МЕТОДИ ЗА УПРАВЛЕНИЕ И АНАЛИЗ НА ИНФОРМАЦИОННИЯ РИСК

Доц. д-р Мариана Петрова

Информационната сигурност[1] цели да предпази информационните ресурси на организацията, без да бъде в противоречие с безопасността на персонала, законите и нормативните актове, както и общоприетите морални принципи.

Най-добрият начин за защита на информацията е в категоризацията на информационните масиви, правилното дефиниране на рисковете за всяка категория данни и изготвяне на финансово изгоден план за смекчаване или ефективно третиране на тези рискове.

1. CRAMM – Central Analysis And Management Method

CRAMM – Английски метод за оценка на риска, съобразен с изискванията на ISO 27001 и дава общо решение на въпросите свързани с риска. Може да се използва като инструмент за бърз анализ на риска или задълбочен анализ. Чрез него може да се получи много информация за организацията и нейните цели.

Първата версия е разработена през 1987 г. с помощта на най-добрите практики на британската индустрия и правителство. CRAMM V5.2 може да се намери в експрес и експерт версия.

Методът CRAMM описва около 400 вида активи, 25 различни заплахи и детайлно разглежда 3500 мерки, категоризирани според различните аспекти на сигурността. Всяка мярка има референтен номер, описание, минимална и максимална стойност на различните щети, ефективност на мярката, индикатор за разходи, препратка към алтернативни мерки. Активът данни е много важен елемент за по-нататъшното изчисляване на риска в този метод и се извършва много прецизна оценка по отношение на конфиденциалността, интегритета и достъпността. Класифициране на заплахите и уязвимостите е изходна база за създаване на т.нар. Матрица на риска, посредством която се определя действителния риск. При вземането на решение, кои мерки ще се прилагат CRAMM осигурява отделен процес и по този начин дали една мярка ще бъде подновена или не, зависи от специфичните критерии на организацията.

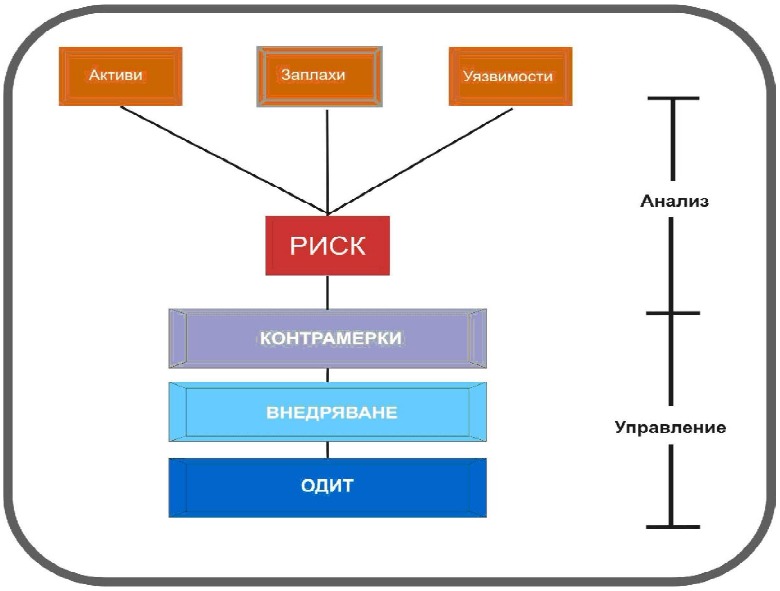
Методът CRAMM има 3 стадия: установяване на целите свързани със сигурността; оценка на риска и изисквания за сигурност; избор и внедряване на контроли. Този метод предлага много добър подход за оценка на риска, отчитайки вероятностите и последствията. Широко използван е във Великобритания, НАТО, Чехия, Холандия, националното здравеопазване. Предимството на CRAMM е в чек листата му с контрамерки. (1)

2. CRISAM – австрийски метод за корпоративния риск.

Разработен е от Calpana Business Consulting GmbH в Линц през 2001 г. като предизвикателство да управляваме несигурността на бъдещето днес. Последната версия е 4 от 2009 г. Включва информация от поредицата от стандарти ISO/IEC 27000, ITIL, CobiT и австрийското ръководство за

[1] Информационната сигурност според ISO/IEC 27001:2006 ISMS е съвкупност от три елемента: конфиденциалност – осигуряване на достъп до информация само на тези, които имат право на това; цялостност – опазване на точността и целостта на информационните методи и методите на обработка; наличност на информацията – осигуряване на наличност на информация към упълномощени лица, когато е нужно.

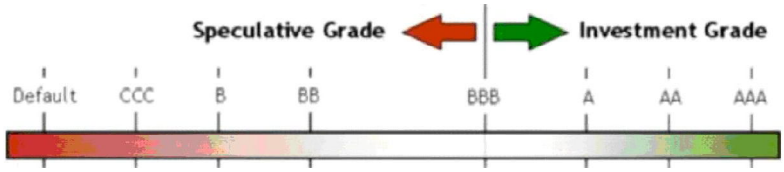
безопасно използване на информацията. Четири са основните документа, който трябва да бъдат определени от ръководството, на най-високо ниво (фиг. 2.).



Фиг. 1. CRAMM метод [18]

Фиг. 2. Основни документи в CRISAM

Първият документ очертава рамката на по-нататъшния процес за оценка на риска. На базата на разработен от Standards & Poors's рейтингов модел за класификация (фиг. 3.) се определя състоянието на системата. „AAA" е най-високия рейтинг, а „BBB" отразява състоянието към момента.

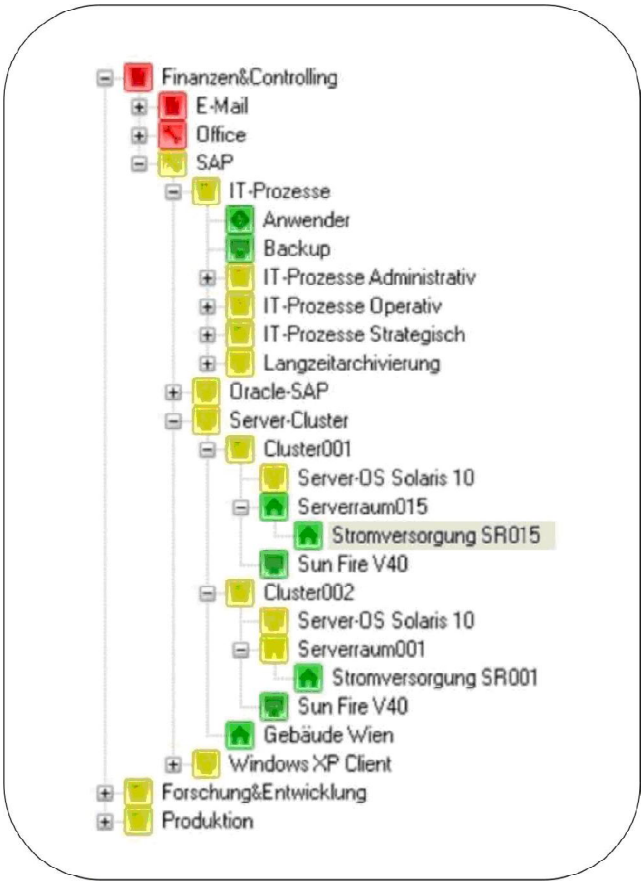


Фиг. 3. Standards & Poors's рейтингов модел

CRISAM предлага възможност точно да се определят собствениците на всички активи, с помощта на съществуващата система за рейтинг, и детайлно описва всички процеси в така нареченото ***Дърво на грешките*** (фиг. 4.), като по този начин много лесно могат да се идентифицират критичните елементи. Отправна точка за техниката Fault Tree Analysis (FTA) – Анализ посредством дърво на грешките, е най-важното нежелано събитие и посредством дървовидна диаграма се анализират факторите, които го причиняват. Оценката на риска се извършва също по рейтингов модел.

3. OCTAVE – Operationally Critical Threats Asset and Vulnerability Evaluation – оперативни критични заплахи на активите и оценка на уязвимостта – безплатен американски метод, създаден през 1999 г. в Carnegie Mellon University в сътрудничество с CERT и използващ секционно-базиран подход за идентифициране на съществуващите рискове. (фиг.5.)

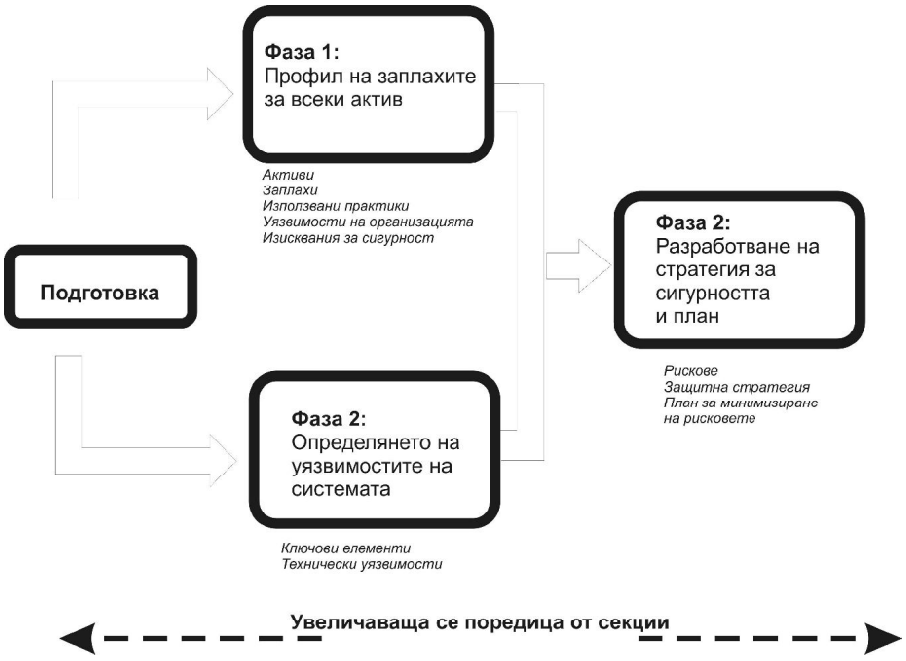
OCTAVE S е специална версия за малки организации, а OCTAVE Allegro се фокусира върху информационните активи. Изпълнението на OCTAVE метода е зависимо от подкрепата на персонала в организацията, затова в подготвителната фаза се прави избор на аналитичен екип, който ще изпълнява отделните стъпки на процеса. Хората – техни специални умения, също се считат за актив в този метод.



Фиг. 4. CRISAM Дърво на грешките

4. EBIOS

EBIOS – френски метод, разработен през 1995 г., за нуждите на френското правителство от ANSSI – Информационна агенция за сигурността на националните системи. Из-



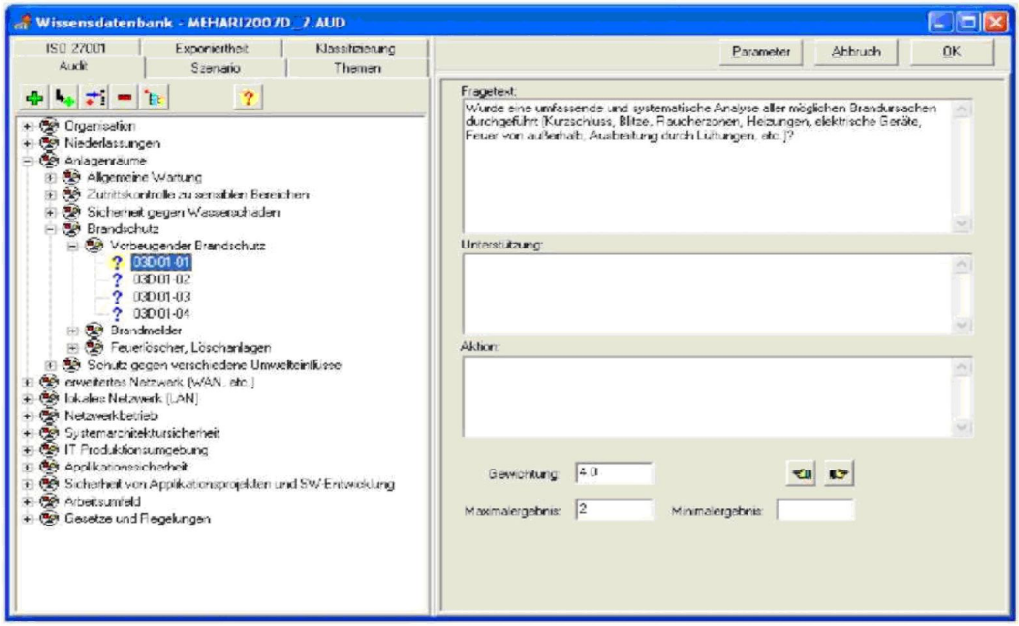
Фиг. 5. OCTAVE Процес на управление

разява нуждите и определя целите, свързани със сигурността. В софтуера EBIOS са интегрирани въпросници, целящи да генерират база от данни за организацията и нейните цели, да ги идентифицират, документират в този инструмент и с помощта на които да се направи последващ анализ на риска.

Лицата, извършващи оценка на риска, не е необходимо да имат специфичен опит, тъй като оценката на потребителите, дадена в тези въпросници, е от решаващо значение за по-нататъшния анализ. Важна част за прилагането на този метод е *анализ на изискванията* – да се определят критериите, на които отговаря рискът, както и специфичните нужди на организацията, свързани със сигурността. На базата на анализа на заплахите и уязвимостите EBIOS предоставя списъци с произхода на атаките в сигурността, причината за заплахите, уязвимите активи и формулира потенциалните последици за организацията. Определянето на критерии за избор на подходящи мерки за противодействие на риск, не е част от този метод.

5. MEHARI (Risicare)

MEHARI е безплатен метод, разработен от френската неправителствена организация CLUSIF. Софтуерът с който се прави анализ на риска за определени отрасли на бизнеса се нарича Risicare (фиг.6). Разработен е през 1998 г. от френската компания BUS S.A. и предоставя модел за управление на риска на базата на каталог от проверки свързане със сигурността. Основният елемент в анализа на риска е одитът, който по различни критерии извършва оценка на съществуващия риск и включва списъци със мерки.



Фиг. 6. Risicare

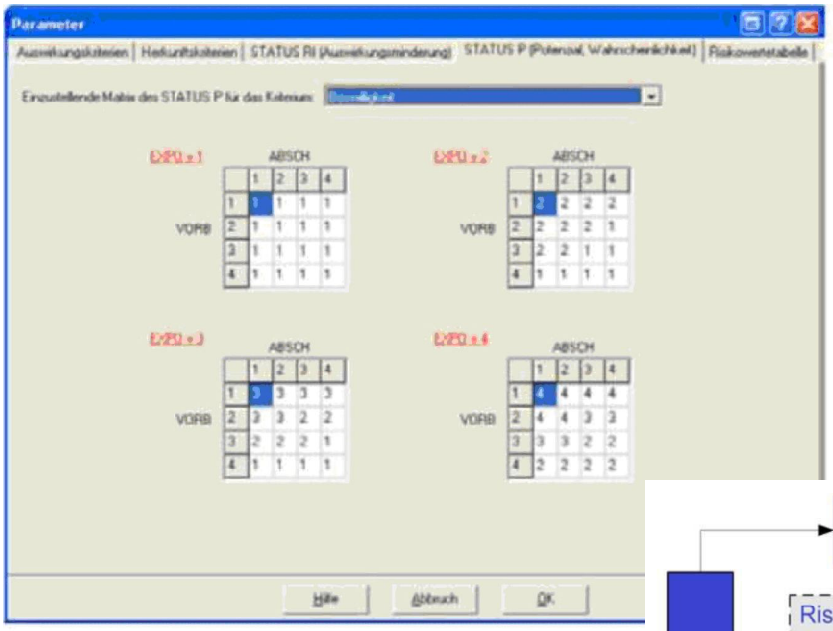
Технологията, използвана в Risicare на метода MEHARI, използва сценарии за идентификация на съществуващия риск.

Всеки сценарий е с уникално име и се отнася за определен актив на организацията, като го анализира на база критериите – поверителност, цялостност и наличност. Методът MEHARI позволява оценка на риска за организацията, посредством матрица на потенциалните заплахи и вероятността от тяхното възникване. (фиг.7.)

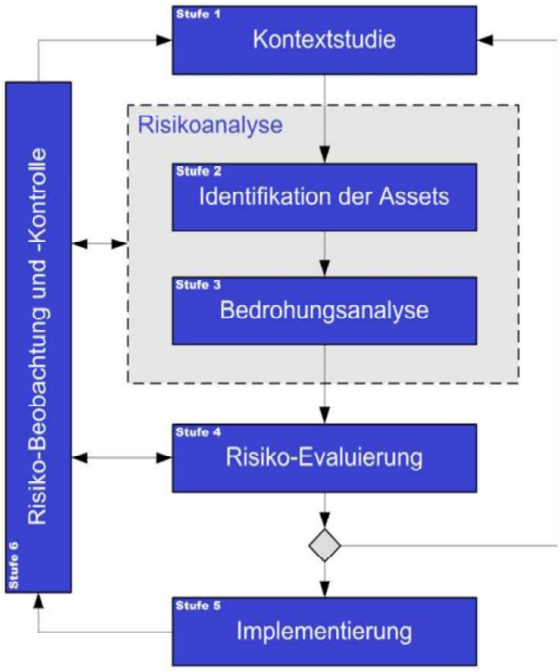
6. ARIMA

ARIMA е нов метод за управление на риска, разработван в Австрия, който се опитва да развие по възможно най-добрия начин процеса описан в ISO/IEC 27005 на базата на съществуващите методи – EBIOS, CRISAM, OCTAVE и CRAMM. За целта е разработен нов модел за изчисляване и

оценка на риска. Процесът при този метод е почти идентичен на ISO/IEC 27005, но етапите са намалени, което внася по-голяма яснота и е улеснение за организациите (фиг. 8.). В първия етап се определя политиката за сигурност на информацията, съгласно изискванията, целите и нуждите на организацията и съобразена със законовата и нормативна база.



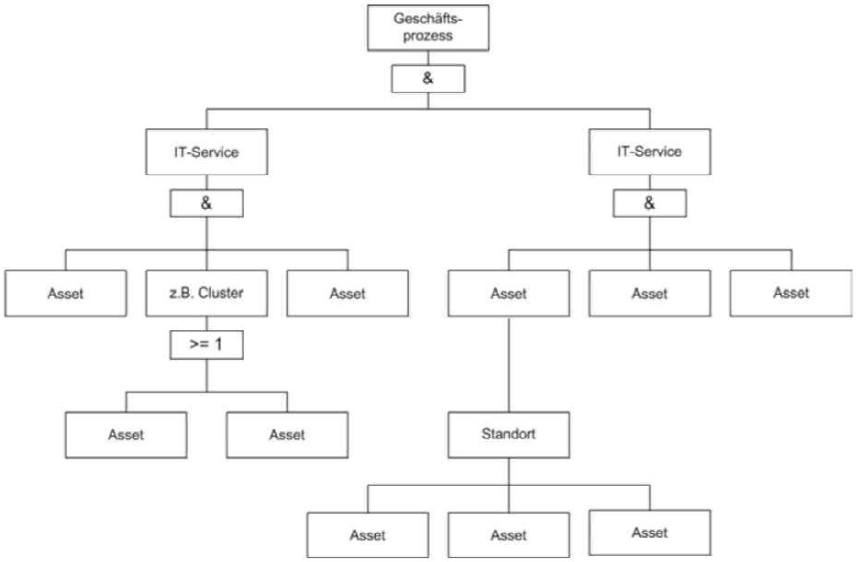
Фиг. 7. Risicare матрица



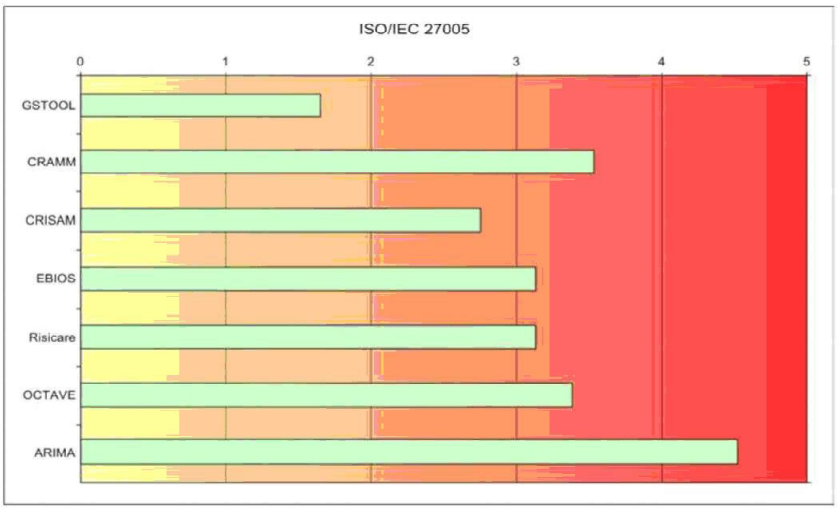
Фиг. 8. ARIMA процес

Дървото на услугите (Tree Service) (фиг. 9) е ключов компонент от този метод и с негова помощ се идентифицират активите за всеки едни процес в организацията. Всеки актив е обвързан с пет категории заплахи – форсмажорни, организационни пропуски, технически грешки, вътрешни заплахи и външни заплахи. Приложен е и списък с 40 потенциални заплахи и техните източници. За пълна и ефективна реализация на този метод се разработват и списъци с уязвимости, съпоставени със идентифицираните заплахи, както и мерки за противодействие и анализ на риска.

Чрез инструмента за реализация на метода ARIMA, който е web-базирано приложение, се очаква да се генерират и примерни доклади за управление. На фиг.10 е показано съотношението между ARIMA и останалите методи за управление на риска по отношение на цялостното изпълнение на стъпките на процеса, описан в ISO/IEC 27005.



Фиг. 9. ARIMA Tree Service [11]



Фиг. 10. Съотношение между ARIMA и останалите методи [11]

Заключение

Информационната сигурност зависи от хора, процеси и технологии. Хората следват процеси и използват технологии, за да предпазят информационните ресурси. Игнорирането на който и да е от тези елементи е равносилно на игнорирането на информационната сигурност като цяло.

Информационната сигурност изисква нови начини на мислене и поведение в рамките на информационните системи и мрежи.

Сигурността на информацията и управлението на риска е инвестиция, насочена към намаляване на оперативните разходи или разходите при разкриване на нови източници на печалба.

РЕЗЮМЕ

Управлението на информационната сигурност и информационния риск е концепция, която съдържа схващането, че организацията съществува, за да предоставя услуги за потребителите в съответствие с техните нужди, и да гарантира икономически най-ефективното използване на ИТ активите и информацията. Разгледани са методи за анализ на риска съгласно ISO/IEC 27005:2009 – GRAMM, CRISAM, OCTAVE, EBIOS, MEHARI, ARIMA.

ABSTRACT

Information security according to ISO / IEC 27001:2006 ISMS is a combination of three elements: confidentiality, integrity, availability of information. It aims to protect the information resources of the organization without being in conflict with the safety of the personnel, the laws and regulations and generally accepted moral principles.

The management of the information security and the information risk is a concept that contains the understanding, that the organization exists to provide services to the users according to their needs and to ensure the most cost-effective use of IT assets and information.

The article discusses methods for risk analysis in accordance to ISO/IEC 27005:2009 – GRAMM, CRISAM, OCTAVE, EBIOS, MEHARI, ARIMA.

ЛИТЕРАТУРА

1. ISO/IEC 27001:2006 ISMS – Requirements

2. ISO/IEC 27005:2009 Information security risk management

3. Регламент № 460/2004 на Европейския парламент и на Съвета от 10 март 2004 г. относно създаване на Европейската агенция за мрежова и информационна сигурност (ОВ L 77,13.3.2004 г., стр. 1)

4. BS 31100:2008 Workshop on British Standard – Code of practice for Risk Management

5. British Standards Institution – http://www.bsigroup.com/

6. http://www.iso27001certificates.com/

7. Angengerbauer, G.: *CRISAM Philosophie.* Calpana Business Consulting GmbH, April 2006. Vom Hersteller erhalten.

8. Alberts, Cristopher und Auder Dorofee:OCTAVE Threat Profiles.CERT http://www.cert.org/archive/pdf/OCTAVEthreatProfiles.pdf

9. BUC S.A.: *Users Guide of RISICARE* 2007 *Enterprise,* 2007

10. Edward J Humphreys – WS 2011-12, Information security risk management, Hagenberg University, Austria

11. I.Schaumьller – Bichl WS 2011-12 – Information Risk Management, Hagenberg University, Austria

12. Prokein, Oliver: „IT-Risikomanagement", Februar 2008

13. *Woody, Carol: Applying OCTAVE: Practitioners Report.* Carnegie Mellon University, http://www.cert.org/archive/pdf/01tr016.pdf

14. http://www.cep.eu/en/home/

15. http://www.mastercontrol.com/company/

16. http://www.quality.government.bg/page.php?sitemap

17. http://www.net-security.org

18. Insight Consulting: *CRAMM v5.1 Information Security Toolkit*, http: //www.cramm.com/files/datasheets/CRAMM%20(Datasheet).pdf

19. Insight Consulting: *The Logic behind CRAMMs Assessment of Mea-sures of Risk and Determination of Appropriate Countermeasures,* http://www.cramm.com/files/techpapers/CRAMM%20Countermeasure%20Determination%20and%20Calculation.pdf

20. Martin, Kevin C&Artur Perez: *GAMP 5 Quality Risk Management Approach.* 2008, http://www.vialis.ch/fileadmin/files/imgs/pdf/ Newsletter/08MJ-Martin.pdf

21.http://www.clusif.asso.fr/fr/ production/ouvrages/pdf/MEHARI-2007-Risikoanalyse.pdf

22. http://www.enisa.europa.eu/

23. http://www.sec.gov/about/laws/soa2002.pdf

24. http://www.nist.gov/index.html

25. http://www.moody.bg/

26. http://www.cpdp.bg/

27. http://www.cramm.com/

28. https://www.bsi.bund.de/EN/Home/home_node.html

29. http://www.ssi.gouv.fr/en/

30. http://ec.europa.eu/governance/impact/index_en.htm

31. http://www.iseca.org/

32. http://www.emsa.europa.eu/documents.html

33. http://www.a-sit.at/de/allgemein/asit_en.php