SocioBrains
ISSN 2367-5721, JOURNAL HOMEPAGE: WWW.SOCIOBRAINS.COM
INTERNATIONAL SCIENTIFIC REFEREED ONLINE JOURNAL WITH IMPACT FACTOR
ISSUE 42, FEBRUARY 2018

SECURITY AND VULNERABILITY OF THE MODERN INFORMATION SYSTEMS IN THE GOVERNMENT AGENCIES, PRIVATE ORGANIZATIONS AND ACADEMIC INSTITUTIONS

Abstract: In this paper a summarized educational research of security and vulnerability of the Information Systems is made. Most of the network system administrators, security professionals, network architects and IT specialists have to know all phases of creation, exploration and maintenance of the modern information systems in academic institutions.

Keywords: Information Systems, Computer and network administrators, LAN, Protocols, Routing, Security, Vulnerability, WAN.

Authors information:

Petar Boyanov
Chief Assistant Professor, PhD,
Lecturer in Department
"Communication and Computer Technologies"
at Konstantin Preslavsky University of Shumen
✉ peshoaikido@abv.bg
Bulgaria

Hristo Hristov
Associate Professor, PhD,
Lecturer in Department
"Management of Security Systems"
at Konstantin Preslavsky University of Shumen
✉ hristov63@abv.bg
Bulgaria

1. Въведение

Същност на информационната система

Информационните системи (ИС) представляват специализирани бази от данни със строго насъбрани и обобщени в определена област данни и съответната система за управление на базата от данни. Натрупаните данни в изградената информационна система могат да бъдат предназначени за работа в най-различни области като национална сигурност, администрация, икономика, наука, компютърна техника, правни науки, бизнес процеси, връзки с обществеността и др [3], [4], [5], [6], [9], [11], [13], [16].

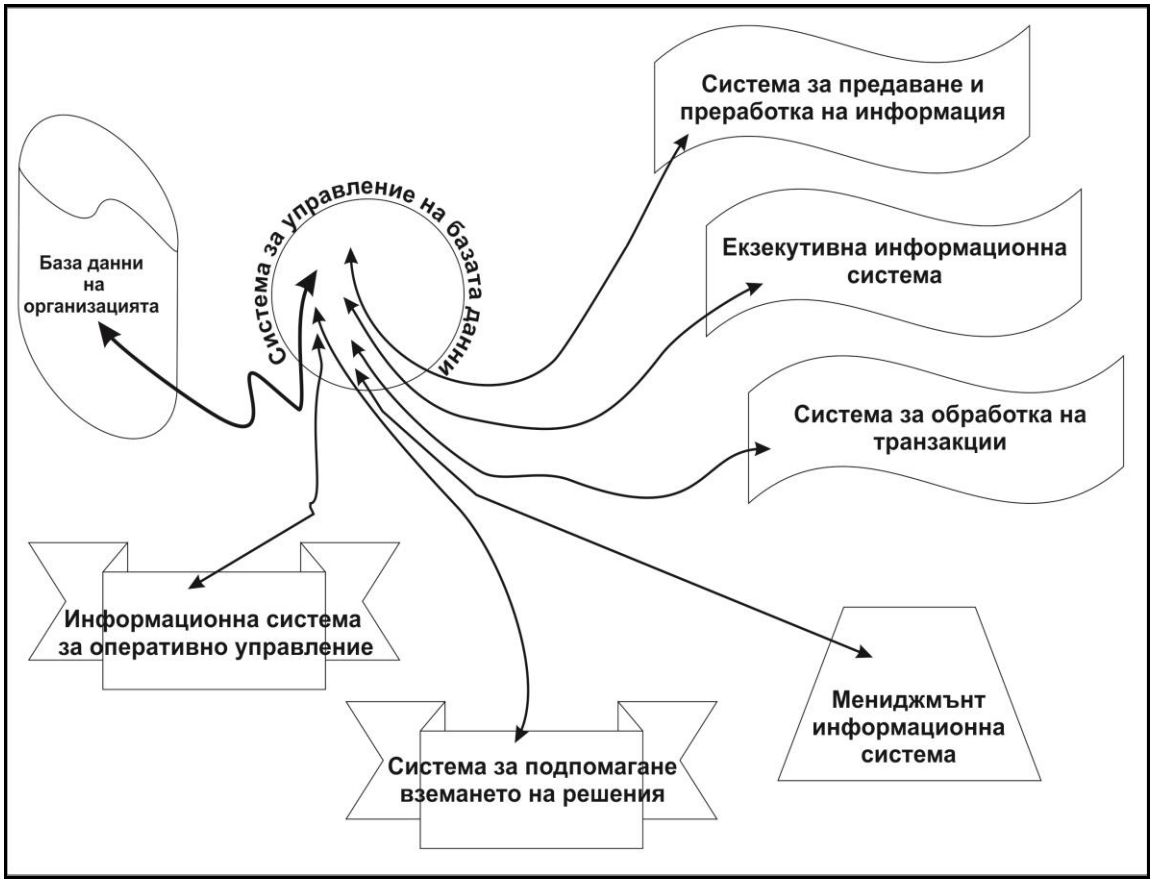
2. Изложение

Съвременната информационна система на дадена организация се състои от следните подсистеми [1], [2], [3], [4], [5], [6], [7], [8], [10], [12], [14], [15]:

- Автоматизирана информационна система (АИС).
- Автоматизирана система за управление (АСУ).
- Компютърна информационна система - Computer Information System (CIS).
- Мениджмънт информационна система - Management Information System (MIS).
- Управленска информационна система (УИС).
- Компютърно базирана информационна система - Computer-Based Information System (CBIS).
- Система за обработка на транзакции (СОТ).
- Система за обработване на данни (СОД).
- Система за предаване и преработка на информация Transaction Processing System (TPS).
- Система за управление на база данни - DataBase Management System (DBMS).

- Информационна система за оперативно управление - Operational Information System (OIS).
- Система за подпомагане вземането на решения - Decision Support System (DSS).
- Екзекутивна информационна система - Executive Information System (EIS).

Архитектурата на информационната система на дадена организация представлява сложна взаимосвързаност на изброените по-горе подсистеми. Това е показано на фиг. 1.

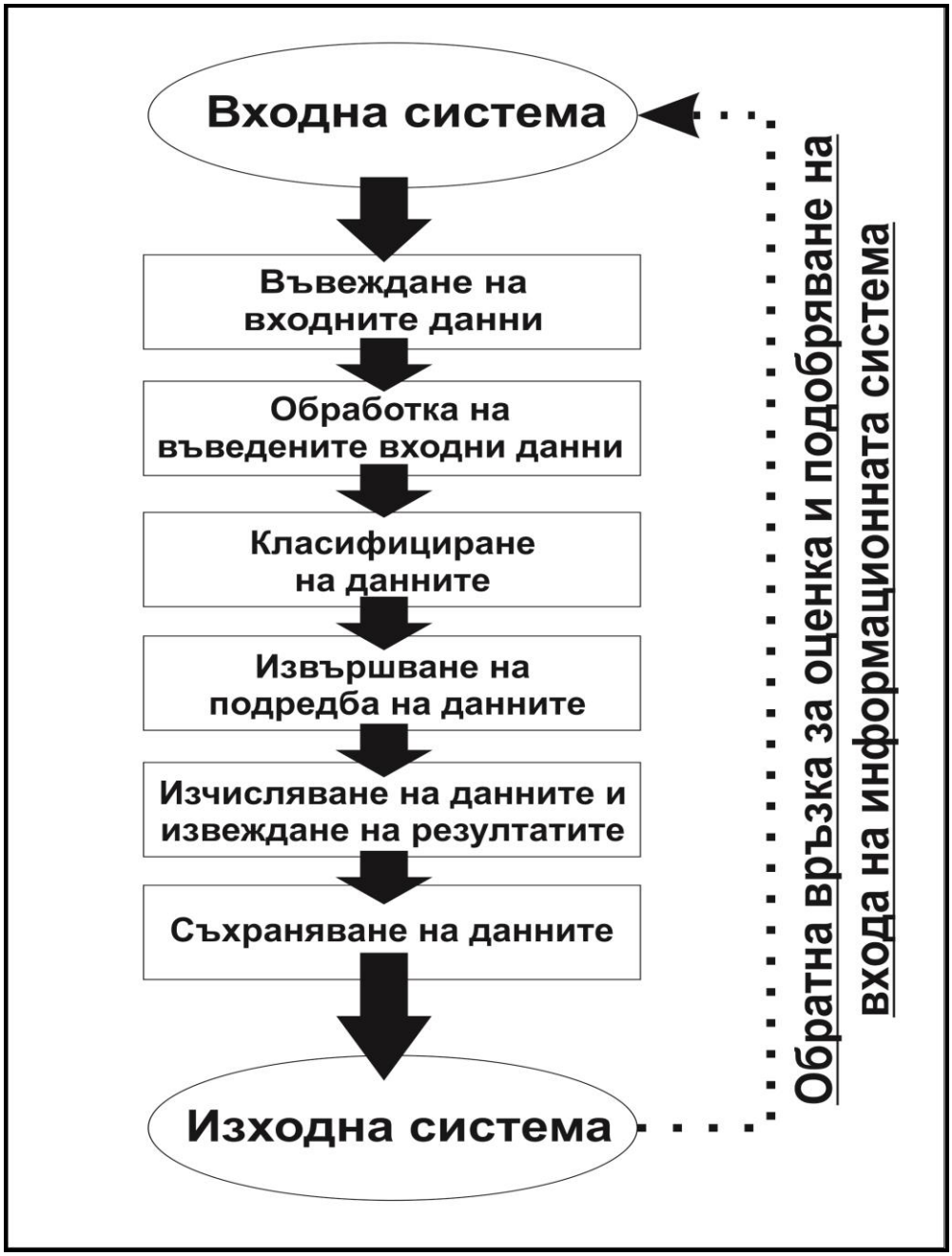


Фиг. 1. Архитектурата на информационната система на дадена организация

Функции на информационната система

Основните функции на информационната система са [1], [2], [3], [4], [5], [6], [10], [12], [13], [14], [16], [17], [18]:

- Въвеждане на входните данни.
- Обработка на въведените входни данни от околната среда или организацията.
- Класифициране на данните.
- Извършване на подредба на данните.
- Изчисляване на данните и извеждане на резултатите.
- Съхраняване на данните. Всичко това е показано на фиг. 2.



Фиг. 2. Функции на информационната система

Уязвимости на информационната система

Уязвимостта може да представлява софтуер, хардуер, услуга, процес или човешка слабост, която може да осигури на киберизвършителя възможност за проникване в компютърната машина на хоста през незащитен отворен порт с цел придобиване на нерегламентиран достъп до информационните ресурси [1], [4], [10], [14], [15], [16], [19], [20], [21].

Уязвимостта представя съществуването или липсата на определени слабости и дупки в защитата на компютърната система [15], които могат да бъдат експлоатирани [7], [8], [9], [10], [11]. В повечето случаи уязвимостта е услуга, стартирана на обикновена компютърна машина или сървър, незакърпени дупки в програмни приложения или в софтуера на използваната операционна система, неконтролирана споделена папка по локалната компютърна мрежа, отворен или нефилтриран порт на защитна стена, изключително слаба физически сигурност, която позволява на всеки човек да проникне в сървърно помещение [4], [5], [6], [8], [10], [12], [15]

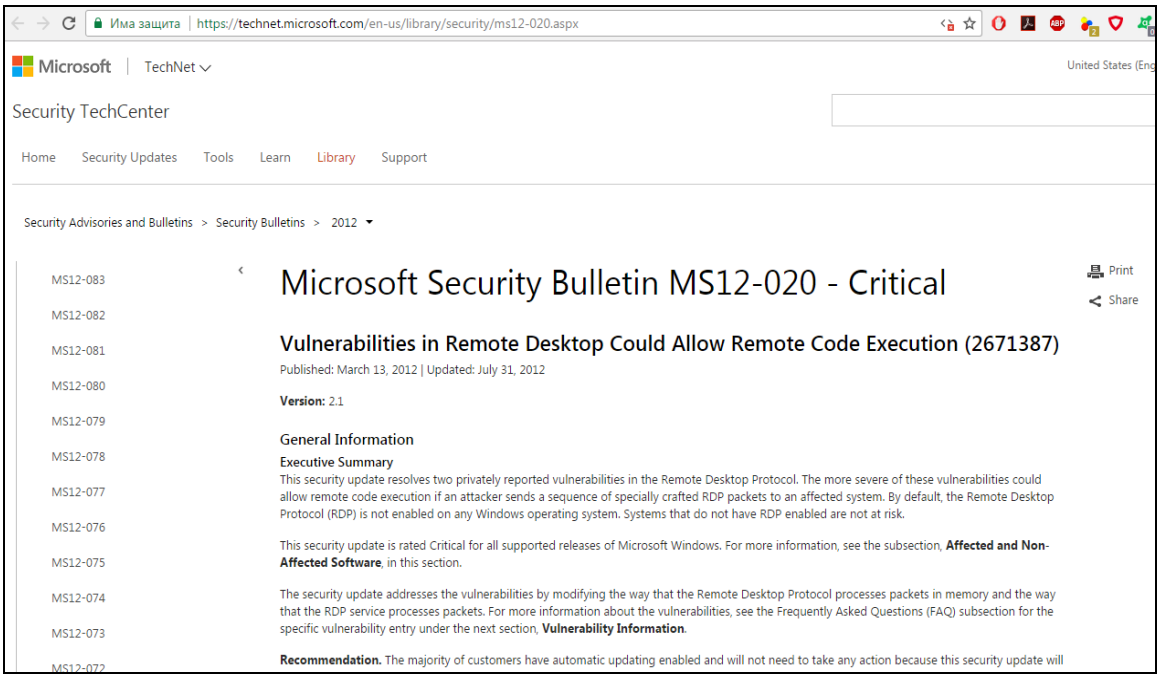
Видовете разпространени уязвимости на информационната система са [2], [3], [4], [5], [16], [17], [18]:

- Физическа уязвимост, свързана с получаване на пряк неоторизиран достъп до информационната система.
- Природна уязвимост, свързана с поява на бури, стихии и други природни явления.
- Апаратна и програмна уязвимост, свързана с неправилно конфигуриране на хардуерните и софтуерните елементи на информационната система.
- Уязвимости в периферните устройства, свързани с поставянето на специални шпиониращи устройства към клавиатурата, мишката, уеб камерата, тонколоните, скенерите и други устройства.
- Уязвимости от електромагнитно излъчване.
- Комуникационни уязвимости.
- Човешки уязвимости, свързани с неспазване на регламентираните правила за защита на информацията.
- Експлоатационни уязвимости и др.

База данни на уязвимостите

Администраторите по сигурността на информацията могат да получат детайлна и изчерпателна информация за най-новите открити уязвимости и слабости в операционните системи чрез базите данни за уязвимости. Едни от най-разпространите бази данни за уязвимости са [2], [4], [5], [7], [8], [9], [10], [11], [13], [14], [17], [19], [20], [21]:

- CVE (Common Vulnerabilities and Exposures).
- OSVDB (Open Sourced Vulnerability Database).
- NVD (National Vulnerability Database).
- EDB (Exploit Database).
- MSB (Microsoft Security Bulletin). Това е показано на фиг. 3.
- US-CERT bulletins и др. Това е показано на фиг. 4.



Фиг. 3. База данни MSB

Фиг. 4. База данни US-CERT bulletins

ЗАБЕЛЕЖКА: Всичките експерименти и изследвания в тази статия са направени в специализирана компютърна лаборатория във Факултета по технически науки при Шуменския университет „Епископ Константин Преславски“, състояща се от няколко хоста и в домашна частна локална компютърна мрежа, състояща се от четири хоста. Всичко илюстрирано и обяснено в тази статия е с научно-изследователска цел и авторите не носят отговорност в случаи на злоупотреба с него.

Чл. 319а. (Нов - ДВ, бр. 92 от 2002 г.) (1) (Изм. - ДВ, бр. 38 от 2007 г.) „Който копира, използва или осъществи достъп до компютърни данни в компютърна система без разрешение, когато се изисква такова, се наказва с глоба до три хиляди лева.” // Наказателен кодекс - Чл. 319а. (Нов - ДВ, бр. 92 от 2002 г.) (1) (Изм. - ДВ, бр. 38 от 2007 г.).

3. Заключение

Благодарение на постигнатите резултати след проведеното изследване с научна и образователна цел се установи, че всеки един системен администратор, професионалист по сигурността и мрежов архитект е необходимо да знаят всички детайли относно функционирането на съвременните информационни системи. В същото време съвременното общество използва редовно вече всички модерни технологии като мобилни смарт телефони, таблети, преносими компютри и киберпрестъпниците намират изключително много уязвимости и слаби места в мобилните и настолните операционни системи.

References:

1. Vasileva R, „Analiz na sastoyanieto na zashtita pri bedstvia v Bulgaria“, NS s mezhdunarodno uchastie "Kursantite i studentite na morskoto uchilishte i naukata", VVMU “N. Y. Vaptsarov", Varna, 26-27 mart 2015 g.
2. Dosev N. Y., Sazdavane na sklad ot danni za opredelyane na riska za informatsionnata sigurnost na korporatsiyata", Nauchna konferentsia s mezhdunarodno uchastie na tema „Kibersigurnostta v informatsionnoto obshtestvo”, Fakultet "A, PVO i KIS", Shumen 2017 g.

3. Dosev N. Y., Nepravitelstveniyat sektor i natsionalnata sigurnost“, Treta mezhdunarodna nauchna konferentsia –„Nauka, obrazovanie, inovatsii“, posvetena na 145 godishninata na BAN i 35 godishninata ot kosmicheskia polet na Georgi Ivanov, 21-23-05. 2014g., Shumen.
4. Tasheva Zh. N., R. A. Bogdanov, Tehnologichni reshenia za informatsionna sigurnost, Izdatelstvo na NVU „Vasil Levski, ISBN 978-954-753-130-7, 2013, 110 s.
5. Tasheva Zh. N., Harduerni i softuerni sredstva za informatsionna sigurnost, Izdatelstvo na NVU „Vasil Levski, ISBN 978-954-753-188-8, 2014, 136 s.
6. Tasheva Zh. N., Informatsionni tehnologii za sigurnost, Izdatelstvo na NVU „Vasil Levski, ISBN 978-954-753-190-1, 2014, 176 s.
7. Tasheva Zh. N., Boyanov P. Kr., "Sravnitelen analiz na zlonamereni ueb-bazirani ataki", Nauchna konferentsia na tema „Zashtitata na lichnite danni v konteksta na informatsionnata sigurnost”, Fakultet "Artileria, PVO i KIS" pri Natsionalniyat voenen universitet „Vasil Levski”, gr. Shumen, Balgraia, ISBN 978-954-9681-49-9, 6 - 7 Yuni 2013, str. 178 – 183.
8. Barry B. I., Chan H. A., Intrusion detection systems, Handbook of Information and Communication Security, Springer Berlin Heidelberg, ISBN: 978-3-642-04117-4, pp. 193 – 205.
9. Beale J., Foster J. C., Snort 2.0 Intrusion Detection, Syngress Publishing, 2003, ISBN: 1-931836-74-4, pp. 650.
10. Bejtlich R., The Practice of Network Security Monitoring: Understanding Incident Detection and Response, No Starch Press, 2013, ISBN-13: 978-1593275099, pp.376.
11. Berenjkoub, Mehdi S. H. F. H., A Taxonomy for Network Vulnerabilities, International Journal of Information & Communication Technology, May 2010, Vol.2, №1, pp. 29-44.
12. Boyanov P., Analysis and assessment of several security vulnerability databases, Third International Scientific Conference Science, Education, Innovation, Dedicated To The 145th Anniversary Of Bulgarian Academy Of Sciences And To The 35th Anniversary Of Georgi Ivanov’s Flightissn, ISBN 978-954-577-969-5, vol. II, Shumen, Bulgaria, 21-23 May 2014, pp. 118 – 122.
13. Dimanova D. "Risk management of critical infrastructure sites and facilities". International Scientific Refereed Online Journal With Impact Factor, 2017, ISSN 2367-5721.
14. Dimanova D, Kuzmanov Z, "Measuring and assessing risk". International Scientific Refereed Online Journal With Impact Factor, Issue 32, april 2017, ISSN 2367-5721. www.sociobrains.com.
15. Fry C., Nystrom M., Security Monitoring, O’Reilly Media, 2009, ISBN: 978-0-596-51816-5, pp. 248.
16. Hekmat S, “Communication Networks”, “PragSoft Corporation”, USA, 2005 г.
17. Helmer, Guy, et al. "A software fault tree approach to requirements analysis of an intrusion detection system", Requirements Engineering 7.4 (2002): 207-220.
18. Nachev, A., S. Zhelezov. Assessing the efficiency of information protection systems in the computer systems and networks. Informatsionnые tehnologii i bezopasnosty, Zhurnal Akad. nauk Ukrainы., Spets. vыpusk, Kiev, 2013, Str. 79-86
19. Ogletree, Terry William, ed. Upgrading and repairing networks. Que Publishing, 2004.
20. Stanev St., Szczypiorski Krzysztof., Steganography Training: a Case Study from University of Shumen in Bulgaria, Intl Journal Of Electronics And Telecommunications, 2016, Vol. 62, No. 3, Pp. 315-318, Manuscript received September 7, 2016; revised September, 2016, DOI: 10.1515/eletel-2016-0043.
21. Tasheva, Z. N., Tasheva, A. T. Combining cryptography and steganography in software system for hiding confidential information, International Journal of Science, Education and Innovation, Volume 1, 2013. ISSN 1314-9784, Association Scientific and Applied Research, pp. 84-92.