ИЗСЛЕДВАНЕ И АНАЛИЗ НА ИНФОРМАЦИОННАТА СИГУРНОСТ ОТ ГЛЕДНА ТОЧКА НА ПОНЯТИЯТА РИСК, ЗАПЛАХА, УЯЗВИМОСТ, ИНЦИДЕНТ И НЕСИГУРНОСТ

Ивайло Николов
Технически университет – Габрово

RESEARCH AND ANALISIS OF INFORMATION SECURITY IN TERMS OF CONCEPTS OF RISK, THREAT, VULNERABILITY, INCIDENT AND INSECURITY

Ivaylo Nikolov
Technical University of Gabrovo

Abstract: *According to the Bulgarian and European legislation there is controversial practice of defining the concepts related to information security. The existence of different definitions of the same legislative terms leads to an obvious contradiction and lack of a single legislative approach in defining the concepts of risk, threat, vulnerability, accident and insecurity. The presented research aims to explore, analyze and summarize key concepts in the field of information security as a basis for further studies and analysis.*

Keywords: *information security, politics of information security, certification*

Въведение

Информационната сигурност е от съществено значение както за частния, така и за публичния сектор. Броят на служителите, оборотите или печалбата на фирмата не са определящи при вземане на решение за осигуряване сигурност на информационните ресурси, тъй като обект на заплаха могат да бъдат както големи, така и малки фирми и организации. Прилагането на технически решения, с необходимото оборудване и продукти, вече не е достатъчно, за да се гарантира правилното управление на информационната сигурност. Сигурността на информацията не е изключителен проблем на информационните технологии, а по-скоро „бизнес" проблем. Общото мнение е, че прилагането на подходящи технологии за решаване на проблема с информационната сигурност е само една част от проблема на сигурността на информацията.

Днес информационната сигурност се постига чрез прилагане на подходящи контроли, свързани с политиката за сигурност, бизнес процеси, процедури, организационна структура и функции на хардуера и софтуера. Тези контроли са необходими за проектиране, изпълнение, наблюдение и преглед за усъвършенстване, за да се осигурят нормални условия за развитие на който е да е бизнес.

Развитието, внедряването и сертифицирането на системи за управление на информационната сигурност осигурява определено ниво на доверие на клиентите, акционери и служители, че тяхната информация ще бъде защитена по подходящ на-

чин. Стандарт ISO 27001 може да се прилага във всички отрасли на промишлеността, търговията и услугите.

Прилагането на международните стандарти ISO / IEC 27000 регламентира измерими показатели за разработване и внедряване на система за управление на информационна сигурност, както и критериите за осигуряване на обективна оценка и удостоверяване на сигурността на информацията. Такива показатели са например финансова информация, информация за интелектуална собственост, данни за персонал или информация, които са им възложени от потребителя или от трето лице.

Специфичните стандарти за информационна сигурност са предназначени за организации със собствен бизнес, чието функциониране зависи от бизнес процесите на информационна система, а опазването на информационните ресурси е от решаващо значение за тяхното функциониране. Една голяма част от тези организации са: банки, ИТ компании, финансови и застрахователни компании, болници, училища, университети, производители на автомобилни части, телефонни центрове, данъчните власти, консултантски фирми и много други организации.

Определяне на нови методи за работа с информация, документиране на същите тези процедури, гарантира, че всички задължителни стандарти са надлежно разработени, описани, внедрени и гарантират опазване на информационните ресурси на организацията.

От първостепенно значение за информационната сигурност е защитата на информацията, запазване на нейната поверителност, цялостност, или наличността. Информационната сигурност е много повече, отколкото използването на подходящи технически решения, предлагани от съвременните информационни технологии.

Цел на изследването е да се събере, обработи и анализира достоверна теоретична информация, която характеризира понятията риск, заплаха, уязвимост, инцидент и несигурност.

Предмет на изследването е законодателството в Република България, Европейски съюз, както и публикуваните научни и научно-приложни резултати от изследвания в областта на информационна сигурност.

За изпълнение целта на научното изследване и предвид предмета на изследването, **научните задачи** са свързани с:

- изследване на действащото законодателство във връзка със значението на понятията риск, заплаха, уязвимост, инцидент и несигурност в контекста на информационната сигурност;
- анализиране на получените резултати с цел систематизиране на понятията;
- изводи във връзка с неточно, неясно или некоректно терминологично приложение на понятията риск, заплаха, уязвимост, инцидент и несигурност;

Научната хипотеза се основава на възможността изследвайки нормативната база и научни разработки в областта на информационната сигурност, да бъдат синтезирани онези понятия, които характеризират най-точно и ясно понятията риск, заплаха, уязвимост, инцидент и несигурност в контекста на системите за управление на информационната сигурност.

Методологията на изследването е свързана с анализ на литературни източници, закони, наредби и правилници във връзка с осигуряване на сигурност на информационните ресурси.

Съгласно Директива 2013/0027 (COD) на Европейски парламент относно мерките за гарантиране на високо общо ниво на мрежова и информационна сигурност в

Съюза, понятието „сигурност“ означава способността на мрежа или информационна система да издържа — при дадено равнище на увереност — на инциденти или злонамерени действия, които повлияват на наличността, автентичността, целостта и поверителността на съхранявани или пренасяни данни или на свързаните с тях услуги, предлагани от или достъпни посредством тази мрежова и информационна система;

Инцидент е събитие, представляващо промяна в нормалната работа на информационните системи[16].

Понятието „инцидент“ според Директира 2013/0027 означава обстоятелство или събитие, което има действително неблагоприятно отражение върху сигурността;

Стойността на информацията се определя от характеристиките, които тя притежава. Някои, от изброените по-долу, характеристики увеличават или намаляват стойността на информацията повече от други [17].

Сигурността се отнася до политиките, процедурите и техническите мерки, които се използват за предотвратяване на неразрешен достъп, промяна, кражба или физическо увреждане на информационните системи. Контролът се състои от всички методи, политики, и организационни процедури, които гарантират безопасността на организационните активи [1].

Когато говорим за съдържанието на сигурност най-общо разбираме състояние на системата, или на неин елемент, за който няма заплахи, които да са в състояние да нарушат нормалното функциониране на този елемент, при което характеристиките на тези заплахи са общовалидни за всички системни елементи и условия[2].

Според определението на Европейската комисия информационната сигурност е защита на мрежите и информационните системи срещу човешки грешки, природни бедствия, технически неизправности или злонамерени атаки.

Информационна сигурност често се разглежда като защита на информацията от неправомерен достъп, използване, разкриване, увреждане, промяна, преглед, запис или разрушаване. Терминът е достатъчно общ, за да бъде използван независимо от формата, която можа да имат данните (напр. електронна, физическа)

Информационната сигурност може да бъде разглеждана в редица насоки като например по отношение на електронното управление [3], и по-конкретно необходимите методи и средства за идентификация [4], безжични сензорни мрежи [5], облачни системи [6]

Управлението на информационната сигурност се основа на идентифициране, елиминиране или ограничаване на рисковете за информационните ресурси.

Изграждането на информационна сигурност в организациите е предшествано от оценка на уязимостите на системите и устройствата. Това е първата стъпка за преодоляване на заплахите за сигурността на информационните ресурси [7]

Заплахата е понятие, с което се обозначават дисбаланси, определени като риск, но постигани и чрез съзнателната дейност на себеподобни. Заплахите са съзнателно търсени, експлоатирани, дори създавани дисбаланси, засягащи жизнените интереси на личността и обществото. Чрез понятието заплаха се отразява реалния факт, че обществото и личността не просто попадат в състояние на несигурност в резултат от собственото си развитие, но също така биват поставени в такова състояние[8].

Една от най-сериозните заплахи за информационната сигурност са човешките грешки. [9]

Заплахите за информационната сигурността могат да бъдат от най-различно естество като например софтуерни атаки, кражба на интелектуална собственост, кражба на самоличност, кражба на устройство или информация, саботаж и манипулиране на информацията. При кражбата на самоличност атакуващият се опитва да получи

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

Несигурността е състояние на недостиг от информация, свързана с разбирането и знанието за дадено въздействие, неговите последствия или вероятност (Георгиев, 2005). Целите могат да имат различни аспекти (финансови, здравни, свързани с безопасността, екологични) и могат да се прилагат на различни нива (стратегическо, структурно звено, продукт или процес).

Информационната сигурност е изложена на редица рискове, които трябва да бъдат щателно изследвани и анализирани. Понятието „риск" е чуждица в говоримия в българския език, която освен, че има няколко, макар и близки значения, в различните исторически периоди променя доминиращото от тях. Това положение е лесно обяснимо тъй като думата риск независимо, че се използва във всички съвременни езици се използва за обозначаване на един типичен ноумен, т. е. на обект, който не може да бъде възприет от човешките сетива и е „единствено умопостигаем"[10].

Други автори разглеждат „риска" като явление от реалния живот, което съществува обективно и не може да се премахне, а само да се ограничи, прехвърли, замести, раздели, компенсира. Под „риск" се разбира въздействие на несигурността върху целите на организацията и нейната сигурност. Риск съществува, когато има неяснота, несигурност и липса на точно решение за бъдещ момент от време [11].

Съгласно Директива 2013/0027 (COD) на Европейски парламент относно мерките за гарантиране на високо общо ниво на мрежова и информационна сигурност в Съюза, понятието „риск" се разглежда като обстоятелство или събитие, което има потенциално неблагоприятно отражение върху сигурността;

Според Закона за финансовото управление и контрол в публичният сектор, „риск" е събитие, което ще повлияе върху постигане на целите на организацията. Рискът се измерва с неговия ефект и с вероятността от настъпването му. [12]

В разпоредба на Закона за храните „риск" е функция от вероятността за възникване на увреждащ здравето ефект и сериозността на този ефект [13].

Според Наредба № 5 от 11 май 1999 г., „риск" е вероятността за настъпване на вреда при конкретни условия на излагане и тежестта на вредата.

Съгласно Регламент (ЕО) № 482/2008 на Комисията от 30 май 2008 година относно изграждане на система за осигуряване безопасността на софтуера, която да бъде въведена от доставчиците на аеронавигационни услуги, и за изменение на приложение към Регламент (ЕО) № 2096/2005 „риск" означава комбинацията от общата вероятност или честотата на възникване на вреден ефект, породен от опасност, и степента на сериозност на този ефект;

Риск е чуждица в говоримия в българския език, която освен, че има няколко, макар и близки значения, в различните исторически периоди променя доминиращото от тях. Това положение е лесно обяснимо тъй като думата риск независимо, че се използва във всички съвременни езици се използва за обозначаване на един типичен ноумен, т. е. на обект, който не може да бъде възприет от човешките сетива и е „единствено умопостигаем"[14].

Процесът по управлението на риска се извършава на различни нива – стратегическо (свързано с управлението на организацията), оперативно (свързано с основните процеси и дейности в организацията) и тактическо (свързано с работата на всеки участник в процеса) [15].

Стандарт ISO 27001 представлява система за защита и информационна сигурност. Целта на тази система е да се гарантира, че всички необходими контроли във връзка с осигуряване на поверителност, надеждност и ограничен достъп до информация, са коректно разработени и приложени в организацията. Сертифицирането е гаранция както за самата организация, така и за клиентите, организации и фирми, служители, партньори и обществото като цяло.

Серията от ISO / IEC 27000 осигурява хармонизиран подход за управление на риска, чрез разработване, внедряване и поддръжка на системи за управление на информационната сигурност [18].

Цел на управление на информационната сигурност е да се гарантира защита на информационните ресурси срещу всички рискове, заплахи, инциденти, случайно или умишлено създадени, чрез изпълнение, контрол, предварително изпитване, поддържане и подобряване на системата за управление на информационната сигурност. Изпълнението на тези политики и правила, е важно да се запази целостта на информационните системи за предоставяне на услуги.

Политиките за информационна сигурност дефинира цялостната визия, правила и процедури за осигуряване на информационна сигурност с оглед на гладкото функциониране, защитата на поверителна информация и по-нататъшното успешно развитие на организацията, както и удовлетвореността на клиентите от обслужването и качеството на обслужване.

Заключение

В националното законодателство не съществува единен подход за дефиниране на понятията свързани с информационната сигурност. Така например понятието „риск" е дефинирано в над седем източници сред които закони, наредби, научни разработки. За унифициране на терминологията в законодателството е необходимо научната общност да систематизира наличните определения с цел постигане на максимална достоверност на понятията и дефинициите в областта на информационната сигурност.

Настоящата разработка може да бъде използвана като основа за бъдещи изследвания в областта на информационната сигурност, както и при иницииране на законодателни промени на основание чл. 18 от Закона за нормативните актове.

Осигуряване на приемливо ниво на информационна сигурност е възможно само и единствено при задълбочено познаване на материята, свързана с опазване на информационните ресурси на организациите.

Литература

1. Сандалски М, Лекции по защита на фирмената информационна система Тема 5 – Модел на информационна сигурност, [online] посетена на 02.03.2016 г., стр. 2
2. Манев, Е., Глобална, регионална и национална сигурност, издателство Софттрейд, ISBN 978-954-334-141-2 ,София, 2012
3. Цонков, Н., Проблеми пред Е-управлението в България, VII Международна научна конференция „Е-управление", юни 2015, Созопол, ISSN 1313-8774, стр. 13

4. Хубенова, М., Електронна идентификация на правните субекти в р. България-актуално състояние и перспективи, VII Международна научна конференция „Е-управление", юни 2015, Созопол, ISSN 1313-8774, стр. 125
5. Davide, E., Romani, S., A New Strategy to Deal with Security Threats in Wireless Sensor Networks, Амоева journal, march 2011, ISSN: 0926-3543, vol. 36, No. 2, p. 5
6. Alqahtani, H., Snat, P. Cloud Computing Security Challenges And Threats, International Journal of Advances in Engineering & Technology, Aug. 2015, ISSN: 22311963
7. Whitman, M. Threats to Information Security, Communications of the ACM, august 2003, Vol. 46, No 8
8. Мичев, С., Философия на сигурността, издателство СофтТрейд, ISBN 978-954-334-172-6, 2015, стр. 73
9. Сандалски М, Лекции по защита на фирмената информационна система Тема 5 – Модел на информационна сигурност, [online] посетена на 02.03.2016 г. , стр. 3
10. Христов, П., Метатеория на риска, София, 2010
11. Слатински, Н. Увод в управлението на риска. Лекция 3. от поредицата „Четири лекции" [online] http://nslatinski.org/?q=bg/node/297, посетен 02.03.2016
12. Закон за финансово управление и контрол в публичната сфера
13. Закон за храните, Обн. ДВ. бр. 90 от 15.10.1999, изм. и доп. ДВ. бр. 28 от 08.04.2016 г.
14. Христов, П., Метатеория на риска, София, 2010
15. Карев, М., Управлението на риска като част от стратегическия мениджмънт на сигурността, Международно научно on-line списание „Наука и технологии", ISSN 1314-4111, Том IV, No 7, 2014, стр. 122
16. Сандалски., М., Лекции по защита на фирмената информационна система Тема 6 – Модел на информационна сигурност, [online] посетена на 18.10.2015 г. , стр. 4.
17. Войноховска, В., Цанков, С., Въведение и ключови понятия, свързани с информационната сигурност, Научни трудове на Русенски университет, 2014, том 53, серия 6.1., стр. 72
18. Izvorska, D., Stoynova, B., Digital Libraries in Support of Web-based Training in Calculus, IJETCAS, New Delhi-110016, India, 2013, issue 4, vol 1, pp 121-124, ISSN (ONLINE):2279-0055,ISSN(PRINTED):2279-0047, 2013