СРАВНИТЕЛЕН АНАЛИЗ НА ПОНЯТИЯТА „ИНФОРМАЦИОННА СИГУРНОСТ“(ИС) И „ЗАЩИТА НА ИНФОРМАЦИЯТА“(ЗИ)

Проф. д-р Иво Великов

Резюме: В тази статия ще се опитаме да дефинираме понятието ЗИ, като го сравним с ИС. Както и да докажем причината за неговото използване. Причината за такова намерение е съвсем проста – двете понятия се използват все по-често, също така често се смесват и като че ли се използват повече машинално и в контекст на синоними.

Винаги сме се колебаели относно мярата между ЗИ и Информационна сигурност като понятия. Търсим както национални, така и чужди мнения и идеи по темата. На първо място обаче е самото понятие „информация“, т.е. обекта на самата защита.

Ключови думи: Сигурност, Информация, Информационна сигурност, Защита на информацията, Комуникационна сигурност, сравнителен анализ, съотношение между ИС и ЗИ.

COMPARATIVE ANALYSIS OF THE CONCEPTS "INFORMATION SECURITY" (IS) AND "INFORMATION PROTECTION" (IP)

Prof. PhD Ivo Velikov

Summary: In this article we will try to define the concept of IP by comparing it with IS. As well as to prove the reason for its use. The reason for this intention is quite simple - the two terms are used more and more often, they are

also often mixed and seem to be used more mechanically and in the context of synonyms.

We have always been hesitant about the measure between IA and Information Security as concepts. We are looking for both national and foreign opinions and ideas on the topic. In the first place, however, is the very concept of "information", ie. the object of protection itself.

Keywords: Security, Information, Information security, Information protection, Communication security, comparative analysis, the relationship between IP and IS.

Стремежът към изясняване на понятията в една определена сфера е ключов за професионализма на експертите. Така те говорят на един свой разбираем език, така притежават и своя организационна култура.[1] Свой език притежават както най-древните, така и най-новите професионални среди. Поради което терминологията в информационната сфера има както нужда, така и достатъчно изследователи:

1. Информация

Информация е:[2]

1. Съобщение, сведение за нещо; осведомяване. *Давам информация. Получавам информация. Източник на информация.*

2. Само ед. Сведения, възприемани и предавани от човека или от специални устройства. *Теория на информацията. прил. информациòнен, информациòнна, информациòнно, мн. информациòнни*.“

[1] В смисъла на Димитрова, Сн., Същност на понятието „организационна култура“ като част от управленската функция „Мотивиране на човешкия фактор“. Годишник том XII, 2015г. ВУСИ, стр.163-172

[2] https://rechnik.chitanka.info/w/%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1% 86%D0%B8%D1%8F (онлайн версия на Български тълковен речник)

Български тълковен речник очевидно доста скромно и лаконично разяснява понятието и в този си опростен вид не може да бъде полезно.

Речник на българския език допълва към т.1 на горното определение:[3]

1. Специална служба в учреждение, която се занимава с даване на необходимите сведения. *Сведения за състоянието на болните се дават в информацията на първия етаж на болницата.*

2. Мястото или помещението, където се намира тази служба.

3. Мат. Основно понятие в кибернетиката, в така наречената теория на информацията, която се стреми да даде количествена характеристика за съдържанието на дадено съобщение. За специалистите обаче, за които често ще се говори по-нататък, информацията има много по-широк смисъл и представлява сигнали, носещи със себе си известни сведения.

(Теория на информацията. Мат. Наука за събиране, предаване, запазване, преобразуване и измерване на информация. Думата „информация" произлиза от латинската дума „informacio", която означава сведение, изложение, разяснение (според Семерджиев произходът е от латинското informare, което в превод означава „придаване на форма"[4]). От фр. information или нем. Information през рус. Информация, така попада и в българския речник)

„Информация е всяка комуникация или представяне на знания като факти, данни или мнения във всякакъв носител или форма, включително текстови, цифрови, графични, картографски, повествователни или аудиовизуални.[5]

---

[3] https://ibl.bas.bg/rbe/lang/bg/%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1% 86%D0%B8%D1%8F/ (онлайн версия на Речник на българския език)

[4] Семерджиев, Ц., Митев, Н., Информационна сигурност, Софттрейд, 2015 г., стр. 20

[5] CNSSI-4009, Инструкция 4009 на Committee on National Security Systems(CNSS) – Glossary, 2015 г.

Информация (кибернетично тълкуване) е съвкупност от сведения, свързани с изменението на състоянието на материалните обекти и възприемането на тези изменения чрез други обекти посредством метода на отражението. Количествена мярка на изменението на материалните обекти.
Информация (според теория на информацията) е съвкупност от сведения за обектите и явленията на материалния свят, разглеждани в аспекта на тяхното предаване в пространството и времето под формата на съобщения и с помощта на сигнали.

Очевидно е, че горните определения показват информацията като обективно свойство на материята. Информацията съществува във всеки материален обект като многообразие на неговите състояния и може да се създава, унищожава, предава, приема, съхранява и обработва. Съществуването на информацията като обективно свойство на материята произтича от нейните фундаментални свойства – структурност, непрекъснато изменение (движение) и взаимодействие между материалните обекти.

Информацията съществува извън нас, постижима е, не при надлежи на никого, тъй като обективно не може да бъде заличена, не може да не съществува.

Всяко представяне на информация за обект или процес върху физически носител се нарича **съобщение**.

„Едно и също информационно съобщение (статия във вестник, обява, писмо, телеграма, справка, разказ, чертеж, радиопредаване и др.) може да съдържа различно количество информация за различните хора в зависимост от натрупаните им знания, от нивото на разбиране на това съобщение и от интереса към него. Така съобщението съставено на японски език не носи някаква нова информация за човек, незнаещ този език, но може би е

високоинформативно за човек, владеещ японски. Никаква нова информация не съдържа и съобщение, изложено на познат език, ако неговото съдържание е непонятно или е вече известно.

Информацията е характеристика не на съобщението, а на съотношението между съобщението и неговите потребители. Без наличието на потребител, дори и потенциален, да се говори за информация е безсмислено.“[6]

Видове информация:[7]

Според начина на получаване:

- Отразена информация –информация, която хората събират чрез сетивата си и съхраняват и обработват в съзнанието си, като използват собствените си умствени възможности. Тази информация не е достъпна непосредствено за други лица. Очевидно тази информация може да бъде визуална, слухова, сензитивна при досег(тактилна), вкусова, обонятелна.

- Материализирана информация –информация, представена върху физически носители. Може да се използва от всеки човек. Именно тя е предмет на науката информатика (тя е и съществен елемент от ЗИ – б.а.).

Според източника:

- Първична (пряка) информация – получена непосредствено от контакт с обекта на интерес;

- Вторична (непряка, опосредствана) информация – получена чрез опосредстване и предаване от друг субект;

- Третична (обобщена, обработена, анализирана) – най-често анализирана информация, която носи ново качество. (б.а. – с последната

[6] https://pomagalo1.com/art/informaciq-ponqtie-za-informaciq-vidove-informaciq-1/35547
[7] http://www.daskalo.com/dobreva20152016/files/2015/11/1-%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F-%D0%B8-%D0%B8%D0%BD%D1%84-%D0%B4%D0%B5%D0%B9%D0%BD%D0%BE%D1%81%D1%82%D0%B8.pdf

наша класификация не ангажираме никого, просто тя ни служи в хода на изследването, т.като при защитата трябва да се съобразяваме с характера на източниците на информация).

Има четири основни вида информационни дейности:

- събиране на информация –търсене на източници на информация, подбирането й по дадени критерии и първична регистрация;
- съхраняване на информация –за пренасянето й във времето е необходима да се оформи, подреди и структурира, за да се осъществи лесен достъп до нея;
- преработване на информация –чрез анализ и синтез се извлича нова информация;
- разпространение на информация –привеждане на информацията в подходяща форма и предоставянето й на заинтересованите получатели.

Горните данни ни служат единствено и само да очертаем парадигмата на понятието информация, т.е. от гледна точка на ЗИ да създадем представата за „информация“ и онези характеристики и страни, които могат да ни служат при нейната защита:

1) Информацията е обективно свойство на материята. Информацията съществува във всеки материален обект като многообразие на неговите състояния и може да се създава, унищожава, предава, приема, съхранява и обработва. Т.е. в смисъла на диалектиката, тя (информацията) се изменя непрекъснато. В контекста на ЗИ трябва да имаме предвид отделните възможни въздействия (създаване, унищожаване и т.н.), като се предвиждат защити при провеждането на всяко действие (които малко по-горе определихме като 4 на брой). Поради което всеки нормативен акт разглежда защитата като „система от мерки“;

2) Информацията съществува извън нас, не принадлежи на никого. Обективно не може да бъде заличена, не може да не съществува. Това положение означава, че абсолютна тайна не може да има, но в следствие на това ЗИ може да се прилага за всяка информация, и спрямо всеки потребител, който проявява интерес. Без наличието на потребител/интерес, дори и потенциален, да се говори за информация, вкл. и за ЗИ е безсмислено;

3) ЗИ разглежда като предмет за защита както отразената, така и материализираната информация. В огромната част от случаите мерките за защита са изпреварващо по отношение на самите носители на информацията (дали са хора, които чрез сензорите са я възприели, или са други физически носители – хартия, дърво, кожа, каменни плочи, дискове, дискети, ,магнитни ленти, аналогови ленти, флаш-памети, физични полета и сигнали и т.н.), и след това на самите съобщения;

4) ЗИ разглежда като обект на защита и първична и вторична информация, т.като са в основата на третичната. Първичната и вторична информация носят познание, третичната – много повече знание (осъзнато и обработено познание). За повече яснота ще дадем пример с разузнаването: „За ЦРУ разузнаването се дефинира като „знание или изпреварващо знание (от англ. – knowledge) за релевантните аспекти на заобикалящия свят, което се използва от политици и военни ръководители за вземане на решения“ (преводът наш – б.а.). Не е съвсем вярно обаче, че разузнаването е директно свързано със знание. По-голямата част от определенията твърдят, че разузнаването е информиране или информационна дейност (т.е. във философски план стои по-близо до понятието „познание“). За да бъде наистина „знание“, е необходимо познаване на обхват, начин на добиване, истинност (достоверност) на информацията, и дори „обоснована истинска

вяра“ (цитираме по памет диалозите на Платон). В този смисъл разузнаването може да бъде знание, когато информацията е проверена, доказана като достоверна, известни са методите на придобиване и сме убедени, че представя действителността по най-точен начин. Това положение изисква информацията да е проверена, а самата тя да бъде в подходяща форма (обработена чрез първичен анализ, дешифрирана, декриптирана, преведена), за да може да бъде анализирана и възприета като знание. Информацията от разузнаването, особено когато е придобита от негласни източници, често не може да се провери или не може да се провери в необходимите разумни срокове, или се проверява, когато събитията или явленията, които третира, са вече отминали. В този смисъл такава информация да се нарича „знание“ е твърде амбициозно. Да не говорим и за факта, че чрез разузнаване може да не се получи знание или да се получи погрешно, невярно информиране, което не е знание в истинския смисъл на думата.“[8] Така и при ЗИ, абсолютно по подобие на разузнаването, имаме информация, която е познание (най-често на първо познавателно ниво – „Къде и какво?“), а при знанието – на второ познавателно ниво – „Защо и как?“, т.е. търсене на причинно-следствени връзки. И двете нива обаче се защитават, т.като са взаимно свързани и обусловени. Логично е третичната (обработена и анализирана информация) да представлява най-съществена ценност и да има повече качество, с което да предизвиква и най-сериозен интерес от всякакви потребители. Логично е също такава информация да бъде най-ревниво и прилежно защитена. По-късно ще представим и едно съществено свойство на третичната информация – трансформацията на нейната стойност и качество, т.е. има обосновани данни, че обработената информация може значително да повиши своето значение.

[8] Великов, И., Кратка теория на разузнаването, Албатрос, 2017 г., стр. 56-57

Горните данни използваме за да дефинираме понятието ЗИ.

ЗИ е достатъчно често срещано понятие, има обаче нееднородно тълкуване. И множество преплитания с понятието информационна сигурност.

Информационна сигурност в САЩ е:[9]

„**Защитата на информацията** и информационните системи от неоторизиран достъп, използване, разкриване, нарушаване, модифициране или унищожаване с цел осигуряване на поверителност, целостта и достъпността.

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.“

Всъщност двете понятия ИС и ЗИ неминуемо са синонимни, взаимно се допълват и взаимно се обуславят. Още при този превод се вижда:

- Дефинирането на едното понятие не може да става без да се използва другото;
- Дефинирането в никакъв случай не става с кратка, точна и ясна дефиниция, каквато биха изисквали широкия кръг от експерти и

[9] NIST Interagency or Internal Report (NISTIR) 7298 Rev. 2, Glossary of Key Information Security Terms, 2019 г., стр. 94

специалисти, най-вече поради сложната многообразна и многопосочна същност на информационната сигурност.

Във същия източник (стр.96) и съгласувано със CNSSI-4009:

„**Политика за информационна сигурност** - Съвкупност от директиви, регламенти, правила и практики, които предписват как организацията управлява, защитава и разпространява информация.

Риск за информационната сигурност - Рискът за организационни дейности и операции (включително мисия, функции, имидж, репутация), организационни активи, лица, други организации и нацията поради потенциал за неоторизиран достъп, използване, разкриване, нарушаване, модификация или унищожаване на информация и/или информационни системи.

Риск - Нивото на въздействие върху организационните операции (включително мисия, функции, имидж или репутация), организационни активи, лица, други организации или нация, произтичащи от функционирането на информационна система, предвид потенциалното **въздействие** на заплаха и **вероятността** за тази възникваща заплаха.“

Следващи изводи, произтичащи от близки и свързани с ИС определения от Речника на NIST (Националния институт за стандартизация и технологии) и Инструкция CNSSI-4009:

- Дефинициите определено са познати в средите на нашите специалисти в областта на сигурността и информационните технологии. Откриваме подобни публикации от страна на такива, вкл. учени и практици, вкл. ИТ компании в български сайтове и източници. Очевидно както нормативната основа у нас, така и експерти и специалисти са взаимствали някаква част от подобни американски източници;

- Има определен технически и технологичен уклон в понятието „информационна сигурност“. Всички други мерки (физически, персонални, документални и т.н.) са в контекста на функционирането на информационната система на организацията, и тя се основава изключително на комуникационно-информационната система и нейната защитеност. За верността на горното, имаме потвърждение от множество експерти, като информационната сигурност главно и почти единствено се разбира като основана на общоприети и на практика задължителни правила. Такива правила са прогласени със стандартите ISO (в нашия случай – от типа ISO 27 000 и следващите го). Към момента тези стандарти са:[10] (б.а. – правим възможно най-точно изброяване, т.като то само по себе си дава представа за обхвата на ИС)

- ISO/IEC 27000:2020 - Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Общ преглед и речник;
- ISO/IEC 27001:2017 Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Изисквания;
- ISO/IEC 27002:2017 - Информационни технологии. Методи за сигурност. Кодекс за добра практика за управление на сигурността на информацията;
- БДС ISO/IEC 27003:2020 - Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Указания;
- БДС ISO/IEC 27004:2017 - Информационни технологии. Методи за сигурност. Управление на сигурността на информацията. Наблюдение, измерване, анализ и оценяване;

[10] https://www.bds-bg.org/standard/index.php?standard_code=270&item_from=120

- БДС ISO/IEC 27005:2018 - Информационни технологии. Методи за сигурност. Управление на риска за сигурността на информацията;
- ISO/IEC 27011:2020 - Информационни технологии. Методи за сигурност. Указания за управление на сигурността на информацията за телекомуникационни организации, базирани на ISO/IEC 27002;
- БДС ISO/IEC 27013:2015 - Информационни технологии. Методи за сигурност. Указания за съвместно внедряване на ISO/IEC 27001 и ISO/IEC 20000-1;
- ISO/IEC 27018:2020 - Информационни технологии. Методи за сигурност. Кодекс за добра практика за защита на личната информация за идентифициране (ЛИИ) в обществени облаци, действащи като обработващи лични данни;
- ISO/IEC 27019:2020 - Информационни технологии. Методи за сигурност. Механизми за контрол на сигурността на информацията за енергоразпределителната индустрия;
- БДС ISO/IEC 27031:2016 - Информационни технологии. Методи за сигурност. Указания за готовност на информационните и комуникационните технологии за непрекъснатост на дейността;
- БДС ISO/IEC 27035-1:2016 - Информационни технологии. Методи за сигурност. Управление на инциденти, свързани със сигурността на информацията. Част 1: Принципи за управление на инциденти;
- БДС ISO/IEC 27035-2:2016 - Информационни технологии. Методи за сигурност. Управление на инциденти, свързани със сигурността на информацията. Част 2: Указания за планиране и подготовка за реагиране при инциденти;

- ISO/IEC 27037:2016 - Информационни технологии. Методи за сигурност. Указания за идентифициране, събиране, придобиване и съхранение на цифрови доказателства;
- ISO/IEC 27038:2016 - Информационни технологии. Методи за сигурност. Спецификация за цифрово редактиране;
- ISO/IEC 27040:2016 - Информационни технологии. Методи за сигурност. Сигурност на съхранението;
- ISO/IEC 27041:2016 - Информационни технологии. Методи за сигурност. Указания за осигуряване на пригодност и адекватност на метод за разследване на инцидент;
- ISO/IEC 27042:2016 - Информационни технологии. Методи за сигурност. Указания за анализ и тълкуване на цифрови доказателства;
- ISO/IEC 27043:2016 - Информационни технологии. Методи за сигурност. Принципи за разследване на инциденти и процеси;
- **БДС ISO 2709:2011 - Информация и документация. Формат за обмен на информация.**

Очевидно само последният стандарт (б.а. – с различна идентификация, поради което е с болд) няма пряко отношение към информационни технологии и по-скоро не е част от тази доста често актуализирана, внимателно анализирана и съответно – развивана, система на информационната сигурност.

В подкрепа на последното твърдение имаме още:

Стандарт (дефиниция)[11] - Правило, условие или изискване:

(1) Описване на следната информация за продукти, системи, услуги или практики:

[11] Information security, NIST Special Publication 800-66 Revision 1, 2008 г., приложение А, стр.6

(I) Класификация на компонентите.

(II) Спецификация на материали, експлоатационни характеристики или операции; или

(III) Разграничаване на процедурите; или

(2) По отношение на конфиденциалността на индивидуално идентифицираната информация.

От казаното до тук става ясно, че ИС е достатъчно широко, сложно и динамично понятие, което има своите проекции във всяка дейност в областта на ЗИ. Освен това, то също като ЗИ е достатъчно добре аргументирано с множество нормативни актове, основани на стандартите и за въвеждане на стандартизацията. Близката връзка на ИС и ЗИ произтича и от необходимостта и при двете понятия да има разписани (б.а. - стандартни) процедури и механизми както за работа с информационните системи, така и за защита на информацията в тях. За да изразим най-добре връзката на ЗИ и ИС, ще използваме за сравнението и трето понятие – Комуникационна сигурност.

2. Комуникационна сигурност - (COMSEC) - Компонент на Информационното осигуряване (б.а. – не сигурност е използван като термин (security, а assurance)), който се занимава с мерки и контрол, предприети за отказ на неупълномощени лица на достъп до информация, получена от телекомуникациите и за гарантиране на автентичността на такива телекомуникации. COMSEC включва **криптосигурност, сигурност на предаването, сигурност на емисиите и физическа сигурност на COMSEC материали**.[12]

[12] NIST Interagency or Internal Report (NISTIR) 7298 Rev. 2, Glossary of Key Information Security Terms, 2019 г., стр. 38

Комсек в този случай, по дефиниция и по съдържание е елемент на ИС. Тя е достатъчно развита в стандарти, като технологичните решения са в нейната основа. През 2020 г. за определени мероприятия подготвихме превод с обработка и коментари на Регламент 4300B.200 - Communications Security (COMSEC - Version 3, 2016 г.) на Министерството на вътрешната сигурност на САЩ. Това е нов и модерен документ, който с малки изключения урежда политиката в тази сфера на практика за цялата държавна администрация на САЩ. Версията от 2016 г. ме заинтригува поради своята актуалност, поради изчистената си и максимално ясна структура, както и поради очевидната си практичност, повсевместност и приложимост. За последните две качества по-скоро трябва да потърсим практиците в ИТ – сектора, но е факт, че терминологията и най-новите разпоредби в нашата страна се доближават максимално и дори в определени части са директно заимствани от американската нормативна уредба.[13]

Изводи от превода на Инструкцията Комсек 4300 на САЩ: (б.а. – от цялата студия предлагаме само крайните изводи, т.като представят целта и съдържанието на този регламент по най-достъпен начин)

1. Необходими са указания чрез нарочни документи за покриване на минимални стандарти по защита на информацията. Тези документи задават точно минималните стандарти. Не се задължава никой, но и не се ограничават организациите след покриването на минималните стандарти да повишават и подобряват защитата на материалите и ключовете за тях чрез повишаване на изискванията и покриване на допълнителни критерии. Тази политика се установява от държавата, т.като там се намират очевидно най-сериозните аналитични способности и познаване на средата за сигурност. С

[13] Великов, И., Комуникационна сигурност, Сборник научни трудове MATTEX 2020, Университетско издателство „ Епископ К.Преславски“ – Шумен, 2020 г., ISSN& 1314-3921, стр.3-62

тези политики се задължават и всички органи и институции, които са контрактори на държавата или по някаква причина трябва да работят със защитена информация;

2. Допускат се различни варианти на съхранение на материали и ключовете към тях, но с ясно и категорично съобразяване с нивото на защитената информация и съответните минимални стандарти;

3. Няма никакви указания или предписания какви/откъде трябва да бъдат технологиите или самите устройства, които се използват. Т.е. от пазара може да се вземе това, което е най-подходящо за конкретния случай. Материалите и устройствата просто трябва да отговарят на минималните определени стандарти за сигурност. В редките случаи, когато се препоръчва някакво устройство, се препоръчват поне няколко разновидности. Пример са устройствата за достъп: Federal/DoD Public Key Infrastructure (PKI), Personal Identity Verification (PIV), или Common Access Card (CAC);

4. Двойният ТПИ (TPI – Two Person Integrity) контрол над използваните криптографски кодове и ключове намалява до минимум възможността за злоупотреби, нарушения и грешки при тяхното използване. У нас такъв контрол не се използва, поне за сега;

5. Изключително гъвкаво се използват комбинации от класифицирани и некласифицирани (но с ограничен публичен достъп) обозначения на материали и съответните мерки за защита. Т.е. от една страна се търси ограничаване на достъпа до ключове и кодове, вкл. и до информация от високо ниво на защита чрез класифициране на информация и достъп, от друга – използване на по-широка експертиза в полза на защитата, на самата информация и на процедури за осведомяване на професионалисти и заинтересовани, като не им се дава знание за заключването, предаването, съхранението и вида на информацията, чрез обозначенията

НЕКЛАСИФИЦИРАНО или ЗА ОФИЦИАЛНО ИЗПОЛЗВАНЕ. Тази система напомня в известна степен на съществуващата у нас преди 2002 г., когато всяко ведомство създаваше своя система за защита на различните тайни от публичен достъп по своите нужди с подзаконов нормативен акт;

6. Очевидно е, че контролът е по всяко време и повсеместен. У нас за обучение се правят протоколи в свободна форма на всяка организация, тук се водят дневници по образец и се съхраняват непрекъснато. Тук достъпът до материалите (кодове и ключове) се защитава най-малко на същото ниво като самите материали, като многократно се подчертава този факт, ние също го имаме като текст в ЗЗКИ, но съхранението на ключове за помещения, компютърни пароли, ключове за РАК-шкафове и т.н. не се спазва толкова стриктно. Отчетността и строгата отговорност при получаване на достъп до кодове и ключове за криптиране разшифроване тук е очевидно по-сериозна. Всъщност защитата на ключовете е по-лесно реализируема, т.като става дума за ограничен брой обекти за защита, държавата не може да контролира самите ползватели толкова ефективно през работно и още повече в извънработно време, но може да „закове“ процедурите по използването;

7. Много подробно са разписани някои ключови процедури като приемане на материали на ръка, сдаване, съответно приемане на длъжности като Комсек мениджър, инвентаризация, ангажименти на изходящия мениджър и т.н. Вниманието на процедурата по сдаване/приемане на длъжности по защита на информацията очевидно се счита за критична по отношение на сигурността. В такива текстове документът прилича много повече на наръчник;

8. Подробно са разработени варианти за действие при критични и кризисни ситуации, при компрометиране на сигурността. Тези варианти са много полезни в извънредни положения, при бедствия, аварии и катастрофи,

при преместване на офиси и помещения на организацията и дори при масово текучество на кадри. Отново имаме прилика с наръчник за действие с прости и ясни последователности от действия;

9. Правилата, създадени в този документ в огромната си част са превърнати в стандарти, т.е. в някои случаи това дори е директно заявено (напр. в §7.8., където за унищожаването са заявени „необходими национални стандарти за Комсек“). Такова отношение към настоящия документ показва възприемането му като норма/закон, дори догма по отношение на комуникационната сигурност;

10. Изключително внимание се обръща на унищожаването на материали и информация. Редът и изискванията са строги, но методите са многобройни, съобразени със съответните физически носители на информацията. При спазване на процедурата се търси ефективен краен резултат, а самите методи на унищожаване не са толкова важни и могат да бъдат импровизирани, в зависимост от ситуацията;

11. Вероятен общ извод от този документ е: защитата на информация се гради на нивото на потребителите с най-ниска квалификация, т.е. защитата на информацията чрез Комсек трябва да е понятна и достъпна на абсолютно всички лица, които имат достъп до защитена така. Тук няма място за самопроизволни действия или някакво особено творчество. Опирайки се на традициите на прецедентното право в САЩ очевидно е извършена огромна събирателна и аналитична работа, изследвани са множество случаи (това е просто очевидно при вмъкваните забележки и забрани в текстовете тук, както и при приложенията по-долу към документа) и добри практики;

12. Министерството на вътрешната сигурност е създадено непосредствено след атентатите от 9/11 през 2001 г. То представлява най-голямата административна реформа в САЩ след Втората световна война.

Очевидната му връзка с атентатите е изисквала нови и ултрасъвременни подходи както към защитата на необходимата информация, така и към нейното своевременно разпространение и предаване към съответните органи за предотвратяване на преки или косвени заплахи за територията или гражданите на страната. Този последен факт е причина за формата и съдържанието на документа. Поради което този документ още е и елемент от една сериозна и мащабна нормотворческа тенденция в началото на века.

Доколкото не трябва да се възприема едно единствено становище (дори и на най-напредналата в информационно отношение държава – САЩ), потърсихме и аналогични източници в Русия. Без изненада откриваме, че терминологията е просто достатъчно еднаква като тази в САЩ, т.е. специалистите в ИТ сектора имат достатъчно връзка и са намерили достатъчно професионализъм, за да овладеят и да използват речник, който е универсален и се разбира навсякъде.

3. Информационна сигурност и защита на информацията в Русия

Изненадата е по отношение на мярата между ИС и ЗИ. „Информационна сигурност (английска Information Security, както и също - английски InfoSec) – е практиката за предотвратяване на неоторизиран достъп, използване, разкриване, изкривяване, модификация, проучване, запис или унищожаване на информация. Тази универсална концепция се прилага независимо от формата, която данните могат да приемат (електронна или, например, физическа). **Основната задача на информационната сигурност е балансирана защита на поверителността, целостта и наличността/достъпността** (б.а. – достъпност добавихме като синоним за да съпоставим с американското разбиране по-горе, както и на практика да се забележи безспорното пълно подобие) на данни, като се вземе предвид целесъобразността на приложението и без никакви увреждания на работата

на организацията. Това се постига предимно чрез многостепенен процес на управление на риска, който идентифицира дълготрайни активи и нематериални активи, източници на заплахи, уязвимости, потенциална експозиция и възможности за управление на риска. Този процес е придружен от оценка на ефективността на плана за управление на риска.

За да стандартизират тази дейност, научните и професионални общности са в постоянно сътрудничество, насочено към разработването на основна методология, политики и индустриални стандарти в областта на техническите мерки за защита на информацията, правната отговорност и стандартите за обучение на потребители и администратори. Тази стандартизация е до голяма степен повлияна от широк кръг закони и разпоредби, които регулират начина на достъп, обработка, съхранение и предаване на данни. Прилагането на каквито и да било стандарти и методологии в дадена организация може да има повърхностен ефект само ако културата на непрекъснато усъвършенстване не е правилно внедрена.“[14] Горната информация не претендира за научност, т.като е от Уикипедия на руски език. Не бива обаче да се отказваме от този най-широк източник, просто защото той наистина съвпада с разбирането за „информационна сигурност“ до момента в САЩ.

Информационната сигурност се основава на дейности за защита на информацията - осигуряване на нейната поверителност, достъпност и цялост, както и предотвратяване на всякакво компрометиране в критична ситуация. Такива ситуации включват природни, причинени от човека и социални бедствия, компютърни откази, физически отвличания и други подобни. Въпреки че воденето на архиви на повечето организации в

[14]https://ru.wikipedia.org/wiki/%D0%98%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%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C

света все още се основава на хартиени документи, изискващи подходящи мерки за информационна сигурност, нараства броят на инициативите за въвеждане на цифрови технологии в предприятията, което води до ангажиране на специалисти по сигурността на информационните технологии (ИТ) за защита на информацията. Тези специалисти осигуряват информационна сигурност на технологиите (в повечето случаи някакъв вид компютърни системи). Трябва да се отбележи, че компютър в този контекст означава не само битов персонален компютър, но цифрови устройства с всякаква сложност и предназначение, вариращи от примитивни и изолирани, като електронни калкулатори и домакински уреди, до индустриални системи за управление и суперкомпютри, свързани с компютърни мрежи. Най-големите предприятия и организации, поради жизненоважната важност и стойност на информацията за своя бизнес, наемат специалисти по информационна сигурност, като правило, като собствен персонал. Тяхната задача е да защитят всички технологии от злонамерени кибератаки, често насочени към кражба на поверителна конфиденциална информация или прихващане на контрол върху вътрешните системи на организацията.

Информационната сигурност като сфера на заетост се развива и нараства значително през последните години. Тя е породила много професионални специализации, като мрежова и свързана с нея инфраструктура, сигурност на софтуер и бази данни, одит на информационни системи, планиране на непрекъснатостта на бизнеса, електронно откриване на записи и компютърна криминалистика. Специалистите по информационна сигурност имат много стабилна заетост и голямо търсене на пазара на труда. Мащабни проучвания, проведени от организацията (ISC) [2], показват, че през 2017 г. 66% от лидерите на информационната сигурност са признали остър недостиг на работна ръка в

своите подразделения, а според прогнозите до 2022 г. недостигът на специалисти в тази област ще възлезе на 1 800 000 души по целия свят[15].

„**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.“

„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** .

Защитата на информацията е набор от мерки, насочени към гарантиране на поверителността и целостта на обработваната информация, както и на наличността/достъпността на информация за потребителите.“[16]

---

[15] Andress, J. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. — Syngress, 2014. — 240 стр. — ISBN 9780128008126

[16] http://www.aup.ru/books/m6/8_4.htm - Асаул, А.Н., Организация предпринимательской деятельности, Учебник. СПб.: АНО ИПЭВ, 2009. 336с (глава Пета - Безопасность предпринимательской деятельности
5.4. Информационная безопасность)

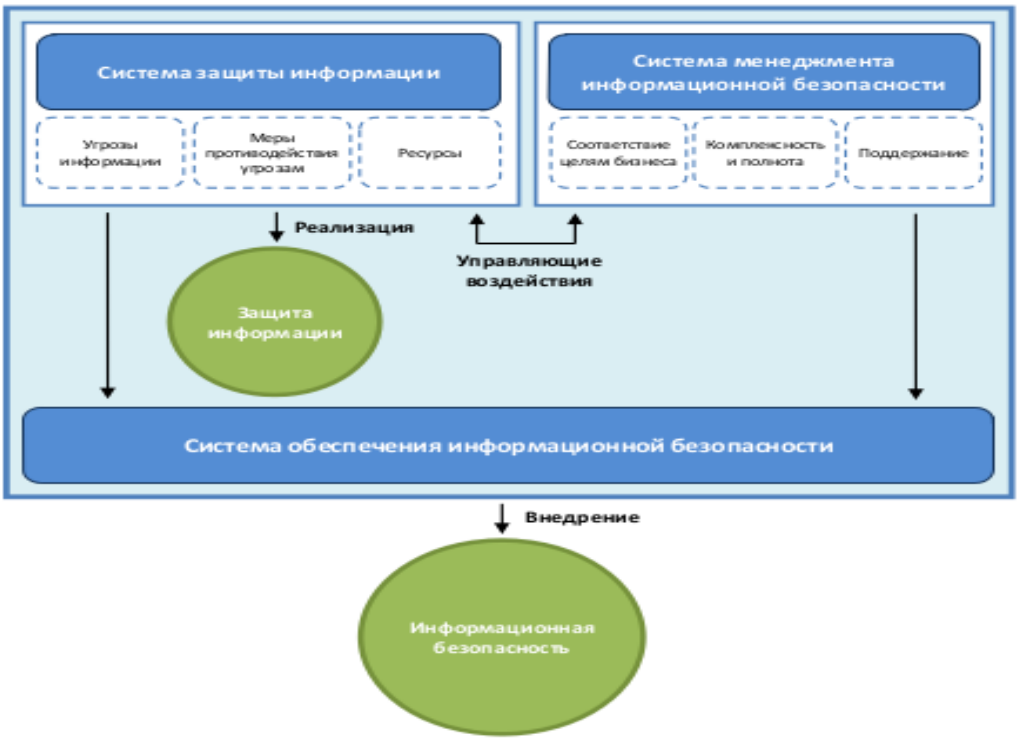
От казаното до тук според руските източници следват най-малко два важни извода:

- Съвпадението на смисъла и терминологията с всички други изследвани източници е безспорно;
- Има категорично разширително разбиране за ИС (на първо място като разширява/развива непрекъснато обхвата на мерки, процедури и дейности, и на второ място – като надхвърля разбирането за ИС над определението за ЗИ (което определение категорично ни се струва по-широко и общо, както и по-обхватната политика, включваща не само специалисти и експерти, или изпълнители в работата с информационни технологии, но и всички служители от всяко ниво в организациите). Че стремежът към непрекъснато разширяване на обхвата на ИС съществува, това е ясно и видимо, особено по отношение на разширяващото се нормативно уреждане чрез стандартите ISO, които обхващат все повече от полето на ЗИ и го универсализират. Бегъл поглед върху стандартите показва, че всички са развити или доразвити след 2016 г., но много от тях и през 2020 г.

Тук въпросите идват директно: ЗИ изглежда по-абстрактна и предполага по дефиниция по-широк поглед. Тогава как ИС е ЗИ плюс защита на поддържаща инфраструктура? Защитата на инфраструктурата не е ли и ЗИ? А дали не разменяме понятията ЗИ и ИС? Или най-малкото преводът на двете безспорно близки и синонимни понятия да ни пречи за правилното им разбиране?

Нещо повече, има източници на руски език, които се опитват да направят сравнение на ИС и ЗИ, като старателно са изведени дефиниции отвсякъде в руски нормативни и научни източници, вкл. държавен стандарт на Руската федерация. Налице са 8 дефиниции за информационна сигурност (б.а. – прави се разлика от „сигурност на информацията“), 3 дефиниции за защита на информацията, които не казват нищо ново. Продължава обаче да се твърди, и дори схематично е представено, че Система за ЗИ + Система за

управление на ИС създават съвместно Системата за информационна сигурност. Не се съгласяваме, най-вече поради изкуственото отделяне на Система за управление на ИС (мениджмънт на ИС) от самата ИС, както и поставянето на системата за управление в подчинено йерархично положение:[17]Ако мениджмънта на ИС е отделна система, то технологичната и експертна част също би трябвало да бъде отделна система:



Съвсем кратък поглед върху горната схема, позволява да бъде отхвърлена като погрешна.

„Възможно е да се определи системата за **информационна сигурност** като **организиран набор от органи, средства, методи и мерки за защита на информацията от разкриване, изтичане и неоторизиран**

[17] https://www.securitylab.ru/blog/personal/aguryanov/29946.php

достъп.“[18] По това определение обаче идва само един извод: Система за информационна сигурност= ЗИ. Следващите текстове също го подсказват: Последователността на действията при разработването на обектна система за информационна сигурност. **Преди да се пристъпи към разработването на система за информационна сигурност, е необходимо да се определи какво е интелектуална собственост** за организацията (или физическо лице)(б.а. – а самото определяне е ЗИ, още повече, че се признава, че това е необходимо действие **преди** самата система за ИС).

… Именно с това трябва да започнем създаването на система за защита на информацията. Тогава, **независимо от размера на организацията и спецификата на нейната информационна система,** е необходимо:

- определяне на границите на управлението на информационната сигурност на съоръжението (б.а. - това е само по себе си мярка на ЗИ, най-малкото в ЗЗКИ и ЗЗЛД тези граници са определени изключително точно);

- провеждане на анализ на уязвимостта (б.а. – има го и при ЗИ и при ИС);

- изберете контрамерки за осигуряване на информационна сигурност (б.а. – това също е ЗИ, макар че и при определени дейности ИС);

- определя политиката за информационна сигурност;

- проверете системата за защита;

- изготвяне на план за защита;

- прилагане на план за сигурност (управление на сигурността).

(последните 4 изисквания са както ИС, така и ЗИ,

[18] Асаул, А.Н., Организация предпринимательской деятельности, Учебник. СПб.: АНО ИПЭВ, 2009. 336с (глава Пета - Безопасность предпринимательской деятельности, 5.4. Информационная безопасность)

Към първото изискване в горната класификация: Определяне на границите на управлението на информационната сигурност на обект. Целта на този етап е да идентифицира всички възможни „болезнени точки“ на обекта, които могат да създадат неприятности от гледна точка на сигурността на информационните ресурси, които имат определена стойност за организацията.

За работа на този етап трябва да се събере следната информация:

1. Списък на информация, представляваща търговска или служебна тайна.

2. Организационна и щатна структура на организацията… (б.а. – следват още 4 изисквания, които се свързват непосредствено с ИС - използваните политики, схеми, технологии, процедури, но тези първи две неминуемо се свързват с дейността и ангажиментите на абсолютно всички служители, и те не са ИС по смисъла на поверителност, достъпност и цялост, както и предотвратяване на всякакво компрометиране в критична ситуация (виж по-горе). Тези първични изисквания не са буквално **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**(отново виж по-горе). Както и ИС е определена като „състояние“ на информацията.

Всъщност това е съществена разлика – ИС е по-скоро установяване на една практика, състояние или стандартно положение на защитеност на информацията. Самото установяване на това състояние е гарант за защитеност и с това сме съгласни. ЗИ обаче е с добавена съвкупност от действия, мерки, процедури и участие на целия

персонал, всъщност ЗИ е процес, който се развива непрекъснато, обновява, анализира и допълва.

В този ред на мисли идва и коментар на проф. Ц.Семерджиев: „Информационната сигурност е защитеност на държавата на стратегическо, оперативно и тактическо равнище…“[19] Т.е. отново „състояние“, което се установява с определени критерии, в случая стандартите или други документи. Същият автор, безспорен авторитет в тази област, има научен труд „Сигурност и защита на информацията“ от 2012 г., който подсказва неразривната връзка и проникване между двете понятия. Дефинирането на ИС там е абсолютно същото.[20]

4. Допълнителни сравнения в полза на мярата между ЗИ и ИС

Добавяме още един пример на съотношение между понятия, който смятаме за подходящ тук: През 2007 г. се наложи да търсим мярата между „Контраразузнавателна дейност“ и „Защита на сигурността“, понятия, които използвахме при научен труд. Тогава: **Контраразузнавателна дейност** зад граница е дейност, провеждана от службите за сигурност на собствена и чужда територия, непосредствено насочена против посегателствата срещу нашата държава, извършвани от разузнавателните органи на чужди държави и използуваните от тях организации и лица.

Осъвременото тогава определение е категорично по- точно по отношение на обекта на посегателствата, но по своята същност не променя основното взаимоотношение“ държава /служби за сигурност/ - разузнавателни органи на други държави”.

Сигурността на ВС зад граница (б.а. – ставаше дума за нашите контингенти) е съвкупност от състоянието, когато са надеждно защитени

[19] Семерджиев, Ц., Митев, Н., Информационна сигурност, Софттрейд, 2015 г., стр.17
[20] Семерджиев, Ц., Сигурност и защита на информацията, Софтрейд, 2012 г., стр.12

личния състав, материалните средства, информацията и мероприятията на контингента, мерките, необходими за постигането на това желано състояние, и структурите, отговорни за тези мерки.

Определението е изведено въз основа на Речник на специалните понятия в разузнаването и сигурността на НАТО и глава 4, на "Операциите за хуманитарно подпомагане", с автор Ст. Стойчев и др..

Разглеждаме понятието с такава триединна насоченост, т.к. по този начин **субектите на дейността, сравнени с тези на контраразузнавателната работа, се разширяват с различни държавни и международни органи, организации и лица, които имат отношение към проблема, военното командване (чрез мерки по охрана или чрез участие в мероприятия по линия на цялото ръководство на мисията) и самите участници; посочени са обектите на заплахи, а субектите на заплахите не са ограничени, т.е. те могат да произтичат както от чужди специални служби, така и от престъпни организации, социални, природни, военни и др. обстоятелства и събития.** Определението съдържа и управленски аспект, като посочва целите на дейността /защита/, средствата за постигането й /реализиране на определени мероприятия/, както и участие на "организации", т.е. ръководни и изпълнителски звена със своя структура.[21]

Смятаме, че в подобно отношение (б.а. – като Комсек и ИС, като контраразузнавателна работа спрямо сигурност) се намират ИС и ЗИ. Докато ИС включва само дейността на заети с или чрез ИТ, най-малкото специалисти или експерти (без да изключваме и ръководители), то ЗИ използва всички служители, вкл. външни организации и лица, служби за сигурност и обществен ред (б.а. – които могат понякога да са решаващ

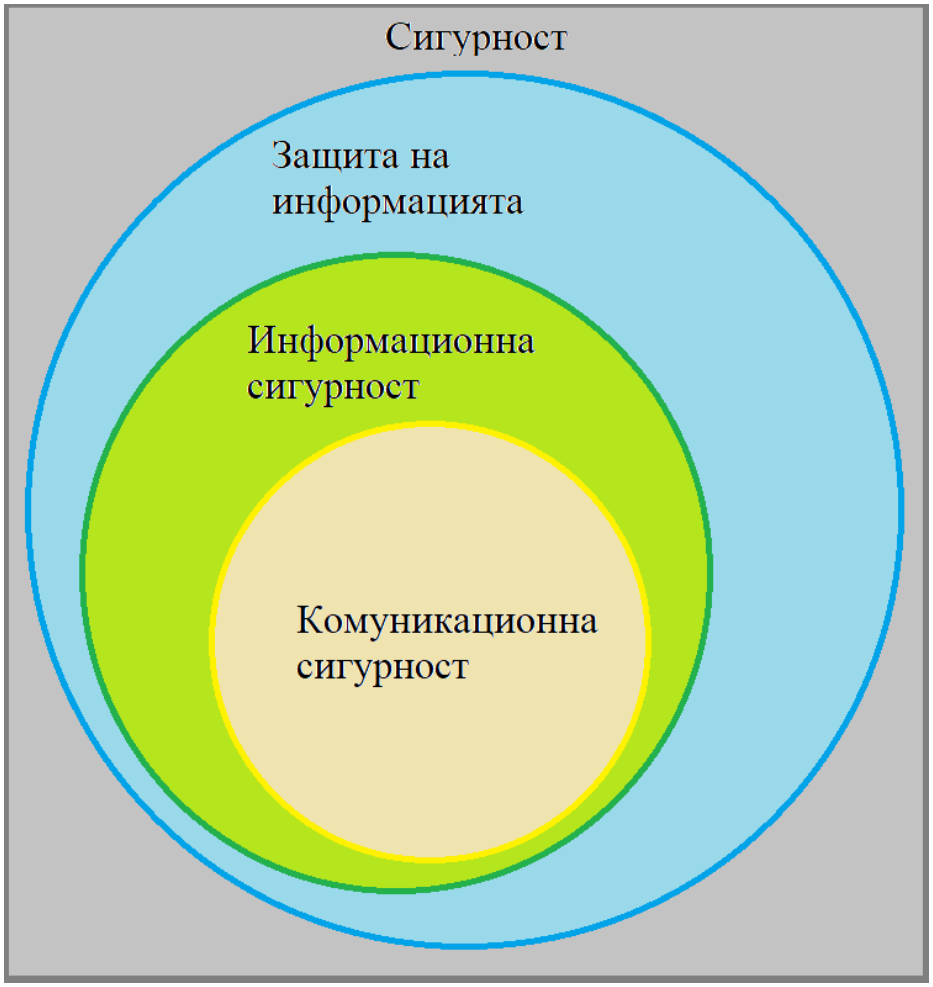
[21] Великов, И., Защита на сигурността на военни контингенти зад граница, дисертация, АМВР, 2007 г., стр.51

фактор за сигурността на информацията и организацията въобще), фирменото разузнаване и контраразузнаване (ако има такива), дори просто съседи като физически и юридически лица, консултанти и др. Постигането и поддържането на ИС се осъществява чрез ЗИ.

Имахме съществени колебания, дали по-правилно ще бъде понятието да се измени на „Защита на сигурността на информацията“, най-малкото така става ясно, че защитата не е застинало положение, не е състояние, а проактивна и динамична дейност, процес на непрекъснато развитие и обогатяване на сигурността на информацията. Тук обаче основното притеснение идва от отсъствието на подобна комбинация както в американската, така и в руската, така и в нашата специализирана литература и правни източници. Дори и да е семантично по-точно, практиката е установила вече популярни понятия като „Информационна сигурност“ (англ.: Information Security, рус.: Информационная безопасность), Защита на информацията (англ.: Information Protection, рус.: Защита информации), и едва ли е необходимо да търсим по-голяма симбиоза на двете и без това родствени понятия.

5. Същност и съдържание на ИС и ЗИ (изводи)

По нашите убеждения схематично, чрез кръгове на Ойлер, съотношението на Комсек, ИС и ЗИ трябва да изглежда така:



Онагледяването няма никакви претенции за количествено правилно съотношение, то не е и възможно, с оглед на динамиката на процесите (комуникационната сигурност расти и приближава ИС, ИС расте още по-бързо и доближава ЗИ, която от своя страна също се развива, без обаче да надхвърля значително досегашните си параметри).

Съдържанието на отделните елементи:

1) Комсек (комуникационна сигурност) - отказ на неупълномощени лица от достъп до информация, получена от телекомуникациите и за

гарантиране на автентичността на такива телекомуникации. COMSEC включва:

- Криптосигурност;
- Сигурност на предаването;
- Сигурност на емисиите и
- Физическа сигурност на COMSEC материали.

В отделните части могат да се видят ясно определения, централен орган и органи на местно ниво – мениджърите на Комсек акаунти (б.а. - **система от органи**); необходими технологични решения и технически характеристики на системите; мерки и процедури за сигурност и защита на помещения, апаратура и процеса на работа; условия и ред за достъп до Комсек материал (на практика е персонална сигурност по начина, който се разбира по нашия ЗЗКИ); физическа сигурност и контрол върху изпълнението и използването на Комсек материали; откриване, контрол и закриване на Комсек акаунти на служители; задължения на служителите, ползващи Комсек акаунти; отчетност на Комсек материали; унищожаване на Комсек материали; Комсек одитиране; Планиране при извънредни ситуации (за апаратура и ключове в особено застрашаваща среда се предвижда дори физическото им унищожаване, ако има опасност да попаднат в чужди ръце); инциденти при Комсек – докладване и разследване (б.а. – всичко изброено след системата от органи, на практика е **система от мерки за комуникационна сигурност**).

2) Информационна сигурност (ИС) е политика за сигурност и защита на информацията, основана на използването на информационни технологии, механизми и процедури за защита на апаратурата и процесите, както и обезпечаване на подходящ квалифициран персонал и ръководители за работа в информационната среда (б.а. – определението на автора).

Абсолютно необходимо е да се отбележи триединната насоченост на това определение: система на материално-техническата част, система на организационно-управленската част и система на персоналната сигурност. По отделните направления тази система включва: (б.а. – като изброим съдържанието й, ще стане ясно, че при ИС се изисква конкретна експертиза в ИТ)

- Определения и дефиниции на понятия в областта на ИС;
- Системи за управление на сигурността на информацията (б.а. – **системи от органи и системи от мерки отново**). Изисквания и добри практики на системи за управление на сигурността на информацията;
- Информационни технологии;
- Методи за сигурност на ИТ – Управление на риска; Наблюдение, измерване, анализ и оценяване; управление на сигурността на информацията за телекомуникационни организации, базирани на ISO; Указания за съвместно внедряване на ISO; Кодекс за добра практика за защита на личната информация за идентифициране; Указания за готовност на информационните и комуникационните технологии за непрекъснатост на дейността; Управление на инциденти, свързани със сигурността на информацията; Указания за идентифициране, събиране, придобиване и съхранение на цифрови доказателства; Спецификация за цифрово редактиране; Сигурност на съхранението; Указания за осигуряване на пригодност и адекватност на метод за разследване на инцидент; Принципи за разследване на инциденти и процеси;
- Информация и документация. Формат за обмен на информация;
- Обучение и квалификация на персонала;
- Комуникационна сигурност.

(б.а. – до тук избягваме да използваме все по модерната „киберсигурност“. Английската дума „cyber”,при употребата си на български език почти винаги се среща като представка на други думи. В изключително редки случай може да се използва и самостоятелно. В най-общ план може да приемем, че смисловото значение на думата „cyber” включва: електронни данни, електронна информация, електронни съобщения, информационни технологии, информационни и компютърни системи и/или пренос или обработка на тези данни, информация, съобщения чрез вече споменатите информационни технологии, информационни и компютърни системи. Така например в теорията и практика все по-често се употребяват термини като киберсигурност, киберпрестъпност, киберпрестъпление, киберотбрана, киберзащита, киберпротиводействие, кибертормоз, киберразузнаване и т.н.[22] В такъв случай понятието киберсигурност не надхвърля по никакъв начин ИС. Дори и при особеностите на бизнеса и частния сектор[23])

3) Защита на информацията (ЗИ) по определение е набор от мерки, насочени към гарантиране на поверителността и целостта на обработваната информация, както и на наличността/достъпността на информация за потребителите. Определението е достатъчно абстрактно и в най-общ смисъл сме съгласни с него. По съдържанието си ЗИ включва:

- ИС (б.а. – безспорно на първо и най-значимо място, още повече поради разширяващото се приложно поле на ИС, изпълващо все повече съдържанието на ЗИ);

[22] Хорозова, В. Съвременни тенденции в разузнаването и разузнавателния процес. Въведение в киберразузнаването, София, Списание ”Национална сигурност”, брой 4 /2020 година, ВикториИздат, ISSN: ISSN: 2682-941X – онлайн

[23] Хорозова, В. Фирмено киберразузнаване. Определение, система от понятия, цел, обект, източници. Сборник Доклади от годишна университетска научна конференция 28-29 май 2020 година, Издателски комплекс на НВУ „Васил Левски” ISSN 1314-1937, стр 88-98

- Система за управление на ЗИ (отново включва система от органи и система от мерки);

- Разузнаване, контраразузнаване, вътрешна сигурност, звено за сигурност и охрана (държавни, корпоративни, фирмени и др.) за защита на информацията;

- Дейности по осигуряване и квалифициране на персонал (дейността на отдели и дирекции „Човешки ресурси“ има отношение към ИС за създаване на длъжностни характеристики и провеждане на конкурси за набиране на експерти и специалисти в областта на ИТ, но също и към набиране на целия останал персонал)

- Логистика и финансиране на ЗИ;

- Обучение на персонала. Изграждане на корпоративна култура, интегритет и лоялност на персонала.

Като цялост обхватът на ЗИ е достатъчно по разнообразен и по-широк от всички експертни и специализирани дейности в ИС. Необходимо е също да се отбележи, че обхватът на ИС се разширява с все по-висока скорост към ЗИ, доближава ЗИ и се изпълва със ново съдържание от/към и в посока ЗИ (напр. все повече служебни дейности ще изискват стандартизиране или поне единно за сферата на дейност или държавата регламентиране). Последното положение се вижда много ясно при защитата на лични данни: Бихме могли да отбележим четири различни модела за защита на личните данни:[24]

• изчерпателно законодателство;

• секторно законодателство;

• саморегулация и

• технологични защити.

[24] Великов, И., Киряков, З., Основи на защитата на информацията, ЕВУИМ, 2016 г., ISBN 978-954-2959-26-7, стр.162

Възникнали и развивани в обратен на изброяването ред, ЗЛД преминава през собствена за фирмата защита чрез определени методи и средства, която на един етап преминава във фирмена регулация въобще, регулация (дори и доброволна) в отрасъла, за да се достигне до общодържавна изчерпателна и универсална за всички субекти на територията регулация. Вероятно Общия регламент за защита на данните от 2016 г. (GDPR) е следващо ниво на защита на лични данни – универсализиране на защитата в рамките на целия ЕС. Там се разглеждат някои последни идеи за използване и защита на информацията (напр. „профилиране“, вкл. „финансово профилиране на лица“[25]). Очевидно по отношение на личните данни имаме изначално високо ниво на мерки по ЗИ (преимуществено неспециализирани и от лица с по-ниска компетентност, вкл. разбира се и от квалифицирани в разузнаване или контраразузнаване лица, но като странична или съпътстваща неосновна тяхна дейност), но постепенно с развитието на регулацията в съюзен и държавен аспект делът на ИС нараства, намесата на все повече квалифицирани експерти и специалисти е била наложена (напр. в момента всяка организация си определя „лице по сигурността на информацията“, според GDPR е Data Protection Officer, което е достатъчно близо до отдавна и много по-уредена с регламенти дейност на защитата на класифицираната информация, където аналогът е Data Security Officer, „служител по сигурността на информацията“. Въпреки много различното звучене на български език, очевидно в оригинал тези длъжности изглеждат доста близки, т.е. експертни. Цялостната идея и цел на GDPR всъщност е подобна на идеята при класифицираната информация, от една страна – повишаване

[25] Минева, Ст., „Новата рамка за защита на личните данни – гарантиран баланс между правото на защита на личния интерес и защитата на обществения интерес”, Сборник научни трудове, Политиката на Европейския съюз по защитата на информацията и личните данни: научна конференция, Шумен, НВУ "В. Левски", 2018, с.51. ISBN 978-954-9681-89-5

на нивото на защита на данните на физическите лица[26] в условията на информационното общество, и от друга – уеднаквяване на критерии и изисквания за осъществяване на самата защита, най-вече за да може да прави одит и мониторинг на организациите навсякъде в ЕС.

Но изводът е, че ЗЛД черпи идеи от ЗКИ, развива регламентацията и по този начин ИС измества по-общата ЗИ и постепенно заема все повече от нейната функционалност.

Още един важен довод за използването на ЗИ. В технократските среди ИС вероятно е по-познато, но сред ръководители и мениджъри, и най-вече в правния мир – ЗИ е по-популярния термин. За основа ми служат нормативните актове, които са в тази област:

- Закона за ЗАЩИТА НА класифицираната ИНФОРМАЦИЯ;
- Закона за ЗАЩИТА НА личните данни (които данни са обособен и широкоспектърен дял от видовете защитена ИНФОРМАЦИЯ);
- Закон за ЗАЩИТА НА търговската тайна (отново вид ИНФОРМАЦИЯ, която казано просто, за да може информацията да се счита за търговска тайна, тя трябва да има икономическа стойност, не трябва да бъде общоизвестна за по-голямата част от населението, и не трябва да бъде информация, която би могла да бъде открита от други страни по подходящ начин поради усилията, положени от собственика да запази информацията поверителна).

Ако приемем, че наименованията на първите два закона са доста сродни, или приети с еднаква цел през 2002 г., то третият закон има съвсем различен характер и цел, и е приет през 2019 г., т.е. ЗИ представлява траен и съвкупен интерес за системата на националното нормотворчество.

[26] Виж Минева, Ст., «Значението на правото на личен живот и неприкосновеност на личността в информационното общество», Научен алманах ВСУ „Черноризец Храбър». Юридически науки и обществена сигурност, 2018, с. 108, ISSN 1313-7263

Горните текстове не ангажират институции или органи, те представят собствен възглед за мярата между ЗИ и ИС. И са опит за създаване на организационна култура най-малко сред експерти в нашата страна, и като преподавател – в образователната система, особено по проблемите на националната сигурност. [27]

Авторът е член на ДКСИ, бивш служител на служба за сигурност, дългогодишен преподавател в Академията на МВР, експерт и изследовател в областта на сигурността. За контакти – сл. 02/9333 603, e-mail – manoflight@abv.bg

[27] Димитрова, Сн., Системата на образование - част от системата за национална сигурност. Годишник на ВУСИ, 2017- с. 70 -76- ISSN 2367-8798