INFORMATION SECURITY IN XXI CENTYRY – CONCEPTUAL ISSUES

Prof. Bojidar Violinov Bojinov, PhD, Tsenov Academy of Economics, Svishtov, Bulgaria,
b.bojinov@uni-svishtov.bg

Abstract: The massive penetration of ICT in the daily activities of the people, firms and society, combined with the use of a wide range of high-tech innovation, change the functionality of society whole. The very important aspect of new digital economy is information security as its key components. The main objective of this study is to clarify the nature of information security, the main types of threats, as well as the common conceptual framework and approaches to information security. In this aspect, the object of this study is information security in today's world, the subject is focused on opportunities to prevent and minimize the negative impact of information risks and threats. The research thesis is that the threats to information security reflect changes in the economic, technological and organizational environment in which it operates modern economy.

Key words: information, information security, informacion society

ИНФОРМАЦИОННАТА СИГУРНОСТ ПРЕЗ XXI ВЕК – КОНЦЕПТУАЛНИ АСПЕКТИ

Проф. д-р Божидар Виолинов Божинов, Стопанска академия „Д.А. Ценов“,
b.bojinov@uni-svishtov.bg

Резюме:
Широкото навлизане на информационни и комуникационни технологии в ежедневните дейности на хората, икономическите субекти и обществото като цяло, съчетани с използването на широк набор от високотехнологични иновации, променя и начина на функциониране на обществото като цяло, като особено важен аспект във функционирането на тази нова дигитална икономика играе сигурността на информацията като нейна основа и ключова компонента. Основната цел на настоящето изследване е изясняване на същността на информационната сигурност, основните видове заплахи, както и общата концептуална рамка и подходи за осигуряване на информационна сигурност. В този аспект, обект на изследването е информационната сигурност в съвременния свят, предмета е фокусиран върху възможностите цел превенция и минимизиране на негативното въздействие информационните рискове и заплахи, а изследователската теза е, че заплахите за информационната сигурност отразяват промените в икономическата, технологична и организационна среда в която функционира икономиката.

Ключови думи: информация, информационна сигурност, информационно общество

ИНФОРМАЦИОННАТА СИГУРНОСТ ПРЕЗ XXI ВЕК – КОНЦЕПТУАЛНИ АСПЕКТИ

Проф. д-р Божидар Виолинов Божинов, b.bojinov@uni-svishtov.bg
Катедра „Финанси и кредит"
Стопанска академия „Д.А. Ценов"

Масовото навлизане на високите информационни и комуникационни технологии в ежедневните дейности на хората, икономическите субекти и обществото като цяло, съчетани с използването на широк набор от свързани с тях високотехнологични иновации, променя и начина на функциониране на обществото като цяло. Те водят до „експанзия на нови продукти, отрасли и инфраструктура, постепенно образуващи нова технико-икономическа парадигма, която направлява предприемачите, мениджърите, новаторите, инвеститорите и потребителите както в техните лични решения, така и във взаимоотношенията им през целия период на разпространение на този технологии"[1]. Глобалната информатизация на икономиката и обществото, от своя страна поражда редица взаимосвързани процеси, свързани с глобализацията на икономиката (чрез интернационализация на бизнеса, международно разделение на труда и международен пазар на готовата продукция), науката (интензификация на процесите на международен обмен на научна информация и създаване на международни научни екипи), образованието (развитие на системите за дистанционно обучение, създаване на виртуални университети, изграждане на международни университетски партньорства), културата (създаването на електронни библиотеки и картинни галерии, музейни експозиции) и обществото като цяло (изграждане на основите на информационното общество)[2]. По отношение на икономиката, новите информационни и комуникационни технологии до такава степен промениха начина на правене на бизнес и създадоха изцяло нови информационно-базирани отрасли, че вече говорим за съществуване на нов вид икономика, определяна като „информационна"[3], „мрежова"[4], „Интернет"[5], „кибер"[6] икономика.[7] Особено важен аспект във функционирането на тази нова

---

[1] **Перес, К**. Технологические революции и финансовый капитал (Динамика пузырей и периода процветания). Издателство „Дело", Москва, 2011, с. 31.

[2] **Макарова, Н.В., Волков, В.Б**. Информатика. Питер, Москва, 2011, с. 50.

[3] Информационна икономика (Information economy, Knowledge economy) е икономика, основана на знанията, в която голяма част от БВП се формира от дейности по производство, обработка, съхраняване и разпространение на информация и знания, като в тази дейност участват над половината от заетите. Вж. **Гринберг, А.С.. Король, И.А.,** Информационный менеджмент. Юнити-дана, Москва, 2003, с. 14.

[4] Европейската комисия определя мрежовата икономика (networked economy) като „среда, в която всяка компания или индивид, намиращ се в коя да е точка на икономическата система, могат с помощта на интернет –технологиите да контактуват лесно и с минимални разходи с всяка друга компания или индивид по повод на съвместна работа, за търговия, за обмен на идеи и ноу-хау или просто за удоволствие". Мрежовата икономика е традиционна икономика съчетана с информационни ресурси и технологии. **Бугорский, В.Н**. Сетевая экономика. Финанси и статистика, Москва, 2008, с. 13.

[5] Интернет икономика се отнася до правенето на бизнес чрез пазари, чиято инфраструктура е базирана на Интернет и Световната мрежа. Интернет икономиката се различава от традиционната икономика по множество начини, включително: комуникация, сегментация на пазара, стойности на разпределение и цена. Вж. https://bg.wikipedia.org/wiki/Интернет_икономика (последен достъп 19.08.2016 г.).

[6] Думата **cyber** произхожда от гръцката дума **κυβερεω** (kybereo) – направлявам, ръководя, контролирам. Уилям Гибсън използва термина **кибер пространство** в научно-фантастичната новела Neuromancer за описание на глобална компютъризирана информационна мрежа в която данните са кодирани в тримерна, многоцветна форма. Вж. **Lehto, M.**, Phenomena in the Cyber World. In Lehto, M, Neittaanmaki, P., Cyber

дигитална икономика играе **сигурността на информацията** като нейна основа и ключова компонента.

Основната цел на настоящето изследване е изясняване на същността на информационната сигурност, основните видове заплахи, както и общата концептуална рамка и подходи за осигуряване на информационна сигурност. В този аспект, обект на настоящото изследване е информационната сигурност в съвременния свят, предметът е фокусиран върху възможностите цел превенция и минимизиране на негативното въздействие информационните рискове и заплахи, а изследователската теза е, че заплахите за информационната сигурност отразяват промените в икономическата, технологичната и организационната среда в която функционира съвременната икономика.

Идеята за обособяването на посегателствата върху компютърно съхраняваната и обработваната информация в отделна група престъпления възниква още през 60-те години на XX век, когато са констатирани и първите опити за компютърна манипулация, компютърен саботаж, компютърен шпионаж и незаконно използване на компютри, които основно са насочени към финансови посегателства и незаконно използване на телекомуникационни услуги.[8] Възникване на идеята за активно управление на компютърната и информационна сигурност се лансира едва в началото на 80-те години на XX век с масовото навлизане на персоналните компютри в ежедневието на хората и съпътстващата поява на първите компютърни вируси.

Някой автори обособяват четири ери в развитието на заплахите пред компютърната и информационна сигурност:[9]

- „Ера на невинност" (от началото на 80-те години на XX век до 2000 година) – характеризира се с появата на първите компютърни вируси и други форми на зловреден код (malware) и осъществявани хакерски атаки към ключови институции. Като особеност на този период може да се посочи, че зловредния код и хакерските атаки са насочени за доказване на интелектуалното превъзходство на реализиращия ги, а не към унищожаване на атакуваните системи. Управлението на сигурността се свежда до „закърпване" на установените пробиви в системите;
- "Ера на самодоволство/удовлетвореност" (2000 – 2004) – бурното развитие на електронната търговия и свързаните с нея платежни средства правят този сегмент от дигиталната икономика особено атрактивен за престъпни посегателства с цел финансово обогатяване. Множеството успешни атаки поставят на дневен въпрос нуждата от повишаване на сигурността в новите условия;
- "Наваксване" (2005-2010) – засилването на компютърната престъпност принуди фирмите да обърнат сериозно внимание и да „наваксат" пропуснатото като увеличат инвестициите си в решения за гарантиране на информационната сигурност и критичната инфраструктура;
- „Тук и сега" (от 2010) – експоненциалното нарастване на броя на заплахите за информационната сигурност, съчетани с иновативните подходи на атакуващите, както и разширяване на обхвата (вкл. правителствени информационни системи) и

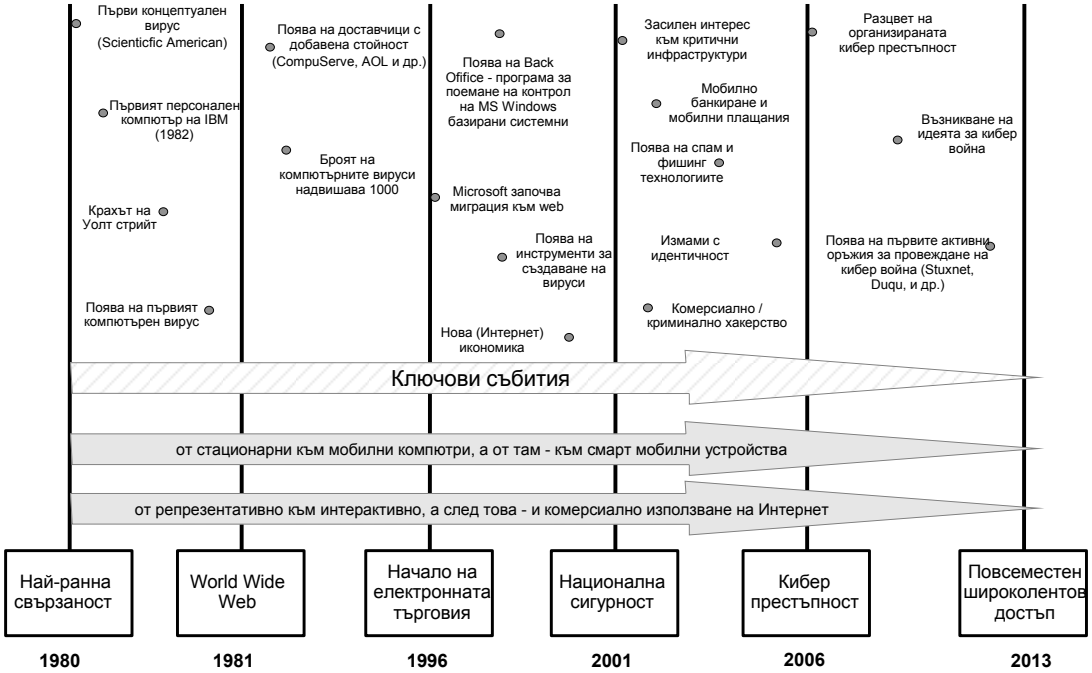
Security: Analysis, Thechnology and Automation, Intelligent Systems, Control and Automation: Science and Engineering 78, Springer International Publishing, Switzerland, 2015, p. 4.

[7] **Бугорский, В.Н.** Сетевая экономика. Финанси и статистика, Москва, 2008, с. 11.

[8] **Sieber, U.** Legal Aspects of Computer-Related Crime in Information Society. COMCRIME Study, European Commission, 1998, p. 19; **Goodman, M.D., Brenner, S.W.** The emerging consensus on criminal conduct in cyberspace", UCLA Journal of Law and technology 3, 2002, 12; **McKnight, G.** Computer Crime. London, Joseph, 1973; **Parker, D.B.** Crime by Computer. New York, Scribner, 1976 по: **Clough, J.** Principles of Cybercrime. Cambridge university press, New York, 2010, с. 3.

[9] Transforming cybersecurity using COBIT®5, 2013, с. 12-13.

промяната на целите на атаките (вкл. целенасочено унищожаване на атакуваните системи), ангажира не само бизнеса, но и държавата в решаване на проблемите на информационната сигурност в съвременното общество.



Фиг. 1. Развитие на дейностите и заплахите в кибер пространството
Източник: Адаптирано по: Transforming cybersecurity using COBIT®5, 2013, с. 12.

Съвременните информационни атаки изискват значителен обем предварителни проучвания, планиране и детайлна подготовка на проникването, вкл. и заличаването на следите след успешната атака, и са свързани с изключително висока степен на сложност на използваните средства и подходи.[10] Съгласно дефиницията на Европейската агенция по мрежова и информационна сигурност като заплаха за информационната сигурност се разглежда „всяко лице или нещо, което действа (или има силата да действа) за да причини, нанесе, пренесе или подкрепи заплаха“ [11]
Информационните заплахи могат да се класифицират по редица признаци. Така например, според мястото си на възникване спрямо обекта на атака, заплахите могат да бъдат:

- *вътрешни* - възникват в границите на обекта, съдържащ класифицираната информация (компютър, мрежа, организация);
- *външни* – възникват извън границите на атакувания обект.

В зависимост от типа на нарушаване на информацията, заплахите биват свързани с[12]:

[10] Transforming cybersecurity using COBIT®5, 2013, с. 14; **ISACA**, Reporting to Targeted Cyberattacks, USA, 2013 .
[11] **The European Network and Information Security Agency**. ENISA threat landscape: Responding to the evolving threat environment. 2012 по: **Lehto, M**. Phenomena in the Cyber World. In: Lehto, M., Neittaanmaki, P. Cyber Security: Analytics, Technology and Automation. Intelligent Systems, Control and Automation: Science an Enginering, Vol. 78, Springer, 2015, с. 9.
[12] **Белов, Е.Б., Лось, В., Меюеряков, Р.В., Шелупанов, Д.А.** Основы информационной безопасности. Москва, Горячая линия – Телеком, 2006, с. 139; **Макарова, Н.В., Волков, В.Б.** Информатика. Питер, Санкт-Петербург, 2011, с. 246.

- *нарушаване на физическата цялост* – унищожаване на физическите носители на информация или физическите елементи на информационните системи, в които тя се обработва и съхранява;
- *нарушаване на логическата цялост*– унищожаване на логическите връзки между отделните съставни части на информационните масиви;
- *нарушаване на съдържанието* – възниква при целенасочена промяна на съдържанието чрез изтриване, унищожаване или подменяне на част от или изцяло на наличната информация.
- *нарушаване на конфиденциалността* – възниква при неоторизирано проникване, придобиване и разпространение на класифицирана информация;
- *нарушаване на интелектуалните права на собственост* – чрез неоторизирано копиране и ползване на защитена от закона информация.

В зависимост от характера на заплахата, тя бива[13]:

- *умишлени информационни заплахи* – в резултат на преднамерена и целенасочена човешка дейност. Обикновено включват кражба на носители на информация, включване в каналите за връзка, прихващане на електромагнитните излъчвания, неоторизиран достъп, разгласяване на информация, копиране на данни и други умишлени действия;
- *неумишлени информационни заплахи*, в резултат на грешки в процеса на обработка на информацията (грешки на ползвателя, оператора, проблем с апаратурата);
- *информационни заплахи в резултат на случайни външни фактори,* най-често стихийни бедствия (урагани, наводнения, земетресения) и инциденти (пожари, аварии, взривове).

В зависимост от източника (непосредствения изпълнител) на заплахата, тя бива: [14]

- *човешкия фактор, работещ с информацията и информационните системи;*
- *техническите устройства, съставна част от информационните системи;*
- *използваните модели, алгоритми, програми за обработка на информация;*
- *възприетата технологична схема за обработка на информацията;*
- *източници от външната среда.*

В зависимост от щетите, които причиняват, информационните заплахи са свързани с реализация на: [15]

- *материални щети,* когато в резултат на осъществената атака са причинени преки материални, най-често финансови, щети;
- *косвени щети,* когато в резултат на осъществения информационен пробив, атакувания обект търпи непреки материални щети, най-често под формата на уронване на авторитета и престижа, загуба на ценна информация, съпътстващи разходи за възстановяване на щетите от атаката и др..

В зависимост от вероятността за възникване, информационните заплахи биват:

- *малко вероятни*;
- *средно вероятни*;
- *силно вероятни*.

В зависимост от възможността за превантивно въздействие и елиминиране, информационните заплахи биват:

[13] **Белов, Е.Б., Лось, В., Меюеряков, Р.В., Шелупанов, Д.А.** Основы информационной безопасности. Москва, Горячая линия – Телеком, 2006, с. 139-140.

[14] **Белов, Е.Б., Лось, В., Меюеряков, Р.В., Шелупанов, Д.А.** Основы информационной безопасности. Москва, Горячая линия – Телеком, 2006, с. 140.

[15] **Макарова, Н.В., Волков, В.Б.** Информатика. Питер, Санкт-Петербург, 2011, с. 245.

- *подлежащи на превенция и управление, вкл. и активно въздействие*;
- *неподлежащи на превенция и управление.*

В зависимост от водещите мотиви за осъществяване на атаката, заплахите за информационната сигурност могат да бъдат групирани като: [16]

- *кибер вандализъм / хакерство* – действие, насочено към промяна / унищожаване на съдържание, или изключване на сървъра поради претоварване на данни;
- *кибер престъпление* – криминално действие осъществено с използване на електронни комуникационни мрежи и информационни системи или срещу такива мрежи и системи;
- *кибершпионаж* - действие, насочено към придобиване на секретна информация (чувствителна, патентна или класифицирана) от индивиди, конкуренти, групи, правителства и противници за целите на натрупване на политическа, военна или икономическа печалба чрез използване на незаконни техники в Интернет, мрежи, програми или компютри;
- *кибер тероризъм* – целенасочени мрежови атаки срещу компютри, мрежи и критични системи, с цел тяхното поражение и последващ страх сред обществото, като средство за постигане на политическите цели на осъществяващите ги;
- *кибер война* – целенасочени държавни действия чрез компютри и информационни технологии за разрушаване на нормалната дейност и комуникация в атакуваната страна при едновременна защита на собствената информация и информационни системи.

Тази класификация, от своя страна, ни позволява да групираме предизвикателствата пред информационната безопасност на следните три нива:

- *информационни заплахи за държавата и обществото,* които се проявяват в следните направления[17]:
    - *заплахи за конституционните права и свободи на човека* в резултат на провеждана от държавата политика по ограничаване на достъпа до информация, както и предоставянето на обществеността на ограничена или манипулирана информация;
    - *заплахи за информационното обезпечение на държавната политика* посредством външни действия по блокиране на дейността на държавните средства за масова информация, както и монополизация на националния информационен пазар от чужди информационни фирми;
    - *заплаха за развитието на националната информационна индустрия*, чрез външни действия по ограничаване на достъпа на страната до най-новите информационни технологии или поставянето ѝ в технологична зависимост от външни информационни решения и продукти, както и изтичане на интелектуален капитал извън националните граници;
    - *заплахи за безопасността на информационните и телекомуникационните средства и системи* в резултат на внедряване на хардуер и софтуер в информационните продукти и системи, реализиращи не предвидени в документацията функции, разработка и разпространение на програми,

[16] **Cavelty, M.** The reality and future of cyberwar. http://mercury.ethz.ch/serviceengine/Files/ISN/115230/ichaptersection_singledocument/d9c3a284-0167-4492-aaa9-45b2176d2eee/en/Reality_and_Future_of_Cyberwar.pdf (последен достъп 19.08.2016 г.); **Lehto, M.** Phenomena in the Cyber World. In: Lehto, M., Neittaanmaki, P. Cyber Security: Analytics, Technology and Automation. Intelligent Systems, Control and Automation: Science an Enginering, Vol. 78, Springer, 2015, с. 9; **Белов, Е.Б., Лось, В., Меюеряков, Р.В., Шелупанов, Д.А.** Основы информационной безопасности. Москва, Горячая линия – Телеком, 2006, с. 9.

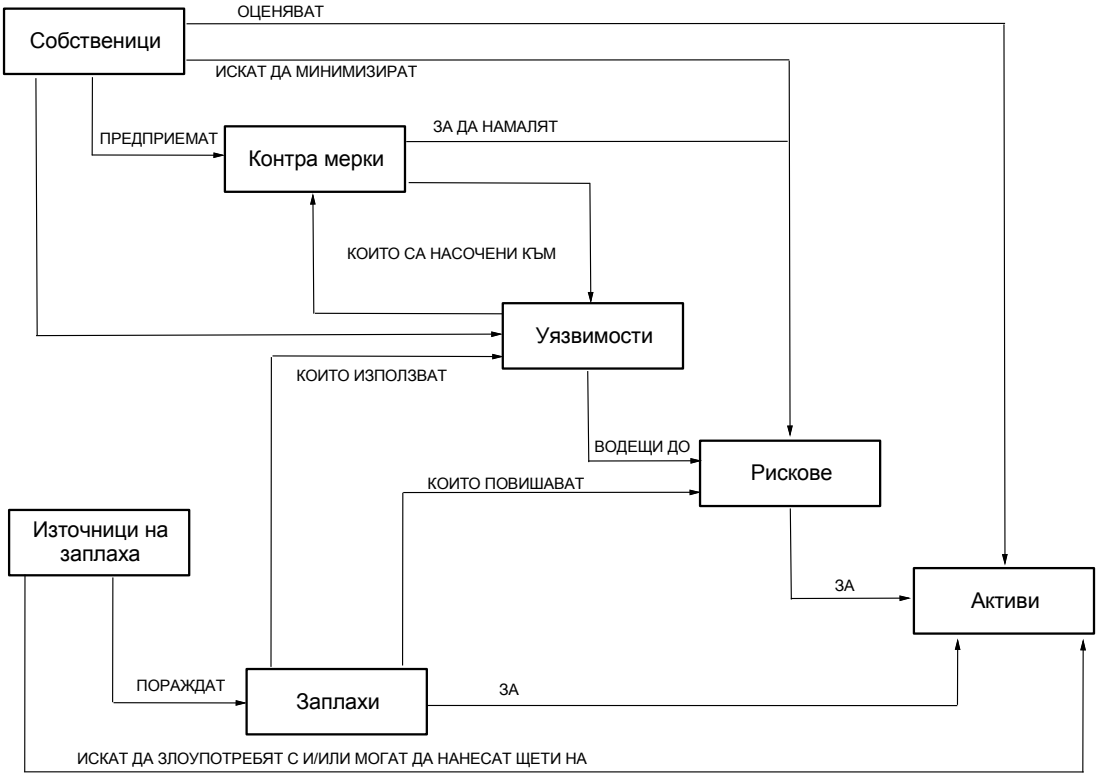
[17] **Макарова, Н.В., Волков, В.Б.** Информатика. Питер, Санкт-Петербург, 2011, с. 237-239.

нарушаващи нормалното функциониране на системите, прихващане на информация в мрежите за предаване на данни, дешифрирането на тази информация, и замяната й с фалшива информация, неоторизиран достъп до информация в бази данни, с цел придобиване, унищожение или повреждане на информацията или системите за нейната обработка.

- *информационни заплахи за организациите,* които основно са насочени към придобиване на конфиденциална информация, основно за целите на фирменото разузнаване, както и манипулации за придобиване, модифициране или унищожаване на информация, с цел осъществяване или прикриване на неправомерно обогатяване или друг вид престъпление;
- *информационни заплахи за индивидите,* които основно са свързани с действия по придобиване на лична информация за индивида, която в последствие да бъде използван за неговото злепоставяне, изнудване или извършване на престъпление от негово име или с негова помощ.

Информационна безопасност – същност, взаимовръзки и подходи

Най-общо, проблемите, свързани с информационните заплахи и информационната сигурност, както и взаимовръзката между отделните участници в този процес могат да бъдат представени чрез следната схема:

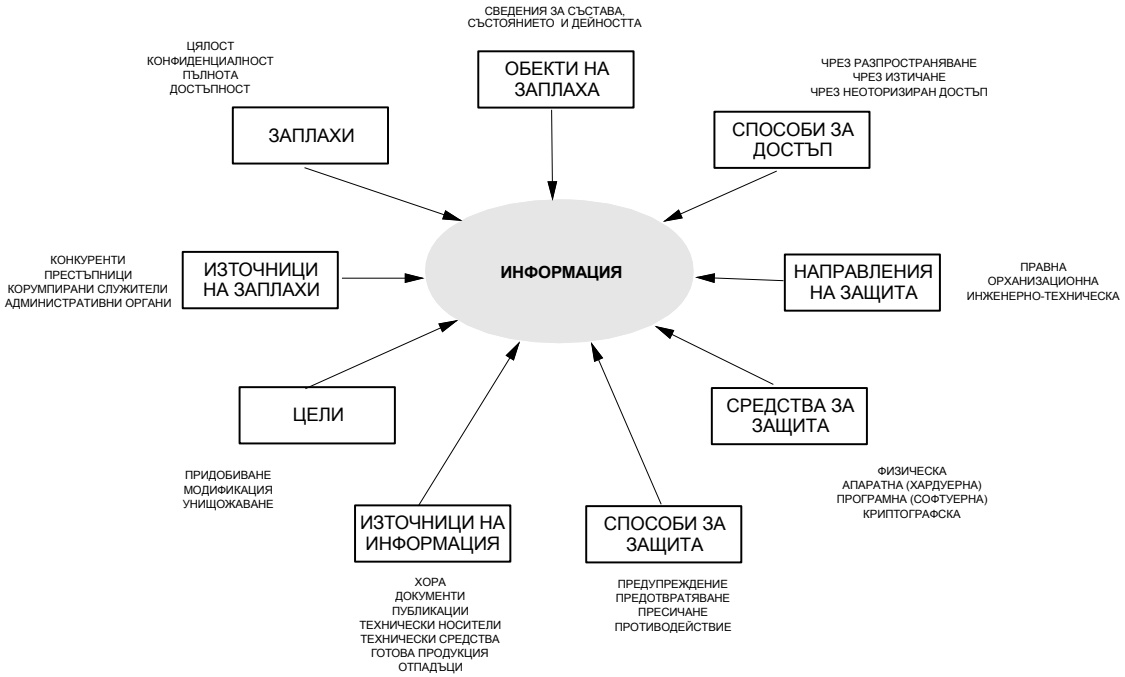


Фиг. 2. Общи понятия, свързани с информационната безопасност и взаимовръзките между тях

Източник: Белов, Е.Б., Лось, В., Меюеряков, Р.В., Шелупанов, Д.А. Основы информационной безопасности. Москва, Горячая линия – Телеком, 2006, с. 229.

Информационна безопасност като понятие може да се дефинира като степента на защитеност на информационната среда на обществото чрез различни средствата и методи чрез предотвратяване на въздействието на информационните заплахи или

минимизиране на вреда от тях. [18] Тя може да бъде определена и като способността на държавата, обществото и личността да обезпечават своето функциониране и развитие с достатъчни и защитени информационни ресурси, както и да се противопоставят ефективно на възникващите информационни заплахи чрез адекватен набор от приложими мерки.[19]



Фиг. 3. Концептуален модел на информационната безопасност
Източник: Белов, Е.Б., Лось, В., Меюеряков, Р.В., Шелупанов, Д.А. Основы информационной безопасности. Москва, Горячая линия – Телеком, 2006, с. 91.

Основните дейности, свързани с реализирането на информационната безопасност, независимо от разглежданото ниво (държава, организация, индивид), трябва да включват пълния комплекс действия, свързани със: [20]

- събиране, систематизация и анализ на сведенията за проблемите, свързани със защитата на информацията;
- формиране въз основа на събраните сведения на научно-обосновани прогнози за възможности за възникване на заплахи;
- научно-обоснована постановка на задачи за защита на информацията в съвременните условия;
- разработка на мероприятия по организация на защитата на информацията;
- разработка на методология и инструментална база за защита на информацията.

От тази гледна точка, основните подходи за осигуряване на информационната безопасност са свързани с: [21]

[18] **Макарова, Н.В., Волков, В.Б.** Информатика. Питер, Санкт-Петербург, 2011, с. 236.
[19] **Белов, Е.Б., Лось, В., Меюеряков, Р.В., Шелупанов, Д.А.** Основы информационной безопасности. Москва, Горячая линия – Телеком, 2006, с. 9.
[20] **Макарова, Н.В., Волков, В.Б.** Информатика. Питер, Санкт-Петербург, 2011, с. 236; **Белов, Е.Б., Лось, В., Меюеряков, Р.В., Шелупанов, Д.А.** Основы информационной безопасности. Москва, Горячая линия – Телеком, 2006, с. 10-11.

- *Регламентацията* - подход, свързан с разработване и реализация на комплекс от мерки и дейности (най-често разработване на правила за достъп и работа с конфиденциална информация), които затрудняват възникването и въздействието на заплахите;
- *Управление* – подход свързан с изграждането на набор от управляващи въздействия върху елементите на системата, обхващащ всеки етап и фаза от функционирането на информационната система, чрез които се способства за решаването на различни аспекти от защитата на информацията (напр. управлението на достъпа може да включва идентификация на лицата, потвърждаване на правата им за достъп до ресурсите по време, място и вид, регистрация на действията, и сигнализация и превенция при опит за неоторизиран достъп до информационните системи и ресурси);
- *Възпрепятстване* – подход, свързан със създаване на различни по вид и сложност бариери (препятствия) по пътя на възникване или разпространение на заплахата, които не позволява тя да се разпростре и да придобие опасни размери (напр. чрез физически ограничения до достъп до помещения и системи, свързани със съхраняване и обработка на конфиденциална информация; блокировки, възпрепятстващи системите или оборудването да влязат в опасен режим на действие, екраниране на помещения, компютърни и телекомуникационни устройства);
- *Маскировка* – подход, при който се предприема набор от действия за преобразуване на конфиденциалната информация, в следствие на което се намалява степента на нейната разпознаваемост и/или се затруднява достъпа до нея (напр. чрез шифриране, маскиране на информационните сигнали, създаване на шумови полета и др.);
- *Нападение* – подход, при който при установяване на опит за неоторизиран достъп до конфиденциална информация, системата прилага набор от активни действия чрез които атакува системите на нарушителя, като целта е нарушителя да премине към защита и да намали или прекрати опита си за взлом върху защитаваните информационни системи;
- *Принуждаване* – подход, при който работещите със защитаваната информационна система под заплаха за материална, административна или юридическа отговорност са принудени стриктно да съблюдават правила за обработка, предаване и използване на защитената информация;
- *Мотивиране (стимулиране)* – подход, при който работещите със защитаваната информационна система вътрешно са мотивирани чрез материални, морални, етически, психологически и други мотиви стриктно да спазват всички правила за обработка, предаване и използване на защитената информация.

Независимо от избрания подход или комбинация от подходи за осъществяване на информационната безопасност в защитаваните информационни системи, те биват реализирани чрез използването на различен набор от средства. Най-общо средствата за осъществяване на информационна защита и безопасност се делят на: [22]

- *Физико-технически средства за осигуряване на защитата на информацията*, които от своята страна включват:
    - *технически средства за защита*, включващи*:*

[21] **Макарова, Н.В., Волков, В.Б.** Информатика. Питер, Санкт-Петербург, 2011, с. 249-250; **Белов, Е.Б., Лось, В., Меюеряков, Р.В., Шелупанов, Д.А.** Основы информационной безопасности. Москва, Горячая линия – Телеком, 2006, с. 246-247

[22] **Макарова, Н.В., Волков, В.Б.** Информатика. Питер, Санкт-Петербург, 2011, с. 250-251.

        - *физически средства за защита* – механични, електрически, електромеханични и др. устройства и системи, които функционират автономно, създавайки различни видове препятствия по пътя на заплахите;
        - *хардуерни средства за защита* – различни електронни и електронно-механични и др. устройства, вградени в хардуера за системите за обработка на данни или допълнително добавяни към него за целите на защита на информацията;
    - *програмни средства за защита* – специализирани софтуерни решения (криптографски, за защита от вируси, файеруоли, и др.), част от автоматизираните системи за обработка на конфиденциална информация, чиято основна цел е защита на информацията от неоторизиран достъп;
- *Организационно-социални средства за осигуряване на защитата на информацията*, които от своята страна включват:
    - *Организационни средства за защита* – специално предвидени организационно-технически дейности, насочени към защита на обработваната и съхранявана информация;
    - *Законодателни средства за защита* – нормативно-правни актове, с помощта на които се регламентират правата, задълженията и отговорностите на всички лица, работещи с конфиденциална информация по отношение нейната защита;
    - *Морално-етични средства за защита* – система от действия, насочени към формиране в работещите с конфиденциална информация система от определени качества, възгледи и убеждения (патриотизъм, разбиране на важността и полезността от защитата на информацията), способстващи за запазване на обработваната от тях конфиденциална информация.

От изложеното до тук става ясно, че за да се постигне максимално пълна и адекватна защита на конфиденциалната информация е необходимо да се изгради цялостна система, свързана с нейната защита. Това, от своя страна, позволява да определим *системите за защита на информацията* като съвкупност от взаимносвързани средства, методи и мероприятия, насочени към „предотвратяване унищожаването, изкривяването, неоторизираното получаване на конфиденциална информация, чрез достъп до различни физични полета, електромагнитни, светлинни и звукови вълни или веществено-материални носители във вид на сигнали, образи, символи, технически решения и процеси“[23].

Така изградените системи за защита на информацията трябва да бъдат комплексни, като интегрират и съгласуват всички съставни модули и компоненти, така че да възпрепятстват максимално всеки неоторизиран опит за достъп до конфиденциална информация, като същевременно не създават излишни затруднения за оторизираните ползватели на информационната система. Освен това, те трябва да са подчинени и изградени в съответствие на единна концепция за защита на информацията (концептуално единни), да са адекватни на поставените пред тях изисквания, достатъчно гъвкави и удобни за ползване, с оглед бързата им и лесна адаптация при промяна на заплахите или технологията на обработка на информацията, както и да са функционално самостоятелни (независещи от други системи и ресурси),

[23] **Белов, Е.Б., Лось, В., Меюеряков, Р.В., Шелупанов, Д.А.** Основы информационной безопасности. Москва, Горячая линия – Телеком, 2006, с. 141.

осъществяващи пълен контрол върху всички аспекти на обработката на информацията и с възможност за активно противодействие на всеки опит за неоторизиран достъп. [24]

References:

1. Алавердов А.Р. Организация и управление безопасностью в кредитно-финансовых организациях. Московская финансово-промышленная академия. Москва, 2004.
2. Арнаудов, Д., Крумова, А. Сигурност и защита на информационните системи. Част 1. Варна, ВСУ „Черноризец Храбър“ Университетско издателство“, 2007
3. Белов, Е.Б., Лось, В., Меюеряков, Р.В., Шелупанов, Д.А. Основы информационной безопасности. Москва, Горячая линия – Телеком, 2006.
4. Божинов, Б. Банковата сигурност – основни проявления и аспекти. Народностопански архив, бр. 3, 2016.
5. Бугорский, В.Н. Сетевая экономика. Финанси и статистика, Москва, 2008.
6. Визгунов, А., Визгунов, Ар. Уровень защищенности от несанкционорованного доступа как ключевой показатель качества системь дистанционного банковского обслуживания. Информационнье технологии в бизнесе, Бизнес-информатика, №2 (12), 2010.
7. Върбанов, Р. Интернет технологии в бизнеса и мениджмънта. Велико Търново, Фабер, 2015.
8. Гринберг, А.С.. Король, И.А., Информационный менеджмент. Юнити-дана, Москва, 2003.
9. Макарова, Н.В., Волков, В.Б. Информатика. Питер, Москва, 2011.
10. Павлов, Г., Пудин, К. Информационната сигурност в организацията. София, Университетско издателство „Стопанство“, 2011.
11. Перес, К. Технологические революции и финансовый капитал (Динамика пузырей и периода процветания). Издателство „Дело“, Москва, 2011.
12. Семерджиер, Ц. Сигурността и защитата на информацията. София, Класика и стил, 2007.
13. Целков, В., Стоянов, Н., Исмаилов, О. международни стандарти и добри практики за защита на информацията. София, За буквите – О писменехь, 2010
14. Шишманов, К. Рисковете при използването на интернет банкирането и отговорността на потребителите. // Финансите и стопанската отчетност - състояние, тенденции, перспективи: Юбилейна международна научнопрактическа конференция, Сборник доклади, Т. 1., Свищов , 2013.
15. Cavelty, M. The reality and future of cyberwar. http://mercury.ethz.ch/serviceengine/Files/ISN/115230/ichaptersection_singledocument/d9c3a284-0167-4492-aaa9-45b2176d2eee/en/Reality_and_Future_of_Cyberwar.pdf (последен достъп 19.08.2016 г.).
16. Clough, J. Principles of Cybercrime. Cambridge university press, New York, 2010.
17. Goodman, M.D., Brenner, S.W. The emerging consensus on criminal conduct in cyberspace”, UCLA Journal of Law and technology 3, 2002.
18. ISACA, Reporting to Targeted Cyberattacks, USA, 2013.
19. Lagazio, M., Sherif, N., Cushman, M. A multi-level Approach to understanding the Impact of Cyber Crime on the Financial Sector.
20. Lehto, M., Phenomena in the Cyber World. In Lehto, M, Neittaanmaki, P., Cyber Security: Analysis, Thechnology and Automation, Intelligent Systems, Control and

[24] **Белов, Е.Б., Лось, В., Меюеряков, Р.В., Шелупанов, Д.А.** Основы информационной безопасности. Москва, Горячая линия – Телеком, 2006, с. 263-264.

Automation: Science and Engineering 78, Springer International Publishing, Switzerland, 2015.
21. McKnight, G. Computer Crime. London, Joseph, 1973.
22. Parker, D.B. Crime by Computer. New York, Scribner, 1976.
23. Sieber, U. Legal Aspects of Computer-Related Crime in Information Society. COMCRIME Study, European Commission, 1998.
24. The European Network and Information Security Agency. ENISA threat landscape: Responding to the evolving threat environment. 2012.
25. Transforming cybersecurity using COBIT®5, 2013.
26. https://bg.wikipedia.org/wiki/Интернет_икономика (последен достъп 19.08. 2016).