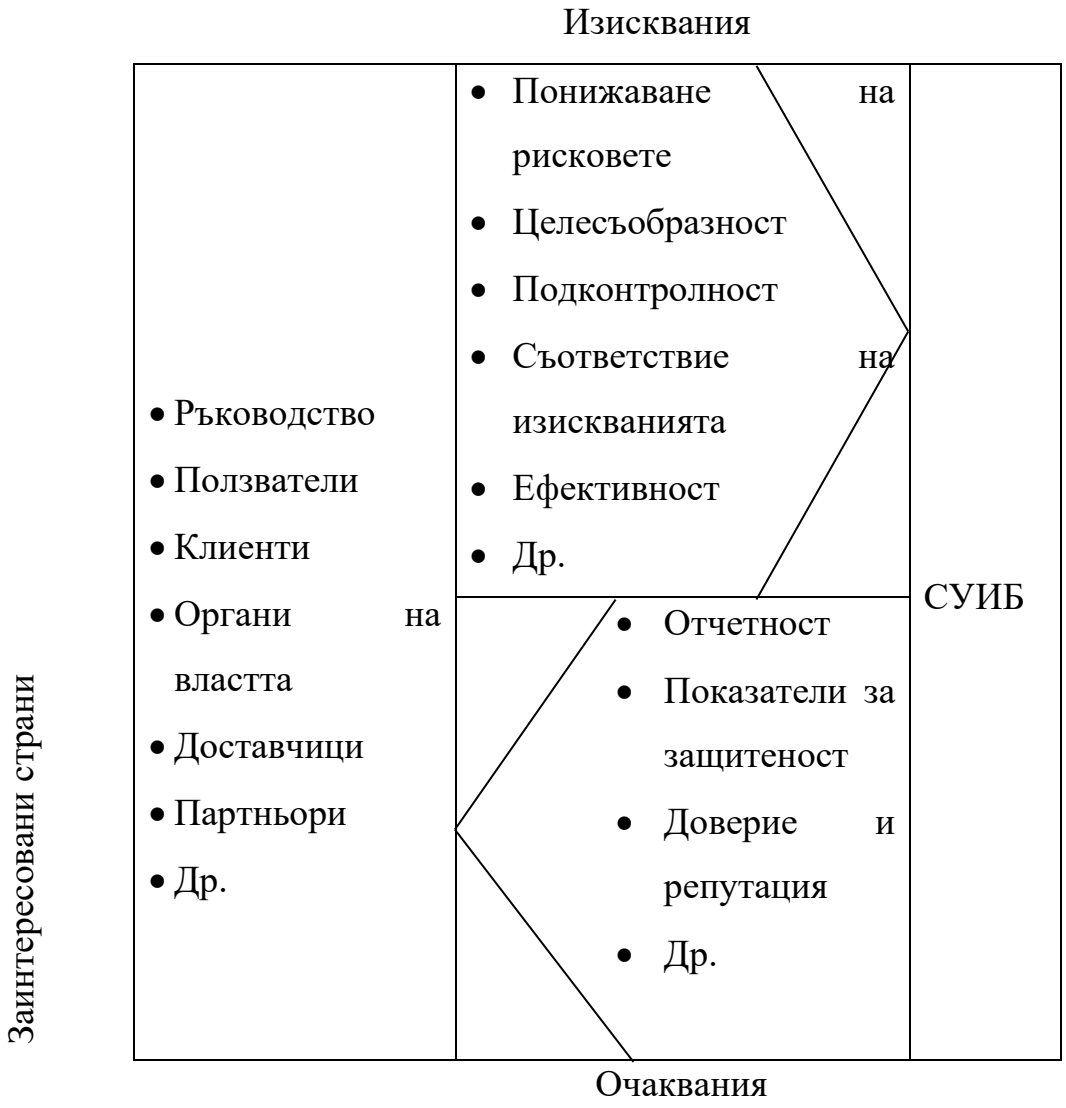
среда цикъл за управление на качеството PDCA (Plan, Do, Check, Act). Стандартът ISO/IEC 27002 има по-скоро характер на справочник, който описва пълния набор от възможни за използване мерки за защита на информацията, от които организацията има възможност да избере тази, която е най-подходяща за нея.



Фиг. 6 Взаимовръзка между ISO/IEC 27001 и ISO/IEC 27002

В стандарта ISO/IEC 27001 са дефинирани препоръки свързани с функционирането на СУИБ като комплексна система, която е предназначена за защита на информационните активи на организацията от заплахи за минимизиране на рисковете. От гледна точка на бизнеса СУИБ представлява една от множеството системи съществуващи в организацията,

към която предявени определени изисквания и която е длъжна на отговори на изискванията и да е в състояние на възстанови вложените в нейното в нейното разработване и внедряване (Фиг. 7).



Фиг. 7 Място на СУИБ в бизнес организацията

В съответствие с изискванията на стандарта, СУИБ включва в себе си пълния комплекс от действия за осигуряване на информационната безопасност, включително организиране на дейностите и управлението на рисковете, както и непосредственото прилагане на мерките за защита на информацията. Кои от методите за защита на информацията от тях да бъдат избрани, се определя въз основа на анализа и оценката на рисковете при

информационната безопасност, тоест от размера на възможните щети от осъществяването на заплахите за конфиденциалността, цялостността и достъпността на информацията. Изборът се определя още и от необходимостта от изпълняване на нормативните задължения към държавата, партньорите и към другите заинтересовани страни.

Така предлагания подход позволява стандартът да се използва за разработване и внедряване на СУИБ в организации от всякакъв размер и ниво на нормативно регулиране.

Стандартът ISO/IEC 27001 е съвместим с другите видове стандарти на системите за управление на качеството, такива като ISO 9001, ISO 14000, ISO 31000, ISO/IEC 38500, ISO/IEC 20000, ISO/IEC 22301 и др. Това позволява да бъде използван единен подход и принципи при тяхното разработване, обща терминология, да бъдат дефинирани и разработвани интегрирани процеси по отделните направления на контрола на качеството на произвежданата продукция, опазване на околната среда, стратегическото управление на организацията и управлението на ИТ-услугите, осигуряване на непрекъснатост на дейността на организацията и не на последно място информационната безопасност. Което, от своя страна, предоставя възможност да бъде изградена добре структурирана и прозрачна система за управление на организацията и да бъде повишена общата ефективност на управляемите процеси.

Реализация на стандарта отчитайки нормативните изисквания за защита на информацията

Днес могат да бъдат дефинирани следните основни области на нормативно регулиране на СУИБ:

1. Защита на персоналните данни.
2. Защита на критическата информационна инфраструктура.
3. Защита на автоматизираните системи за управление на технологичните процеси.

4. Защита на държавните информационни системи.

5. Защита на финансово-кредитните системи.

Основни регулиращи органи - Държавна комисия по сигурността на информацията, Министерство на електронното правителство и други агенции. Въпреки, че регулаторите формират собствени подходи за защита на информацията, във всяка нова редакция на техните нормативни документи все по-ясно се забелязва връзката с принципите, изискванията и подходите на стандарта ISO/IEC 27001.

В банковата среда решенията в областта на информационната безопасност на базата на оценка рисковете се използват успешно отдавна. Този подход се определя от международните съглашения на Комитета от Базел, нормативните документи и препоръките на централите на отделните банки.

По този начин, в юридическите изисквания и в препоръките на националните регулаторни органи са използвани същите принципи и методи за организиране на дейностите свързани със защитата на информацията, както тези в стандартите на ISO и на Международната електротехническа комисия (IEC).

Като основа за дефиниране на нормативни изисквания при създаването на единна СУИБ може да бъде използван стандартът ISO/IEC 27001.

6. Предимства и недостатъци от внедряването на ISO/IEC 27001

При сертифициране на организацията в съответствие с международния стандарт ISO/IEC 27001 те получават ясно очертани конкурентни предимства:

- **Защитава информацията във всичките и нейни форми.**

СУИБ (ISMS (Information Security Management System) - осигурява модел за установяване, внедряване, функциониране, наблюдение, преглед и подобрение на защитата на информационните активи за постигане на целите на бизнеса. Моделът се основава на дългогодишни добри практики. ISMS използва като основа за внедряване оценката на организацията на рисковете за сигурността и дефинирането на приемливи нива на риск, разработени за ефективното му третиране.

СУИБ помага за защитата на всички форми на информация, включително цифрова, хартиена, интелектуална собственост, фирмени тайни, данни на устройства и в облака, хартиени копия и лична информация.

- **Помага на организацията да съхрани възможностите за бъдещи договори** с компании, които изискват притежаване на сертифицирана СУИБ и да облекчи участието в търгове по обществени поръчки;
- **Увеличава устойчивостта на компанията към атаки**

Внедряването и поддържането на СУИБ значително повишава устойчивостта организация срещу кибератаки.

- **Намаляване на разходите за информационна сигурност**

Благодарение на подхода за оценка и анализ на риска от СУИБ, организациите могат да намалят разходите, свързани с безразборното добавяне на слоеве от защитни технологии, които може и да не проработят.

- **Реагиране на променящите се заплахи за безопасността**

Постоянно адаптирайки се към промените както във външната среда, така и вътре в организацията, СУИБ понижава заплахите от непрекъснато променящите се рискове.

- **Подобряване на фирмената култура**

Холистичният подход на Стандарта обхваща цялата организация, а не само ИТ, а обхваща също и хора, и процесите и технологиите. Това позволява на сътрудниците лесно да разберат рисковете и да предприемат

мерки (контроли) за безопасност като част от ежедневните си работни практики.

- **Осъществява защита за цялата организация**

СУИБ защитава цялата организация от технологични рискове и други, по-разпространени заплахи, такива като лошо информиран персонал или неефективни процедури.

- **Осигурява централна рамка**

СУИБ предоставя рамка (основа) за осигуряване на безопасността на информацията на организацията и управление на всичко на едно място.

- **Защитава поверителността на данните**

СУИБ предлага набор от политики, процедури, технически и физически средства за контрол за защита на поверителността, наличността, достъпността и целостта на информацията.

Във връзка с непрекъснатото развитие на технологиите, с непрекъснатото нарастване на обемана съществуващите информационни ресурси и появата на нови, все по подробни и строги нормативни изисквания все повече се увеличават и разходите за осигуряване на информационната безопасност.

Все по-важни стават въпросите, свързани с обосноваването на необходимите разходи свързани с разработването, внедряването и поддържането на СУИБ и с ефективността на нейната дейност. При тези условия е необходимо да бъдат избягвано нежеланото дублиране на процесите свързани със защитата на информацията, да бъдат изключени корпоративните «двойни стандарти», да бъде издигната защитата на информацията на качествено по-високо ниво и да бъдат защитени (оправдани) инвестициите и средствата изразходвани за осигуряване на информационната безопасност.

Към **предимствата от внедряването на стандарта** в организацията могат да бъдат отнесени също:

- **Обосноваване на необходимите икономически разходи** за информационна безопасност;
- **Повишаване на ефективността на организирането на дейността свързана със защитата на информацията** и с предотвратяването на възникването на ситуации с нея;
- **Получаване на възможност за международно сертифициране на СУИБ**, което дава конкурентни предимства и потвърждава зрелостта на компанията, води до повишаване на доверието на партньорите, клиентите и потребителите.
- **Съвременните общества**, като реакция на Covid-19, **избраха самоизоляцията.** Основноо работно място на сътрудника вече се явява неговият дом, а не неговия офис. Поради тази причина възниква необходимостта отново да бъдат оценени рисковете за информацията и за процесите основани на нея. Например, вече не е критично важно осигуряването на надеждно шифриране на wi-fi в офиса, защото там няма никой. Главните инструменти за работа и места за съхраняване на данните се преместиха в «облака». В същност главният офис се премести в облака и физическата локация на организацията загуби смисъл. Фокусът се измести върху услугите, които организацията използва и/или продава.

Към предимствата при използването на стандарта ISO/IEC 27001 в като основа за **защита на търговската чувствителна информация и изпълняването на нормативните изисквания свързани със защитата на личните данни, на банковата тайна, на критическата информационна инфраструктура, на държавните информационни системи и публични регистри**, **на АСУ на технологичните процеси, на националната система за междубанкови преводи.** Към тях могат да бъдат отнесени:

- **общата система за организиране на разпоредителната и разпределителната на документация** свързана с осигуряването на информационната безопасност на организацията, която води до

минимизиране на дублирането на документи, до повишаване на качеството и удобството при тяхното използване, до подобряване на анализационната дейност;

- **концентриране на компетенциите и знанията, свързани с осигуряването на информационната безопасност** в единна организационно-управленска структура;
- **оптимизиране на всички разходи направени за внедряването на организационните и техническите мерки за защита на информацията поради реализацията на унифициран (стандартизиран) комплект от мерки** за защита на информацията в рамките на цялата организация;
- **понижаване на разходите свързани с модернизирането и усъвършенстването на действащата система за информационна безопасност** на организацията, ако са настъпили промени в нормативните изисквания, на базата на наличната възможност за прилагане на тясноспециализирани коригиращи мерки за защита на информацията, вместо да бъде извършено пълно преразглеждане на документите и процесите.

Към **недостатъците на подхода, ограниченията и трудностите при внедряването на стандарта** в организацията могат да бъдат отнесени:

- В предлагания от стандарта подхода съществуват и свои ограничения. Основното се състои **в ниската детайлизация на изискванията и поради тази причина, необходимост от привличане в дейността зя тяхната реализация на опитни експерти, притежаващи много висока квалификация.** Това е цената, която трябва да бъде платена за гъвкавостта и адаптивността на стандарта.
- Друго много **важно ограничение при процедурата за внедряване на стандарта може да се яви «големият и ненужен багаж» от остарели правила и методи свързани с осигуряването на защитата на информацията в организацията**. В много организации управленските

процеси дълги години са се формирали движейки се по пътя на излишното и често неоправдано формализиране. Поради тази причина много често мениджмънтът на организацията без особено желание се заема с кардинално преработване на системата. При така възникналата ситуация единственият начин за успешно разработване и внедряване на процедурите, отговарящи напълно на изискванията на стандарта се явява осъзнаването и приемането, от страна на висшия мениджмънт, на важността на целите и задачите стоящи пред него за постигане на информационна безопасност. Без безусловна поддръжка от страна на висшето ръководство, внедряването на стандарта е невъзможно, защото в основата на приемането на ключовите решения в СУИБ е заложена готовността на ръководството да предприеме всички необходими изменения и ограничения, да осигури финансовите и човешките ресурси.

7. Практики при внедряването на стандарта ISO/IEC 27001 в чужбина.

Стандартът ISO/IEC 27001 е един от най-динамично развиващите се стандарти по информационна безопасност. Това е видно не само от заложените серията от стандарт обеми от полезни знания, но и от статистиката. Проучване на ISO за стандартни сертификати за система за управление за 2020 година.

Данните, събрани за проучването са:

• брой валидни сертификати за държава към 31 декември (Валиден сертификат е този, който е издаден от орган за сертифициране, акредитиран от членове на IAF MLA през годината на проучването или през двете години преди него, който все още е валиден на 31 декември от годината на проучването)

• брой сектори на държава, обхванати от сертификатите, съгласно класификацията на 39 EA сектори.

• брой обекти на държава, обхванати от техните сертификати (Обектът е постоянно място, където дадена организация извършва работа или услуга).

Проучването съдържа:

• обзорна таблица, показваща общия брой валидни сертификати и общия брой обекти за всеки стандарт

• подробни резултати за всеки стандарт, обхванат от проучването с данните по държави за броя на сертификатите и броя на обектите и общия брой сектори. Броят на секторите на държава е в отделен файл, наречен "Сектори по държава"

По данни от последния публикуван отчет на ISO за 2020 година (септември 2021 г., Таблица 2), броят на сертифицираните в глобален мащаб компании е нараснал значително от 44 486 на 84 166 бр.

Най-голямо количество сертификации на СУИБ са осъществени в Япония, Китай, Великобритания, Индия, САЩ, Германия, Италия и други страни от Европейския съюз. Тенденцията за ръст на сертифицирането по този стандарт може би се дължи и на възникналата необходимост от изграждане на ефективна система за управление на информационната безопасност за да могат да бъдат покрити всички изисквания на General Data Protection Regulation (GDPR).

Таблица 2. *Сертифицирани компании в глобален мащаб към 2021 г.*

	Total valid certificates	Total number of sites
ISO 9001	916 842	1 298 666
ISO 14001	348 218	568 518
ISO/IEC 27001	44 486	84 166
ISO 22000	33 735	39 981
ISO 45001	190 429	251 136
ISO 13485	25 656	35 253
ISO 50001	19 721	45 082
ISO 22301	2 205	4 662
ISO/IEC 20000-1	7 846	9 927
ISO 28000	520	968
ISO 37001	2 065	5 946
ISO 39001	936	2 305

В Отчета на ISO за 2020 година (септември 2021 г.) са посочени сертифицираните организации по страни (Приложение 1), от което се вижда най-разпространен е стандартът в Китай – 12 403 бр., на второ Япония – 5 646 бр., на трето място Великобритания с 3 327 бр., на четвърто място е Индия с 2 226 бр. и на пето място Германия с 1 281 бр. В България са сертифицирани 372 организации, което в съответствие с обема на икономиката ни е едно добро постижение (International Organization to Standartization, 2021).

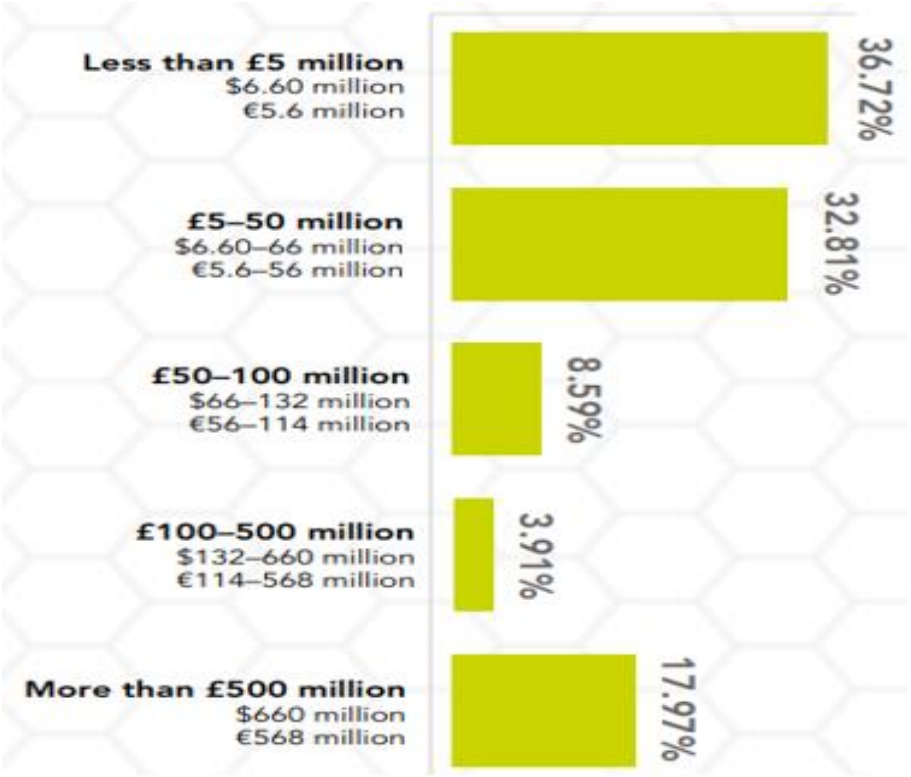
В същия отчет (Приложение 2) са представени данни за разпределението на сертификатите по сектори от икономиката. Най-разпространено е сертифицирането в сектор „Информационни технологии“ – 10167 бр., на второ място „Други услуги“ – 1359 бр. и на трето място „Транспорт, складиране и комуникации“ – 620 бр., а най-много са издадени

в неуточнен сектор – 32372 бр. (International Organization to Standartization, 2021).

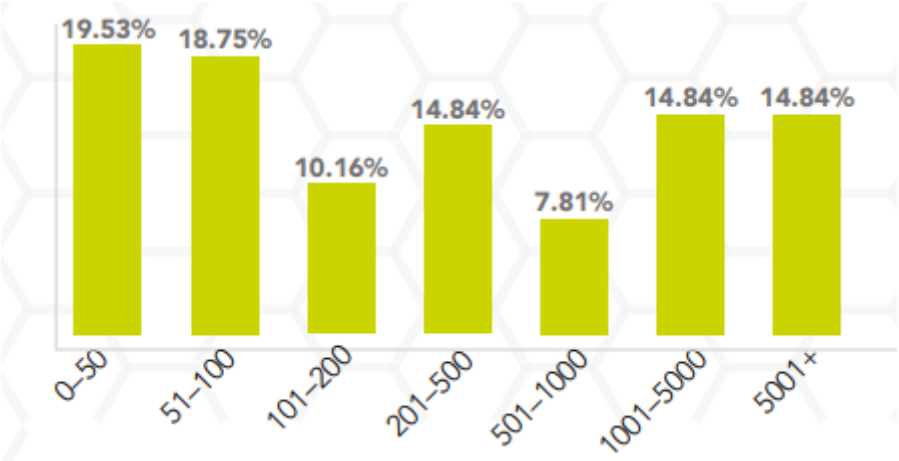
Постоянният интерес и нарастването на броя на компаниите внедряващи този стандарт в света не е случаен, а се дължи на ясно изразените конкурентни предимства получавани при неговото използване. Така, проучването, което е извършила компанията IT Governance в компаниите, които са внедрили ISO/IEC 27001, показва следните резултати:

- 98% от отговорилите са заявили, че са внедрили стандарта за да повишат нивото на информационната сигурност на компанията;
- 67% са отбелязали актуалността на стандарта в отрасъла, в който оперират;
- 56% от отговорилите считат, че внедряването ще им донесе нови конкурентни предимства;
- в 56% от компаниите е нараснала способността им да отговарят и изпълняват нормативните юридически изисквания;
- 77% от компаниите използват стандарта едновременно с други инструменти за контрол в сферата на информационната безопасност;
- 71% от компаниите са получили запитвания от страна на клиенти за потвърждаване на изпълнението на изискванията на ISO/IEC 27001.

Фиг. 8 Участници в анкетата (по държави)

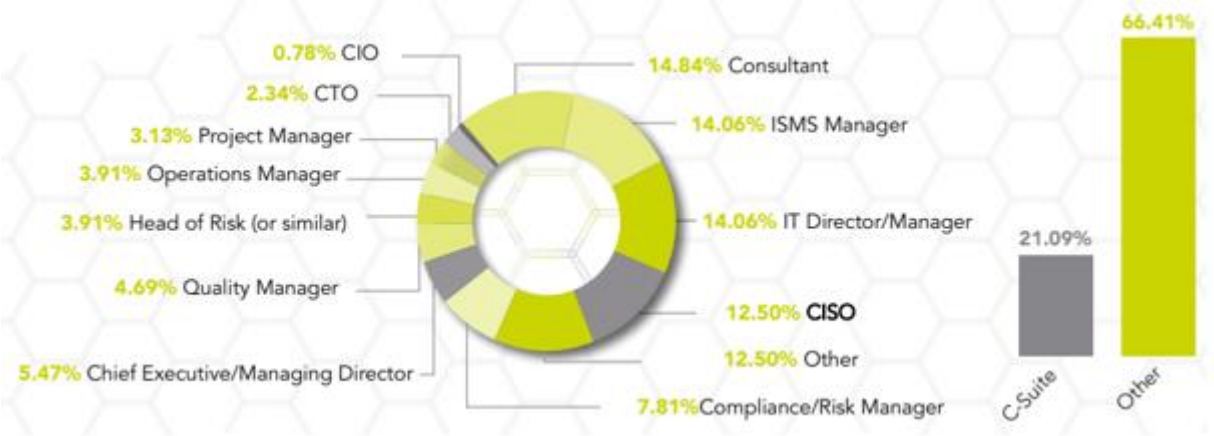


Фиг. 9 По годишни приходи

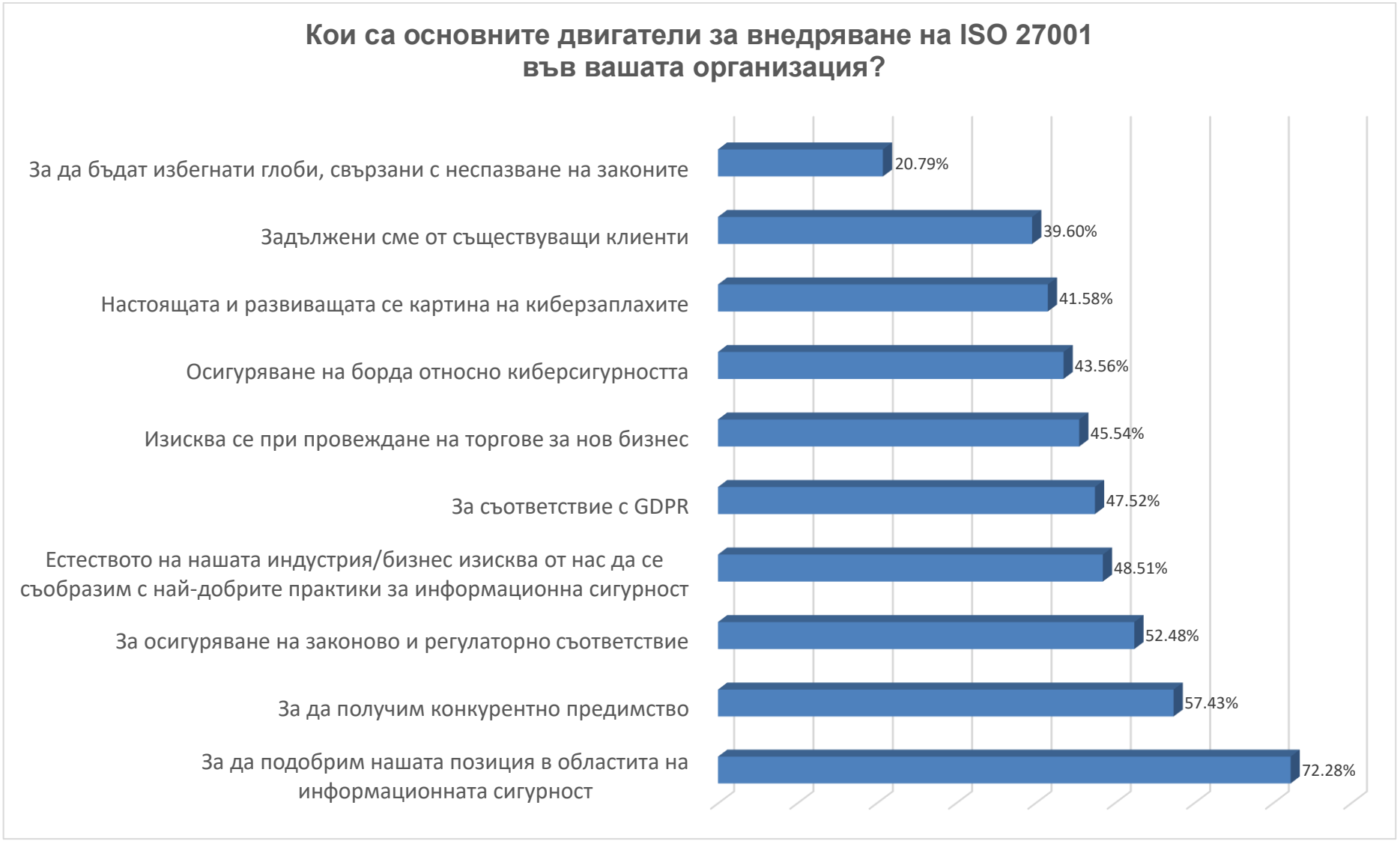


Фиг. 10 По размер на организацията (брой на служителите)

Фиг. 11 По сектори на индустрията



Фиг. 12 По заемана длъжност на интервюирания



Фиг. 13 Основни двигатели за внедряване на ISO 27001 в организацията

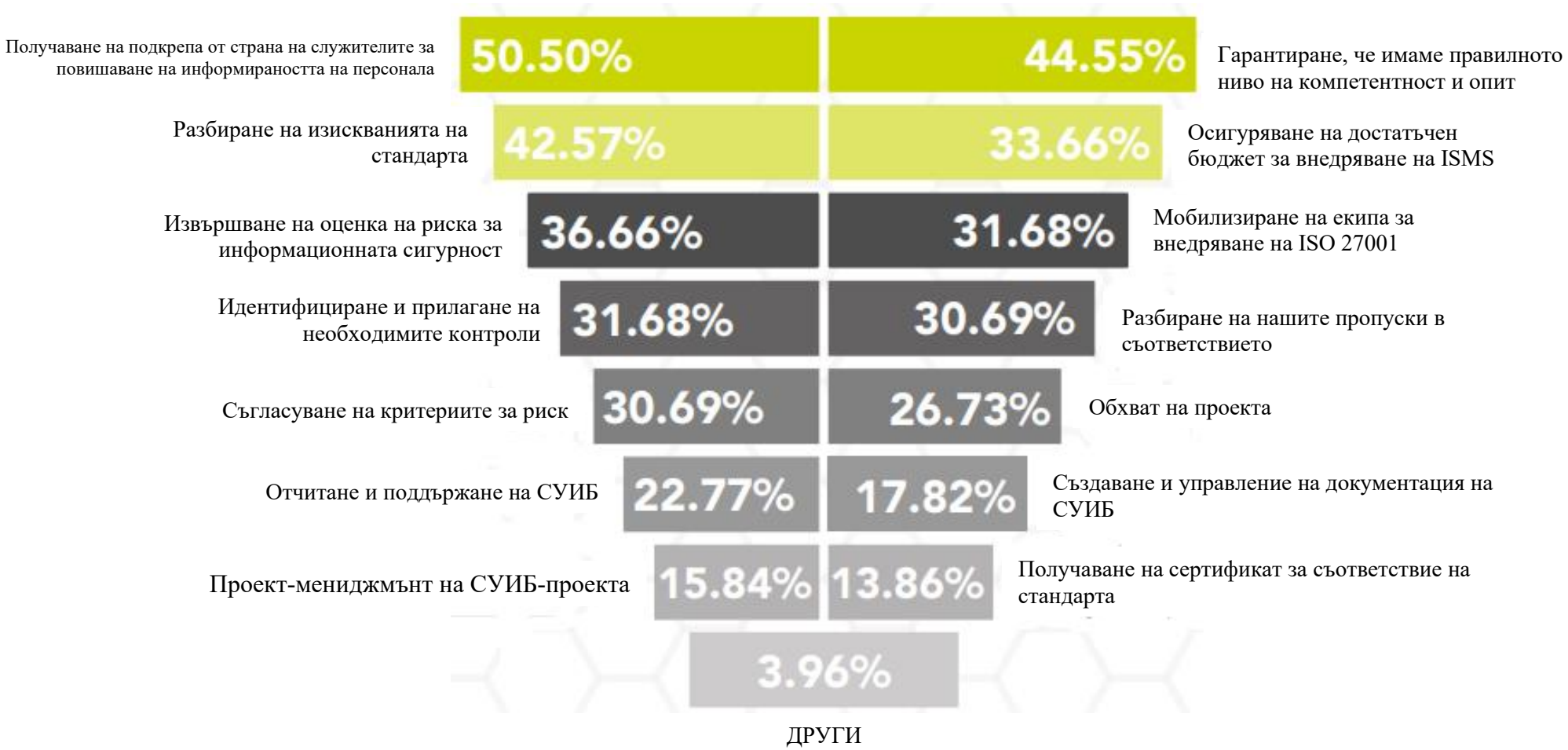
Фиг. 14 Най-важни ползи от внедряване на ISO 27001 в организацията

Като единственият подлежащ на одит международен стандарт, който дефинира изискванията към СУИБ, ISO 27001 сертификат демонстрира, че информационната сигурност на организацията се управлява в съответствие с най-добрите международни практики.

Повече от 70% от респондентите съобщават, че подобряването на информационната сигурност е най-големият двигател за прилагане на ISO 27001, като други основни мотиви за приемане на стандарта за тях са спечелването на конкурентно предимство на пазара - 57%. 52% от анкетираните считат, че сертифицирането е необходимо за осигуряване на законово и регулаторно съответствие, а за постигане на съответствие с GDPR - 48%.

Подкрепено от резултатите от проучването (и в тясно съответствие с двигателите за прилагане на ISO 27001), подобрената информационна сигурност е най-голямото предимство, предоставено от постигането на сертифициране, като 89% заявяват, че това е „най-важната“ полза от прилагането на стандарта.

Фиг. 15 Други подчертани ключови предимства



Фиг. 16 Основни предизвикателства при внедряването на ISO 27001?

Постигането и поддържането на акредитиран сертификат по ISO 27001 може да бъде предизвикателство и много организации съобщават, че се борят с ключови области на прилагането на ISO 27001.

8. Практики при внедряването на стандарта ISO/IEC 27001 в България (на примера на TUV Nord Bulgaria).

Една от водещите международни сертифициращи организации в България - от TUV Nord Bulgaria развива активна дейност за сертифициране на организации по Стандарта ISO/IEC 27001 - Системи за управление на сигурността на информацията. В следващата Таблица 3. е показано разпределението на организациите по предмет на дейност.

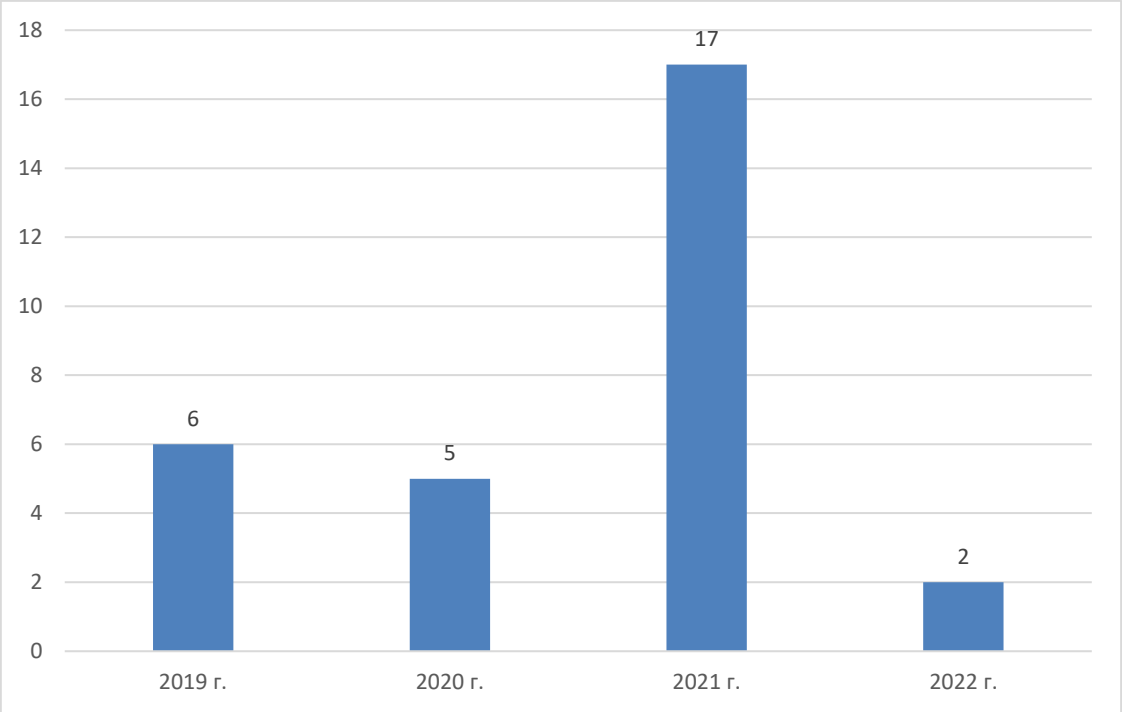
Таблица 3. *Сертифицирани от TUV Nord Bulgaria организации по предмет на дейност(по данни на TUV Nord)*

№	Предмет на дейност	Брой
1	Информационни технологии, софтуер	5
2	Разработване на софтуер и продажби	1
3	Разработване на софтуер и консултантска дейност	1
4	SMART HOME СИСТЕМИ & BMS СИСТЕМИ	1
5	Информационна сигурност	1
6	Строителство	1
7	Представителство на SAP, Microsoft и Cisco	1
8	Водоснабдяване и канализация	1
9	Газоразпределение	1
10	Инженеринг в топлофикацията	1
11	Търговия и маркетинг	1
12	Информационни технологии, видеонаблюдение и дигитализация	1
13	Телекомуникация	1
14	Производство на интелектуални и материални продукти	1
15	Информационни технологии, поддръжка, хостинг	1
16	Електронна търговия	1
17	Консултантска дейност	1
18	Събиране и обработване на отпадъци	1
19	Инженеринг в енергетиката, транспорта и индустрията	1

20	Счетоводни услуги	1
21	Информационни услуги, бази данни	1
22	Информационни технологии и реклама	1
23	Организиране на лотарийни игри	1
24	Изграждане, поддържане и използване на обществена електронна съобщителна мрежа и физическа, инфраструктура	1
25	Охранителна дейност	1
26	Консултантска и търговска дейност	1

Информацията показва, че стандартът може де бъде прилаган във всички типове организации, независимо от техния размер и вид на дейност, то преобладаващо се внедрява от организации, които са от сектора на информационните и комуникационните технологии и създаването на софтуер. Това се дължи на предлаганите от организациите информационни услуги, обработването на лични данни и чувствителна за клиентите информация, поддържане на големи бази от данни. Унищожаването или нарушаването на целостта на данните би довело до сериозни проблеми и дори до преустановяване на дейността, включително и до съдебни процедури с клиенти. Ръководствата им поставят на първо място информационната безопасност и се стараят да решат тези проблеми чрез внедряване на този стандарт.

Интересът на компаниите, които са се обърнали към TUV Nord и са се сертифицирали през последните години варира и това е отразено във Фиг. 17.



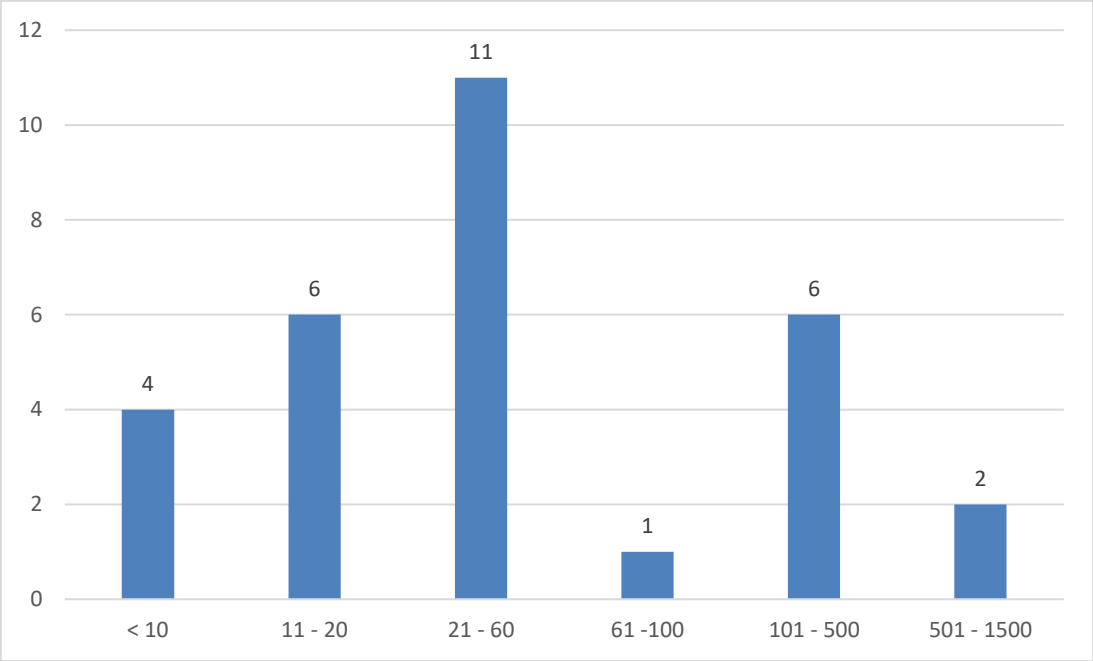
Фиг. 17 Сертифицирани компании, в съответствие със стандарта ISO 27001:2013 за последните 4 години (по данни на TUV Nord Bulgaria към юли 2022 г.)

Интересът незначително намалява (от 6 на 5 фирми) през 2020 г., но това може да бъде резултат от епидемията от COVID-19, неяснотата в перспективите за развитие на икономиката и на отделните бизнеси, изчакващата стратегия на мениджърите. Въпреки това интересът рязко се увеличава (17 организации) през 2021 г., което се дължи на подобрените перспективи за растеж на икономиката в международен и национален мащаб.

Въпреки растежа през 2021 г. тенденцията за 2021 г. не е ясно очертана, но най-вероятно отново ще бъде отбелязан спад, дължащ се най-вече на очертаващата се стагнация в икономиката, повишаване на цените на енергоресурсите и влиянието на военния конфликт в Украйна.

Анализът на организациите, които са внедрили стандарта показва, че най-голям е делът на организациите със сътрудници от 21 до 60 – 11 бр. Това се дължи на няколко неща: а)достатъчен финансов ресурс, б)наличен квалифициран, компетентен и мотивиран човешки ресурс, в) обработване и

поддържане на сравнително големи (свои и/или собственост на клиентите) бази от данни. На второ място с по 6 бр. са организациите със състав (11-20) и (101-500). Причините са различни. В групата 101-500 влизат организации, предметът на дейност който включва: административна дейност; инженеринг в енергетиката, транспорта и индустрията; изграждане, поддържане и използване на обществена електронна съобщителна мрежа и физическа инфраструктура; събиране и обработване на отпадъци; охранителна дейност; изработка, доставка, внос и поддръжка на софтуерни продукти. Не е налице устойчива зависимост. В групата 11-21 влизат организации, предметът на дейност който включва: компютърни и интернет-технологии, разработване на софтуерни продукти, консултантска дейност, разработване на проекти; информационна сигурност и информационни технологии; търговия и маркетинг; производство на интелектуални и материални продукти. Причините се състоят в стремежа на малките компании да подобрят своята конкурентоспособност чрез демонстриране пред клиентите сериозно отношение към информационната безопасност, както към своята, така и към техните информационни ресурси. В групата от 501 до 1500 влизат две големи компании, които са държавни и имат значение за националната сигурност, което е отчетено от техния принципал. В групата < 10 служители влизат организации, чиито предмет на дейност включва: информационни технологии, телекомуникации, ИТ поддръжка и хостинг, консултантски услуги. Това са малки, високотехнологични компании, които предоставят специализирани услуги и им се налага при кандидатстване по проекти и по държавни поръчки да демонстрират високо ниво на информационна безопасност.



Фиг. 18. Размер на организациите сертифицирани в съответствие със стандарта ISO 27001:2013 (по данни на TUV Nord Bulgaria към юли 2022 г.)

9. Необходимост от разработване на Система за управление на информационната безопасност на организацията в съответствие с ISO 27001.

Винаги, преди да вземем стратегическо решение и да започнем изпълнението този много сериозен проект, си задаваме въпроса – „За какво е необходим сертификат по ISO 27001“.

Причините могат да бъдат разделени на три вида: „Действително ми е необходим за повишаване на ефективността на компанията и на информационната сигурност“, "Да го имам за всеки случай" и "Модерно е, въпреки че цената за сертифициране и доста висока".

Една от причините, която може да подтикне компанията да се заеме със сертифициране, се явява препоръката на консултанта, който е успял да изманипулира висшето ръководство, че това е панацея за всичките им проблеми. Друга причина може да бъде ултимативна заповед от

мениджмънта на компанията „майка“ (без ясно разбиране за необходимостта от такава сертификация).

Към правилните причини могат да бъдат отнесени:

- изискванията на бизнеса;
- необходимостта от преминаването на ново по-високо ниво;
- законодателно изискване;
- създаване на ценност за акционерите или за клиентите;
- повишаване на стойността на компании.

Ако компанията просто желае да провери и валидира поддържането на информационната безопасност, то не е необходимо да предприема толкова сложна процедура като сертифициране по стандарта ISO 27001. За тази цел е целесъобразно да бъдат използвани други средства – не толкова скъпо струващ одит или използване на специализирани инструментални средства за проверка на съответствието.

Каква е ролята на информационната безопасност в съвременната организация?

Ако се разгледа дейността на която и да е компания, то, съгласно Engelbart Doug, всички нейни функции и процеси могат да бъдат разделени на 3 категории:

1. Основната дейност на компанията, която е предназначена за "заработване на пари" – произвеждане на стоки, предлагане на услуги и др.

2. Действия за усъвършенстване на основната дейност - повишаване на ефективността на доставките, оптимизация на използването на ресурсите, понижаване на разходите и др. (Георгиева, 2014).

3. Действия за усъвършенстване на предходната категория – управление на качеството. Важно е да се отбележи, че това трябва да бъде не просто управление на качеството като формално съответствие на някакви дефинирани процедури или технически изисквания, а като ценност за техните потребители. Ако потребителят не може да почувства и оцени тази

ценност, то въпреки наличието на всички придобити сертификати, награди и др., тотой няма приеме новия продукт, услуга или процес.

За съжаление информационната сигурност не може да бъде отнесена към първата категория функции. Може да се предположи, че ИС може да бъде отнесена към категория 2, но все пак е много трудно да се докаже как ИС влияе върху понижаването на разходите или върху повишаването на ефективността на конкретния процес. Логично е управлението на информационната сигурност да бъде отнесено към третия вид функции.

Често консултантите рекламират пред клиентите очаквания ефект от сертифицирането, а именно "качествен скок" в резултатите от дейността. Много от компаниите не притежават необходимите ресурси, въпреки това предприемат съответните действия за радост на сертифициращите организации. В резултат всички са доволни – компанията е получила сертификат за съответствие, а другата страна е получила финанси.

Всяка компания може да декларира, че защитава своите системи и следи за безопасността на предаваните данни. Но дали всичко е така на практика и доколко наистина добре ги защитава? Сертифицирането на СУИБ в съответствие с международния стандарт ISO 27001 отговаря на тези въпроси на клиентите и потребителите и едновременно с това позволява да бъде икономисано време за събиране и предоставяне на доказателства.

10. Теоретични принципи за разработване на Система за управление на информационната безопасност на организацията.

Стандартите от серията за системи за управление на сигурността на информацията са под общото наименование **Информационни технологии. Методи за сигурност. Те** включват:

БДС ISO/IEC 27000 Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Общ преглед и речник.

БДС ISO/IEC 27001 Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Изисквания.

БДС ISO/IEC 27002 Информационни технологии. Методи за сигурност. Кодекс за добра практика за управление на сигурността на информацията.

БДС ISO/IEC 27003 Информационни технологии. Методи за сигурност. Указания за внедряване на система за управление на сигурността на информацията.

БДС ISO/IEC 27004 Информационни технологии. Методи за сигурност. Управление на сигурността на информацията. Измерване.

БДС ISO/IEC 27005 Информационни технологии. Методи за сигурност. Управление на риска за сигурността на информацията.

БДС ISO/IEC 27006 Информационни технологии. Методи за сигурност. Изисквания за органите, извършващи одит и сертификация на системи за управление на сигурността на информацията

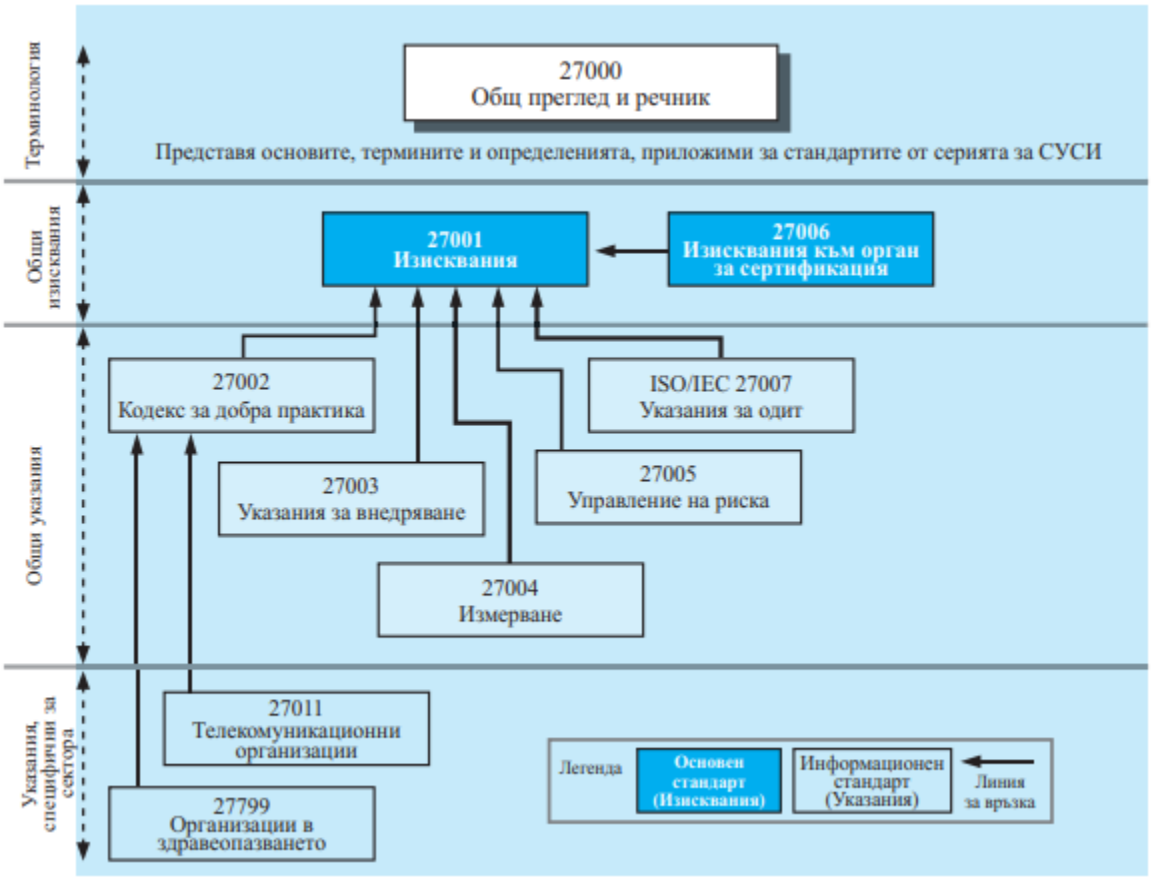
ISO/IEC 27007 Информационни технологии. Методи за сигурност. Указания за одит на системите за управление на сигурността на информацията

ISO/IEC TR 27008 Информационни технологии. Методи за сигурност. Указания за одитори, свързани с механизмите за контрол на сигурността на информацията.

БДС ISO/IEC 27011 Информационни технологии. Методи за сигурност. Указания за управление на сигурността на информацията за телекомуникационни организации, базирани на ISO/IEC 27002

БДС ISO/IEC 27799 Информатика в здравеопазването. Управление на сигурността на информацията в здравеопазването на основата на ISO/IEC 27002.

Взаимовръзката между стандартите от серията за СУИБ е показана на следната фигура (фиг.19).

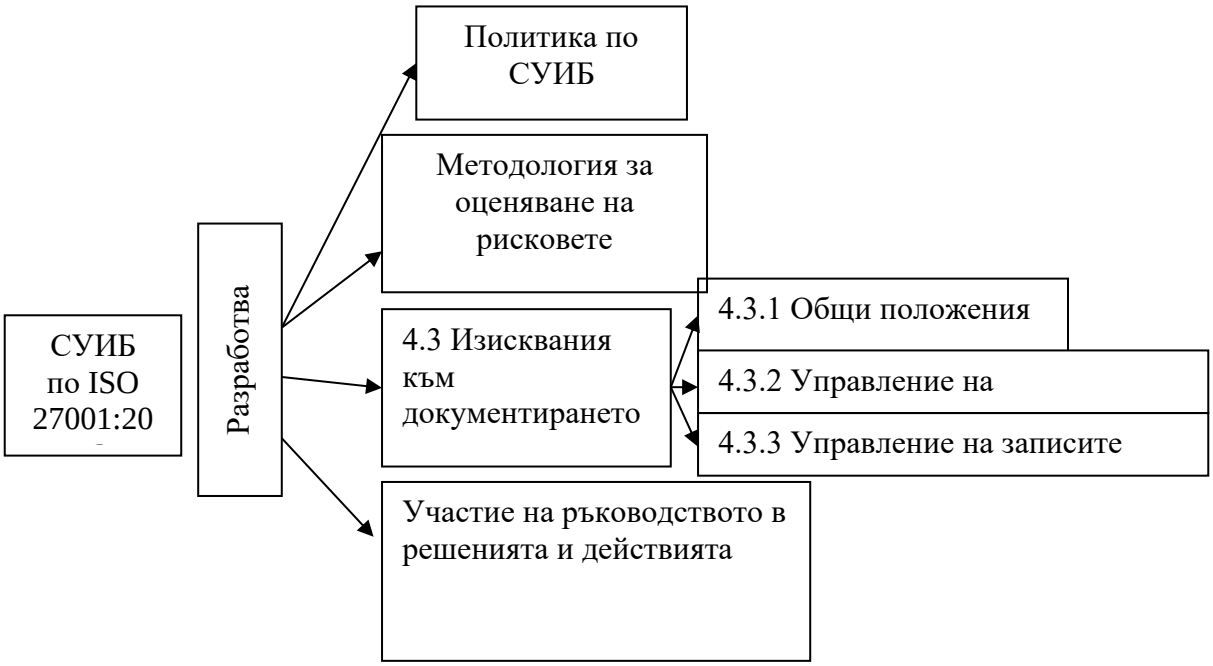


Фиг. 19 Взаимовръзка между стандартите от серията за СУИБ

Нивото на информационната безопасност (ИБ) трябва да съответства на потребностите на организацията и изисква точно излагане на основните правила, принципи и задачи. Изисква адекватнато им реализация в повторяеми и контролируеми защитни мерки, внедряване в практиката на мерките със силите на сътрудниците на организацията при оперативно отразяване на текущата ситуация за да могат сътрудниците да предприемат необходимите управленски действия. Най-добрият метод за реализация на

това е идеите, практическите мерки и резултаи от дейността по осигупяването на ИБ в да бъдат представени в документална форма, което ще позволи да бъде определена структурата на взаимодействието на правилата и реализиращите ги практически действия, и да доведе до всеки сътредник, на съответвоното ниво на процесса, правилата и изискванията за осигуряването на ИБ, които трябва да бъдат спазвани при изпълнението на своите задължения. Необходимо е също така да бъде определен реда за контрола за тяхното спазване.

На базата на това се получава нов «клон» в схемата на СУИБ (Фиг. 19).



Фиг. 20 «Клон» в схемата на СУИБ

Как следва да бъде организирана системата за документално осигуряване на СУИБ? Всеки тип документ трябва допълнително да бъде характеризиран със съответните въпроси, които влияят на неговия жизнен цикъл: за кого е предназначен (кой трябва да го познава; кой ще го съгласува и утвърждава; колко често той може да бъде променян.

Формално документите могат да бъдат разделени на програмни (справочни) и оперативни (съдържащи резултатите от дейността). От гледна точка тези документи се разделят, съответветно, на „документ“ и „записи“. В съответствие със стандарта, документация на СУИБ трябва да вкбючва информация за:

- Документирана и утвърдена политика по СУИБ, нейните цел и област на функциониране;
- Процедури и мерки за управление, които се използват от СУИБ;
- Методология за оценяване на рисковете за ИБ;
- Резултати от оценяването на рисковете и планове за тяхното обработване;
- Процедури за оценяване на резултатите от функционирането на СУИБ
- Доказателства за функционирането на СУИБ.

Особено важно при разработването на документацията е избора и формата, в който ще бъде представена информацията. При разработването на системата от документи на СУИБ възникват противоречия между трудоемкостта (потребността от ресурси) при първоначалното създаване на документите и по-нататъшното им поддържане в актуално състояние. От една страна има желание броят на видовете (номенклатурата) и количеството на самите документи да бъде минимално, защото по-малкото количество по-лесно се управлява, по-бързо може да се приключи с подготовката на целия комплект документи. От друга страна, ако СУИБ непрекъснато се развива, документите периодически или достатъчно често, се налага да бъдат коригирани и усъвършенствани. Документите, които осигуряват СУИБ са включени в общия «бюрократичен цикъл» на организацията, който се изразява в алгоритъма „разработване-съгласуване-утвърждаване“. Поради тази причина, колкото по.високо е нивото за утвърждаване и съгласуване на документите, толкова по-дълъг ще бъде

цикълът за въвеждане в действие на новите версии на документите, толкова по-трудно те ще се поддържат в актуално състояние.

Системата от документи на СУИБ трябва да бъде построена по йерархична схема с максимално общи и абстрактни документи на най-високото йерархично ниво и с повишаване на конкретността в процеса на приближаване към практическата част. Стандартът ISO 13335-1 предвижда четири нива на политиките (правилата) на информационната безопасност:

- корпоративна политика на безопасност;
- политика за информационна безопасности;
- корпоративна политика на безопасност на информационните и комуникационните технологии;
- политика на безопасност на отдельните системи базирани на информационни и комуникационни технологии.

Интерпретации на изискванията на стандарта:

Ниво на документите	Типове документи
Първо ниво	Политика на СУИБ, Политика на информационна безопасност, Концепция за информационна безопасност.
Второ ниво	Частни политики на информационната безопасност (осигуряване на физическа безопасност, предоставяне на достъп, използване на Интернет и на електронна поща, ИБ в технологичните процеси и др.)
Трето ниво	Инструкции, изисквания, порядки, ръководство, методически инструкции и програми за обучение, изисквания към конфигурациите и др.
Четвърто ниво	Записи в системните регистри на ОС, СУБД и ИС; регистри на информационните активи; заявки и изпълнени разрешения за предоставяне на достъп; записи в регистрите за обучения и инструктажи по ИБ, протоколи от изпитания, актове, задължения за неразгласяване на конфиденциална информация и др.

Фиг. 21 Нива и типове документи в СУИБ

Документите, които са отнесени към различни нива в йерархията, имат различен по продължителност жизнен цикъл.

Ниво на документите	Колко често се променят
Първо ниво	Рядко (измененията касаят стратегическото ниво)
Второ ниво	Не често (при настъпили изменения на ниво тактически решения)
Трето ниво	Относително често
Четвърто ниво	Непрекъснато

Документите на високите нива трябва да бъдат максимално обобщаващи и абстрактни. Те ще бъдат променяни при промени на

стратегическо ниво - смяна на стратегията на бизнеса, внедряване на нови стандарти, кардинална замяна на информационната систем и др. Подчиненните, според йерархията, документи (трето ниво) могат да се променят доста по-често – при внедряване на нови продукти, нови технологии за осигуряване на ИБ, формиране на допълнителни учебн курсове или разработване на алгоритъм за резервно копиране на информацията. На четвърто ниво записи се генерират непрекъснато и с времето, най-вероятно, ще се налага да бъдат уточнени техните формати.

Ниво на документите	**Ниво на утвърждаване**
Първо ниво	Съвет на директорите, собственик.
Второ ниво	Изпълнителен директор или негов заместник, който отговаря за ИБ.
Трето ниво	Ръководител на блоковете ИТ, ИБ, учебни модули.
Четвърто ниво	Изпълнител.

Документите от високо ниво (напр. Политика на СУИБ), които определят стратегическите подходи за осигуряване на ИБ, се утвърждават на ниво собственик или съвет на директорите. Частните политики, които определят правилата за информационната безопасност в отделните сфери, могат да бъдат утвърдени на ниво изпълнителен директор или отговорен ръководител, но при това е необходимо да съществува широк кръг за съгласувания в подразделенията, които тези сфери на дейност засягат.

Инструкциите и другите практически документи представляват работни документи на подразделенията, които използват инфраструктурата за осигуряване на ИБ. Те ги създават, коригират и променят. В някои случаи конкретни документи от трето ниво могат да изискват утвърждаване на ниво ръководство на организацията. Доказателствата за функционирането на ИБ, при необходимост, се валидизират чрез подписа на изпълнителя.

Необходимо е правилно да се управляват версиите на документите при тяхното правилно разпространяване сред сътрудниците, за които са те са предназначени.

Процедурата за управление на документите трябва да е в състояние да осигури:

- утвърждаване на съответните документи на необходимото ниво на управляващата структура на организацията;
- преразглеждане и модернзиране, ако е необходимо, на конкретни документи;
- осигуряване на идентификация на направените промени и на статута действащата версия на документите;
- осигуряване на достъп до работните версии на документите, там където те ще бъдат използвани;
- съществуващ ред за идентифициране на документите и за предоставяне на достъп до тях;
- осигуряване на достъп до документите на оторизираните сътрудници, както и гарантиране, че техният жизнен цикъл (предаване, съхраняване и унищожаване) се извършва в съответствие с нивото на класифициране на тяхната конфиденциалност;
- идентифициране на документите, които са зададени извън организацията;
- контролиране на разпространението на документите;
- предотвратяване на използването на стари версии на документите;
- внедрена идентификация на остарелите версии на документите, ако процедурата предвижда съхраняването им поради някаква цел.

Процедурата за управление на документтите на СУИБ е необходимо да бъде оформена в отделен документ, който съдържа в себе си списък и предназначение на всички документ, периода и условията за тяхното преразглеждане, кой се явява собственик на всеки един от документите, кой,

кога и по какъв начин съгласува и утвърждава конкретния документ, за кого е предназначен всеки конкретен тип документ и др.

Всички правила за създаване, изменения, съгласувания и утвърждавания на документите трябва да съответстват на утвърдените в организацията правила за документооборота.

Трябва да се има предвид, че процедурата за преразглеждане на документите не е задължително да подразбира задължително промяна на документа. Полезно е да бъде предвидена, за някои специфични типове документи, процедура за потвърждаване на тяхната актуалност, през сравнително продължителни, но регулярни периоди от време.

Свидетелствата за функционирането на СУИБ също трябва да бъдат формирани във вид на документив, които съществуват на хартиен и/или на електронен носител. Към свидетелствата за функционирането на СУИБ могат да бъдат причислени различните заявки и временни разрешителни за предоставяне на достъп, записи в регистрите на операционните системи, на СУБД и на приложния софтуер, резултати от функционирането на системите за предотвратяване на прониквания и отчети за резултатите от проведени тестове за защитеност от несанкционирано проникване, актове от проведени проверки на конфигурациите на работните места и на сървърите и др. Даденият клас документи се дефинират в стандарта като «Записи».

Процедурата за управление на записите трябва да осигурява техния контрол и гяхната защита от модифициране, защото, при определени условия, те могат да се превърнат в материали и доказателства за извършване на разследване на инциденти свързани с информационната безопасност и качеството на съхраняването на данните определя дали те могат да бъдат признати за легитимни или да бъдат признати за такива, които не заслужават доверие.

Процедурите за управление на записите трябва да:

- осигуряват ясност, еднозначност, простота, идентифицируемост и възможност за възстановяване на документалните свидетелства;
- бъдат използвани методи за управление, които осигуряват идентификация, съхраняване, защита на конфиденциалността и цялостността на информацията, за търсене, за определяне на сроковете за съхраняване и реда за тяхното унищожаване.

Като пример, може да бъде представен малък «вертикален» фрагмент от списъка на типовете документи, които са част от системата за документиране на СУИБ, например, осигуряване на информационна безопасност при предоставяне на достъп до Интернет (Таблица 4):

Таблица 4. Списък на типовете документи, част от системата за документиране на СУИБ

Ниво на документите	**Документи**
Първо ниво	- Политика за информационна безопасност на организацията. - Концепция за осигуряване на информационната безопасност на организацията.
Второ ниво	- Частна политика за информационна безопасност на организацията при работа с Интернет ресурси. - Термини, които се използват в документите за информационна безопасност.
Трето ниво	- Алгоритъм за предоставяне на достъп на потребителите до Интернет ресурсите. - Описание на профилите за достъп (списък от разрешения и забрани) до Инернет ресурсите. - Схема на компютърната мрежа, която е включена към мрежата на Интернет. - Карта за настройване на прокси-сървъра. - Карта за настройка на междумрежовия екран между сегментите на вътрешната мрежа и демилитаризираната зона (DMZ). - Карта за настройване на работната станция за осигуряване на достъп до Интернет.

	- Инструкция за потребителя за реда за използване на ресурсите в Интернет. - Описание и квалификационни изисквания към функционалната роля на «Администратор на системата за достъп до Интернет». - Длъжностна характеристика на сътрудника, който изпълнява функцията «Администратор на системата за достъп до Интернет».
Четвърто ниво	- Заявка-нареждане за включване на потребител до Интернет ресурси. - Списаък (регистър) на потребителите, които са включени към Интернет, с описание на профила на достъпа. - Регистър на прокси-сървъра за достъпа на потребителите до Интернет ресурсите. - Регистър на системата за открити несанкционирани прониквания (IDS) в сегмента на мрежата, расположен в DMZ. - Отчет за прониквания в DMZ, които са установени от IDS. - Акт от проведена проверка на конфигурацията на междумрежовия екран. - …

Посоченият примерен списък съвсем не е изчерпващ даже за избраното направление и в голяма степен зависи от конкретните технологични решения и поддържането им, а също така и от подходите използвани за осигуряване на информационната безопасност.

Ето няколко общи препоръки за създаването на документите на СУИБ.

➢ Трябва да бъде разработен отделен документ под името «Речник на термините», който е общ, като минимум, за документите от първите две нива. Той трябва да бъде използван при разработването на останалите документи и трябва да бъде посочен в тях във вид на препратка.

➢ За да бъде извършено стандартизиране на формите на документите трябва в приложенията към документите от високо ниво да бъдат посочени

формите на подчиненните документи, особено на тези, които се явяват доказателства за някакво изпълнение на дейност (отчети, форми на запитвания и др.). от една страна това води до известно усложняване на процедурата при първоначалното разработване на документите, но от друга страна, ако всички свързани документи бъдат разработени като елементи от процедурата, то веднага се получава готова за използване технология.

- Честа грешка при подготовката на документите от високо ниво (политика и частни политики, положения и др.) се явява внасянето непосредствено в текста на документите на конкретни фамилии, имена на системи и др. подобни. Това води, съответно, при замяна на сътрудника (изпълнителя) да се стартира продължителна процедура за съгласуване и утвърждаване на «нова» версия на този документ. Целесъобразно е такива «променливи» величини още в началото да бъдат изнесени в приложенията, в подчинените документи или в записите (документи от четвърто ниво).

- При създаването на «практични» документи е добре при описването на изпълнението на една или друга функция да се посочва не длъжността, а функционалната роля, например «Администратор на антивирусна система» или «Оператор на системата за резервно копиране», а в отделен документ да се води регистър на сътрудниците, които изпълняват една или друга роля. Това води до удължаване на „жизнения цикъл на документа“, без да се налага необходимост от неговото коригиране и осигурява гъвкавост при неговото използване.

- Всеки документ трябва да съдържа признак за своя собственик (отговорен сътрудник), областта на действие и условията за неговото преразглеждане.

- Документите и записите на СУИБ могат да съществуват както в хартиена, так и в електронна форма. За предоставяне на одиторите или на проверяващите копия от тези документи, които съществуват в електронна

форма, трябва да бъдат разработени и утвърдени съответни процедури и да бъдат определени техните отговорни изпълнители.

На базата на всичко това трябва да се отбележи, че ако разработването на документите от високо ниво (политики и др.) може да бъде възложено на външни консултанти, то документите и записите от ниските нива трябва да се разработват и поддържат в актуално състояние от сътрудниците на организацията, които са максимално въвлечени в процеса на поддържането на функционирането на СУИБ.

Едно от най-важните ограничения и пречки, които възникват при внедряването стандарта могат да се явят „тежкото наследство“ от морално остарели правила и подходи за осигуряване на сигурността на информацията. Много често в различни организации организационните процеси са се формирали дълги години и са излишно формализирани. Поради тази причина много често ръководството им с голямо нежелание се захваща да преустрои кардинално съществуващата систем.

В такава ситуация предпоставка за успешна реализация на изискванията на стандарта се явява осъзнаването, от страна на ръководството на важността на целите и задачите на информационната безопасност. Без активната подкрепа и поддръжка от страна на топ мениджмънта, внедряването на стандарта е практически невъзможно, защото в основата на приемането на ключовите решения при изграждането и поддържането на СУИБ лежи готовността да бъдат извършени необходимитее изменения и ограничения, да бъдат осигурени и предоставени необходимите финансови и кадрови ресурси.

11. Предимства от внедряването и сертифицирането на СУИБ, съответстваща на стандарта ISO 27001

В следващия раздел ще бъде представен подхода за разработване, внедряване и сертифициране на СУИБ според изискванията на **ISO 27001** и свързаните с това трудности и проблеми, които трябва да бъдат решени.

Стандартът ISO 27001 осигурява:

- Определяне на целите свързани с информационната безопасности на организацията, с направленията и принципите на дейността в сферата на ИБ;
- Определяне на подходите за анализиране, оценяване и управляване на рисковете в организацията;
- Управление на информационната безопасност в съответствие с приложими юридически и нормативни изисквания;
- Използване на единен подход за създаване, внедряване, експлоатация, наблюдение, анализ, поддръжка и усъвършенстване на системата за ИБ за постигане на набелязаните от организацията цели;
- Дефиниране на всички процеси свързани с управлението на СУИБ;
- Определяне на важността и статута на мероприятията свързани с осигуряването на ИБ;
- Използване на процедурите за вътрешни и външни одити за определяне на степента на съответствие на внедрената СУИБ на изискванията на стандарта;
- Възможност за предоставяне на актуална и достоверна информация на клиентите, партнъорите и на всички други заинтересовани страни за политиката на организацията осносно ИБ.

Предимства от внедряването и сертифицирането на СУИБ съответстваща на стандарта ISO 27001:

- Независимо потвърждаване, че по правилния начин в организацията се управляват рисковете, спазват се процедурите за мениджмънт на ИБ,

които постоянно се анализират и усъвършенстват от отговорния за това персонал;

- Повишаване на доверието у клиентите, партньорите и у другите заинтересовани страни;
- Постигане на устойчиво развитие и функциониране на компанията;
- Повишаване на имиджа на организацията на вътрешния и на външния пазар, получаване на международно признание;
- Постигане на ефективни и адекватни мерки за защита на информационната система от реални заплахи за информационната безопасност;
- Предотвратяване или понижаване на загубите от инциденти свързани с информационната безопасност;
- Демонстриране на определено ниво на ИБ за гарантиране на конфиденциалността на информацията на заинтересованите страни;
- Доказаване, пред заинтересованите страни, спазването на действащата нормативна база (изпълнението на системата от задължителни изисквания);
- Демонстриране на определено ниво на «зрялост» на системата за управление за да бъде гарантирано високото ниво на обслужване на потребителите и на партньорските компании;
- Демонстриране на резултатите от провежданите задължителни вътрешни и външни надзорни одити на системата за управление на ИБ, оценка на ефективността от постоянното й усъвършенстване.
- Повишаване на стойността на нематериалните активи на компанията, понижване на застрахователните плащания, което повишава цената на компанията като цяло;
- Понижаване на операционните разходи и премахване на «кръстосаното» финансиране в единната СУИБ;

- Разширяване на възможностите за кандидатстване за изпълнение на проекти по големи обществени поръчки обявявани от държавната и местната администрации;
- Съществено облекчаване на провеждани процедури по одит за съответствие с PCI DSS, ISO/IEC 20000-1.

Полезно предимство се явява ефективното управление на аутсорсинга на базата на ясно дефинирани критерии за оценка на доставчиците на услуги и за отговорността на всяка една от страните. Конкурентно предимство се явява също представяне на доказателство, че разглежданите процеси за осигуряване на информационната сигурност на организации са в състояние да удовлетворят изискванията на заинтересованите страни в дългосрочен план, определените рискове са оценени и се управляват.

Сертифицирането на СУИБ за съответствие на изискванията на ISO/IEC 27001(единственото общоприето в света потвърждение за съответствие на международните изисквания. Емпиричните изследвания показват, че тези организации, които са сертифицирали своите СУИБ по изискванията на международния стандарт, получават отстъпки, които са съизмерими с разходите направени от организациите за сертифициране.

12. Анализ на системата за управление на информационната безопасност от ръководството.

Необходимо е ръководството системно и редовно да извършва анализ на СУИБ за поддържане на нейната адекватност. За изпълнение на това изискване, в съответствие с разработената и внедрена СУ, ръководството на организацията трябва да бъде запознато със състоянието на СУИБ на базата на записите, отчетите и резултатите от вътрешните и външните одити. То трябва да обработи и анализира събраната информация и да приеме решения за извършване на коригиращи действия.

Поддръжка и усъвършенстване на системата за управление на информационната безопасност.

СУИБ се нуждае от постоянно усъвършенстване в резултат на натрупването на знания за нюансите и детайлите свързани с управляемите процеси, от постоянно предприемане на коригиращи действия, ако е разкрито, тя не съответства на конкурентната среда, от организиране на превантивни действия за отстраняване на самите причини за възникване на потенциални несъответствия.

Цели и методи за управление на СУИБ.

Това е най-разработваният раздел от ISO 27001, който включва в себе си обемен, подробен и ясно структуриран списък от цели и практически мерки, които трябва да бъдат предприети при осигуряването на ИБ - от дефиниране на политика по информационна безопасност до управление на достъпа до информационните ресурси и до непрекъсваемостта на основните процеси.

Внедряване и сертифициране на СУИБ в съответствие с ISO 27001.

Наличието на сертификат за съответствие с изискванията на стандарта в компанията се явява важен фактор, когато евентуалните партньори вземат решение дали да си сътрудничат с нея. Много компании желаят да съответстват на изискванията на стандарта и са склонни да инвестират сериозни средства в това. Но не всичко се случва по идеалния начин. Често сертифицираните организации, които притежава този стандарт нарушават изискванията на стандарта като по този начин поставят под съмнение самата идея за покриване на изискванията и сертифицирането в съответствие с тях. Поради тази причина често ръководствата на компаниите често се питат дали си заслужава да бъдат инвестирани сериозни средства и време за това.

Особено важно е да не се пропуска, че според философията на ISO 27001, не се сертифицира компанията и системата за защита, а ПРОЦЕСА.

Това е най-важната разлика на този стандарт от изискванията заложени в "Общите критерии" или изискванията при атестирането на автоматизирани системи. Това много често се пропуска или е налице неразбиране. Ако е сертифициран един единствен процес, то съществуват още много на брой процеси, всеки от които може да се превърне в „слабо звено“. Неправилно е да се казва "нашата организация е сертифицирана по ISO 27001". Това не само, че не е вярно, но и показва че не се разбира същността на стандарта.

Стандартът не дефинира кои конкретни процеси трябва задължително да бъдат идентифицирани, за да могат в последствие да бъдат сертифицирани. Тази заложена в стандарта гъвкавост го прави едновременно универсален, но в същото време и сложен за внедряване за много от компаниите, които не притежават необходимите експертни знания и квалификация на сътрудниците. При разработването на СУИБ основните сложности не се проявяват при управлението на безопасността, а са свързани с правилното идентифициране на основните процеси. Например, особено важно е дефинирането на самото понятие "процес". Някои от компаниите го разбират по най-елементарния начин: „Всичко, което извършва отделът (подразделението) за информационна безопасност се явява „процес на осигуряване на информационната безопасност“. Това тълкуване, обаче, се явява прекалено опростено и не винаги е правилно. Особено трудно се идентифицират сложните процеси, които протичат през няколко отдела или звена на компанията. Тези процеси много трудно се поддават на управление, трудно се контролират и още по-трудно се оценява и измерва тяхната ефективност. Трудности възникват и от това, че собствениците на тези процеси много често не се явяват специалисти в областта на информационната безопасност. Ако компания, сертифицирана по ISO 27001, е успяла да идентифицира и управлява точно такъв процес, то тя очевидно притежава висок капацитет. Ако тя е осъществила просто сертификация на "процес за информационна безопасност" само и

единствено в самия „Отдел за защита на информацията“, то това представлява опошляване на идеята. Според много специалисти точно тези процеси, които протичат от начало докрай през няколко подразделения (отдели), тоест тези, които протичат хоризонтално, а не вертикално през структурите на компаниите, заедно с техните „собственици“ отразяват истинската същност на процесния подход. Важно е да се отбележи, че при правилна организация на такъв процес, неговият „собственик“ може на практика да осъществява оперативно управление, защото е налице внедрен алгоритъм и точно дефинирани граници.

Един от основоположниците на научния подход при изграждането на системи за управление на качеството Едуард Деминг счита, че "задачата на мениджмънта се състои в усъвършенстване на системите, а не в постоянната намеса в оперативната дейност". Именно с това трябва да се занимава и CISO (англ. Chief Information Security Officer) - ръководителят на отдела за IT-безопасност, (главен) директор по IT-безопасност. CISO може да бъде подчинен както на CIO, така и на CSO.

Това е много важно отличие в разбирането за ролята и изискванията към CISO в България и в развитите страни. В нашите компании много често ръководителят отговарящ за Информационна безопасност (ИБ) продължава по установена традиция да се занимава с оперативната дейност, въпреки че в същото време неговата основна задача се състои в създаване на ценност за потребителите. Поради тази причина собственикът на процеса „ИБ“ и ръководителят на звеното ИБ — не винаги това е едно и също лице. Въпреки, че при наличие в компанията на позиция „CISO“, което се намира на правилно ниво в йерархията, то той ще изпълнява ролята на собственик на процеса (или на процесите). От това произтичат и редица сложности.

За да може този процес да бъде ефективен, собственикът му обикновено се стреми и се опитва да завладее всички ресурси, които са достъпни за него (често даже за сметка на други процеси в компанията). За

да не бъде допуснато това и за да се оптимизира използването на ресурсите е необходима намесата и решенията на функционалните ръководители. Най-голямата заплаха за компанията, според Деминг, това е „оптимизацията на базата на собствените интерес" (на управляващия процеса), против интересите на компанията и на бизнеса. В случая с информационната безопасност заплахата се проявява максимално ясно, защото отделените за този процес ресурси ли не се осигуряват въобще, или се осигуряват в недостатъчен обем за ефективното и резултативно управление на този процес. Поради тази причина е изключително важно да бъдат поддържани работещи контакти с преките ръководители и с мениджърите на функционалните подразделения, когато се дефинира и разработва проходния (преминаващия през повечето функционални звена) процес „Информационна безопасност“.

Когато в компанията се придържат към внедряването на процесния подход, тогава задължително трябва да бъдат отчитани, като минимум, два принципа за разработване на процеса:

1. Технологията за изпълняване на процеса - как се изпълнява дейността, която се описва от процеса.
2. Технология за управление на процес - как тази дефинирана дейност се управлява.

Втората част също може да бъде разделена на две дейност: организация на самия процес и координация при неговото изпълнение, което е изключително важно именно за проходните процеси.

Когато става дума за ISO 27001, обикновено се има предвид само втората част от процеса (системата за управление). Но в същото време, ако в компанията не съществуват инструменти, с които да се управлява, или тази дейност не е организирана, то тогава как може да бъде внедрена система за управление?

Същността на всеки процесен подход се състои в постигане на максимално възможен резултат, в сравнение със съществуващата ситуация и съществуващия резултат. Резултати от управлението на процеса се оценяват от потребителите, а не от този, който е разработил процеса и го управлява (собственика на процеса). Целта на мениджмънта при внедряването или при усъвършенстването на конкретен процес е не той да получи много висока оценка от всички, с изключение от страна на потребителите. Потребителят ще приложи максимални усилия да го заобиколи използвайки всички позволени и непозволени методи. Това често е обяснението на многото неудачи свързани с внедряването на някакви неудобни за използване, "тежки и тромави" системи за защита. Те може и да са в състояние да решат проблемите свързани с информационната безопасност (вируси, „червеи“, изтичане на информация, несанкциониран достъп и т.н.), но не се възприема с ентусиазъм от използващите ги.

Много често мениджърите говорят прекалено много за самия процес забравяйки за какво се прави всичко това. Стремежът, който съществува е да се управлява процеса заради самия процес, което не е необходимо на никого. Например, компанията е разработила внедрила и сертифицирала система за управление на процеса „Информационна безопасност“. Възникват резонните въпроси: „Какъв ефект е постигнат?“, „Какво ни даде това?“. Най-често мениджмънта и компаниите се хвалят с това, че е получен сертификат по ISO 27001:2013, а не с резултатите от усъвършенстваната дейност на компанията, в която и за която този процес е бил внедрен. Като че ли всичко е изпълнено правилно и както е дефинирано в стандарта и в свързаните с него документи, но въпреки това не е налице съществен ефект или пък този ефект не може да бъде изчислен (определен).

В същото време ISO 27001, как и редица други стандарти свързани с безопасността, представлява подборка от най-добрите световни практики.

Те се базират на възвръщаемостта, получена в реалния живот от въвеждането на определени защитни технологии или мерки.

Мениджърите често си задават въпроса дали всичко това си заслужава усилията или отново формално внедряваме някаква система само и единствено за да получим така желания от нас сертификат. Ръководителите си мислят, че с получаването ва сертификата са преминали успешно финалния стадий в процеса на управление на информационната безопасност, но напротив, дейностите по управление на безопасността продължава и това е един перманентен процес.

В какво се състои проблема и в какво се изразява спецификата на ситуацията в България?

Каква е причината и какви са препятствията, които пречат за ефективното внедряване на система за управление на информационната безопасност и на процесния подход? Причината се корени в отсъствието на ясно дефинирана система, която да е ориентирана към получаване на резултат, която е насочена към изпълняване на конкретни цели, количествено измерими на всеки един етап. В същото време трябва да се има предвид, че информационната безопасност се намира в неравностойна ситуация отколкото, например, финансовите цели и резултати, при които ясно са определени крайните целеви показатели, които в крайна сметка определят дали периодът е успешен или неуспешен за компанията. В информационната безопасност обаче обикновено не се дефинират крайни целеви показател, нито пък се внедрява и използва система за оценяване на създаването на ценност за потребителя на всеки един етап. В тази система е много е важно приемането и утвърждаването на цели, които за разлика от финансовите, е необходимо да бъдат по-скоро качествени, отколкото количествени. И тези цели, от стратегически до операционни, трябва да бъдат привързани към всички процеси, свързани с информационната безопасност. Трябва да не се пропуска, че това се отнася към цялата верига

за създаване на ценност за потребителя, а в същото време най-интересни и сложни се явяват именно проходните процеси.

Една такава система работи ефективно само ако се вземат предвид и се отчитат конкретните интереси на всички участници в така сформираната верига за създаване на ценност за потребителите. Казано по друг начин, всички цели и показатели за тяхното оценяване трябва да бъдат много добре балансирани. Не случайно прилагателното е „балансирани“. Световна тенденция през последните години показва все по-широкото използване на системи с балансирани показатели. Тя може напълно успешно да бъде използвана и в сферата информационната безопасност, макар че не е толкова лесно, особено защото факторите, които представляват ценност за потребителя, могат да бъдат няколко. Също много на брой могат да бъдат и клиентите, процесите и звената във веригата за създаване на ценност.

В резултат на това се получава много голямо кълбо от преплетени интереси и връзки, които е необходимо да бъдат балансирани, а това се явява доста сложна задача по редица причини.

Една от сериозните причини се изразява в това, че системата за управление у нас често е все още в сферата на теориите и концепциите, а не в успешната практика. Пример за това е „Процесният подход“, който е описан още в стандарта ISO 9001:2000 и широко се използва от много компании по света. Има се предвид самия подход, без да е обвързан с информационната безопасност. За компаниите в България използването на този подход все още не се превърнало в стандарт, но все по-широко започва да се прилага под натиска на сертифициращите организации. Поради тази причина много неразбираеми за нас неща и термини се тълкуват по-широко според разбиранията на тези, които използват метода, а те не винаги съответстват на идеите на специалистите, разработили процесния подход.

От тук произтича и втората причина: огромно количество консултанти, по време на консултирането и подготовката за сертификация

по стандарта ISO 27001 предлагат на компаниите някакви свои трактовки и разбиране за този стандарт. Практически почти нито един от тях не е сертифицирал своята компания по изискванията на стандарта. И често се получава така, че компания с трима или петима служителя консултира и подготвя за сертификация компании с хиляди служители и с множество различни процеси, за които консултантът понякога няма представа.

В цял свят развитието на стандартите за управление следва логичен път. Отначало управлението на компанията и на отделните процеси в нея, а едва след това управление на информационната безопасност. Често някои мениджъри без да организират ефективно управление на целия бизнес, започват да се опитват да внедрят управлението на тази "второстепенна" или даже "третостепенна" задача. В редица случаи това се опитват да правят паралелно, но от това ситуацията само се влошава.

Въпреки сравнително дългата си история, стандартът ISO 27001 продължава да има преобладаващ теоретичен характер и не особено успешна практика. Необходимо е още време за всички: за потребителите, за консултантите, за регулаторите. Лоша практика е ситуацията, когато управлението на информационната безопасност и сертификацията на системата по стандарта бъде осъществена формално, както в болшинството от случаите с ISO 9001:2015. Това само дискредитира прекрасната, сама по себе си, идея за сертифициране на информационната безопасност.

13. Разработване и внедряване на СУИС в съответствие със стандарт ISO 27001:2013

В стандарта ISO 27001 се съдържа кратко описание на стъпките по създаването, съпровождането и усъвършенстването на СУИС. Всяка стъпка трябва да предоставя гъвкав, базиран на оценка на рисковете подход при осигуряването на информационната сигурност.

1. ОБЛАСТ ЗА ИЗПОЛЗВАНЕ НА СУИС.

Преди вземане на решение за разработване и внедряване на СУИС е необходимо да бъде определена областта, в която тя ще бъде използвана.

При дефинирането на областта за използване на СУИС трябва да бъдат отчитани:

- информационните и физическите активи. Под информационни и физически активи се разбират данни, сървъри и работни станции, мрежово оборудване, софтуер и др. Пристъпването към създаване на СУИС трябва да започне с инвентаризация на наличните информационни и физически активи и оценка на тяхното значение. Инвентаризацията на активите трябва да се извършва с помощта на софтуерни системи за инвентаризация или системи за оценка на сигурността, които притежават такава функционалност;
- изисквания към използваните информационни технологии: изисквания от всякакъв характер към бизнеса, които биха наложили използването на определена информационна технология, приложен софтуер и др.;
- задължения свързани с поддържането на контакт. Това включва правителствени нормативни юридически разпоредби, договори с трети страни, които биха оказали влияние на особеностите при използването на информационните и физическите активи.

2. ОЦЕНЯВАНЕ И ОБРАБОТВАНЕ НА РИСКОВЕТЕ СТОЯЩИ ПРЕД ИНФОРМАЦИОННАТА СИГУРНОСТ

След като бъде определена областта на използване на СУИС, следващата стъпка е провеждане на определяне и оценяване на рисковете за информационната безопасност при защитаването на информационните и физическите активи.

При анализирането и оценяването на рисковете за информационната безопасност трябва да бъдат определени:

- актуалните заплахи пред информационната безопасност;
- актуалните уязвимости, които могат да бъдат използвани за реализиране на заплахите за информационната безопасност;
- вероятностите за реализация на заплахите за информационната безопасност и негативните последствия от тяхната реализация;
- нивата на рисковете за информационната безопасност и тяхната приемливост за организацията;
- защитните мерки за компенсиране на рисковете, свързани с информационната безопасност;
- нивата на рискове за и информационната безопасност, които ще продължат да съществуват, ако бъдат реализирани предвидените мерки за тяхното неутрализиране.

Оценката на рисковете за информационната безопасност се провеждат, в крайна сметка, за приемане на добре претеглени управленски решения за тяхното предотвратяване.

Оценяването на рисковете за информационната безопасност представлява итеративен процес, но резултатите, които са били получени при първичното оценяване играят много важно значение при вземането на решения за поредността, по която ще бъдат внедрявани защитните мерки СУИС.

Следващият етап се състои в определяне на това по какъв начин трябва да се реагира на идентифицираните вече рискове при осъществяване на заплахите за информационната безопасност. Могат да бъдат приложени три възможни сценария – съзнателно приемане на съществуващия риск, стремеж към понижаване на риска, избягване на риска или прехвърляне на риска, например, на застрахователя.

Висшето ръководство трябва да вземе отговорно решение коя от изброените стратегии ще бъде реализирана по отношение на всяка идентифицирана актуална заплаха за информационната безопасност. Тези защитни мерки, които ще бъдат внедрявани в СУИС трябва ефективно да могат да компенсират неприемливите, от гледна точка на мениджмънта рискове за информационната безопасност.

Тъй като обемът от работа свързан с управлението на рисковете за информационната безопасност е много голям, то следва, ако е възможно, да се предприемат мерки за автоматизация на този процес. За автоматизиране на процесите за анализиране, оценяване и обработване на рисковете за информационната безопасност могат да бъдат използвани системи от клас Security GRC (SGRC - Security Governance, Risk, Compliance).

Обработване на рисковете представлява модификация на рисковете, който може да включва в себе си:

- избягване на риска чрез отказване от изпълняване на действия, които могат да доведат до рискове;
- приемане или увеличаване на риска с цел постигане на бизнес цели;
- отстраняване на източниците на риска;
- изменение на вероятността за реализация на риска;
- изменение на очакваните последствия от реализацията на риска;
- прехвърляне (разделение) на риска;
- съхраняване на риска.

3. ВНЕДРЯВАНЕ НА ЗАЩИТНИ МЕРКИ

Следващата стъпка, след оценяването и вземането на конкретни решения по обработването на рисковете за информационната безопасност, се явява внедряването на защитните мерки.

Защитните мерки, които влизат в СУИС, могат да бъдат разделени на два класа:

1. организационни (процеси за управление и осигуряване на информационната безопасност, документационно осигуряване на информационната безопасност;
2. технически (междумрежови екрани, системи за откриване и предотвратяване на несанкционирано проникване, антивируси и др.).

Изискванията към процесите за управление на информационната безопасност са определени в ISO 27001. Изискванията към защитните мерки от технически характер и процесите за осигуряване на информационната безопасност са определени в ISO 27002. Този набор обаче може да бъде коригиран въз основа на резултатите от оценката и обработването на рисковете за информационната безопасност.

Актуалната версия на стандарта 27002 се състои от следните домени:

- Политика за информационна безопасност;
- Организация на информационната безопасност;
- Безопасност, свързана с персонала;
- Управление на активите;
- Контрол на достъпа;
- Криптография;
- Физическа защита и защита от външни въздействия;
- Осигуряване на информационната безопасност при експлоатация;
- Безопасност при обмен на информацията;

- Придобиване, разработване и обслужване на информационните системи;
- Отношения с доставчиците;
- Управление на инцидентите свързани с информационната безопасност;
- Аспекти на информационната безопасност в управлението на непрекъснатостта на бизнеса;
- Съответствие на изискванията.

4. ПРОВЕЖДАНЕ НА ВЪТРЕШЕН ОДИТ

Следващият етап при създаването на СУИС включва необходимостта от разработването и реализирането на програма за провеждане на вътрешен одит.

В т. 9.2 от стандарта ISO 27001 са определени някои от аспектите на програмите за вътрешен одит. При осъществяването на вътрешния одит е необходимо да бъде ясно дефинирано по какъв начин ще бъдат оценявани внедрените вече защитни мерки, а също така и критериите за провеждане на одита.

За автоматизиране на процес за вътрешен одит на СУИС също могат да бъдат използвани системи от класа Security GRC.

5. ОСИГУРЯВАНЕ НА НЕПРЕКЪСНАТО УСЪВЪРШЕНСТВАНЕ НА СУИС

Заключителният етап от създаването на СУИС в съответствие с ISO 27001 представлява внедряване на механизъм за обратна връзка за осигуряване на непрекъснато усъвършенстване на цялата система. Най-често използваният метод за изпълняване на това изискване се явява прилагането на модела за зрялост за всички елементи на СУИС.

Зрелостта на СУИС може да бъде оценена, например, по следната скала съдържаща четири нива:

0 – никой не се занимава с информационната безопасност, ръководството не осъзнава важността на задачите свързани с осигуряването на информационната безопасност.

1 – информационната безопасност се разглежда от ръководството като чисто «технически проблем», липсва единна политика по отношение на информационната безопасност.

2 – информационната безопасност се разглежда от ръководството като комплекс от организационни и технически мероприятия, които са насочени за изпълняване на изискванията на регулиращите органи, определен е отговорник за осигуряване на информационната безопасност.

3 – информационната безопасност се явява част от корпоративната култура на организацията, финансирането се осъществява в рамките на специално определен бюджет.

За да съответства на международния стандарт ISO 27002:2013 - Кодекс за добри практики за управление сигурността на информацията (клаузи 5, 6, 7 и 8) организацията трябва да извърши определени дейности:

1. Да дефинира Общите положения и контекста на средата, в който работи организацията:

- С помощта на стандарта могат да бъдат подбрани контроли;
- Разбиране, че защитата на информацията се явява критична дейност за устойчивата дейност на организацията;
- Определяне на решаващите аспекти, свързани със защитата на активите и с оценката на рисковете;
- Включване на всички служители в дейностите, свързани със защита на информацията;
- Осигуряване на подкрепа от страна на акционерите, доставчиците и от другите заинтересовани страни.

2. Да определи своите изисквания към сигурността, които произтичат от:

➢ Оценката на риска за информационната сигурност;

➢ Изучаване и прилагане в пълна степен на правните, нормативните, регулаторните, договорните изисквания;

➢ Отчитане на съществуващата социална и културна среда в и извън организацията;

➢ Дефиниране на система от принципи, цели и бизнес изисквания свързани с обработката, преработването, съхраняването, комуникацията и архивирането на информацията, които организация ще разработи за поддържане на своите дейности.

➢ Ресурсите, които организацията е осигурила за изпълнението на контролите, трябва да съответстват на вредите за бизнеса, които има вероятност да възникнат при проблеми със сигурността, при положение, че тези контроли няма да бъдат прилагани.

3. Да избере, разработи и внедри подходящи контроли:

➢ Организацията може да избере контроли от съответния стандарт, от друг комплект от контроли или сама да създаде свои уникални контроли.

➢ Когато подбира контролите ръководството трябва се отчита и да се основава на получените резултати от цената на риска;

➢ Някои от подбраните контроли могат да се разглеждат като ръководни принципи и могат да бъдат прилагани в повечето организации.

4. Да разработи свои собствени указания.

➢ При разработването стандартът може да се разглежда като основа за дефиниране на специфични за организацията указания;

➢ Не всички контроли от стандарта могат да бъдат прилагани във всяка една организация;

➢ Когато ръководството решава да създаде допълнителни специфични за организацията контроли, е полезно те да съдържат препратки към клаузи

от този стандарт, за да се улесни дейността свързана с проверката за съответствие.

5. Да вземе под внимание всички съображения, свързани с жизнения цикъл.

➢ Информацията притежава собствен естествен жизнен цикъл, който протича през следните етапи: от създаване и възникване, през съхраняване, обработване, използване и предаване, до нейното евентуално унищожаване или отпадане;

➢ Трябва да бъде отчетена ценността на информацията и риска за нея (тя може да се променя през целия цикъл), като сигурността остава от значение на всички негови етапи;

➢ Трябва да се има предвид, че информационните системи имат жизнен цикъл, в който те са замислени, уточнени, проектирани, разработени, тествани, изпълнени, използвани, поддържани и в крайна сметка бракувани и отстранени. На всеки един етап сигурността на информацията трябва да бъде вземана предвид.

6. Да бъдат отчетени всички свързани стандарти.

➢ Стандартите от семейството 27000 ISO/IEC предоставят допълнителни изисквания (или консултации) по отношение на други аспекти от цялостния процес на управление на информационната сигурност;

➢ ISO/IEC 27000 дава общи сведения за СУИБ и семейството стандарти - дефиниции, термини, обхват и цели на всеки стандарт;

Стандартът дефинира 14 клаузи (раздели), всяка от които съдържа една или няколко категории. Общият брой дефинирани категории (цели) е общо 35, като всяка от тях съдържа една или няколко контроли.

Дефинирани са общо 114 категории, (механизми за контрол).

Организацията трябва строго да спазва дефиницията за контрола.

Подготовката за сертификация по принцип протича в два основни етапа:

1. Разработване на система за управление (и всички необходими за това процедури);
2. Внедряване на системи за управления на ИБ.

За осъществяване на първия етап е препоръчително използването на консултанти. Вторият етап, внедряването, се осъществява със силите на самата компания, т.е. сътрудниците на компанията трябва да разработят съответните необходим процедури, да организира и наложи тяхното стриктно изпълнение, да разработят методики за проверки и методи за контролиране на тяхната ефективност и т.н.

Могат да бъдат идентифицирани следните основни етапи при разработването на СУИБ:

1. Инвентаризация на наличните активи, свързани с осигуряването на информационната безопасност в компанията.
2. Категоризиране на наличните активи.
3. Оценяване на защитеността на информационната система.
4. Оценяване на информационните рискове пред компанията.
5. Обработване на информационните рискове, включително определяне на конкретните мерки за защитаване на критически важните активи.
6. Внедряване на разработените мерки за обработване на рисковете.
7. Контрол върху изпълнението на определените мерки и оценяване на тяхната ефективност.

13.1. Методологии за разработване на СУИБ.

1. Методология за инвентаризиране на активите.
2. Методология за категоризиране на активите.

3. Методология за оценяване на информационните рискове.
4. Методология за обработване на информационните рискове.

За всяка процедура, свързана с осигуряването на СУИБ, трябва да бъде разработена съответната Инструкция. Списъкът от такива инструкции може да бъде в следния вид:

1. Инструкция за осигуряване на съхраняване на конфиденциалната информация (заявление за конфиденциалност).
2. Инструкция на потребителя за осигуряване на информационната безопасност.
3. Инструкция за работата на системния администратор за осигуряване на информационната безопасност.
4. Инструкция на администратора отговарящ за безопасността.
5. Инструкция за управление на достъпа на ползвателите до информационната система.
6. Инструкция за защита от вредоносен софтуер.
7. Инструкция за създаване и поддържане на резервно копие на информацията.
8. Инструкция за работа със външни носители на информация (флаш памет, външен хард диск).
9. Инструкция за използване на мобилни компютри.
10. Инструкция за използване на средства за криптографска защита на информацията.
11. Инструкция за реда за извършване промени в информационната система.
12. Инструкция за управление на инцидентите свързани с информационната безопасност.
13. План за непрекъсваемост на воденето на бизнеса.
14. Регламент за осигуряване на физическа безопасност.

13.2. Дейност на ръководството на организацията, свързана със СУИБ

Едно от базовите условия за ефективното функциониране на СУИБ се явява въвличането на ръководството на организацията в процеса на управление на ИБ. Абсолютно всички служители трябва да разберат, че първо, цялата дейност свързана с осигуряването на информационната безопасност е инициирана от ръководството и е задължителна за изпълнение, второ, ръководството на организацията лично контролира функционирането на системата за управление на информационната безопасност и трето, самото ръководство изпълнява същите тези правила за осигуряване на ИБ, както и всички останали сътрудници на организацията.

13.3. Дефиниране на област на сертифициране

Целесъобразно е СУИБ да бъде разработена за цялата компания като. Процедурите включени в системите за управление е задължително да бъдат изпълнявани от всички звена в организацията. Едновременното внедряване на система за управление на информационната безопасност за всички процеси (бизнес процеси) създава проблеми на мениджмънта. Поради тази причина далеч по-лесно е системата за управление да се внедрява поетапно, стъпка по стъпка. По този начин, след успешното внедряване на система за управление на един процес в организацията и получавайки сертификат за нейното съответствие на стандарта, то е възможно (по-лесно и с по-малко разходи на време и ресурси) да се осъществи разширяване на областта на сертификация (scope) в съответствие с поетапното внедряване на всички останали процеси в организацията. Още на етапа на разработването на СУИБ ръководството трябва много внимателно да анализира и ясно да формулира (определи) областта на сертификация. Ръководството, с

помощта на консултанта, трябва ясно да формулира в коя конкретно подсистема на организацията ще бъде внедрена и ще функционира системата за управление. По време на сертификационния одит одиторите от сертификационната организация внимателно проверяват изпълнението на всички процедури на СУИБ само и единствено в рамките на дефинираната област на сертификация (scope).

Важно е да се има предвид, че описанието на областта на сертификация е необходимо да бъде направено изключително подробно, много точно да бъдат определени параметрите на всички активи, които влизат в областта на сертификация.

- *Провеждане на предварителен одит на организацията.*

Предварителният одит позволява да бъдат систематизирани и оценени съществуващите документи, доколко отговарят на изискванията на стандарта и след това да се определят насоките на дейностите свързани със създаването на системата за управление на информационната безопасност на организацията.

Основната цел на предварителния одит се състои в обективното оценяване на текущото състояние на съществуващата СУИБ и доколко тя е адекватна на поставените от ръководството цели и задачи. След това, на получената информация и проведения анализ се разработват препоръки за усъвършенстване на съществуваща СУИБ или изграждането на съвършено нова такава.

По време на провеждането на предварителния одит консултантската компания решава следните основни задачи:

- анализ на съществуващата структура на организацията;
- анализ на защитаваните области от дейността на организацията и съществуващите вътрешни нормативни и разпоредителни документи;

- анализ на съществуващата структура и на функционалните особености на използваните ИКТ в автоматизираната система за събиране, обработване, предаване и съхраняване на информацията;
- проверка за изпълнението на изискванията на ISO/IEC 27001:2013 към СУИБ;
- разработване на комплексни препоръки към методологическото, организационно-управленското, технологическото, техническото и хардуерното осигуряване за разработването нова или за оптимизиране на съществуващата СУИБ.

На практика решаването на посочените задачи се изпълнява в следните етапи:

➢ Планиране на всички мероприятия свързани с одита. На този етап консултантите извършват събиране и обобщаване на организационните и разпоредителните документи, отраслови нормативи и стандарти, недокументирани решения и практики и други работни материали, които имат отношение към въпросите свързани със създаването на СУИБ и на информационните системи на организацията. Разработване, съгласуване и утвърждаване на планове за мероприятията по одита.

➢ Проверка за съответствието на ISO/IEC 27001:2013. Този етап се състои в: дефиниране на областите на дейност и ключовите бизнес процеси в организацията, които трябва задължително да бъдат защитени на първо място; провеждане на анкети и интервюта със сътрудниците на организацията, анализ на вътрешните нормативни и разпоредителни документ; анализ на съответствието на информационната безопасност на изискванията на стандарта.

➢ Оценка на рисковете за информационната безопасност. Аналитическият и инструменталния анализ на локалните информационни мрежи и информационни ресурси на организацията. Осъществяване на

консултации със специалистите, оценяване на съответствието на фактическото ниво на безопасност на информацията и анализ рисковете.

- Систематизиране на получените резултати от обследването и формиране на документална отчетност. Предоставяне на обобщаващ заключителен доклад на ръководството на организацията.

При разработването на системата за управление на информационната безопасност трябва да бъдат решени следните основни задачи:

– анализ на структурата на организацията, на функционалните особености за изграждане на работните процеси и на използваните в тях информационни технологии. Определяне на защитаваната област на дейност на организацията;

– идентифициране, систематизиране и определяне на ценността на активите на организацията;

– анализ на рисковете за информационната безопасност, определяне на възможните пътища за тяхното реализиране (несанкционирано въздействие върху подсистемите и процесите), категоризиране на рисковете според тяхната критичност. Оценяване на възможните щети от тяхното реализиране. Изчисляване на ефективността от внедряването на комплексните мерки за понижаване на рисковете;

– разработване на Политики за информационна безопасност на компанията;

– разработване на Процедури за понижаване на рисковете;

– разработване на Положения за използваемост на контролите, включващи комплекс от мерки за ИБ в съответствие с Приложение А на стандарта;

– разработване на комплексни препоръки за методологическо, организационно, управленско, технологично, техническо и хардуерно осигуряване на ИБ;

– анализ и оценка резултатите от внедряването на СУИБ;

Основните етапи от изграждането и внедряването на СУИБ на организацията включват:

– Планиране и подготовка на плановете на мероприятията. Извършва се събиране на организационни и разпоредителни документ и други работни такива, които касаят въпросите свързани с изграждането и функционирането на информационните системи на организацията, планираните за използване механизми и средства за осигуряване на ИБ. Разработване, съгласуване и утвърждаване на планове с мерки по определените етапи, които се утвърждават от ръководителя.

– Проверка за съответствие на стандарта. Осъществяване на интервюта и анкети с мениджъри и сътрудници от различни подразделения на организацията.

– Анализ на съществуващите документи, изхождайки от съществуващата организационна структура с последващо уточняване или дефиниране на защитаваната област от дейността. Разработване на ескизен проект на политики за ИБ на организацията.

– Анализ и оценяване на рисковете за ИБ. Разработване на методики за анализ и управление на рисковете. Анализиране на локалните мрежи и информационните ресурси на организацията за откриване на заплахите и уязвимостите на защитаваните активи. Инвентаризация на активите. Консултации със специалистите в организацията и оценяване на съответствието на фактическо ниво на безопасността. Изчисляване на рисковете, определяне на текущото и на допустимото ниво на риска за всеки конкретен актив. Извършване на ранжиране на рисковете, избор на комплекс от дейности (контроли) за понижаване и изчисляване на теоретическата ефективност на внедряването.

– Разработване и реализиране на планиране на мерки. Разработване на Положение за използваемост на контролите в съответствие със стандарта.

Разработване на План за обработване и отстраняване на рисковете. Подготвяне на отчети до ръководителя на организацията.

– Разработване на нормативни и организационни и нормативни документи. Разработване и утвърждаване на окончателна Политика по ИБ и съответните й положения. Разработване на вътрешни стандарти, процедури и работни инструкции, които да осигуряват нормално и стабилно функциониране на СУИБ.

– Реализиране и оценяване на ефективността на извършените комплексни мерки за понижаване на рисковете за ИБ, утвърдени от ръководителя на Плана за обработване и отстраняване на рисковете.

– Обучение на сътрудниците. Разработване на планове и мероприятия и внедряване на програми за обучение и повишаване на компетенциите на сътрудниците за ефективно запознаване с принципите на ИБ на всички ръководители и сътрудници, но на първо място на тези от тях, които са заети в подразделения, участващи в осигуряването на безопасността на ключовите процеси.

– Систематизиране на резултатите от обследването и подготовката на отчетността. Представяне на резултатите от дейностите на ръководителите на организацията. Подготвяне на документите за съответствие със ISO/IEC 27001:2005 и предаването им в сертифициращата организация.

– Анализиране и оценяване на резултатите от внедряването на СУИБ. Разработване на препоръки за усъвършенстване на СУИБ.

– Трябва да се отбележи, което е много важно, че провеждането на втори вътрешен предсертификационен одит на СУИБ не е задължителен, но е силно препоръчителен преди сертифицирането, за да бъдат уточнено изпълнението на изискванията на стандарта и препоръките на консултанта.

- *Дефиниране на правила за ИБ.*

За всяка система за управление, включително и тази за СУИБ, трябва да бъдат разработени и подробно описани моделите за управление на

обекта. Тези модели съдържат подробно описание на съставните части и начините, по които те си взаимодействат, целите поставени пред управлението, базовите функции, начините за описване на моделите (езиците), инструментите, които ще си взаимодействат при функционирането на системата.

Определяне на Политиката на СУИБ. Тази дейност на мениджмънта осигурява „моделирането на СУИБ“. Политиката включва сферата, областта и границите, в които действа СУИБ. Взема под внимание основната дейност на организацията (субект) - компания, учреждение, финансова институция, в интересите на които е изградена и се поддържа СУИБ, осигуряват се материални, човешки и финансови активи и технологии, собственост на субекта. Определят се основните цели, които трябва да бъдат изпълнени при разработването на СУИБ, направленията и принципите, които ще бъдат използвани при осигуряването на информационната безопасност, като при това точно изпълняват нормативните и договорните изисквания.

Политиката на системата за управление на информационната безопасност определя основните методи за организиране на система за осигуряване на ИБ ката обект на управлението и поради тази причина трябва да съдържа в себе си и принципите, които биха осигурили нейната управляемост.

Моделирането на обекта на управление се изразява в дефиниране на областите, в които тя ще бъде прилагана, и границите на действие на СУИБ. То се описва с термини и отчита процесите на икономическа активност, организационната структура, взаимовръзката и местоположението на активите и технологиите. Най-често това представлява подробен списък на информационните активи, които притежават (по презумпция) ценност за компанията, както и обектите на притежаваната инфраструктура, осигуряващи нейната «работоспособност» и/или нейната «защитеност».

В рамките на Политиката определените обекти могат да бъдат дефинирани сравнително окрупнено, а подробния списък се отразява в процедура «А.7. Мениджмънт на активите».

Тук задължително трябва да бъдат определени с подробно и детайлно описване и обосноваване всякакви изключения от областта на действие на СУИБ, ако рисковете по съответните активи и свързаните с тях обекти са обработени по такъв начин, че те да не оказват влияние върху способността и/или върху задължението на организацията да предостави и гарантира ниво на защита на информацията, удовлетворяващ всички вътрешни и външни нормативни изисквания. Тук, например, могат да бъдат причислени външните, по отношение на организацията, центрове за обработка на данни или «облачните» услуги, взаимоотношенията с доставчиците, които са определени в договорите за нивата на обслужване (SLA), а остатъчните рискове са „покрити“ чрез застраховане.

«Контурът за управление» за управление на СУИБ се определя от задачите, които трябва да реши СУИБ и трябва да бъде формулирана във вид на Концепция за осигуряване на информационната безопасност и включваща в себе си целите, основните направления и принципите на действие в определената област. Концепцията трябва да отчита всички изисквания на процесите, съществуващата нормативна база, в която функционира организацията, както и договорните задължения свързани със защитата на информацията. Основа на СУИБ концепцията трябва да прилага и утвърждава дефинираните принципи за управление на рисковете за информационната безопасност в организацията.

В съответствие със стандарта 27001, политиката на СУИБ се разглежда като разширена политика за ИБ, като по принцип политиката на СУИБ има приоритет пред политиката за информационна безопасност.

Политиката на СУИБ и/или Политиката за информационна безопасност трябва да бъдат документирани в съответната форма (вж.

„Изисквания към документирането“) и е необходимо да бъдат утвърдени от висшето ръководство на организацията.

Стандартът допуска Политиките на СУИБ и ИБ да бъдат описани в един документ. Въпреки това е прието, че Политиката за ИБ трябва да бъде изложена кратко и ясно и публикувана в публичната сфера (включително на сайта на организацията или в средствата за масова информация). Концепцията за информационна безопасност и основните положения на Политиката на СУИБ, може да има по-разширен характер, но също така и по-конфиденциален характер и да бъде документ, който е предназначен изключително за вътрешно-организационно ползване. Ако това е налице, то то естествено е по-добре те да бъдат оформени във вид на два различни документа.

Например, политиката на СУИБ на търговска банка може да бъде определена по следния начин:

- Разработване на система за осигуряване на информационната безопасност, съответстваща на изискванията на стандарта;
- Целта на защитата на информацията се състои в осигуряване на работоспособността на организацията в условията на умерени заплахи, на безопасността на сътрудниците и потребителите, защитеност на осъществяваните операции;
- За осигуряване на информационната безопасност трябва да бъде структурирано звено със собствен бюджет, кооптираме към него, като заместник ръководител, отговарящия за икономическата безопасност на банката;
- Звеното оперативно се отчита за резултатите от своята дейност пред куратора, а един път на шест месеца пред висшето ръководство;
- Областта на действието на СУИБ се разпространява върху всички подразделения и звена, освен тези, които се предоставят на собствениците на наемното помещение (противопожарна охрана, телефонните

комуникации, външната физическа охрана на периметъра на сградата (ако съществува такава), но въпросите свързани с информационната безопасност се разписват в договорите с наемателите;

- Необходимо е да бъде разработена система за документална поддръжка на СУИБ и да бъдат разработени съответните документи. Отговорник – звеното за ИБ;
- Рисковете за информационната безопасност трябва да се обработват като операционни рискове, като периодически се осъществява анализ на рисковете за информационната безопасност. Отговорници – звеното за управление на рисковете, звеното за ИБ, звеното за информационни технологии, отговорниците за развитие на бизнеса;
- Контролът за дейността на звеното за информационна безопасност се осъществява от службата за вътрешен контрол.

Политиката на СУИБ дефинира основните задачи и методи за осигуряване на информационната безопасност в организацията. Същите трябва по-късно да бъдат доразвити и отразени в съответните документи, процедури и ясно определени мерки за осигуряване на информационната безопасност.

В процедурите на СУИБ е необходимо да бъде предвидено, че Политика може и трябва периодически и/или при определен инцидент да се преразглежда, уточнява и усъвършенства, защото нейните положения дефинират стратегията за функциониране и развитие на СУИБ в организацията. Към събитията, които налагат промяна на концепцията на СУИБ, могат да бъдат отнесени: сливания и поглъщания на компании, съществени изменения в архитектурата на информационните системи, прехвърляне на голяма част от дейностите и услугите на аутсорсинг и други стратегически събития.

Определяне на методологията за оценяване на рисковете. Всяка система за управление преследва конкретна, поставена от висшето

ръководство на организацията цел. Постигането на тази цел се явява резултат от изпълнението на „базовите функции“. Например, целта на един полет на самолет е да прелети от т. А до т. Б при минимално време с минимални разходи. Според стандартите от серията 27000 целта на СУИБ се състои в минимизиране на рисковете пред информационната безопасност в условията на неопределеност на средата, която формира заплахи за информационните средства. Например, дефиниран е списъкът с видовете заплахи, но не е изяснено коя от тях и по какъв начин тя ще се прояви. Следователно, необходимо е при разработването, внедряването и усъвършенстването на СУИБ да бъде подбран подход за оценяване на риска. Това означава да се избере методология за оценяване на рисковете за информационната безопасност, да се дефинира списък на най-актуалните рискове и обекти, които са уязвими при тяхното настъпване. Да бъдат определени нивата на заплахи и на възможните загуби, да бъдат определени методите, с помощта на които могат да бъдат минимизирани и се разработят принципи за обработване на рисковете.

Дефиниране на изисквания към документирането. СУИБ трябва да бъде описана на разбираем за тези, които ще работят в нея, език в рамките на техните компетенции. Трябва да бъдат разработени документи, които да описват различните аспекти от функционирането на СУИБ. За обикновения потребител инструкциите за това как да определи една или друга заплаха за информационната безопасност трябва да бъдат ясни и такива, които не предполагат тълкования. Например, при постъпване на документи в администрацията от фронт-офиса и как те да бъдат обработени. За инженера, който настройва корпоративната мрежа са необходими инструкции за настройка на всяко конкретно устройство в зависимост от конфигурацията и утвърдените правила за предаване, споделяне и ползване на информацията. Потребителите трябва да са наясно как да отчитат своето участие и принос за събитията, които влияят на информационната

безопасност. На по-високо йерархично се намира политиката за осигуряване на информационната безопасност в конкретната област. Например при работа с информационни ресурси в Интернет или при предоставяне на оторизиран достъп до информационните ресурси. На още по-високо ниво в йерархията се намира политиката за информационна безопасност (на много нива), която дефинира стратегическите подходи за осигуряване на ИБ. След като бъде разработена адекватна структура на документацията, по-късно може да се пристъпи към разработване на документи за осигуряване на оптимизиране на разходите за труд и достатъчно гъвкави за по-нататъшно поддържане и усъвършенстване.

Приемане на решения и извършване на действия от страна на ръководството при осигуряването на системата за управление на информационната безопасност. Най-важният въпрос във всяка управленска система се състои в това кой отговаря за нея – управителят или зам.-директорът който отговаря за информационната безопасност. Колкото по-отговорно и внимателно е анализиран, разработен и внедрен, на практика, даден въпрос, толкова по-устойчиво функционира системата, която притежава всички необходими ресурси, с отработен алгоритъм за решаване на проблема при неговата ескалация на съответното ниво на приемане на решения при съответстващо ниво на компетентност на служителя.

13.4. Инвентаризация на всички активи на организацията

Първото нещо, което трябва да се определи, това е какво се явява ценен или критически актив за компанията от гледна точки на информационната безопасност. Стандартът ISO 17799, който подробно описва процедурите на системата на управление, определя следните видове активи:

- Налични информационни ресурси, които включват всички файлове и бази от данни, сключени договори с контрагенти, документирана система, документирани резултати от научноизследователска дейност, други документи, материал свързани с обучението и др;
- Софтуерни продукти;
- Материално ресурси, които включват цялото хардуерно оборудване, периферни устройства, средства за комуникации и др.;
- Обслужване, което включва обслужване на комуникационните системи за осигуряване на дейността и др.;
- Служителите на компанията със своята квалификация и опит;
- Нематериалните ресурси, които включват репутацията и имиджа на организацията.

Необходимо е да бъде определено какво нарушение информационната безопасност и на кои от активите би нанесло неприемлива вреда на организацията. Така може да се определи кой от активите може да бъде определен като ценен за организацията и защо е необходимо той да бъде отчетен в процеса на анализиране на информационните рискове.

Инвентаризацията на активите се състои изготвяне на пълен списък на ценните активи на организацията. Естествено този списък се изготвя от собствениците на конкретните активи. „Собственик на актива“ е сътрудник в организацията, на който ръководството на компанията е възложило отговорността и задължението да управлява създаването, разработването, поддръжката, използването и защитата на поверените му активи. Това съвсем не означава, че „Собственикът на актива“ фактически (юридически) притежава имуществени права върху активите. [ISO/IEC 27001:2013].

Анализиране, оценяване и категоризиране на активите на организацията.

Когато се анализират, оценяват и категоризират активите, трябва на първо място, да се оцени критичността на тези активи за процесите в

компанията – да се определи какви щети ще понесе организацията, ако възникне нарушение на информационната безопасност на активите.

Този процес предизвиква сериозни сложности, тъй като ценността на активите се определя на базата на експертните оценки извършвани от техните собственици. При осъществяването на този процес се извършва обсъждане на предстоящото разработване на системата за управление на активите между собствениците и консултантите. Това съдейства на собствениците на активите да си изяснят по какъв начин трябва да бъде оценявана ценността на активите от гледна точка на ИБ, защото за собствениците самият процес за определяне на критичността на активите се явява нова и нерутинна дейност. Всеки един от собствениците на активи използва различни методики за оценка, защото консултантите разработват оригинални такива за тях. Освен това тези методики могат да съдържат в себе си конкретни критерии и показатели, които да са актуални за конкретната организация и които трябва да бъдат отчетени при извършването на оценяването на критичността.

Оценяването на критичността на активите трябва да се осъществява по три параметъра:

1. Конфиденциалност;
2. Цялостност;
3. Достъпност.

Трябва да се оценява щетата, която организацията ще понесе, когато бъдат нарушени конфиденциалността, цялостността и/или достъпността на активите.

Оценяването на критичността на активите може да бъде извършвано с използването на парични единици и в нива. Обаче, отчитайки факта, че за анализирането на информационните рискове са необходими стойности изразени в парични единици, то когато имаме оценяване на критичността на активите по нива, то тогава е необходимо да бъде определяна оценката на

всяко ниво в парични единици. За базова оценка на рисковете е достатъчно да бъде използвана скала съдържаща три нива - ниско, средно и високо. Ако използваме тази скала за оценяване на всяко ниво в парични единици, то тази оценка трябва да се осъществява на базата на следните принципи (Таблица 5).

Таблица 5. *Принципи за оценяване в парични единици*

Ниво	**Изчисляване в парични единици**	**Определяне от гледна точка на влиянието на репутацията на компанията**
Ниско ниво	Незначителна щета	Незначително влияние на репутацията на компанията
Средно ниво	Значителна или голяма щета	Съществено влияние върху репутацията на компанията или ощетяване на нейните интереси
Високо ниво	Голяма щета	Уронване на репутацията компании и на интересите й. Сериозна заплаха за продължаване на дейността на компанията.

Таблица 6. *Скала на три нива за оценка в условни парични единици*

Ниво	**Оценка на нивото, у.е.**
Ниско	до 100 х.
Средно	от 100 х.. до 1 млн.
Високо	над 1 млн.

Когато се подбира скала е необходимо да бъдат отчитано:

- Колкото по-малко на брой са нивата, толкова точността на оценката е по-неточна (по-груба);

➢ Колкото повече на брой са нивата, толкова по-сложно се извършва оценяването – по-сложно е да бъде определена разликата между, ниво n и ниво n+1 (по 10 бална скала).

Стремежът е да се открие „златната среда“ за да може от една страна точността да не пострада много и в същото време и сложността да не надвишава допустимите граници.

Трябва да се има предвид, че когато се изчисляват информационните рискове е достатъчно да бъдат използвани примерни стойности за критичността на активите, не е необходимо активите да бъдат оценявани с точност то 1-на парична единица. Все пак паричното изразяване на критичността, въпреки всичко, трябва да се направи.

Принципите за оценяване на критичността на всеки един от активите:

1. Информационните активи се оценяват на базата на размера на евентуално нанесената щета на организацията при несанкционирано разкриване на информация, модификация или недостъпност до информационните масиви в течение на определен период от време;

2. Софтуерните продукти, материалните ресурси и обслужващите системи се оценяват, като правило, на базата на тяхна достъпност и/или тяхната работоспособност. Трябва да се изчисли каква щета ще понесе организацията ако бъдат унищожени активите или бъде затруднено тяхното функциониране. Например, спирането на функционирането на системата за кондициониране за по-дълъг период от три дни ще доведе до спиране на функционирането на фирмените сървъри, до невъзможност до данните в тях, което ще доведе до генериране на загуби за организацията;

3. Конфиденциалността и цялостността на сътрудниците на организацията се оценяват като се отчита техния достъп до информационните ресурси, техните права за достъп и до модификация на масивите от данни. Достъпността на сътрудниците се оценява на базата на тяхното отсъствие от работното място – каква щета ще понесе

организацията ако сътрудникът отсъства от работното си място в рамките на определен период от време. Необходимо е да се отчита натрупания опит от сътрудника, придобитата квалификация, изпълнението на някакво специфични операции;

4. Репутацията на организацията може да бъде оценена по отношение на информационните ресурси. Необходимо е да бъде оценена щетата, която ще понесе репутацията на организацията, ако бъде нарушена нейната информационната безопасност.

Категоризирането на активите е необходимо да бъде изпълнявано в съответствие с точно описана документирана процедура на компанията. На разположение на одиторите от сертифициращите органи, освен формалния документ, в който е отразен резултата от категоризирането, трябва да бъдат представени методиките, въз основа на които е извършено оценяването и обема и обхвата на данните използвани за тази дейност.

13.5 Оценяване на защитеността на информационната система на организацията

Когато се извършва анализ на информационните рискове трябва да бъдат оценявани не само критичността на активите, а и нивото на тяхната защитеност.

Когато се анализира защитеността на информационната система е необходимо да се определят заплахите за действащите активи, както и уязвимостта на ИС, в която работят разглежданите активи и които биха довели реализацията на заплахите. Заплахите и уязвимостите трябва да се разглеждат винаги свързани едни с други. Няма нужда да се разглежда уязвимост, ако чрез нея няма възможност да се реализира нито една заплаха. Обратното, заплаха, която няма възможност да се реализира, защото липсва уязвимост, няма смисъл да се разглежда. Различните по вид заплахи и

уязвимости притежават различно относително тегло за ИС. Трябва да бъдат определени кои от разкритите заплахи и уязвимости са най-актуални, а кои от тях са не толкова значими. Това означава да бъде определена вероятността за реализация на заплахите чрез уязвимостите. Вероятността за реализация на уязвимостта може да се определи чрез скали в рамките от 0 до 1 (или от 0 до 100%).

Заплахите, уязвимостите, както и вероятностите за осъществяването им се определят чрез провеждане на технологически одит на защитеността на ИС на организацията. Този одит може да бъде проведен както от специалисти от организацията (т.нар. вътрешен одит), така и от външни одитори-консултанти (външен одит).

13.6. Оценяване на информационните рискове

При изграждане на частта от общата система за управление, базирана на подхода за оценяване на ***бизнес рисковете*** и имаща за цел изграждането, внедряването, действието, наблюдението, поддръжката и подобрението на сигурността на информацията е необходимо да бъде приложен системния подход.

Забележка: Системата за управление включва организационната структура, политики, планиране, отговорности, практики, процедури, процеси и ресурси. [3.33 ISO 20000:2018]

Във всяка компании, колкото и перфектно да са разработени елементите на управление на информационната безопасност, все пак съществуват заплахи, уязвимости и потенциални рискове. Поради тази причина за осигуряване на конкурентоспособността и постигане на установените бизнес цели организацията трябва да направи всичко възможно за да дефинира, оцени и да обработи всеки един от тях, или поне тези, които са най-релевантни. Тази дейност се нарича управление на

рисковете, което може да варира от подсъзнателни решения до напълно осъзнати, основани на сложни методологии и механизми свързани с обработката на данни, които могат да бъдат използвани към широк спектър от области на рискове, включително и към рискове, свързани с информационната безопасност. Самата природа на рисковете прави риск мениджмънта сложна дейност, но много често той излишно се мистифицира и много организации правят този процес още по-сложен като предприемат ненужни или извънредно сложни действия.

Процесът на управление на рисковете според правилата на стандарта ISO/IEC 27001 включва:

1. Методология за оценка на рисковете. Необходимо е да бъдат дефинирани правила за изпълнение на дейностите, свързани с оценката на рисковете, за да може цялата организация да извършва по един и същ начин.

2. Реализиране на оценката на рисковете. След като правила са определени, може да стартира идентифицирането на потенциалните проблеми, които могат да възникнат и да определени кои от тях са недопустими и трябва да бъдат обработени. Трябва да бъде проведено търсене, анализ и оценка на потенциалните рискове.

3. Реализиране на риск-терапии: необходимо е да се открие по какъв начин могат да бъдат намалени рисковете чрез използване на минимални инвестиции (по-подробно по-долу).

4. Отчет за оценката на риска на СУИБ: Необходимо е да бъдат фиксирани (протоколирани) всички извършени дейности над рисковете, не само тези, които са свързани със сертифицирането, но и тези, които са свързани с бъдещето на бизнес организацията. Тези резултати могат да бъдат използвани и в бъдеще.

5. Заявление за използваемост. Този документ обобщава резултатите от обработването на рисковете и ще бъде използван от одиторите при сертифицирането като основен (опорен) документ.

6. План съдържащ мерки за управление на рисковете. В този план трябва да бъде определено кой ще бъде отговорен за реализирането на всеки елемент от управлението, в какви срокове, в рамките на какъв бюджет и т.н. Този разработен план, съдържащ мерки за управление на рисковете, е много важно да бъде одобрен от ръководството, защото реализацията на всички планирани елементи на управление изисква значителни времеви ресурси, усилия и ще изисква сериозни финансови разходи. Без участието на висшия мениджмънт това няма как да се случи.

Тук ще бъдат разгледано подробно как може да бъде реализиран всеки етап, като бъдат отчетени най-разпространените подходи, които се използват от организациите по света.

1. Как да бъде разработена методология за оценяване на рисковете в съответствие с изискванията на ISO/IEC 27001, като се използват общоприетите подходи:

ИЗИСКВАНИЯ	ОБЩ ПОДХОД
1) Необходимо е да бъде определен начина, по който ще бъдат откривани рисковете, които биха довели до загуба на конфиденциалността, цялостността и/или достъпността на информацията.	Рисковете могат да бъдат определени на базата на активите, заплахите и уязвимостите, въз основана процесите в организацията, на отделиите като се използват само заплахите, а не уязвимите места, или всяка друга достъпна методология.
2) Необходимо е да бъде определен начина, по който ще бъде избрани отговорниците за отделните рискове.	Трябва да бъде избран сътрудник, който едновременно е заинтересован от отстраняването на риска и в същото време заема достатъчно висока позиция в ръководството на организацията, за да е в състояние да организира тази дейност.
3) Необходимо е да бъдат определени критериите за оценка на последствията и за оценка на вероятността от възникване на риска.	Трябва да бъдат оценени по отделно последствията и вероятността от настъпване за всеки един от дефинираните за организацията рискове. При това, за тяхното измерване, могат да бъдат използвани всякакви подходящи скали.

ИЗИСКВАНИЯ	ОБЩ ПОДХОД
4) Необходимо е да бъде определен начина, по който ще бъде изчисляван риска.	Това обикновено се извършва чрез събиране или умножение. Ако се използва скалата нисък-среден-висок, то това е същото, ако използваме скалата 0-1-2.
5) Необходимо е да бъдат определени критериите за обработване на рисковете.	Ако използваният метод за изчисляване на риска дава значения от 1 до 10, то може да се приеме решение, че приемлемливото ниво на риска е, например, 7 – това ще означава, че само тези рискове, които са оценени на 8, 9 и 10, се нуждаят от обработване. Освен това, може да бъде изучен всеки индивидуален риск и да се приеме решение, кой от тях трябва да бъде разгледан, а кой - не, основавайки се на своето собствено разбиране и опит, без да се налага да бъдат използвани скали.

Фиг. 22 Общоприети подходи за оценяване на рисковете в съответствие с изискванията на ISO/IEC 27001

2. Оценка на рисковете или как да бъдат съпоставени активите, заплахите и уязвимостите:

Действащата към момента версия на стандарта ISO/IEC 27001:2013 позволява да бъдат идентифицирани рисковете чрез използване на всяка една методология. В същото време методологията, заложена в редакцията 2005 година, изискваща идентифициране на активите, заплахите и уязвимостите, си остава актуална.

Идентифицирането на риска представлява първата половина от процеса на оценяване на риска. Това дава възможност да бъде използван списъка с активи, заплахи и уязвимости подредени в колони. Тук трябва да бъдат включени допълнителни информации, например идентификатор на риска, отговорници за рисковете, влияние, вероятност и т.н. Препоръчително е да бъдат изчислявани елементите колонка след колонка, а не ред след ред. Това дава възможност първоначално да бъдат изброявани всички налични активи, а след това да се започне търсенето на заплахи за всеки един от активите, и едва след това да се търсят уязвимостите за всяка заплаха.

Ето пример за това как могат да бъде представено съпоставянето на тези три компонента:

АКТИВ	ЗАПЛАХА	УЯЗВИМОСТ	РИСК
Хартиен документ	Пробив в системата за водоснабдяване и канализация	Документът не се съхранява в херметична опаковка	Загуба на цялостността на информацията
		Отсъства резервно копие на документа	Загуба на цялостността на информацията
	Несанкциониран достъп	Документът не заключен в каса (шкаф)	Загуба на конфиденциалността на информацията
Дигитален документ	Разрушаване на твърдия диск на компютъра	Няма резервно копие на документа	Загуба на достъпността и цялостността на информацията
	Вредоносен код	Антивирусната програма не се обновява по правилния начин	Загуба на конфиденциалността, цялостността и достъпността
	Несанкциониран достъп	Схемата за контрол на достъпа не е дефинирана по правилния начин	Загуба на конфиденциалността,

АКТИВ	ЗАПЛАХА	УЯЗВИМОСТ	РИСК
		Бил е предоставен достъп на прекалено много хора	цялостността и достъпността
IT-мениджър	Недостъпност до този сътрудник	Не съществува никаква опция за замяна за тази позиция	Загуба на достъпност
	Чести грешки	Некомпетентност	Загуба на цялостността и достъпността

Фиг. 23 Пример за представяне на съпоставянето на компонентите

Възниква резонния въпрос, а колко рискове организацията е длъжна да идентифицира? Мениджмънтът трябва да се съсредоточи само върху най-важните заплахи и уязвимости, включвайки всички активи. Препоръчително е за всеки един от активите да бъдат идентифицирани пет заплахи, а за всяка заплаха – две възможности. Така е възможно да бъдат получен 500 рисков за средна компания с 50 актива, което е напълно управляемо.

3. Как могат да бъдат оценени последствията и вероятностите при анализа на рисковете.

Втората половина при оценяването на рисковете се състои в това да бъде разчетено, доколко е голям този риск. Това се постига чрез оценяване на последствията (често наричани въздействия), които биха произтекли, ако рискът е бил материализиран, и оценка на това, доколко е голяма вероятността, че той ще се случи. Притежавайки тази информация, лесно може за де изчисли нивото на риска.

Съществуват два основни метода за оценяване на вероятностите за настъпване на събитието и на последствията: качествен и количествен. При качествената оценка на риска основно внимание трябва да бъде насочено към възприемането от страна на заинтересованите страни на вероятността от възникване на риска и влиянието върху съответните организационни аспекти (например, финансови, имиджови и др.). Това възприятие може да бъде представено в различни скали, например, „нисък – среден – висок“ или „0-1-2“, които да бъдат използвани за определяне на окончателното значение на риска. Количествената оценка на риска се фокусира върху фактическите и измеримите (количествените) данни, а така също на специални математически и изчислителни бази от данни за изчисляване на значенията на вероятностите и въздействията, обикновено изразяващи значението на риска в парично изражение.

Ако организацията се нуждае от опростена и бърза оценка на рисковете, то е възможно да бъде използван метода за качествена оценка, който се използва от болшинството организации. Но, ако е необходимо да бъдат инвестирани сериозни ресурси за решаване на въпросите свързани с информационната безопасност, то тогава е необходимо да бъдат инвестирани средства и време за количествена оценка на риска. Един от най-използваните методи за обосноваване на необходимите инвестиции в осигуряването на ИБ се явява определянето на стойността на инцидента, а също така и потенциалната възвращаемост, които тези инвестиции могат да донесат на организацията.

Качествената оценка на риска, от своя страна, включва два метода за анализ на рисковете: проста оценка на риска и детайлна оценка на риска. При простата оценка на риска се оценяват последствията и вероятността от неговото осъществяване. За определянето на риска се използват скали за оценка, отделно на последствията и отделно на вероятностите за всеки риск (например, от 1 до 10). Колкото по-голям е мащаба, толкова по-точни са резултатите, в същото време толкова по-високи са разходите на време, което ще бъде изразходвано за извършване на оценката.

Пример за простена оценка на риска.

При детайлното оценяване на риска, вместо оценяването на два елемента (последствие и вероятност), трябва да бъдат оценени три елемента: стойност на активите, заплахата и уязвимостта. Например:

- Актив: ноутбук
- Заплаха: кражба
- Уязвимост: сътрудниците не знаят как да защитят своето мобилно устройство
- Последствия: 3 (по скала от 0 до 5)
- Вероятност: 3 (по скалата от 0 до 5)

Изчисляването на риска се осъществява чрез събиране или умножение. Ако се използва скалата „нисък-среден-висок“ (може също да се използва и скалата „0-1-2“).

Изчисляване на риска с помощта на събиране:

- Проста оценка на риска: последствия (3) + вероятност 3) = риск (6);
- Детайлна оценка на риска: стойност на активите (2) + Значение на заплахата (2) + Значение на уязвимостта (2) = риск (6).

За детайлната оценка на рисковете може да бъде използвана скала от 0 до 4 за оценка на стойността на активите и по-малки скали (от 0 до 2) за оценяване на заплахите и уязвимостите. Това се дължи на това, че тежестта на последствията трябва да бъде такава, като тежестта на вероятността, защото заплахата и уязвимостта, заедно, “представляват” вероятността. Тяхната максимална добавена стойност е равна на 4.

След като бъдат изчислени рисковете, трябва да бъде оценено, дали те са приемливи или не, а след това да се премине към следващата стъпка – обработване на рисковете.

4. Внедряване на обработка на рисковете свързани с информационната безопасност.

Целта на обработването на рисковете е да бъдат контролирани опасностите, които са разкрити по време на тяхната оценка. В по-голямата част от случаите това ще означава понижаване на риска чрез понижаване на вероятността от настъпване на инцидента (например, ламиниране на документацията (използване на херметична опаковка) и/или понижаване на въздействието на активите (например, херметични врати). При разглеждането на рисковете организацията трябва да съсредоточи своето внимание върху тези, които не се явяват приемливи. Ако това не бъде направено то тогава ще бъде трудно да бъдат определени приоритетите и да се осигури финансиране за понижаване на всички открити рискове.

Варианти за обработване на риска:

➢ ***Понижаването на риска*** е най-разпространен подход и включва в себе си внедряване на гаранции (средства за контрол), такива като система за защита от изтичане на информация и от претоварване с информация. За тази цел се използват елементите за управление от приложение А от ISO/IEC 27001 и всякакви други и лементи за управление, които организацията счита за целесъобразни.

Когато е избран подхода за понижаване на риска, трябва да бъде осъществен един от трите типа управление:

a) Дефиниране на нови правила, които се документират чрез планове, политики, процедури, инструкции и др.

b) Внедряване на нови технологии, например: системи за резервно копиране на информацията (backup), места за аварийно възстановяване в алтернативни центрове за обработване на данните.

c) Промяна в организационната структура, например: въвеждане на нова длъжностна функция или промяна на задълженията на съществуващия персонал.

➢ ***Избягването на риска*** се проявява в прекратяване на изпълняването на определени задачи или процеси, когато е установено, че те носят рискове, които са прекалено големи за да могат да бъдат смекчени чрез използване някои от дрегите подходи. Например, може да бъде забранено използването на ноутбук извън пределите на помещенията на организацията, ако рискът за несанкциониран достъп до него е прекалено висок, или да бъдат внедрени средства за криптозащита за даденото устройство.

➢ ***Прехвърляне на риска*** – това означава, че рискът се преадресира към друга страна. Например, закупуване на застрахователна полица за сградата, като с това се прехвърля част от финансовия риск върху застрахователната компания. За съжаление този подход няма никакво влияния върху самия инцидент и заради това по-добра стратегия се явява използването на този вариант заедно вариантите 1 и/или 2.

➢ ***Съхраняване на риска*** – най-нежелателния вариант. Това показва, че организацията приема риска и няма да предприема нищо по него. Този вариант трябва да се използват само тогава, когато разходите за смекчаване на последствията са повече отколкото загубите, които ще инкасира организацията, ако инцидентът се състои.

За да бъдат повишени шансовете за избор на най-ефективните варианти за обработка и контрол, следва да бъдат разгледана и обсъдена възможността за привличане на специалисти в интердисциплинарни области (например, IT-персонал за IT -контрол; HR-специалисти, ако обработката включва тренинги и др.). Тези решения изискват активното участие на ръководството от съответното ниво. Ако са налице съмнения, относно това кой може да вземе тези решения, то трябва да се осъществи консултация с инициатора на проекта от страна на висшето ръководство.

След като са избрани методите за обработка, трябва да бъде оценен остатъчния риск за всеки неприемлив риск, който е дефиниран по-рано по време на процеса за оценка на риска. Например, ако е определено, че последствията от възникването на събитието са на ниво 4 и вероятността е на ниво 4 по време на оценяването на риска (което означава, че риска е 8 при използване на метода на събирането), то остатъчния риск може да достигне 5, ако сме оценили, че следствията ще се понижат до ниво 3, а вероятността до ниво 2 благодарение на мерките, които са планирани за провеждане.

След приключването на обработката на рисковете се осъществява обобщаване на данните в отчета за оценка и обработка на рисковете. Трябва да се направи подробен обзор на процеса и да се изпълнят изискванията на стандарта за съхраняване на информацията и за процеса за оценка и обработване на рисковете.

5. Важност на заявлението за приложимост

Заявлението за приложимост се явява основно свързващо звено между оценката, обработката на рисковете и реализацията на информационната безопасност. Необходимо е да бъде извършено следното:

- Да се дефинират мерки за контрол, които са необходими по причини, които са различни от всякакви разкрити рискове (например, поради юридически или договорни изисквания).
- Да се обосноват включването и изключването на средствата за контрол от Приложение А и от другите източници.
- Да се създаде обобщена форма за възможни за осъществяване мерки за контрол, която да бъде представена на ръководството и тя да бъде поддържана в актуално състояние.
- Да се документира дали вече е осъществен всеки използваем елемент за управление. Добър вариант, който много често е искан от одиторите, се изразява в това да бъде представено доказателство за това как се осъществява всяка използвана контрола (например, позоваване на документ или кратко описание на използваната процедура или оборудване).

Всеобхватното представяне, което се съдържа в заявлението за използваемост (какво трябва да бъде направено в сферата на информационната безопасност, защо това трябва да бъде направено и как това да бъде направено), притежава следните предимства:

- Това принуждава организациите постоянно и системно да планират своята информационна безопасност, да оптимизират всички решения относно разходите (например, закупуване на ново техническо оборудване или промени в процедурите и инструкциите, назначаване на служители).
- Прецизно изработеното заявление за използваемост позволява да бъде минимизирано количеството на другите документи. Например, може да бъде документиран определен елемент от управлението, но описанието на

самата процедура за този елемент може да бъде много кратко, Това може да бъде описано в заявлението за приложимост.

- Заявлението за приложимост предоставя на одиторите препоръки за разбиране на подхода на организацията за осигуряване на информационната безопасност и проверка дали организацията е реализирала своите средства за контрол, по начин, който е планирала. Това представлява ръководен документ при провеждането на on-site одита.

6. План за мерки за отстраняване на рисковете (план за мерки за управление на рисковете)

Планът за мерки за отстраняване на дефинираните рискове представлява "екшън план за действия", в който е необходимо да бъдат дефинирани мерки за безопасност, които трябва да бъдат осъществени, определени отговорниците за тяхното провеждане, конкретни срокове за провеждането им и какво количество ресурси (финансови и човешки) трябва да бъдат осигурени. Резултат от проведения процес на обработване на рисковете се явява планът за мерки за управление на рисковете, който се разработва след заявлението за използваемост. Това се налага поради факта, че този документ определя необходимите средства за контрол, които трябва да бъдат осъществени, отчитайки пълната картина на информационната безопасност и не само резултатите от обработването на рисковете, но и юридическите нормативни и договорни изисквания. Планът за мерки за елеминиране на рисковете представлява пресечната точка, в която завършва теорията и започва практическата работа в съответствие с ISO/IEC 27001. Адекватната оценка и обработването на рисковете, а също и добре дефинираното заявление за използваемост предоставя много добър работещ план за действия за осигуряване на информационната безопасност на организацията.

Основни предимства от управлението на рисковете:

➢ *Стратегически подход за управление на рисковете.* Изразява се в прилагане на правилен подход при създаването и разпределянето на ресурсите и в правилния начин за избор на точно определения момент, като се отчитат не само и единствено потребностите на организацията, но и потребностите на потребителите, клиентите и на другите заинтересовани страни.

➢ *Прецизно определяне на ролите.* Висшето ръководство, техническия персонал, потребителите и заинтересованите страни, експертите, т.е. всички, които се занимават с информационната безопасност, трябва да им бъдат възложени и да изпълняват определени функции (например, вземане на решения, определяне на рисковете, изпълняване на определените процедури и др.). Това представлява един от най-ефективните икономически методи за елиминиране на рисковете за информационната безопасност.

➢ *Действия, съответстващи на разкритите заплахи.* Един и същ възникнал риск може да доведе до различни подходи за неговото елиминиране в различните организации, в зависимост от техните потребности и очаквания. Простото копиране на добри практики и подходи от конкурентни компании не дава добри резултати. Организациите трябва много добре да разгледат и да определят собствените си възможности и граници за да има пълно покриване на действията по отношение на риска и поставените цели.

Рискът може да бъде дефиниран и като „влияние на неопределеността върху поставените цели“. Поради тази причина, ако неопределеността се управлява по ефективен начин, то това дава възможност рискът да бъде понижен. От гледна точка на стандарта ISO/IEC 27001 това означава, че информацията в организацията може да бъде ефективно защитена и използвана и по този начин да бъдат постигнати поставените цели. Когато организацията системно анализира, дефинира, оценява и разглежда пълния

набор от съответните рискове, то тя ще бъде в състояние да предотвратява нежелани ситуации и да намали до минимум негативните последствия за нея. Определяйки и управлявайки рисковете, организациите ефективно могат да се справят с потенциалните проблеми преди те фактически да се възникнат.

Изисквания за оценка на риска при създаване на Система за управление на информационна сигурност (СУИБ)

1. Създаване и управление на СУИБ

1.1 Създаване на СУИБ

При създаването на СУИБ организацията трябва да извърши следните дейности:

- Да бъде дефиниран подход за **оценка на рисковете** в организацията:
  1) Да се определи метода, който ще бъде използван за оценяване на **рисковете в организацията.**
  2) Да се дефинират критерии за приемане на определените **рисковете.**
- Да се идентифицират **рисковете в организацията**:
  1) Брой и видове на активите и отговорниците за тях.
  2) Видове заплахи за активите.
  3) Уязвимости на активите.
  4) Въздействието върху активите, при нарушаване на информационната сигурност
- Да анализират и **оценят рисковете** за организацията:
  1) Да се оцени загубите за бизнеса от пробив в сигурността (нарушаване на информационната сигурност).
  2) Да се оцени **вероятността** от пробив в сигурността.
  3) Да се оцени нивото на **риска в организацията**.
  4) Да определи дали дефинираните **рискове** са приемливи.

- Да се определят и оценят вариантите за елиминиране или намаляване на рисковете чрез:
    1) Прилагане на подходящи за вида риск **контроли**.
    2) Приемане на остатъчния **риск.**
    3) Избягване на **риска.**
    4) Прехвърляне на **риска** към друга организация**.**
- Да се определят **цели и контроли за въздействие върху риска.**
- Ръководството да одобри **остатъчните рискове.**
- Ръководството на организацията официално да разреши внедряването и стартирането на СУИБ
- Да бъде разработена и утвърдена **Декларация за приложимост**.

1.2 Създаване, наблюдение, управление и преглед на СУИБ

Организацията трябва да **преглежда оценката на риска** и нивата на остатъчния и приемливия риск през планирани интервали от време, като взема в предвид настъпилите промени във организацията и във външната среда.

2. Ангажираност на ръководството

Ръководството трябва да предостави доказателства за своята ангажираност, чрез определяне на критерии за приемане на риск и критерии за приемливо ниво на риска в организацията.

3.1 Входни елементи за прегледа на ръководството

Входните елементи за прегледа на ръководството трябва да включват данни за уязвимостите и заплахите, които са били неправилно третирани при предишни оценки на **рисковете.**

3.2 Изходни елементи от прегледа на ръководството

Изходните елементи от Прегледа на ръководството трябва да включват решения и действия, свързани със:

- Актуализиране на плановете, свързани с оценяването и въздействието върху риска;

- Изменения, свързани с промяна в дейността на организацията или с промени във външната среда.
- Нивата на риска и/или критерии за приемане на рисковете.

4. Превантивни действия

Организацията трябва да определи променените рискове и превантивните действия, свързани с тях, като насочи вниманието си върху значително променените рискове.

Приоритетът на всяко едно от превантивните действия трябва да бъде определен въз основа на базата на резултатите от оценката на **риска**.

Приложение А

Цели по контрола и механизми за контрол

Цели и Контроли, свързани с оценка на риска:

A.6.2.1,	A.11.7.1
A.8.1, A.8.2,	A.12.6,
A.9.2.1, A.9.2.5	A.14.1.2,
A.10.1.4, A.10.2.3, A.10.3,	A.15.3.1

ISO/IEC 27005:2018 - Информационни технологии. Техники за сигурност. Управление на риска за информационна сигурност.

Структура на стандарт ISO/IEC 27005:

- Обзор - Клауза 6
- Установяването на контекста - Клауза 7
- Оценка на риска - Клауза 8
- Третиране на риска - Клауза 9
- Приемане на риска - Клауза 10
- Комуникиране на риска - Клауза 11 (и консултиране)
- Мониторинг и преглед на риска - Клауза 12

Annex A. Определяне на обхвата и границите на процеса за управление риска за информационната сигурност.

Annex B. Идентификация и оценка на активи и оценка на въздействието

Annex C. Примери за типични заплахи

Annex D. Уязвимости и методи за оценка на уязвимост

Annex E. Методи за оценка на риска за сигурност

Annex F. Ограничения за редуциране на риска

Риск за информационна сигурност

Потенциална възможност дадена ***заплаха*** да използва ***уязвимости*** на ***актив*** или на група от активи и по този начин да донесе *вреда* на организацията. Измерва се чрез комбинацията от ***вероятността*** да се случи това събитие и ***последствията*** от него. [3.61 ISO 27000:2018]

Уязвимост *(vulnerability)*

Слабост на актива или контрола, която може да бъде използвана от заплаха [3.77 ISO 27000:2018]

Заплаха *(threat)*

Потенциална причина за нежелан инцидент, който може да доведе до увреждане система или организация. [3.75 ISO 27000:2018]

Актив (asset)

Всяко нещо, което има стойност за организацията

Забележка: Има различни типове активи:

- Информация
- Софтуер, като компютърна програма
- Физически, като компютър
- Услуги
- Хора и тяхната квалификация, умения, опит
- Нематериални, като репутация и имидж

Вероятност (probability, likelihood)

Обективна възможност да настъпи дадено събитие. [3.40 ISO 27000:2018]. *Използва се количествена или качествена оценка за честота на настъпване.*

Въздействие (impact)

Неблагоприятна промяна на нивото на постигане на бизнес целите.

Избягване на риска (risk avoidance)

Решение за избягване ангажимент с риска или действие за избягване на рискова ситуация

Намаляване на риска (risk reduction)

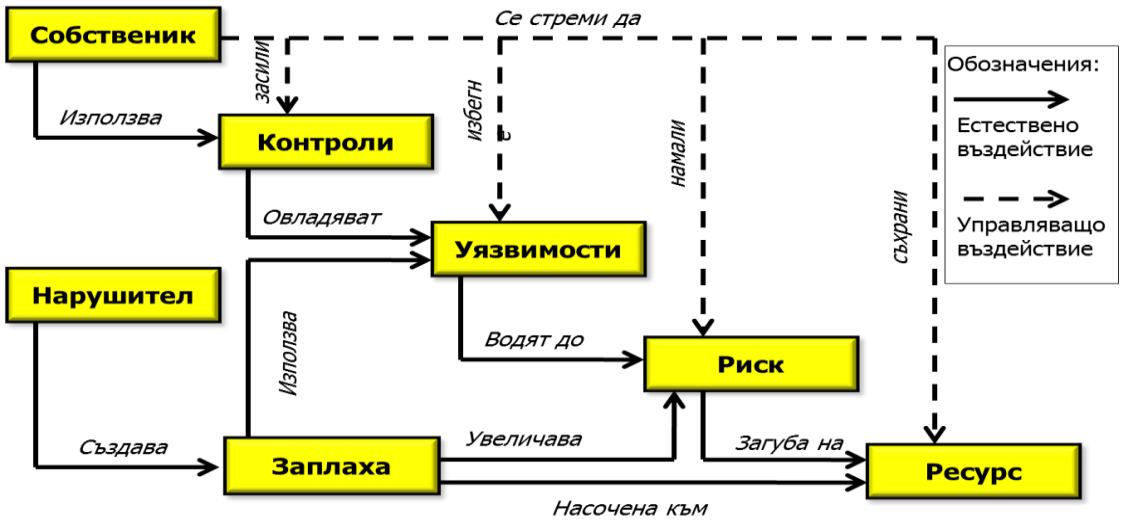
Действия, предприети за намаляване на свързаните с риска възможност или негативни последствия или и двете.

Задържане на риска (risk retention)

Приемане бремето на загуба или ползата от печалба от конкретния риск.

Прехвърляне на риска (risk transfer)

Споделяне с друга страна бремето на загубата или ползата от печалба от риск.



Фиг. 24 ISO 27005 – Взаимовръзки

➢ Да се вземе в предвид ***ценността*** (атрактивността, привлекателността) на актива

➢ Използваният метод за оценка трябва:

- Да е приложим и подходящ за организацията;
- Да има доверие от страна на ръководството;
- Да дава ***повторими*** и ***съизмерими*** резултати.

Вероятност за настъпване на инцидент		**Много невероятно**	**Невероятно**	**Възможно**	**Сигурно**	**Много вероятно**
Въздействие върху бизнеса	**Много ниско**	**0**	**1**	**2**	**3**	**4**
	Ниско	**1**	**2**	**3**	**4**	**5**
	Средно	**2**	**3**	**4**	**5**	**6**
	Високо	**3**	**4**	**5**	**6**	**7**
	Много високо	**4**	**5**	**6**	**7**	**8**

Фиг. 25 Матрица с предефинирани стойности

Ниво на заплаха - вероятност за настъпване		**Ниско (Н)**			**Средно (С)**			**Високо (В)**		
Ниво на уязвимост - лекота на експлоатиране		**Н**	**С**	**В**	**Н**	**С**	**В**	**Н**	**С**	**В**
Ценност на актива	**0**	**0**	**1**	**2**	**1**	**2**	**3**	**2**	**3**	**4**
	1	**1**	**2**	**3**	**2**	**3**	**4**	**3**	**4**	**5**
	2	**2**	**3**	**4**	**3**	**4**	**5**	**4**	**5**	**6**
	3	**3**	**4**	**5**	**4**	**5**	**6**	**5**	**6**	**7**
	4	**4**	**5**	**6**	**5**	**6**	**7**	**6**	**7**	**8**

Фиг. 26 Влияние на нивата на заплахи и уязвимости върху ценността на активите

Описание на заплахите (a)	Последствие (ценност на актива) (b)	Вероятност за възникване на заплахата (c)	Измерение на риска (d)	Подреждане на заплахите (e)
Заплаха A	5	2	10	2
Заплаха B	2	4	8	3
Заплаха C	3	5	15	1
Заплаха D	1	3	3	5
Заплаха E	4	1	4	4
Заплаха F	2	4	8	3

Фиг. 27 Категоризиране на заплахите

13.7. Заявление за използваемост

По резултатите от оценката и обработването на рисковете трябва да се изработи Заявление за използваемост. Този документ задължително трябва да бъде представен при сертифицирането. Той трябва да съдържа в себе си всички изисквания на Приложение А към стандарта ISO 27001 с описание дали тези изисквания се изпълняват в организацията. Ако някои от изискванията не се изпълняват, то задължително трябва да бъде описана причината за неговото неизпълнени. Такава причина може да бъде резултатът от оценяването на рисковете. Ако в документа се декларира, че изискванията се изпълняват, то е необходимо да бъдат описани всички документи, които съответстват на тяхното изпълнение.

В Приложението А към стандарта ISO 27001 са описани всички изисквания за осигуряването на информационната безопасност, които задължително трябва да се изпълняват в организацията. Поради тази причина Заявлението за използваемост се явява завършващо решение свързано с понижаването на информационните рискове за организацията.

13.8. Документирани процедури

Стандартът изисква всички мерки свързани с понижаването на рисковете да бъдат оформени документално. За ефективно управление на информационната безопасност трябва да бъдат разработени процедури, които да бъдат документирани във вид на инструкции, политики, регламенти, които да се изпълняват от конкретни сътрудници. Всяка отделна процедура трябва да бъде описана в съответния документ. Документираните процедури са задължителен елемент на СУИБ. За функционирането на СУИБ е необходимо да бъде разработена база от

нормативни документи, които описват всички процедури в областта на информационната безопасност.

Основни документи свързани с управлението на информационната безопасност са Политиката за управление на информационната безопасност и Политиката за информационната безопасност. Политиката за управление на информационната безопасност описва общия подход за управление на ИБ. Политиката за информационна безопасност описва основните процедури за осигуряване на информационната безопасност като в нея са описани позоваванията на конкретните документи от СУИБ.

Освен всичко изложено по-горе, необходимо е да бъдат разработени методологии и инструкции, които подробно и ясно да описват процедурите

13.9. Обучение на служителите на организацията

Трудно могат да бъдат разгледани конкретни методи за понижаване на информационните рискове, защото те могат съществено да се различават един от друг поради особеностите на конкретната информационна система. От друга страна системните администратори и отговорниците по информационна безопасност много добре знаят какви средства за защита е необходимо да бъдат внедрени в СУИБ.

Ще разгледаме основно един от методите за понижаване на рисковете – обучение на потребителите на информационната система, който се изисква от ISO 27001, но който много често предизвиква сложности при неговата реализация.

Вътрешният нарушител, служителят в организацията, заема първо място сред основните заплахи за СУИБ. Това се дължи най-вече на това, че външният периметър в организациите е защитен сравнително надеждно. Освен това служителите на организацията се явяват легитимни потребители на ИС. Те задължително трябва да имат достъп базата от данни и до

конфиденциалната информация на организацията за да могат да изпълняват своите преки служебни задължения. Внедрените средства за защита много често не са в състояние да обезопасят информацията от вътрешния нарушител. Основни методи, които въздействат върху служителите на организацията, са нормативните документи, които дефинират отговорностите на служителя за извършваните действия и предоставят информация на сътрудниците по отношение на въпросите свързани с информационната безопасност. За повишаване на квалификацията (осведомеността) на служителите в организацията в областта на информационната безопасност се организират различни вътрешни и външни тренинги и обучения.

Обученията на служителите могат да се организират под формата на очни и задочни курсове с последващо оценяване на резултатите от тях. За съжаление провеждането на обучения в големите компании и организации често създава сложности, тъй като е сравнително сложно да бъдат организирани курсове за голямо количество служители, а много често и ръководителите не са склонни да се лишат от своите сътрудници за един по-продължителен период от време за да участват в многочасови семинари. В тази ситуация е по-целесъобразно обученията на сътрудниците да се организират чрез използване на платформи за дистанционно обучение, в рамките на които потребителите и за специалистите да бъдат запознати с различни курсове под формата на ролеви игри, тестове и др.

13.10. Управление на инциденти със сигурността на информацията.

Управлението на ***инцидентите*** и подобряването на сигурността на информацията. Необходимо е да се осигури последователен и ефикасен подход към управление на ***инцидентите*** със сигурността на информацията,

включително съобщаване за събития и слабости, свързани със сигурността. Процедурите трябва да включват:

1. Отговорности и процедури
2. Докладване за събития, свързани със сигурността на информацията
3. Докладване за слабости в сигурността на информацията
4. Оценяване на събития, свързани със сигурността на информацията, и вземане на решения за тях
5. Реакция на инциденти със сигурността на информацията
6. Изводи от инцидентите със сигурността на информацията
7. Събиране на доказателства

Инцидентът представлява събитие, свързано със сигурността на информация *(information security event)*

Идентифицирането на събитие в системата показва възможен пробив в политиката за сигурност на информацията, или отказ на защитите, или предварително неизвестна ситуация, която може да бъде свързана със сигурността. [3.30 ISO 27000:2018]

Инцидентът, свързан със сигурност на информация *(information security incident)* предсавлява тделно събитие или серия от нежелани или неочаквани събития, свързани със сигурността на информацията, които с голяма вероятност могат да предизвикат компрометиране на бизнес дейностите и да заплашат сигурността на информацията. [3.31 ISO 27000:2018]

Управлението на инцидент, свързан със сигурността на информацията *(information security incident management)* представлява процес за откриване, докладване, оценяване, реагиране, обработване и извличане на поуки от инциденти, свързани със сигурността на информацията. [3.32 ISO 27000:2018]

Криминалистиката за информационна сигурност *(information security forensics)* представлява прилагане на техники за разследване и анализ за

улавяне, запис и анализ на инциденти по сигурността на информацията. [3.1 ISO 27035:2011]

Необходимо е да бъде сформиран екип за реагиране на инциденти за сигурност на информацията *(information security incident response team - ISIRT)*. Той включва група от доверени членове на организацията с подходящи умения, която се занимава с инцидентите свързани със сигурността на информацията по време на целия им жизнен цикъл. [3.2 ISO 27035:2011]

При управлението на инцидентите в организацията дейността трябва на протича през следните фази:

1. Планиране и подготовка
2. Откриване и докладване
3. Оценка и решение
4. Отговор
5. Поуки

1. *Планирането и подготовка трябва да включва следните основни дейности:*

- Създаване и поддържане на политика за управление на уязвимостите, събитията и инцидентите;
- Създаване и поддържане на политики за управление на риска и сигурността на информацията;
- Създаване, поддържане и документиране на подробна схема (процес) за управление на инциденти за сигурността на информацията;
- Създаване на Екип за реагиране на инциденти за сигурност на информацията (ISIRT);
- Създаване и запазване на подходящи отношения и връзки с вътрешни и външни организации;

➢ Създаване и поддържане на техническа помощ и организация в подкрепа на схемата за управление на инциденти за сигурността на информацията;

➢ Разработване на програма за обучение и осъзнаване на слабости, събития и инциденти;

➢ Тестване използването на схемата за управление на инциденти по сигурността на информацията, нейните процеси и процедури.

Организацията трябва да разработи и въведе алгоритъм за управление на възникнали инциденти свързани с със сигурността на информацията. Той трябва да включва следните дейности:

1. Да бъде определено дали събитията свързани със сигурността на информацията предизвикват инциденти.
2. Разработване на алгоритъм за управление на инцидентите свързани с информационната сигурност до тяхното приключване.
3. Дефиниране на мерки за неутрализиране на уязвимостите свързани със сигурността на информацията в организацията.
4. Дефиниране на поуки и подобрения.
5. Разработване и внедряване на определени подобрения.

Дейностите свързани с управлението на инцидентите трябва да включва следните фази:

2. *Откриване и докладване. Тази фаза трябва да включва следните основни дейности:*

➢ Трябва да бъде разработен алгоритъм за откриване и съобщаване на заинтересованите страни за настъпването на събитие, или за наличие на уязвимост, които са се появили в резултат на:

- Сигнали от системите за наблюдение на сигурността (antivirus, honey pot, tar pit, log monitoring system, ISMS);
- Сигнали от системи за наблюдение на мрежи (firewalls, network flow analysis, web filtering systems);

- Анализ на регистри от устройства, услуги, хостинг, както и различни други системи;
- Ескалация на аномални събития, открити от ИКТ;
- Ескалация на аномални събития, открити от Help Desk;
- Доклади от потребители
- Външни уведомления, идващи от трети страни

➢ Събиране на информация за събития или уязвимости. Тази фаза трябва да включва следните основни дейности:

8. Разработване на инструкция за осигуряване на правилно вписване (в Точката на Контакт) на всички дейности, резултатите от тях и приемане на мерки(решения) за по-късен анализ;

9. Гарантиране на възможност за използване на събраните доказателства в електронен вид пред съда (ISO/IEC 27037:2012);

10. Разработване на инструкция за контрол върху измененията и поддържане на база от данни за връзките между събитие/инцидент/уязвимост. Тя се изпълнява от специален Екип за реагиране на инциденти свързани със сигурността на информацията – ISIRT);

11. Анализиране на ескалирането на възникналите инциденти;

12. Разработване на документ за регистриране в специално разработена система за проследяване на възникналите инциденти.

Организацията трябва да разработи инструкция за откриване на настъпили събития в организацията и да дефинира възможните им източници:

- Потребители;
- Преки ръководители или ръководители по сигурността;
- Клиенти;
- IT отдели;
- IT Help Desk;

- Управлявани услуги (телекомуникации, инфраструктура, доставчици) Възможни източници на събития;
- Екип за реагиране на инциденти за сигурност на информацията – ISIRT;
- Други звена и служители, които могат да открият аномалии по време на ежедневната си работа;
- Средствата за масова информация (новини, печатни медии, TV);
- Уебсайтове.

Организацията трябва да разработи инструкция за докладване за настъпили събития. В нея е необходимо да бъдат определени конкретните данни за докладване и проследяване, например, Дата и час на откриване; Наблюдения; Информация за контакт.

3. *Организацията трябва да дефинира и приеме критерии за оценяване и приемане на решения. Основните дейности, които ще бъдат извършвани включват:*

➢ Критерий за преценяване (в Точката на Контакта) дали събитието е инцидент или не. При преценяването е необходимо да се използват собствени скали за оценки, по които да се бъде определено въздействието върху основните свойства на информацията чрез установяване на:

- Вида на въздействието (физическо, логическо);
- Засегнатите активи, инфраструктура, информация, процеси, услуги, приложение;
- Ефекта върху основни услуги на организацията.

➢ Разработване на процедура за преценяване и потвърждаване, от Екипа за реагиране на инциденти за сигурност на информацията – ISIRT, на извършената оценка;

➢ Прилагане на процедурата за по-нататъшни оценки и/или решения;

- Проведените обучения трябва да гарантират, че всички участници, особено тези от ISIRT, правилно да описват всички дейности за по-късен анализ;
- Разработване на инструкция за начина на събиране и осигуряване на годни за използване доказателства в електронен вид;
- Трябва да бъде разработена система, която да осигурява контрол върху измененията и поддържане на база от данни за връзките между събитие/инцидент/уязвимост. Тази система се поддържа и управлява от Екипа за реагиране на инциденти за сигурността на информацията – ISIRT);
- Разпределяне на отговорностите, свързани с управлението на инцидентите, сред сътрудниците чрез въвеждане на подходяща йерархия за оценяване, вземане на решения и последващи действия;
- Дефиниране и поддържане на формални процедури за работа;
- Ред за документиране на цялата информация за събитията;
- Подробно документиране на цялата информация за инцидентите и на последвалите действия;
- Периодично актуализиране на базата от данни за връзките между събитие/инцидент/уязвимост.

Организацията трябва ясно да дефинира правата и задълженията на Приемащото лице, което да извърши оценяването и приемането на началното решение (в Точката на Контакт). Приемащото лице в Точката за контакт трябва да:

- потвърди приемането на комплект от информация;
- въведе информацията в базата от данни за връзките между събитие/инцидент/уязвимост;
- изиска и изясни всяка налично допълнителна информация;
- познава и прилага правилата за събиране на годни за бъдеща употреба доказателства;

Организацията трябва да разработи процедура, която да гарантира, че цялата необходима информация, която да се изисква от приемащото лице в Точката за контакт, е налична и съдържа:

- Дата и час на събитието;
- Документирана информация за това какво видяно и направено (включително какви инструменти са използвани) и защо;
- Местоположение на потенциалните доказателства за събитието;
- По какъв и начин са проверени и архивирани доказателствата;
- Как и къде се съхраняват конфиденциалните доказателствата.

Организацията трябва да определи формата на доклада и задължителното му съдържание. Докладът трябва да съдържа описание на фактите и начина за потвърждаване на следната информация:

- В какво се изразява инцидентът;
- Как е настъпил, от какво или от кого;
- Какво е засегнал или може в бъдеще да засегне.
- Въздействието на инцидента върху дейността на организацията;
- Дали инцидентът се определя като значим или не, в съответствие с приетата скала за класифициране.
- Начин, по който са били предприети действия до момента.

Могат да бъдат посочени следните примери за негативно въздействие:

1. Нерегламентирано разкриване на информация.
2. Неоторизирана промяна на информация.
3. Отказ от приемане на информация.
4. Неналичност на информация и/или услуга.
5. Разрушаване на информация и/или услуга.
6. Намалена работоспособност на услугата.

Примери за реални заплахи за организацията:

1. Финансова загуба.
2. Прекъсване на бизнес операции.

3. Накърняване търговските и икономически интереси.
4. Нарушаване на лична информация.
5. Нарушаване на правни и регулаторни задължения.
6. Нарушаване операции за управление и бизнес.
7. Загуба на репутация.
8. Повреда или загуба на човешки живот.
9. Социални сътресения.

Потвърждаване на оценка (в ISIRT[1])

Организацията трябва ясно да регламентира критериите за оценяване и потвърждаване на решението за това дали дадено събитие трябва да се класифицира като инцидент. Тази отговорност е вменена на ISIRT.

Приемащото лице в ISIRT трябва да направи следното:

- Да потвърди получаването на Формата за докладване (попълнена доколкото е било възможно това) в Точката на Контакт;
- Да въведе Формата за докладване в базата данни за събитие/инцидент/уязвимост, ако това не е вече направено в Точката за Контакт и актуализира базата данни, ако е необходимо;
- Да се потърси разяснения от Точката за Контакт, ако това е необходимо;
- Да прегледа съдържанието на Формата за докладване;
- Да събере всякаква допълнителна информация.

Ако инцидентът е определен от ISIRT като реален, то той е длъжен да извърши по-нататъшна оценка, като се потвърди възможно най-скоро следното:

- В какво се състои инцидентът, как е настъпил, от какво или кого, какво е засегнал или може да засегне, въздействието на инцидента за дейността на организацията, дали инцидентът се определя като значим или не (по

[1] ISIRT Information Security Incident Response Team (Екип за реагиране при инциденти със сигурността)

приетата скала за класификация), необходимо ли е предприемане на кризисни действия;

- При умишлена човешка техническа атака на информационна система, услуга и / или мрежата:
  - Колко дълбоко е проникнал в системата, услугата и/или мрежата, и какво ниво на контрол има нападателят
  - Какви данни са били преглеждани от нападателя, вероятно копирани, променяни или унищожени
  - Какъв софтуер е копиран, променен или унищожен от нападателя
- Преките и непреки ефекти (например отворен физически достъп поради пожар, информационна система е уязвими поради някакъв софтуерен дефект, неизправност на комуникационна линия или поради човешка грешка)
- Как инцидентът по сигурността на информацията е бил третиран до момента и от кого.

Трябва да се прилага процес на приоритизиране с цел присвояване на инцидента на най-подходящото лице или група от лица в ISIRT за да се улесни получаването на адекватен отговор на инцидента.

Приоритетите следва да бъдат определени в съответствие с неблагоприятните въздействия от инцидента върху бизнеса.

За инциденти с еднакъв приоритет - инцидент, който лесно може да бъде решен се разглежда преди инцидент, изискваща по-голямо усилие.

4. Отговор.

Организацията трябва да дефинира критерии, по които ISIRT да определи дали инцидентът е под контрол, или не е. ISIRT предприема необходимия отговор, ако инцидентът е под контрол или предизвиква кризисни дейности чрез ескалация на функциите за работа в кризисна

ситуация, ако инцидентът не е под контрол, или той е довел до тежки последици за организацията.

ISIRT трябва да ангажира всички вътрешни ресурси и да идентифицира външните ресурси, които са необходими за реагиране на инцидента.

ISIRT трябва да се провежда, ако това е необходимо, криминална експертиза и класифициране на инцидента, в съответствие с утвърдената рейтингова скала.

ISIRT трябва да ескалира дейността си за по-нататъшна оценка и/или приемане на необходимите решения.

ISIRT трябва да може да гарантира, че всички негови членове, а и участниците правилно описват всички дейности за да могат те по-късно да бъдат анализирани.

ISIRT трябва да осигури годни за използване доказателства в електронен вид.

ISIRT трябва да отговаря за осигуряването на контрола върху измененията и поддържането на база от данни за връзките между събитие/инцидент/уязвимост.

ISIRT трябва да отговаря за комуникирането с други вътрешни сътрудници и с външни организации във връзка с настъпилия инцидента и съответните подробности свързани с него.

След като инцидентът е бил разследван и предложените мерки са съгласувани, последващите дейности трябва да включват:

- Разпределяне на отговорностите за управлението на инцидента чрез дефиниране на подходяща йерархия на персонала в организацията;
- Осигуряване на формализирани и документирани процедури за работа за всеки ангажиран сътрудник (преглед и изменение на доклади, повторна оценка на щетите, уведомяване).

- Документиране на инцидента за осигуряване на данни за последяващи действия и актуализиране на базата от данни за връзките между събитие/инцидент/уязвимост.
- Използване на регламентираните в цялостната документация на СУИБ последващи действия.
- Актуализиране на базата от данни за връзките между събитие/инцидент/уязвимост.

Видове отговори свързани с инцидента:

- Незабавен отговор;
- Оценка на контрола върху инцидента;
- По-късен отговор;
- Отговор при настъпила кризисна ситуация;
- Криминалистично разследване – анализ.
- Комуникация;
- Ескалация.
- Регистриране и управление на промените.

5. *Поуки. Поуките от управлението на инцидентите се изразяват в:*

- Събиране на всяка достъпна допълнителна информация за анализиране по време на криминалистичното разследване;
- Документиране на поуките от управлението на инцидента;
- Дефиниране и извършване на подобрения свързани с контрола върху сигурността на информацията;
- Определяне и извършване на подобрения в процедурата за оценяване на риска и за докладване на резултатите от Прегледа на ръководството;
- Дефиниране и извършване на подобрения в схемата за управление на инцидентите в СУИБ.

13.11. Непрекъснатост на процесите

При разработването на СУИБ е необходимо да бъда разработена документация за управление на процесите, които да съответстват на Международния стандарт ISO/IEC 27031:2011. Информационни технологии. Методи за сигурност. Указания за готовност на информационни и комуникационни технологии за непрекъснатост на бизнеса.

Необходимо е да бъдат отчетени всички аспекти на сигурността на информацията при управлението на ***непрекъснатостта на дейността***.

Непрекъснатостта на сигурността на информацията трябва да бъде заложена в системите за управление на ***непрекъснатостта на дейността на организацията*** *(Information Security Continuity).*

Изискванията, на които трябва да отговаря разработваната документация (процеси и процедури за осигуряване на непрекъснати дейности по сигурност на информацията) трябва да отговаря на [3.29 ISO 27000:2018].

Опазването на поверителността, целостта и наличността на информацията задължително трябва да бъдат отчетени при разработването на документацията. Могат да бъдат включени също други свойства като автентичност, отчетност, надеждност и неотхвърляемост [3.28 ISO 27000:2018].

Организацията трябва да дефинира своите конкретни изисквания за сигурността на информацията и за непрекъснатостта на управлението на сигурността на информацията в неблагоприятни ситуации - криза или бедствие.

Организацията трябва да разработи, документира, внедри и осъществява поддържка на процеси, процедури и механизми за контрол, за да осигури необходимото ниво на непрекъснатост за сигурността на информацията по време на неблагоприятни ситуации.

Организацията трябва да проверява, през редовни интервали от време, разработените и осъществени механизми за контрол на непрекъснатостта на сигурността на информацията, така че да гарантира, че те са действащи и ефикасни при възникване на неблагоприятни ситуации.

Необходимо е организацията да осигури готовност на средствата за обработване на информация за действие при извънредни ситуации.

Средствата, които са необходими, за обработване на информацията трябва да бъдат осигуряване с излишък, достатъчен за отговаряне на изискванията за готовност.

Организацията трябва да създаде условия за управление на непрекъснатостта на дейността(business continuity management) чрез разработване на комплексен процес за управление, който идентифицира потенциалните заплахи за дадена организация и въздействията на тези заплахи върху цялостната дейност, ако се реализират. Тя трябва да осигури рамка за постигане на устойчивост на организацията с възможност за ефикасен отговор, който да защити интересите на основните заинтересовани страни, нейната репутация, търговската марка и дейностите, създаващи стойност. [3.2 ISO 27031:2011]

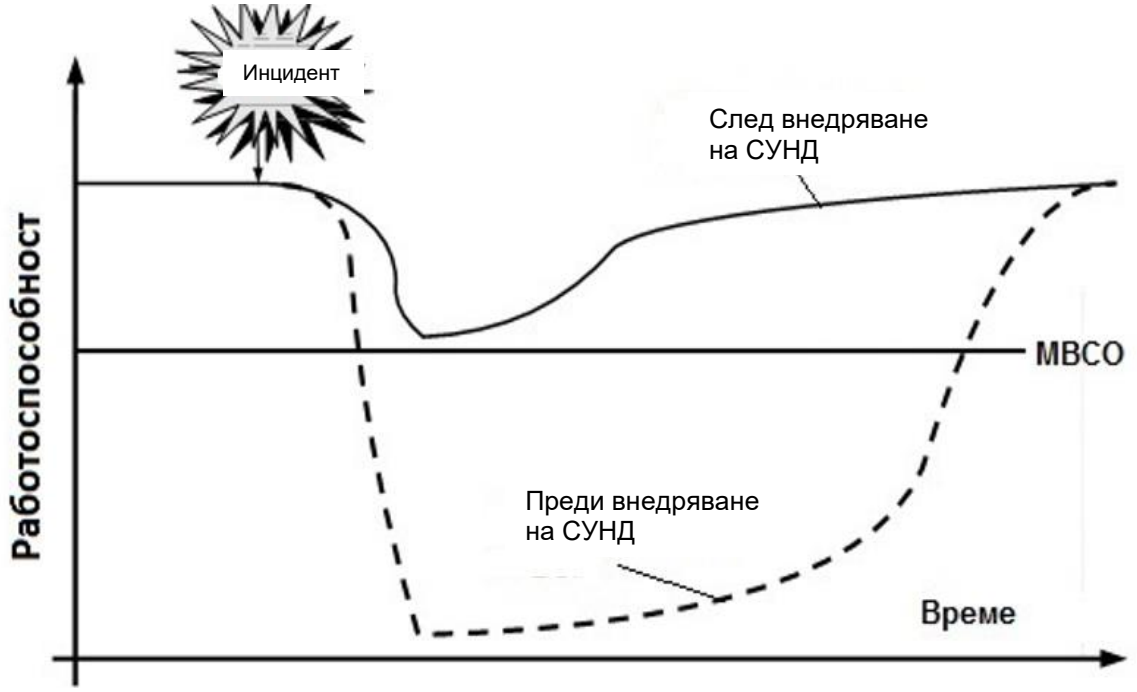
Система за управление на непрекъснатостта на дейността – СУНД *(Business Continuity Management System - BCMS)*

Организацията трябва да разработи цялостна система за управление, която установява, внедрява, функционира, наблюдава, преглежда, поддържа и подобрява непрекъснатостта на дейността й. Тя трябва да включва структурата на организацията, политиките, планирането на дейностите, отговорностите, процедурите, процесите и ресурсите.

Минималната цел по непрекъснатост на дейността (*Minimum Business Continuity Objective (MBCO))* трябва да включва минимално ниво на услуги и/или продукти, което е приемливо за организацията за постигане на нейните бизнес цели по време на нарушение.

Готовност за непрекъснатост на ИКТ дейността (*ICT readiness for business continuity (IRBC)) включва с*пособността на организацията, да поддържа своята дейност по предотвратяване, разкриване и отговор на прекъсване и при възстановяване на ИКТ услуги. [3.10 ISO 27031:2011]

Концепция за Готовност за непрекъснатост на ИКТ дейността *(ICT readiness for business continuity - IRBC)*



Фиг. 28 Непрекъснатост на ИКТ дейността *(ICT readiness for business continuity - IRBC)*

Организацията трябва да разработи План за непрекъснатост на дейността *(*Business continuity plan), който да включва документирани процедури, определящи как тя да реагира, възстанови, възобнови и доведе дейността си до предварително определено ниво на изпълнение след прекъсване поради настъпване на нежелана ситуация. Обикновено това включва ресурси, услуги и дейности, които са необходими за да се осигури непрекъснатост на критични за дейността функции. [3.3 ISO 27031:2011]

Ръководството на организацията дефинира Целево време за възстановяване *(Recovery Time Objective (RTO))*, в рамките на което трябва

да бъдат възстановени минималните нива на услуги и/или продукти и поддържащите системи, приложения или функции, след като е настъпило прекъсването. [3.13 ISO 27031:2011]

Ръководството е необходимо да разработи и ясно дефинира документиран План за възстановяване след бедствие *(disaster recovery plan*), който трябва да бъде изпълнен за да бъдат възстановени способностите в областта на ИКТ, когато настъпи прекъсване. [3.8 ISO 27031:2011]. В Плана се определя Целева точка на възстановяване *Recovery Point Objective (RPO),* във времето, до която данните трябва да бъдат възстановени, след като е настъпило прекъсване *(за да се даде възможност на дейността да функционира след възобновяване).*

В стандарта са определени следните принципи на IRBC, които трябва строго да се спазват при разработване на документацията на СУИБ:

1. Предотвратяване на инциденти

Защита на ИКТ услугите от заплахи - екологични и хардуерни повреди, оперативни грешки, злонамерени атаки и природни бедствия. Тази защита има решаващо значение за поддържането на желаните нива на наличност за системите на организацията.

2. Откриване на инциденти

Откриване на инциденти при първа възможност(навреме) ще сведе до минимум въздействието им върху услугите, до намаляване на усилията за възстановяване и запазване на качеството на услугите.

3. Отговор на инциденти

Навременната и правилната, по най-подходящия начин, реакция на възникналия инцидент ще доведе до по-ефективно оползотворяване и минимизиране на престоите. Ако това не бъде постигнато поради неправилно ненавременно реагиране то това неминуемо ще доведе до това, че сравнително малкият инцидент да прерасне в нещо много по-сериозно.

4. Възстановяване

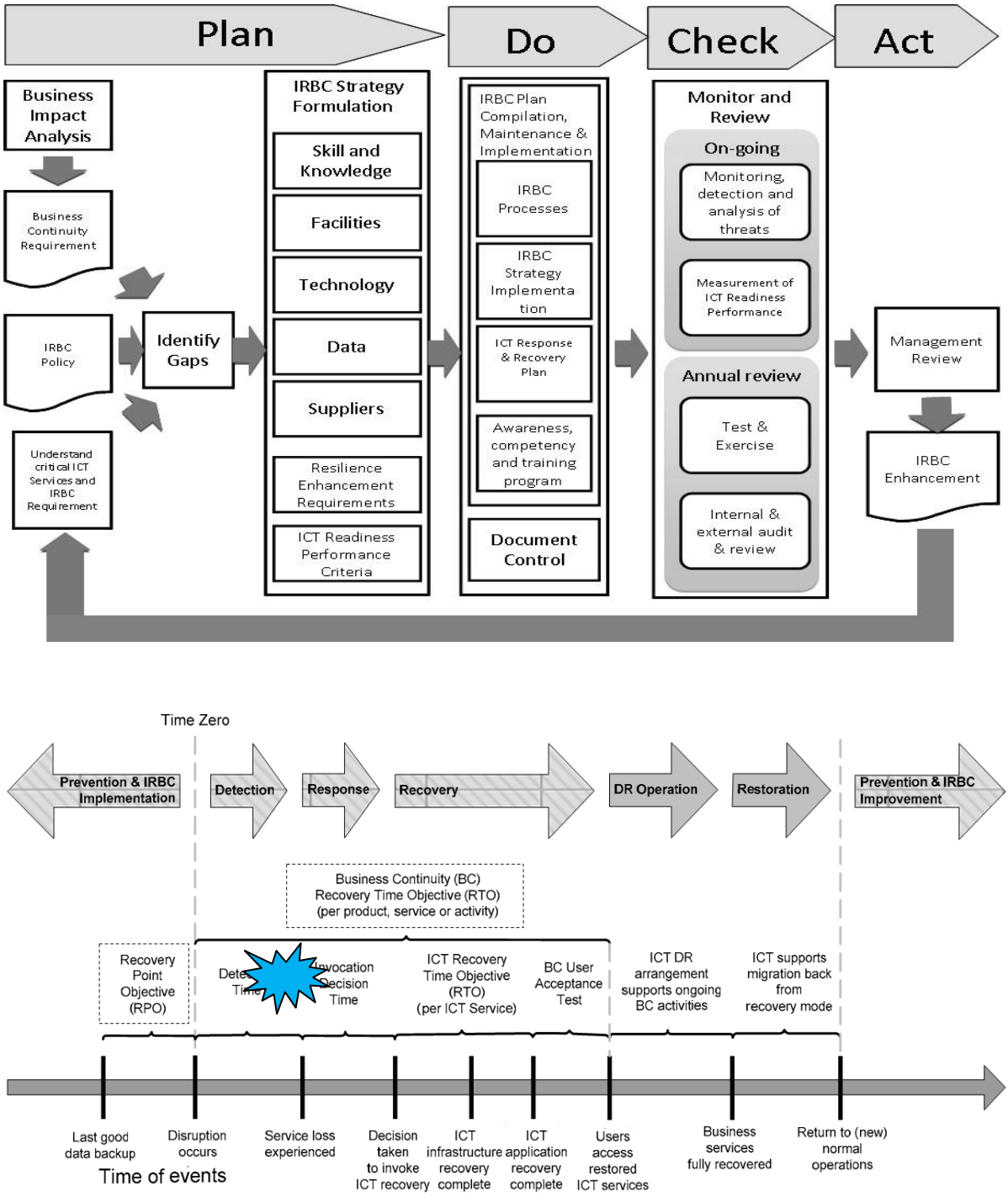
Организацията трябва да разработи и прилага подходяща стратегия за възстановяване, която да гарантира своевременното възобновяване на услугите и поддържането на целостта на данните. Вникването в приоритетите за възстановяване позволява определените като най-критични услуги да бъде възстановени първи. Услуги с по-малко критичен характер, могат да бъдат възстановени по-късно, или в някои случаи - не напълно.

5. Подобряване

Поуките от малки и големи инциденти трябва да бъдат документирани, анализирани и преразглеждани. Разбирането на тези уроци ще позволи на организацията да се подготви по-добре, да контролира и избягва инциденти и прекъсвания.

Елементите на IRBC задължително трябва да включват следните елементи:

1. Персонал - специалисти с подходящи умения и знания, както и компетентни кадри за backup
2. Устройства - физическата среда, в която са разположени ИКТ ресурси
3. Технология - хардуер, софтуер, мрежа
4. Данни - данни от приложения, гласови данни и други типове данни
5. Процеси – документиране, управление на конфигурация на ИКТ, възстановяване и поддържане на ИКТ услуги
6. Доставчици – верига доставчици.



Фиг. 29 IRBC и основни етапи по време на прекъсването

Организацията трябва да определи дали непрекъснатостта на сигурността на информацията е обхваната от процеса на управление на непрекъснатостта на дейността или от процеса на управление на възстановяването след бедствие в съответствие със стандартите ISO

22301:2019 Сигурност на обществото. Системи за управление на непрекъснатостта на дейността. Изисквания. и ISO 22313:2020 Сигурност на обществото. Системи за управление на непрекъснатостта на дейността. Указания.

Ръководството на организацията трябва ясно да дефинира своите изисквания за сигурността на информацията. Те се определят тогава, когато се планира непрекъснатостта на дейността и възстановяването след нежелан инцидент или ситуация.

Внедрените механизми за контрол на сигурността на информацията, които е разработила организацията, трябва да продължат да функционират по време на неблагоприятно събитие. Ако механизмите за контрол на сигурността не са в състояние да продължат да осигуряват информацията, трябва да бъдат създадени, внедрени и поддържани други механизми за контрол, които да поддържат допустимо ниво на сигурност на информацията.

Планът за осигуряване на непрекъсваемостта на сигурността на информацията може да има примерно следното съдържание:

1) Основание за разработване на плана.
2) Критерии за задействане на плана.
3) Отговорници – титуляр, заместник, средства за връзка.
4) Действия за идентифициране на проблема.
5) Разпределяне на отговорностите и последователността на действията.
6) Критерии за ефективно изпълнени на плана.
7) Последователност от действия за възстановяване на нормалната работа.
8) Начин на промяна на плана.
9) Копия на плана, разпределение.
10) Приложения към плана – подробни планове за отделни звена, системи, ситуации, ако е необходимо.

13.12. Разработване на контроли

Организацията трябва да разработи следните контроли, в съответствие с Annex A:

- Information security policies (2 controls)
- Organization of Information security (7 controls)
- Human resource security (6 controls)
- Asset management (10 controls)
- Access control (14 controls)
- Cryptography (2 controls)
- Physical and environmental security (15 controls)
- Operations security (14 controls)
- System acquisition, development, and maintenance (13 controls)
- Supplier relationships (5 controls)
- Information security incident management (7 controls)
- Information security aspects of business continuity management (4 controls)
- Compliance (8 controls)

1. Насоки за управление сигурността на информацията

Цел на контролата: Да предостави насоки за управление и поддържане на информационната сигурност в съответствие с изискванията на бизнеса и съответните закони и наредби.

Политиките свързани със сигурността на информацията трябва да включват следните дейности.

- Да се определи набор от политики за информационна сигурност, одобрени от ръководството, публикувани и доведени до знанието на служителите и съответните външни заинтересовани лица.
- Политиките за сигурност на информацията трябва да бъдат подлагани на преглед през планирани интервали или при настъпване на значителни промени, за да се гарантира постоянно тяхната актуалност, адекватност и ефикасност.

2. Организация на информационната сигурност. Вътрешна организация.

Цел на контрола: Да установи управленска рамка за въвеждане и контрол на реализирането и оперирането на сигурността на информацията в рамките на организацията.

- Разпределянето на ролите и отговорностите за сигурността на информация изискват определяне и разпределяне на всички отговорности свързани със сигурността на информацията;
- Трябва да бъдат разделени противоречивите задължения и области на отговорност, за да бъдат намалени възможностите за неоторизирано или неумишлено модифициране, или злоупотреба с активите на организацията;
- Трябва да се поддържат подходящи контакти със съответните оторизираните органи;
- Трябва да бъдат поддържани подходящи контакти с групи със специален интерес или други форуми на специалисти по сигурността и професионални асоциации (http://ncs.nlcv.bas.bg – Национален портал за киберсигурност https://govcert.bg - Национален Център за Действие при Инциденти в Информационната Сигурност)
- Независимо от вида на проекта трябва да бъде отчетена сигурността на информацията при управление на проекти.

3. Мобилни устройства и работа от разстояние.

Цел по контрола: Да осигури надеждност и сигурност при отдалечена работа и използване на мобилни устройства.

- Трябва да бъдат приети политика и поддържащи мерки за сигурност при управлението на рисковете, които се привнасят при използването на мобилни устройства.
- Всички идентифицирани изисквания за сигурност трябва да бъдат разгледани, преди да се даде достъп на клиентите до информацията или активите на организацията.

4. Сигурност на човешките ресурси

Цел по контрола: Да се осигури, че служителите, страните по договор или трети лица разбират своите отговорности и са подходящи за ролята, която ще изпълняват, за да се намали опасността от кражба, измама или неправилно използване на средства.

- Трябва да бъде извършвано проучване и проверка на биографичните данни на всички кандидати за постъпване на работа в организацията в съответствие със законите, нормативните актове и етиката. Кандидатите трябза да отговарят на изискванията свързани с дейността, класификацията на информацията, до която те ще имат достъп, и предполагаемите рискове от това.
- Договорните споразумения със служителите и доставчиците трябва да определят техните отговорности и отговорностите на организацията по отношение на сигурността на информацията.

5. По време на извършване на дейността

Цел на контрола: Да се гарантира, че служителите и доставчиците познават и изпълняват своите задължения свързани със сигурността на информацията.

- Ръководството трябва да изисква от служителите и доставчиците да прилагат всички мерки за сигурност на информацията в съответствие с установените политики и процедури в организацията.
- В съответствие със своите работни функции всички служители на организацията и, когато е уместно, доставчиците трябва да получат подходящо обучение с цел осъзнаване и редовно актуализиране на техните знания свързани с политиките и процедурите на организацията.
- За служителите, които са извършили нарушение по отношение на сигурността на информацията, трябва да се прилага официален и оповестен дисциплинарен процес.

6. Прекратяване или промяна на трудовите отношения

Цел по контрола: Да се защитят интересите на организацията, като част от процеса на промяна или прекратяване на трудовите правоотношения.

- Отговорностите и задълженията по отношение сигурността на информацията при прекратяване или промяна на трудовото отношение трябва да бъдат определени, оповестени на служителя или доставчика и приведени в действие.

7. Управление на активите

Цел на контрола: Да се идентифицират активите на организацията и определят съответните отговорности за тяхната защита.

- Всички активи, свързани с информационните ресурси и средствата за обработване на информация, трябва да бъдат ясно идентифицирани и тези активи трябва да бъдат описани в поддържан опис.
- Активите, които са описани и поддържани в описа, трябва да бъдат притежавани от собствениците им.

➢ Трябва да бъдат посочени, документирани и прилагани правила за допустимото използване на информацията и активите, свързани с информацията и средствата за обработване на информация.

➢ Всички служители и потребители от трета страна при прекратяване на техните трудово-правни отношения, договор или споразумение трябва да върнат всички притежавани от тях активи на организацията.

8. Класифициране на информацията

Цел на контрола: Да се гарантира, че информацията получава подходящо ниво на защита, в съответствие с нейното значение за организацията.

➢ Информацията трябва да бъде класифицирана според изискванията на нормативните актове, нейната стойност, критичност и чувствителност към неоторизирано разкриване или модифициране.

➢ Трябва да бъде разработен и приложен съответен набор от процедури за дефиниране на информацията в съответствие с класификационната схема за информацията, утвърдена от организацията.

9. Работа с информационни носители

Цел на контрола: Да се предотврати неоторизирано разкриване, изменение, премахване или разрушаване на информация, съхранявана върху носителите.

➢ Трябва да има внедрени процедури за управлението на сменяемите информационни носители в съответствие с класификационната схема, приета от организацията.

➢ По време на транспортиране носителите, съдържащи информация, трябва да бъдат защитени от неоторизиран достъп, използване не по предназначение или подправяне.

➢ Ненужните носители трябва да се унищожават по сигурен начин, като се използват официалните процедури.

13.13. Внедряване на процедурите в системата за управление на информационната безопасност

Внедряването на процедурите се изразява в информиране на съответните сътрудници за всички правила и срокове за изпълнение на конкретната процедура, регулярен мониторинг и контрол върху изпълнението на процедурата, както и оценяване ефективността й, въвеждане на коригиращи и превантивни мерки. Всички тези дейности по процедурите трябва да се осъществяват в съответствие с модела PDCA.

Общоприета практика е привлечените консултант да разработят „План за внедряване на СУИБ“. В него трябва да бъде ясно описана последователността от действия, които трябва да бъдат спазвани при внедряването на процедурите, методите за контрол и начините за извършване на проверките за изпълнението на процедурата.

Необходимо е да се бъде осигурена пълно съответствие на всички части на основната част на стандарта, и изборно на контроли. Изборът на всяка една от контролите е необходимо да бъде обоснован. Ако в резултат на анализа се стигне до извода, че някои от контролите е невъзможно да бъдат приложени, то тогава задължително трябва да бъде представено или някакво обяснение или някаква алтернатива.

Необходимо е да се направи анализ на дейността и структурата на организацията и нейната информационна обезпеченост с информационна и компютърна техника, устройствата и местата за съхраняване на информацията (вътрешни или външни сървъри).

Анализът трябва да включва и оценяване на влиянието на доставчиците – доставчици на външни услуги за техническа поддръжка, всички «физически» доставчици на стоки и материали, физическа охрана на офиса върху сигурността информацията на организацията.

В новосъздадения екип за подготовка на документацията за сертифициране е необходимо да бъдат включени: представител на висшето ръководство, сътрудник/ци запознати с това каква и организационната структура и как функционират информационните системи на организацията и консултант (външен за организацията) по информационна безопасност и по профилното законодателство.

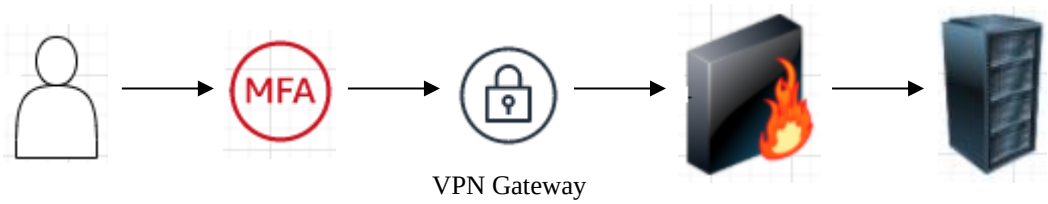
Какво трябва дя бъде направено на първия етап.

Всички етапи на дейността по сертифицирането трябва да бъдат добре описани. Много често възникват реакции на отричане на необходимостта от такова сертифициране, недоволство, съпротивление в малки, добре функциониращи компании с добър психологически климат. В такива компании всяка една бюрократична иновация среща стена от неразбиране, документацията много бързо остарява, дори преди да е довършена. Основния проблем, който се явява се е сложността как да бъде обяснено на сътрудника с дълъг стаж защо изведнъж се налага да бъдат променяни наложили се и функциониращи утвърдени с годините практики. Но, трябва да бъде отбелязано, че именно в малките компании най-добре и най-бързо се проявяват резултатите от подготовката.

Ето няколко препоръки, от които могат да се възползват мениджърите на компаниите при етапа на стартиране на проекта за разработването на СУИБ:

1. **Разработване на блок схема и посочване на връзките в корпоративните информационни системи.** Стандартът изисква да бъдат определени границите и сферите на информационните системи». Това може да бъде осъществено чрез просто излагане на хартиен носител, но най добре

е всичко да започне с начертаване на схемата на информационните системи. Това изглежда много просто, а за една малка компания даже излишно, но «картината» променя много неща. Примерна схема може да включва ноутбуци, сървъри, VPN и Firewalls с ненабиващи се на очи детайли – протоколи на VPN, backups. Могат да бъдат добавени облачни сървъри, естествено.



* MFA - Многофакторно удостоверяване (MFA) добавя слой на защита към процеса на влизане. При достъп до акаунти или приложения потребителите предоставят допълнителна проверка на самоличността, като сканиране на пръстов отпечатък или въвеждане на код, получен по телефона.
** VPN - виртуална частна мрежа. В процеса на присъединяване не се използват физически кабели, чрез това присъединяване никой друг не може да вижда вашите данни или действия в Интернет.

Фиг. 30 Блок схема и връзки в корпоративните информационни системи

2. Необходимо е да бъде създадена обща папка за документацията свързана със стандарта. Най-простия, но и най-ефективен начин е създаване на обща папка в SharePoint, където за всяка контрола и точка от стандарта е създадена отделна подпапка със съответното име. В тези папки се съхранява цялата документация. Например:

A.6.1.3 Contact with authorities

A.6.1.4 Contact with special interest groups

A.6.1.5 Information security in project management

A.6.2.2 Mobile device

A.6.2.2 Telewrking

A.7.1.1 Screening

A.7.1.2 Employment Terms

A.7.2.2 Information security awareness, education and training

A.7.2.3 Disciplinary Process

3. Необходимо е да бъдат разработени политики предвиждайки в тях някакъв запас от гъвкавост. Преди да се разработят политиките екипът трябва много внимателно да се запознае с изискванията на стандарта ISO27002. Той дава насоки за това, какво е необходимо, а те ще бъдат задължително проверявани от одиторите. Всеки документ може да бъде разработен по различен начин и в различен стил. Например – политиката по паролите. Може да бъде записано в документа, че задължително трябва да съдържа минимум 8 символа, или да бъде записано, че паролата трябва да бъде «достатъчно сложна» и да отразява изискванията на информационните системи.

4. След като документацията е разработена е необходимо да бъде подложена на сериозна проверка и анализ след един период от време. По този начин се предоставя време и възможност на политиките да «отлежат». Повторното им разглеждане за повторения, излишни определения и изисквания, конкретизирането и прецизирането им води до повишаване на тяхното качество. Все пак е по-лесно една политика да бъде променена, отколкото да бъде написана отново.

Системата управление на информационната безопасност може да се счита за внедрена ефективно функционираща едва тогава, когато всички нейни процедури поне веднъж са преминали през фазите на модела PDCA, открити и решени са всички проблеми, които са възникнали при тяхното внедряване.

Към осигуряването на информационната безопасност трябва да се подхожда комплексно и своевременно, да се изпълняват всички изисквания на международните стандарти в областта на управлението на ИБ - ISO/IEC 27001:2013 и ISO/IEC 17799:2005.

Една от най-важните процедури при разработването на СУИБ в съответствие със стандарта ISO/IEC 27001:2013 е „Управление на инциденти за сигурност на информацията“.

Разработените процедури и документацията на СУИБ, свързана с управлението на инцидентите, трябва да съответстват на **международния стандарт ISO/IEC 27035:2011 „**Информационни технологии. Методи за сигурност, Управление на инциденти за сигурност на информацията“(заменил ISO/IEC TR 18044:2004).

В стандарта (клаузи от 0 до 10) не съществува позоваване на инциденти. Връзката между целите (задачите) за управление и средствата за управление и средствата за тяхната реализация са заложени са заложени в Приложениие А и са непосредствено взети и са съгласувани с тези, които са изброени в разделите от 5 до 1 в ISO/IEC 27002:2013 [1] и трябва да се използват в контекста на т. 6.1.3.

13.14. Вътрешен одит на СУИБ.

Ръководството трябва да е сигурно, че всички разработени и внедрени методи и принципи на СУИБ функционират така, както се е очаквало и „оптимистичната информация за успехите“, постъпваща от сътрудниците. изпълнителите, съответства на действителността. Поради тази причина е необходимо да бъдат организирани и периодически провеждани независими оценки (одити) за оценка на съответствието на одитираните процеси и процедури на СУИБ на изискванията и на стандартите, на вътрешните документи, а също и дали те функционират по предвидения начин.

Вътрешните одити на СУИБ са регламентирани от Международния стандарт ISO/IEC 27007:2017 Информационни технологии. Методи за сигурност. Указания за одитиране на системи за управление сигурността на информацията.

Организацията трябва да извършва вътрешни ***одити*** на системата за управление на информационната безопасност, в съответствие с международен стандарт ISO/IEC TR 27008:2019 Информационни технологии. Методи за сигурност. Указания за одитиране на контроли за сигурността на информацията, през планирани интервали, за да осигури информация дали системата за управление на сигурността на информацията:

- съответства на собствените изисквания на организацията
- изискванията на ISO/IEC 27001
- е ефикасно внедрена и поддържана.

Необходимо е организацията да:

- Да планира, създаде, внедри и поддържа програма(и) за ***одит***, включително честотата, методите, отговорностите, изискванията за планиране и докладване.
- Програмата(ите) за ***одит*** трябва да взема(т) предвид важността на засегнатите процеси и резултатите от предишни ***одити.***
- За всеки ***одит*** да определи критериите и обхвата на ***одита.***

Необходимо е организацията да:

- избере ***одитори*** и да провежда ***одити***, които осигуряват обективност и безпристрастност на процеса на ***одит***;
- осигури резултатите от ***одитите*** да бъдат докладвани на съответното ръководство;
- съхранява документирана информация като свидетелство за програмата(ите) за ***одит*** и за резултатите от ***одита***.

Указанията за одитиране на СУИБ се базират на Annex A – Практически указания за одит на СУИБ ISO/IEC 27007:2017. В неговите раздели са определени:

- **Критерии за одита** – Клаузи и контроли от ISO 27001

- **Свързани стандарти** – от фамилията 27000 и други (ISO 17021, ISO 19011, ISO 31000)
- **Доказателства за одита** – документи, записи, активи, данни
- **Практически указания за одитиране** – какво да се провери, как да се провери, на какво да се обърне внимание

В съответствие с Анекс 1 трябва да бъде одитиран обхвати на СУИБ, нейната политика и прилаганите методи за оценяване на риска. В стандарта ISO 27001 това са точки 4.3, 5.2, 6.1.2.a,b.

На одит, в съответствие с Анекс 2, подлежат идентификацията, анализа и оценката на риска, идентифицирането и оценяване на възможности за влияние върху риска. Това са точките 6.1.2.c,d,e от Стандарта.

Одитирането по Анекс 3 включва проверка на избора на целите и механизмите за контрол, критериите за приемане на остатъчния риск, полученото разрешение за внедряване на СУИБ, включително и Декларацията за приложимост (точки 6.1.3.a,b,c,d,f от Стандарта)

Според Анекс 4 трябва да се одитират внедряването и работата на СУИБ (точка 8.1), Анекс 5 - мониторинга и прегледа на СУИБ (точка 9.1).

Одитирането на Анекси 6, 7, 8 и 9 включват одитиране съответно на поддържането и подобряването на СУИБ (точка 10); документацията на СУИБ (точка 7.5, и още в 13 места на стандарта ISO:27001 – документирана информация); управлението на отговорностите (точка 5.3); вътрешния одит и Прегледа на ръководството на СУИБ (точки 9.2, 9.3).

Одиторите трябва да спазват указанията за одитиране на контролите за сигурността на информацията.

Основните раздели включват: 7. Методи за преглед и 8. Дейности.

Приложения включват следните Анекси: A: Практическо ръководство за проверка на техническо съответствие и B: Първоначално събиране на информацията.

Методите за преглед при извършването на вътрешен одит включват:

– Изследване (*examination*)

– Интервю (*interview*)

– Тест (*test*)

Методът за преглед *Изследване* (*examination*) включва:

1. Обекти

• Спецификации (политики, планове, процедури, изисквания, проекти и др.);

• Механизми (приложени функционални в хардуер, софтуер, фърмуер (firmware) и др);

• Процеси (системни операции, управление, обучение и др.)

2. Одиторски действия:

• Преглеждане на политики, процедури, инструкции за сигурност на информацията;

• Анализиране проектна документация на системи, спецификации на интерфейса;

• Наблюдение backup операции;

• Преглеждане резултати от изпитания на планове за извънредни ситуации;

• Наблюдаване процеса за реакция на инциденти;

• Изучаване технически наръчници и ръководства за администратори и/или потребители;

• Проверяване, изучаване и наблюдаване на операции при информационни системи;

• Проверяване, изучаване и наблюдаване на процеса за управление на изменения в системите;

• Проверяване, изучаване и наблюдаване на процеса за управление на журнални записи (logs) в системите;

• Проверяване, изучаване и наблюдаване на системи за физическа сигурност;

3. *Атрибути*
    - Генерализирано изследване;
    - Фокусирано изследване;
    - Детайлно изследване;
    - Представително изследване;
    - Специфично изследване;
    - Всеобхватно изследване

Методът за преглед *Интервю (interview)* включва:

1. *Обекти:*
    - Отделни служители;
    - Групи от служители
2. *Одиторски действия – интервюта на:*
    - Ръководители;
    - Собственици на активи и/или рискове;
    - Служители по сигурността на информацията;
    - Служители по управление на персонала;
    - Мениджъри по сигурността на информацията;
    - Служители по поддръжка на съоръженията;
    - Оператори на информационни системи;
    - Системни администратори;
    - Мрежови администратори;
    - Администратори на сайтове;
    - Управители на сгради;
    - Мениджъри по физическа сигурност;
    - Потребители
3. *Атрибути:*
    - Генерализирано интервю;

- Фокусирано интервю;
- Детайлно интервю;
- Обхващащо (обхвата) интервю;
- Представително интервю;
- Специфично интервю;
- Всеобхватно интервю

Методът за преглед Тест (test) включва:

1. *Обекти:*

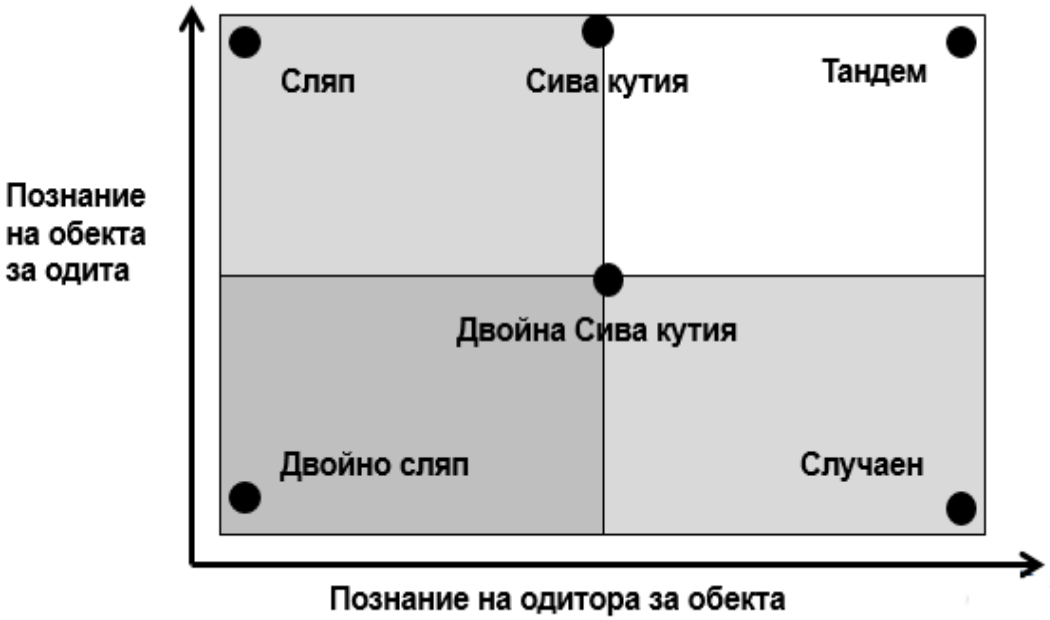
- Механизми (приложени функционални в хардуер, софтуер, фърмуер (firmware) и др);
- Процеси (системни операции, управление, обучение и др.)

2. *Одиторски действия:*

- Тестване контрола на достъпа, идентификация, автентификация, прилагани механизми;
- Тестване настройките за сигурност в конфигурации;
- Тестване устройствата за физически контрол;
- Провеждане тест за проникване в ключови компоненти на информационни системи;
- Тестване операциите за backup;
- Тестване способността за реагиране на инциденти;
- Тестване устройствата за физически контрол;
- Тестване планове за извънредни ситуации;
- Тестване възможностите на системите за откриване, предупреждаване и отговор на прониквания;
- Тестване прилагани алгоритми за криптиране;
- Тестване механизмите за идентифициране на потребители и управление на привилегии;
- Тестване на механизмите за оторизация (даване на права, разрешаване);

- Тестване каскадната устойчивост на мерките за сигурност

3. *Видове тестове:*
   - Сляп тест;
   - Двойно сляп тест;
   - Тест сива кутия;
   - Двоен тест сива кутия;
   - Тандем тест
   - Случаен тест



Фиг. 31 Видове тестове

Стандартът ISO/IEC 27008:2019 включва действия, които се изразяват в *Подготовка; Разработване на план; Провеждане на прегледи; Анализ и докладване на получените резултати.*

Практическото ръководство за проверка на техническо съответствие, Анекс А включва: Техническа проверка на защитата от злонамерен софтуер посредством Контрола А.12.2.1 - Механизми за контрол срещу злонамерен софтуер; Техническа проверка на регистриране на събитията посредством

Контрола А.12.4.1- Регистриране на събития; Техническа проверка на управлението на привилегии посредством Контрола А.9.2.3 - Управление на привилегировани права за достъп; Техническа проверка на управлението на backups посредством Контрола А.12.3.1 - Резервиране на информация; Техническа проверка на управлението сигурността на мрежите посредством Контроли А.13.1. - Управление сигурността на мрежи и Техническа проверка на управлението на отговорностите на потребителите посредством Контрола А.9.3.1 - Използване на тайна информация за автентификация.

Алгоритъмът за организиране и провеждане на вътрешен одит трябва да включва следните дейности:

1. Разработване на процедури, алгоритъм и документи за вътрешните проверки на СУИБ.

2. Подбор и обучение на одиторите,

3. Формиране на одит-екипи,

4. Разработване на програма за провеждане на вътрешните одити за съответната календарна година, който включва избор на варианти за провеждане на одитите и разработване на шаблон разработване и оформяне на програмите за одити.

5. Разработване на планове за одитите през съответната годината, което включва: определяне на критерии за оценяване на съответствието; определяне на продължителността на одита; и разработване на шаблон за разработване и оформяне на плана за одита.

6. Разработване на въпросник в съответствие с утвърдените критериите на одита.

7. Планиране и подготовка на провеждането на одита на място.

8. Провеждане на одита в подразделенията на организацията, което включба следните дейности: провеждане на встъпително съвещание с представителите на отделните звена в организацията на клиента; събиране и фиксиране на откритите доказателства от изпълнението на одита;

регистриране на откритите отклонения; провеждане на заключително съвещание с представителите на организацията-клиент.

13.15. Преглед от ръководството на СУИБ

Ръководството на организацията трябва да планира по какъв начин, дефиниран в документацията на СУИБ, периодично (поне веднъж на година) да провежда извършва цялостен преглед на СУИБ, за да се контролира нейната перманентна пригодност, адекватност и ефективност.

Резултатите от анализа на Прегледа на ръководството трябва да съдържат оценка на текущото състояние на СУИБ и дефинирани предложения за евентуалното коригиране на нейните елементи, за да се гарантира, че се изпълняват изискванията на определената от ръководството политика и се постигат целите на информационната сигурност. Резултатите от проверките трябва да бъдат документирани и съхранявани в съответствие с процедурата и правилата за управление на записите.

Анализът на СУИБ по време на Прегледа от ръководството се основава на събраните входни данни:

1. Резултатите от предишни прегледи на ръководството.

2. Резултати от одити - всички извършени оценки на съответствието на СУИБ на заявените стандарти и принципи, заедно със списъците със задачи и планове за отстраняване на несъответствията и идентифицираните недостатъци.

3. Резултатите от взаимодействието със заинтересованите страни и с тези, чиито дейности са непосредствено засегнати от СУИБ. Приема се за положителна практика да бъде създаден колегиален орган в организацията, например Управляващ комитет по информационна сигурност, в чийто компетенции е решаването на въпросите свързани с организирането на процесите в СУИБ. Тези процеси трябва да съответстват на нивото на

управление дефинирано в Политиката на СУИБ ISMS или в Политиката на информационна сигурност.

4. Информация за методите, средствата и процедурите, които могат да бъдат използвани в организацията за усъвършенстване на СУИБ. Мениджърът, който отговаря за въпросите на СУИБ, трябва да е запознат с най-съвременните тенденции и методи за осигуряване на информационна безопасност. Отговорността за изработването на подобни аналитични материали трябва да бъде възложена на съответните позиции в йерархията или на лицата, упоменати в документите, определящи политиката на СУИБ.

5. Юридически обоснования за осъществяване на превантивни и коригиращи действия. Всички действия, които се използват от СУИБ, трябва да бъдат легитимни, както от гледна точка на политиките за вътрешна информационна сигурност, така и от гледна точка на законодателството. Съответните разпоредби трябва да бъдат отразени в "програмните" документи на СУИС, а формираните процеси и документи, свързани с осигуряването на СУИБ, трябва да преминат експертиза от юридическия отдел на организацията. Препоръчително е представителят на юридическия отдел да се явява член на колегиален орган за управление на СУИБ.

6. Информация за уязвимости и заплахи, които са се появили през изтеклия период и/или не са били адекватно отчетени при предишни оценявания на рисковете в съответствие с документите на СУИБ или в длъжностните (или функционалните) инструкции на отговорните изпълнители. На тях трябва да им бъзе вменено задължението да анализират различните източници на нови уязвимости и заплахи за информационната сигурност (например уебсайтове на антивирусни компании), както и идентифициране на неадекватно обработени уязвимости въз основа на резултатите от мониторинга състоянието на СУИБ, формиране на

подходяща отчетност (например под формата на аналитични бележки) за вземане на подходящи решения.

7. Количествени оценки за резултатите от функционирането на СУИБ (въз основа на разработените и използвани критерии и показатели). Едно от правилата за управление е: „докато не се научиш да измерваш, няма да се научиш да управляваш“. Без някаква, макар и груба, количествена оценка на състоянието и съответния „праг“ за сравнение „повече-по-малко“, е много трудно да бъде оценено качеството на работата на съответното подразделение или метод. За да бъде разработена система от показатели е препоръчително да се използват многобройните ръководства за itSM (IS Service Management, управление на ИТ услуги) и ITIL (IT Infrastructure Library) или да се възползвате от услугите на консултанти, които предоставят подобни услуги. Естествено, използваните критерии и показатели трябва да бъдат документирани, да се определи редът, периодичността и отговорността за тяхното формиране и оценка.

8. Информация за всякакви промени, които могат да повлияят на СУИБ, а именно всякакви промени в бизнес процесите, в архитектурата на информационните системи или в средата за функциониране на инфраструктурните елементи може да наложат промени в общата политика или в специфични направления в отделни мерки, използвани при внедряването на СУИБ. Разглеждането на тези въпроси трябва да бъде документирано в рамките на компетентността на съответните служители или на колективните органи, да бъде включено като допълнителни задачи във внедряване проекти свързани с надграждането на информационната система, особено за критични за бизнес процеси, или да се извършва регулярно като отделни проекти от вътрешни или външни изпълнители.

9. Препоръки за подобряване на СУИБ на базата на резултатите от проведената оценка на съответствието на СУИБ на изискванията на вътрешните или външните стандарти, на нормативните документи или на

заявените принципи, получени в резултат на самооценки или независими одити, съдържащи препоръки за подобряване на СУИБ, трябва да бъдат организирано и системно да бъдат анализирани, превърнати в задания и проекти, фиксирани в плановете и в бюджетите на организацията, с последващ мониторинг на тяхното изпълнение.

Резултатите от анализа на СУИБ от ръководството трябва да бъдат документирани под формата на **изходни данни**, представляващи решения и действия, изразяващи се в задания, проекти за създаване и внедряване на организационни и технически решения, насочени към решаване на :

- подобряване на ефективността на СУИБ;
- актуализиране на плановете за оценка на риска и за неговото обработване;
- модифициране на процедурите и мерките за управление и контрол, които влияят на информационната безопасност, включващи промени в:
    - изискванията за информационна сигурност от страна на бизнес процесите;
    - изискванията за защита на информацията;
    - коригирането на бизнес процесите, които влияят на изискванията към информационна сигурност;
    - вътрешните нормативни документи;
    - договорните задължения;
    - нивата на риска и/или критериите за приемливост на риска;
    - промени в изискванията за ресурси;
    - промени в методите, с помощта на които се оценяват резултатите от контролите.

По този начин наличието в СУИБ на вградени механизми за анализ на текущото й състояние и на нейната ефективност осигурява адекватна информация за нейното състояние и за качеството на функционирането й, което от своя страна трябва да гарантира както адаптирането й към променящия се контекст на средата, така и изпълнението на основната й задача - управление осигуряването на информационната сигурност.

14. Сертифициране на СУИБ на организацията в съответствие със стандарта ISO 27001:2013

Обичайният план за подготовка за сертифициране според изискванията на стандарта ISO 27001 включва следните стъпки:

1. Закупуване на официалния текст (за съжаление той не се разпространява безплатно) и да се изучи стандарта. Не е добра практика да се ползва «пиратско копие». Инвестицията не е толкова сериозна, а и одиторът може да поиска да види вашия собствен екземпляр. Може да планирате една седмица, но понякога отнема две.

2. Избор на квалифициран външен консултант, който вече има поне няколко успешни сертификационни процедури. Консултантът съдейства на организацията при разработването и написването на Body – първата част за съответствието на стандарта, при разработването на основните постановки за стратегията, при дефинирането на изискванията, при оценяването на рисковете за организацията, на базата на своя предходен опит.

Изборът на консултантска компания до голяма степен определя доколко ще бъде успешен проекта за сертифициране на организацията.

Компанията трябва да отговаря на следните базови изисквания:

- наличие на опит и реализирани проекти;

- наличие висок статус, който се определя от натрупания опит и от качеството на реализираните проекти, от наличните отзиви на бивши и настоящи клиенти и делови партньори;
- притежава собствени методики за провеждане на вътрешен одит, за изграждане на СУИБ, за анализиране и управление на рисковете и др. Добре е те да включват в себе си не само изпълнението на директивите на ISO в областта на информационната безопасност, но допълнително са разширени с изискванията на други стандарти и методи;
- работещи в компанията специалисти, които са преминали подготовка в специализирани акредитирани курсове за одит на организации за съответствие на СУИБ на изискванията на стандарта ISO/IEC 27001:2013;
- наличие в компанията на сертифицирани специалисти по различните направления на информационните и комуникационните технологии, които са членове на одит екипа.
- Консултантската компания не трябва да се явява център за поддръжка работещ денонощно. СУИБ представлява закрита вътрешна система, която се управлява и поддържа от група сътрудници на организацията. Поради тази причина отдалеченият мониторинг на състоянието на средствата за защита на информацията, от страна на консултанта е неприемливо. Планирането на тази дейност обикновено отнема от един до два месеца.

3. Отговорният вътрешен сътрудник разработва блок схема на информационните системи на организацията с нейните връзки. Първоначална схема може да бъде разработена за около седмица, но практиката показва, че тя се доработва и усъвършенства до края на дейността.

4. Екипът детайлно проучва Annex A – списъка с потенциално използваемите контроли. От списъка се подбират тези, които са приложими

за организацията и са актуални към дадения момент. Тази дейност обикновено отнема от два до три месеца.

5. За всяка една от избраните контроли от списъка на Annex A трябва да бъде открита и преработена съответната документация, ако такава съществува, и да се разработят допълнителни политики. Тази дейност обикновено се планира да бъде извършена за три месеца, но понякога това отнема шест.

Примери за формализиране на процеси:

- Политика за проверка на кандидат за работа.
- Политика за отдалечена работа (teleworking).
- Политика за безопасност при работа от мобилни устройства.
- Политика за действия при настъпване на инцидент свързан с информационната безопасност.
- Политика за предоставяне на отдалечен достъп.
- Матрица на отговорностите.
- Политика за инвентаризирането.
- Роли и отговорности при поддържане на отношенията с доставчиците (конкретно за всеки доставчик).
- Политика по отношение на персоналните данни.
- Политика по отношение на проектния мениджмънт.
- Политика по отношение бекап-те и архивирането на информацията.

6. Когато комплектът от документи е готов, той се представя на висшето ръководство на организацията за преглед и утвърждаване. Добра практика е комплектът да се раздели на отделни раздели и блокове (по смисъл) за облекчаване на възприемането и осмислянето. Много често висшия мениджър е зает и тази процедура понякога отнема от един до три месеца.

7. След валидирането на документацията следва да бъде проведена информационна кампания сред всички сътрудници на организацията. В

зависимост от размера на организацията това може да отнеме месец, въпреки че подготовката на лектора отнема около два дни. Запознаването на сътрудниците със СУИБ и с процедурите за подготовка за сертифициране дава възможност да бъде затворена точка A_7.2.2 Awareness, както и да бъде получена обратна връзка за качеството и приложимостта на разработените политики и процедури.

8. Следва внедряване на СУИБ със заповед на висшия мениджър.

9. След определен период от време, обикновено шест месеца, се провежда вътрешен предсертификационен одит и преглед от ръководството за оценяване на резултатите от внедряването, ефективността на процесите и готовността за сертифициране по стандарта.

10. Паралелно с внедряването се провежда процедура за избор на сертифицираща организация – запитвания за оферти от сертифициращи организации, проучване на отзиви за тях, оценяване, ранжиране и избор. Тази дейност отнема около един месец.

11. Сключване на договор със сертифицираща организация и планиране на посещението на одит екип за провеждане на сертфикационен одит. Планирането отнема около месец.

Преди да се пристъпи към сертифициране на системата за управление на информационната сигурност е необходимо да бъде оценена нейната готовност. След попълване на този въпросник полученият резултат ще позволи да бъде направено самооценка на организацията и да бъдат идентифицирано състоянието на процесите свързани с основните изисквания на стандарта.

Таблица 7. *Въпросник за самооценка на готовността на организацията за сертифициране по ISO 27001:2013*

	Да	Не
Контекст на организацията		

Определени ли са външните и вътрешните проблеми, които засягат способността за постигане на желаните резултати от вашата система за управление на информационната безопасност СУИБ?		
Съществува ли начин за редовно наблюдаване и преглеждане на тези проблеми?		
Определени ли са нуждите и очакванията на заинтересовани страни, които имат отношение към СУИБ и те преглеждат ли ги редовно?		
Дефиниран ли е обхвата на използване на разработената СУИБ и отчитат ли се външните и вътрешните проблеми, изискванията на заинтересованите страни и всички останали дейности, които се извършват от други организации?		
Разгледани ли са вътрешните и външните проблеми, които могат да повлияят на СУИБ?		
Ръководството запознато ли е с изискванията на заинтересованите страни, включително регулаторни, законови и тези на клиентите?		
Разгледани и документирани ли са съществуващите рисковете, възможностите и свързаните с тях въпроси и изисквания?		
Анализирано и планирано ли е непрекъснато подобрение?		
Лидерство		
Висшето ръководство декларирало ли е своята отговорност за ефективността на СУИБ и комуникирани ли е важността на ефективната СУИБ?		
Разработена ли е политика и цели на СУИБ, които са съвместими с контекста на средата и стратегическата посока за развитие на организация, утвърдени и оповестени ли са те?		
Утвърдени ли са ролите на сътрудниците. Дефинирани ли са правомощия и отговорности за осигуряване на съответствие и докладване, когато е необходимо?		
Разработена и внедрена ли е програма, която гарантира, че СУИБ ще постигне предвидените резултати, изисквания и цели?		
Планиране		
Определени ли са рисковете и възможностите, които трябва да бъдат оценени и обработени, за да се гарантира, че СУИБ може да постигне планирания(ите) резултат(и)?		
Създаден ли е процес за оценяване на риска за информационната безопасност, който включва критерии за приемливост на риска?		
Разработен, внедрен и работещ ли е процесът за оценяване на риска за информационната безопасност? Повторяем ли е той?		
Регистрират ли се последователни, валидни и сравними резултати?		
Организацията планирала ли е действия за справяне с тези рискове и определила ли е възможности за тяхното интегриране?		
Достатъчен ли е процесът за оценка на риска за информационната безопасност, за да се идентифицират рисковете, свързани със загуба на поверителността, целостта и наличността на информация в обхвата на СУИБ?		
Идентифицирани ли са собствениците на рисковете?		

Анализирани ли са рисковете за информационната безопасност, за да се оцени реалната вероятност и потенциалните последици, които биха се случили, ако възникнат, и определени ли са нивата на рисковете?		
Сравнени ли са рисковете за информационната безопасност с установените критерии за риск и приоритизирани ли са?		
Документирана ли е информацията и налична ли е тя при осъществяването на процеса за оценка на риска за информационната безопасност?		
Процесът на обработване на риска за информационната сигурност позволява ли подходящи опции?		
Определени ли са контроли за прилагане на избраната опция за третиране на риска?		
Определени ли са контролите, сравнени ли са с тези изложени в ISO/IEC 27001:2013 приложение А, за да се провери дали не са пропуснати необходими контроли?		
Разработена ли е декларация за приложимост, за да бъдат обосновани изключенията и включванията на изискванията от приложение А, заедно със състоянието за прилагане на контрола?		
Разработен ли е план за третиране на риска за информационната безопасност?		
• Документиран ли е?		
• Собствениците на риска прегледали и одобрили ли са плана?		
• Разрешени ли са остатъчни рискове за сигурността на информацията от собствениците на рисковете?		
Разработен ли е план за определяне на необходимостта от промени в СУИБ и управление на тяхното прилагане?		
Дефинирани, документирани и съобщени ли са в цялата организация измеримите цели и задачи на СУИБ?		
При определянето на целите си организацията определила ли е какво трябва да бъде извършено, кога и от кого?		
Поддържа		
Организацията определила и осигурила ли е необходимите ресурси, за разработването, внедряването, поддръжката и непрекъснатото усъвършенстване на СУИБ (включително хора, инфраструктура и среда за функциониране на процесите)?		
Разработен ли е дефиниран и документиран процес за определяне на компетентността за заемане на определените роли в СУИБ?		
• Документиран ли е този процес и документирана ли е компетентността на лицата, които заемат тези длъжности?		
Организацията определила ли е компетентността и знанията, които трябва да притежават сътрудниците изпълняващи роли в СУИБ?		
Гарантира ли организацията, че лицата, които пряко могат да повлияят върху дейността и ефективността на СУИБ, притежават необходимата компетентност въз основа на подходящо образование, обучение или опит или е предприела действия, за да гарантира, че тези лица могат да придобият при необходимата компетентност?		
Разработена ли е документираната информация, изисквана от стандарта, и необходима за ефективното внедряване и функциониране на СУИБ?		

Документираната информация контролира ли се по начин, който позволява тя да бъде достъпна и адекватно защитена, разпространявана, съхранявана и с контрол на промените, включително документи с външен произход, изисквани от организацията на СУИБ?		
Операция		
Съхранени ли са документирани доказателства, които показват, че процесите са били извършени по план?		
Има ли план за определяне на необходимостта от промени в СУИБ и управление на тяхното прилагане?		
Когато промените се планират, извършват ли се те по контролиран начин и предприемат ли се действия за смекчаване на неблагоприятните ефекти от прилагането им?		
Ако имате възложени процеси, контролирани ли са по подходящ начин?		
Извършват ли се оценки на риска за информационната безопасност на планирани интервали или когато настъпят значителни промени и съхранява ли се документирана информация за тях?		
Организацията планирала ли е действия за справяне с рисковете и възможностите и интегрирането им в системните процеси?		
Документирани ли са тези действия?		
Оценка на изпълнението		
Дефинирани ли са критерии за оценка, подбор, наблюдение на изпълнението и преоценка на външните, за организацията, доставчици?		
Определено ли е какво трябва да се наблюдава и измерва, кога, от кого, методите, които да бъдат използвани и кога ще бъдат оценени резултатите?		
Резултатите от наблюдението и измерването документирани ли са?		
Провеждат ли се периодично вътрешни одити, за да се провери дали СУИБ е ефективна и съответства, както на ISO/IEC 27001:2013, така и на изискванията на организацията?		
Организацията създала ли е програма за вътрешни одити на СУИБ?		
Резултатите от тези одити докладвани ли са на ръководството, документирани ли са и съхраняват ли се?		
Когато са идентифицирани несъответствия, организацията установила ли е подходящи процеси за управление на несъответствията и свързаните с тях коригиращи действия?		
Висшето ръководство извършва ли редовни и периодични прегледи на СУИБ?		
Резултатът от прегледа на управлението на СУИБ идентифицира ли промени и подобрения?		
Документирани ли са резултатите от Прегледа на ръководството, предприети ли са действия и съобщени ли са те на заинтересованите страни, според ситуацията?		
Подобрение		
Идентифицирани ли са действия за контрол, коригиране и справяне с последствията от откритите несъответствия?		

Оценена ли е необходимостта от действие за отстраняване на основната причина за несъответствията, за да се предотврати повторна им поява?		
Изпълнени ли са някакви идентифициращи действия и прегледани ли са те за ефективност, довели ли са те до подобрения на СУИБ?		
Съхранява ли се документирана информация като доказателство за естеството на несъответствията, предприетите действия и получените резултати?		

15. Проблеми, ограничения и трудности при внедряването на стандарта

Подходът, предлаган от стандарта 27001, също има ограничения. Основното ограничение се състои в ниската детайлизация на изискванията, което води съответно до необходимостта от привличане на опитни експерти на високо ниво за тяхното изпълнение. Това е цената, която трябва да се плати за гъвкавостта и адаптивността на стандарта.

Като друго важно ограничение при внедряването на стандарта може да се яви "тежкият багаж (наследство)" от морално остарели правила и подходи свързани с осигуряването на информационната сигурност. В много компании процесите на управление в течение на много години са били прекалено формализирани и ръководството често не е склонно да предприеме кардинален реинженеринг на системата.

В този случай ключът към успешното изпълнение на изискванията на стандарта е осъзнаването, от страна на ръководството, важността на целите и задачите на информационната сигурност. Без подкрепата на висшето ръководство внедряването на стандарта е невъзможно, тъй в основата за вземане на ключови решения в СУИС лежи готовността да се направят необходимите промени, да се въведат ограничения, да се разпределят финансови и човешки ресурси.

Понякога слабият опит на органите за акредитация в областта на спецификите на въпросите свързани с безопасността на информационните

системи им позволява да акредитират сертифициращи организации, в съответствие със Стандарта ISO/IEC 27006 без те да притежават необходимия опит и квалификация. Това се отразява при провеждането на сертификационните и надзорните одити в частта свързана с интерпретацията на някои точки от стандарта.

Практиката показва, че възникват търговски отношения между клиентите и някои органи за сертификация (закупуване на сертификати, консултации, продукти, услуги), което води до понижаване на нивото на процеса на сертификация и на престижа на сертификата като цяло.

Ограниченото време, което е определено за провеждане на одитите, не позволява задълбочена проверка и анализ на изпълнението на процесите и изискванията на стандарта. Това води да използване на чек-листове и до толяма степен до формализиране на процеса.

Организациите изпитват затруднения при определянето, избора и реализирането конкретните методи при разработването на СУИБ и документацията към нея.

Използването на стандарта не гарантира задължително изключване или понижаване на риска от несанкционирано проникване и кражба на конфиденциална информация. Заинтересованите от такова проникване и придобиване на конфиденциална информация, особено сътрудниците, които работат в самата организация, много добре са запознати с процедурите и правилата и могат сравнително лесно да ги преодолеят.

16. Интегриране на ISO 9001:2015 и ISO 27001:2013

Ако организацията е вече е внедрила ISO 9001:2015, а сега и се налага да добави към нея и ISO 27001, то тогава е добре да бъде изградена интегрирана система за управление на двете системи, в която да бъдат отчетени нормативните изискванията и на двете. Това би довело до

намаляване на времето, което би било изразходвано за внедряване и би довело до сериозно намаляване на разходите за труд за поддръжка на двете системи, както и за поддръжка и осигуряване на съответствието им. В началото е необходимо да бъде разгледано това, което се явява общо и за двата стандарта. Ключово значение тук играе доброто планиране. Проектът за внедряване на интегрирана система за управление се основава на текущото състояние на компанията, от гледна точка на съответствието на изискванията на двата стандарта. Важно е да се отбележи, че се извършва не формална дейност, а се търсят способи за рационализиране на процесите и получаване на предимства в дългосрочна перспектива. Общите точки между ISO 9001 и ISO 27001, в които могат да бъдат открити максимално общи неща, на базата на които може максимално да бъде ускорен процеса на на интегриране са:

- *Контекста на организацията*. И двата стандарта изискват идентифициране на вътрешните и външните въпроси, които имат отношение към организацията, но интерпретирани от различни гледни точки. В ISO 9001 процесите се разглеждат от гледна точка на качеството на продукта/услугата, докато в ISO 27001 се акцентира основно върху състоянието на информационната безопасност.

- *Заинтересовани страни и изпълнение на техните изискванията*. В съответствие със стандартите на ISO, в системите за управление на организация трябва да бъдат дефинирани кои са заинтересованите страни и какви са техните изисквания. Тази дейност може да бъде извършена еднократно и съвместно за двата стандарта. В резултат ще се получи един общ, за двата стандарта (ISO 9001 и ISO 27001) списък на заинтересованите страни.

- *Дефиниране на отговорностите и пълномощията*. Разпределянето на правата и задълженията в СУК и в СУИБ се различават, но изискванията и на двата стандарт в тази област си приличат по това, че и двата стандарта

изискват това да се извършава. За тази цел може да бъде използван един общ метод.

➢ *Компетентност, осведоменост, разпространение на информацията и управление на документацията и на записите.* Тези много на брой изисквания са общи не само за ISO 9001 и ISO 27001, но и за всички стандарти от семейството на ISO. Това дава възможност те да се изпълняват с помощта на един общ унифициран процес и за двата стандарта едновременно.

➢ *Вътрешен одит и Преглед от ръководството.* Този въпрос съвсем не е лесно да бъде решен, защото при различните стандарти съществуват различни изисквания за това: кога е необходимо да се извърши одит, какви да бъдат входовете и изходите в процедурата за вътрешен одит, но въпреки това, методът по който се извършава одитния процес е почти еднакъв и при двата. В зависимост от размера на организацията и сложността на процесите, които се извършват в нея, процесите свързани с вътрешния одит и с Прегледа ръководството могат да бъдат изпълнявани по едно и също време или по отделно.

➢ *Несъответствия и коригиращи действия.* И в ISO 9001, и в ISO 27001 тези дейности трябва да бъдат управлявани. Не съществуват никакви причини тези процеси да бъдат разделяни между СУК и СУИБ, защото, изискванията и на двата стандарта могат да бъдат изпълнени с помощта на общи процеси.

След анализирането на горния списък с това, което обединява ISO 9001 и ISO 27001, естествено се достига до извода, че е необходимо да бъде разработена интегрирана система. От друга гледна точка не трябва да се преминава им другата крайност. Ако на консултантите и на разработващите им се струва, че изискванията на двата стандарта са еднакви и могат да обслужват един общ процес, то това не означава автоматично, че резултатът от този общ процес ще бъде еднакъв и за двете системи – СУК и СУИБ.

Логически следва извода, че резултатите от Прегледа на ръководството, както и входните данни на процесите, ще бъдат различни. Същото може да бъде отбелязано и за всички изброени по-горе общи процеси за двата стандарта.

Допълнителни изисквания в ISO 27001.

Разликите между стандартите ISO 9001 и ISO 27001 при различните системи водят до това те да се допълват една друга. Синергията между двете води до успех на организацията. СУК създава повишава потенциала на организацията, а СУИБ го защитава. Трябва да де отдели сериозно внимание на разликите между стандартите. Основните различия между ISO 9001 и ISO 27001 се намират в Параграфите № 6 и № 8. ISO 27001 допълва интегрираната система със следните специфични изисквания:

- *Оценка риска за информационната безопасност*. Организация трябва разработи методология за оценка и обработка на риска за информационната безопасност. Трябва да се отбележи, че не трябва да се смесват тези рискове, с рисковете, които се оценяват и обработват в съответствие със стандарта за качество ISO 9001. За него тематиката за риска няма такова голямо значение, както за ISO 27001. Поради това прилагането на методики от СУИБ към СУК може до ни доведе до недобри резултати и да доведе до сътресения в организацията.
- *Обработка на рисковете и компенсация в информационната безопасност*. На този процес няма аналог в ISO 9001 и затова той трябва да се изпълнява отделно от интегрираната система. ISO 27001 изисква да бъдат внедрени един или повече (до четири) контролни механизми, които са описани в Приложение А на стандарта.

С помощта на интегрираната система може да се получи троен ефект от обединяването на ресурсите и процесите на двата стандарта. Това позволява да бъда икономисани пари и време, да се подобри системата за управление. Чрез интегрираната система за управление може да се

демонстрира на клиентите, на органите за сертификация и на регулаторните органи добро съответствие, както на ISO 9001, така и на ISO 27001 и прилагането на най-добрите практики към момента. Освен това, интегрирайки СУИБ и СУК може да се постигне конкурентно предимство, тъй като така може да се постигне само високо качество, но и то да бъде защитено. Така се подобрява дейността на организацията, понижават се рисковете и се повишава удовлетвореността на потребителите.

ЗАКЛЮЧЕНИЕ

От стандарта ISO 27001 се очаква да подобри основната дейност на организацията и да съдейства за повишаване на качеството на създавания продукт или услуга. За съжаление много трудно може да бъде доказано и измерено как повишаването на информационната безопасност е довело да понижаване на разходите да извършване на дейността и до повишаване на ефективността на конкретните процеси.

Рекламираното от консултантите „изкачване на компанията на качествено ново ниво" много често не може да бъде постигнато от организациите. Стандартът сертифицира ПРОЦЕСА, а не организацията и още по-важно не нейната система за защита. Това е изключително важно, но често не се осъзнава от мениджмънта. Когато се сертифицира един процес, а в компанията съществуват още много други, които не са, то всеки един от тях могат да се превърне, хипотетично, в „слабо звено“. Много често, дори и от самите мениджъри можете да се чуе "наша организация е сертифицирана по ISO 27001", което показва неразбиране на същия.

Стандартът не дефинира кои точно от процесите трябва да бъдат идентифицирани и сертифицирани, което го прави едновременно универсален, но и много сложен за внедряване в организации, които не притежават съответния опит, квалификация и експертиза. Особено често се подценяват тези процеси, които преминават през всички (или през повечето) от подразделенията. Тези процеси се управляват много сложно, още повече, че управляващите ги много често не се явяват специалисти в областта на информационната безопасност. Специалистите считат, че именно използването именно на тези процеси в хоризонталната, а не във вертикалната структура в организацията и техните собственици отразяват истинската същност на изискуемия процесен подход.

За да се управляват ефективно тези процеси е необходимо собствениците им да притежават достатъчно ресурси, а в случая с управлението на информационната безопасност, това се проявява много ясно – ресурси за нея или липсват или са много ограничени и са недостатъчни за ефективното управление.

Идеята при внедряване на един процес се изразява в постигане на по-добри резултати от тези, които са постигнати към момента. Резултатът се оценява от клиента, не от този който управлява процеса. Ако един процес е внедрен (подобрен) и той се оценява положително от всички други освен от потребителя, то това не оправдава направените разходи. Потребителят ще се стреми по всякакъв възможен начин да го избегне.

Много често мениджърите се концентрират и говорят за процеса и забравят (пропускат) да изтъкнат защо се прави всичко това. Внедряването на процеса заради самия процес е безсмислено начинание. Обикновено се набляга на това, че е получен сертификат за съответствие, а не върху получения като резултат от това подобряване на дейността на компанията, заради което и е бил внедрен процеса. Понякога те не могат да разберат как така, при изпълнени всички изисквания на стандарта, не е налице ефект за компанията или пък той не може да бъде изчислен.

В какво се изразяват трудностите при ефективното внедряване на СИБ и на процесния подход? Трудността се проявява в липсата на ясно дефинирана система, която е ориентирана към получаване на резултат, която съдържа ясно определени конкретни цели и те да бъдат измерими на всеки едни етап от процеса. Трябва да се отбележи, че информационната безопасност се намира в по-тежка ситуация отколкото, например, финансите, които имат някаква отчетни критерии и показатели, с помощта на които се определя тяхната ефективност. В ИБ, обикновено, такива показатели липсват. Още повече, липсва система за оценяване на създаването на ценност за потребителя на всеки етап. В този вид системи е

много важно как ще бъдат избрани целите, които за разлика от финансовите трябва да бъдат по-скоро качествени, отколкото количествени. Тези цели трябва да обхващат всички процеси на информационната безопасност – и стратегическите и операционните.

Цялата тази разработена система ще работи ефективно само тогава, когато са отчетени и се спазват интересите на всички участници във веригата за създаване на ценност. В нея всички цели и показатели за оценяването им са балансирани. Съществува проблем, защото факторите, които имат ценност за потребителя, могат да се окажат няколко, клиентите, звената и процесите също могат да бъдат няколко. Като резултат получаваме сложно преплетени интереси и връзки, които трябва да бъдат балансирани. Решаването на тази задача се усложнява и по други причини.

Процесният подход, който е описан първоначално още в стандарта ISO 9001:2000 е навлязъл широко в дейността на компаниите по света. У нас също се внедрява този подход, но без да се обвързва конкретно с информационната безопасност. Това, което е норма в другите страни, за нас все още се използва непълно или във формализиран вид. От тук произтича още една причина – по-голямата част от консултантите, във връзка с подготовката за сертифициране по ISO 27001, предлагат някакви свои тълкования, трактовки и разбиране на този стандарт. Често срещан случай е консултантска компания, която се състои от 3 до 5 сътрудника, да разработи СУИБ и да подготви за сертифициране организация с 1000 и повече сътрудника, със стотици различни и сложни процеси, за които консултантът не винаги има дори представа.

Добрата практика в развитите държави следва своя логически път – първоначално сертифициране на система за управление на качеството и на процесите в организацията, натрупване на опит за работа в такава система и с философията на стандартите от семейството на ISO и следваща стъпка - управление на информационната безопасност. У нас често се пристъпва към

сертифициране по ISO 27001 без да е натрупан опит и експертиза по по-общи системи за управление или това да се извършва паралелно..

Въпреки сравнително дългата си история на съществуване, ISO 27001 все още не се е превърнал в масов стандарт. Необходимо е време за регулиращите органи, за потребителите и за консултантите.

На 25 май 2018 година Директивата за Общо регулиране на защитата на данните в Европейския съюз (GDPR EC) замени Директивата за защита на данните 95/46/ЕС. Новата директива въвежда редица правила свързани със защитата на персоналните (личните) данни в рамките на Европейския съюз. Внедряването на стандарта ISO/IEC 27001 в голяма степен би съдействало за изпълняването на тези изисквания.

В съвременния свят технологиите и комуникациите се развиват изключително бурно и стават все по-зависими от информационните технологии. В същото време, успоредно с това се увеличават сериозно рисковете и заплахите за организациите и за бизнеса. Стандартът ISO/IEC 27001 става все по-популярен, защото широкото използване на ИКТ в сферата на услугите и на бизнеса като цяло, има критично значение за успеха на организациите. Компаниите все по-широко използват ИКТ услуги от вътрешни и външни доставчици, оптимизират бизнес процесите си чрез аутсорсинг. Цялостното управление на информационната безопасност се превръща в една сложна за решаване задача. Увеличава се изискването за по-високо ниво на качеството на предлаганите услугите и гарантиране, че партньорите осигуряващи и използващи информацията изпълняват утвърдените добри практики. Това се явява сериозен мотив и стимул компаниите да внедряват в своята практика утвърдени добри практики за управлението на информационната безопасност и да сертифицират своите СУИБ в съответствие с международния стандарт ISO/IEC 27001.

БИБЛИОГРАФИЯ

Andress, J. (2014). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice.* Aalborg: Syngress.

Arnason, S. T., Willet, K. D. (2017). Как успешно пройти сертификацию по 27000. Пример применения Compliance Management'a, Auerbach Publications.

Baars, H., Hintzbergen, J., Smulders, A., Hintzbergen, K. (2013). Foundations of Information Security Based on ISO27001 and ISO27002, Van Haren Publishing.

Baars, H., Hintzbergen, K., Hint, J. (2012). Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002, Editora Brasport.

Bitterli, P. R. (2015). Building an ISMS based on ISO/IEC 27001 & ISO/IEC 17799, ISACA.

Bhatia, P. (2018). INTRO TO GDPR. A PLAIN ENGLISH GUIDE TO COMPLIANCE, Advisera Expert Solutions Ltd.

Boehmer, W., Haufe, K., Klipper, S. (2017). Managementsysteme für Informationssicherheit (ISMS) mit DIN EN ISO/IEC 27001 betreiben und verbessern, Beuth.

Brenner, M., Felde, N., Homme, W., Metzger, S. (2017). Praxisbuch ISO/IEC 27001: Management der Informationssicherheit und Vorbereitung auf die Zertifizierung. Zur Norm ISO/IEC 27001:2015, Carl Hanser Verlag GmbH & Co.

Calder, Al. (2008). ISO27001/ISO27002: A Pocket Guide, IT Governance Publishing 2008.

Calder, Al. (2017). Nine Steps to Success: An ISO 27001 Implementation Overview, North American edition, IT Governance Ltd.

Calder, Al., Watkins, S. (2015). IT Governance: An International Guide to Data Security and ISO27001/ISO27002, Kogan Page Publishers.

Calder, Al., Watkins, S. (2017). It Governance: A Manager's Guide to Data Security & BS 7799/ISO 17799 2nd Edition. Kogan Page Publishers.

Calder, Al., Watkins, S. (2019). Information Security Risk Management for ISO 27001/ISO 27002, third edition, IT Governance Ltd.

Cesare Gallotti (2022). Information security - 2022 Edition. Risk management. Management systems. The ISO/IEC 27001:2022 standard. The ISO/IEC 27002:2022 controls. Paperback – February 2, 2022.

Honan, B. (2010). ISO27001 in a Windows Environment: The best practice handbook for a Microsoft® Windows® environment, IT Governance Ltd.

Humphreys, E. (2016). Implementing the ISO/IEC 27001:2013 ISMS Standard, Artech House.

International Organization to Standartization. (2021). *THE ISO SURVEY OF MANAGEMENT SYSTEM STANDARD CERTIFICATIONS – 2022. https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1*.

ISMS Auditor/Lead Auditor Training Course ISO 27001 (2011)., Copyright by ITpreneurs Nederland B.V.

ISO/IEC TR 13335-3. Guidelines for the Management of IT Security: Techniques for the Management of IT Security from International Organization for Standardization. www.iso.org.

Kallmeyer, W. (2022). Der Auditfragenkatalog zur ISO/IEC 27001, TÜV Media GmbH, Köln, 01/2022.

Kersten, H., Klett, G., Reuter, J. (2019) IT-Sicherheitsmanagement nach der neuen ISO 27001: ISMS, Risiken, Kennziffern, Springer.

Kenyon, B. (2019). ISO 27001 controls – A guide to implementing and auditing, IT Governance Ltd.

Klipper, S. (2011). Information Security Risk Management: Risikomanagement mit ISO/IEC 27001, 27005 und 31010, Vieweg+Teubner Verlag |Springer Fachmedien Wiesbaden GmbH.

Kosutic, D. (2018). ISO 27001 RISK MANAGEMENT IN PLAIN ENGLISH. STEP-BY-STEP HANDBOOK FOR INFORMATION SECURITY PRACTITIONERS IN SMALL BUSINESSES, Advisera Expert Solutions Ltd.

Kosutic, D. (2016). SECURE & SIMPLE A SMALL-BUSINESS GUIDE TO IMPLEMENTING ISO 27001 ON YOUR OWN, Advisera Expert Solutions Ltd.

Maziriri, T. (2019). ISO/IEC 27001 Lead Auditor: Mastering ISMS Audit Techniques, Independently Published.

Mooney, T. (2015). Information Security A Practical Guide: Bridging the gap between IT and management, IT Governance Ltd.

National Institute of Standards and Technology. U.S. Department of Commerce (Editor: Kissel, R.). (2019). *NIST Interagency or Internal Report (NISTIR) 7298 Rev. 2, Glossary of Key Information Security Terms.* Washington: U.S. Department of Commerce.

Shipman, Al., Watkins, S. (2020). ISO/IEC 27701:2019: An introduction to privacy information management. Publishers: ITGP.

SP 800-60. Guide to Mapping Types of Information Systems to Security Categories. URL: www.nist.gov.

SP 800-30. Risk Management Guide for Information Technology Systems from NIST [National Institute of Standards and Technology]. URL: www.nist.gov.

Van der Wens, C. (2019). ISO 27001 Handbook: Implementing and Auditing an Information Security Management System in Small and Medium-sized Businesses, Independently Published.

Vasudevan, V. (2008) Application Security in the ISO27001 Environment, IT Governance Ltd.

Williams, B. L. (2013). ISO/IEC 27001, NIST SP 800-53, HIPAA Standard, PCI DSS V2.0, and AUP V5.0, CRC Press Taylor & Francis Group 2013.

Watkins, S. (2013). An Introduction to Information Security and ISO27001:2013: A Pocket Guide, IT Governance Publishing.

Аспекти на информационната сигурност и методи за нейното осигуряване. (н.д.). Извлечено от Интернет списание "Postvai.com". ISSN 2535-0838: https://postvai.com/internet/%D0%B0%D1%81%D0%BF%D0%B5%D0%BA%D1%82%D0%B8-%D0%BD%D0%B0-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%82%D0%B0-

%D1%81%D0%B8%D0%B3%D1%83%D1%80%D0%BD%D0%BE%D1%81.html#_ftn5

Георгиев, К., & Георгиева, П. (2015). Предизвикателства пред иновационната парадигма за осигуряване на интелигентен, устойчив и приобщаващ растеж. *Международна научно-практическа конференция "Устойчиво развитие"* (стр. 5-15). Варна: Международно списание "Устойчивот развитие".

Георгиева, П. (2014). Концепция за ER диаграма на предприемаческа система за планиране на нови продукти. *II международна научно- практическа конференция „Икономика и мениджмънт' 2014"- Устойчиво развитие на бизнеса и регионите"*, (стр. 88-96). Варна.

Димитров, Р. (2018). Насоки за оптимизиране счетоводното отчитане на паричните средства по сметки на бюджетни организации в банките. *Бизнес управление, бр. 1*, 60-77.

Туджаров, Х. (Април 2009 г.). *Въведение в информационната сигурност*. Извлечено от https://www.tuj.asenevtsi.com/: https://www.tuj.asenevtsi.com/Sec2009/Sec01.htm

ИНФОРМАЦИОННА СИГУРНОСТ. СТАНДАРТИ ОТ СЕРИЯТА ISO 27000 – ПЕРСПЕКТИВИ И ПРОБЛЕМИ

МОНОГРАФИЯ

Българска
Първо издание

научен редактор:

доц. д-р Сийка Демирова

Технически университет – Варна

Страници: 188
Формат: 60x84/8
23,5 печатни коли

Издател:

ИК “ACCESS PRESS”, България, 2022

ул. Александър Бурмов 32, 5000 Велико Търново, България

Email: office@access-bg.org

http://www.access-bg.org

ISBN 978-619-91511-9-8

Доц. д-р инж. Пламен Цветанов Павлов работи в катедра „Общо инженерство" при Висшето училище по телекомуникации и пощи – София, където понастоящем е и декан на Факултета по телекомуникации и мениджмънт. През 2007 г. защитава докторат по научна специалност „05.02.21 Организация и управление на производството" пред СНС при ВАК. Академичната му кариера преминава като през 2019 г. печели конкурс за академичната длъжност „доцент" по икономика („Иновации и управление на качеството") във Варненски свободен университет „Черноризец Храбър".

Изследователските му интереси са насочени в областта на управлението на информационната сигурност, управлението на иновациите, качеството и логистиката, риск мениджмънта и др. Автор е на над 45 публикации в тези области.

Води лекции и семинарни занятия по „Бизнес управленски системи", „Управление на информационната сигурност", „Управление на качеството", „Иновационен мениджмънт", „Стопанска логистика", „Логистичен мениджмънт", Управление на риска" и др.