

# КОМПЮТЪРНИ НАУКИ И КОМУНИКАЦИИ



Електронно списание на  
Център по информатика и технически науки на  
Бургаски Свободен Университет

ТОМ 5, БРОЙ 1 (2016)

ISSN: 1314-7846

## Списание „Компютърни науки и комуникации”,

### Главен редактор

[prof. d-r Angel Toshkov](#), Bulgaria Burgas, 8001 SanStefano str. 62 Burgas Free University, Bulgaria

### Редакционна колегия

1. [prof. d-r Andon Lazarov](#), Burgas Free University, Bulgaria
2. [prof. d-r Acad. Ivan Popchev](#), Bulgarian Academy of Sciences, Sofia, Bulgaria
3. [prof. d-r Mihail Iliev](#), Technical University of Ruse, Ruse, Bulgaria
4. [prof. d-r Kiril Konov](#), Technical University of Sofia, Research Institute of Communications, Sofia, Bulgaria, Bulgaria
5. [prof. d-r Ivan Kolev](#), Technical university of Gabrovo, Gabrovo, Bulgaria
6. [prof. d-r Vencislav Valchev](#), Technical University of Varna, Bulgaria
7. [prof. d-r Daniela Orozova](#), Burgas Free University, Burgas, Bulgaria
8. [prof. d-r Михаил Фёдорович Меняев](#), Доктор педагогических наук, профессор, Академик Международной Академии Информатизации, Москва, Россия
9. [assoc.prof. d-r. Veselina Jecheva](#), 62 San Stefano Str., Burgas
10. [assoc.prof. d-r. Evgeniya Petrova Nikolova](#), 62 San Stefano Str., Burgas
11. [assoc. prof. d-r Marcin Paprzycki](#), Associate Professor in the Systems Research Institute of the Polish Academy of Sciences, Warsaw, Poland
12. [d-r Yingjie Yang](#), School of Computer Science and Informatics Centre for Computational Intelligence (CCI) and De Montfort University Interdisciplinary Group in Intelligent Transport Systems (DIGITS)
13. [Michela Tramonti](#), Università degli Studi "G. Marconi" Rome Area, Italy

ISSN: 1314-7846

Том 5, № 1 (2016)

Януари-Март, 2016 г.

## Съдържание

### Компютърни науки и комуникации

|                                                                                                                                                              |                     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#">ПОВИШАВАНЕ НА СИГУРНОСТТА ПРИ МОБИЛНОТО БАНКИРАНЕ ЧРЕЗ РЕАЛИЗИРАНЕТО НА АВТОМАТИЗИРАНИ ПРОВЕРКИ НА МОБИЛНОТО УСТРОЙСТВО</a>                      | <a href="#">PDF</a> |
| Бонимир Пенчев Пенчев                                                                                                                                        | 3-8                 |
| <a href="#">МОБИЛНИТЕ ШИРОКОЛЕНТОВИ МРЕЖИ – ЕФЕКТИВЕН НАЧИН ЗА ПРЕОДОЛЯВАНЕ НА ЦИФРОВТО РАЗДЕЛЯНЕ И СТИМУЛИРАНЕ ИЗПОЛЗВАНЕТО НА УСЛУГИТЕ НА Е-УПРАВЛЕНИЕ</a> | <a href="#">PDF</a> |
| Janet Zaharieva                                                                                                                                              | 9-18                |
| <a href="#">МЕТОД ЗА ОПТИМИЗИРАНЕ НА СРОКОВЕТЕ ЗА ПРОФИЛАКТИКА НА СЛОЖНИ ТЕХНИЧЕСКИ СИСТЕМИ В СЪОТВЕТСТВИЕ С НЕОБХОДИМОТО РАВНИЩЕ НА ТЯХНАТА НАДЕЖНОСТ</a>   | <a href="#">PDF</a> |
| Anton Slavchev Georgiev, Nikolov Nikolay, Toncho Papanchev                                                                                                   | 19-27               |
| <a href="#">TESTBED FOR ONE-WAY IP PACKET DELAY MEASUREMENT IN SMART GRID WAMS APPLICATIONS BASED ON IEEE C37.118 (ENGLISH)</a>                              | <a href="#">PDF</a> |
| Мартин Иванов, Розалина Димова                                                                                                                               | 28-38               |
| <a href="#">ИНФОРМАЦИОННАТА СИГУРНОСТ ПРЕЗ XXI ВЕК – КОНЦЕПТУАЛНИ АСПЕКТИ</a>                                                                                | <a href="#">PDF</a> |
| Божидар Виолинов Божинов                                                                                                                                     | 39-50               |
| <a href="#">A MATHEMATICAL METHOD FOR INTEGRATION OF INFORMATION, WHICH IS SIMILAR IN NATURE, FOR THE PURPOSE OF MEDICAL RESEARCH</a>                        | <a href="#">PDF</a> |
| Цветослав Антонов Георгиев                                                                                                                                   | 51-59               |
| <a href="#">Паралелно сравнително разпознаване на лица при идеални и не идеални условия с Hidden Markov Model (HMM) и Sparse разпознаване</a>                | <a href="#">PDF</a> |
| Petya Petrova Petrova                                                                                                                                        | 60-65               |

## **CISCO ACADEMY КЪМ БУРГАСКИ СВОБОДЕН УНИВЕРСИТЕТ**

### **В Сиско академията към БСУ се провежда обучение на курсисти по плана на CCNA Routing and Switching**

#### **Информация за провежданите курсове по CCNA R&S**

**Модул 1 – Introduction to Networks** – въведение в мрежовите архитектури, компоненти и принцип на работа. Преглед на основите на мрежовата комуникация, Интернет, OSI референтния модел. В този семестър са включени теми, разглеждащи в детайли IPv4 и IPv6 адресирането, Ethernet и различните видове преносни среди. След завършване на този семестър курсистите могат да проектират и изградят локални мрежи за нуждите на малки офиси, да проектират и реализират успешно IP адресиране и да конфигурират най-основните функции на маршрутизаторите и комутаторите.

Теми:

1. Живот в мрежов свят.
2. Комуникации в мрежите.
3. Приложно ниво – функции и протоколи.
4. Транспортно ниво на OSI модела.
5. Мрежово ниво и маршрутизация.
6. Адресиране в мрежите. Протокол IPv4.
7. Канално ниво.
8. Физическо ниво на OSI.
9. Ethernet мрежи.
10. Планиране и окабеляване на мрежа.
11. Конфигуриране и тестване на мрежа.

**Модул 2 – Routing and Switching Essentials** – Семестърът включва теми, свързани с описание на мрежовите архитектури, компоненти и принцип на работа на маршрутизаторите и комутаторите в малки и средни мрежи. Курсистите се обучават как да конфигурират маршрутизатори и комутатори на Cisco Systems. След завършване на обучението курсистите могат да конфигурират, наблюдават и поддържат малки и средни офис мрежи, като използват протоколите RIPv1, RIPv2, OSPF, VLAN, Inter-VLAN routing с IPv4 и IPv6.

Теми:

1. Въведение в маршрутизацията и препращането на пакети.
2. Статична маршрутизация.
3. Въведение в динамичната маршрутизация.
4. Маршрутизиращи протоколи с вектор на разстоянието (Distance Vector).
5. Протокол RIPv1.
6. Безкласови маршрутизиращи протоколи. Технологии VLSM и CIDR.
7. Протокол RIPv2.
8. Маршрутна таблица: поглед отблизо.
9. Протокол EIGRP.
10. Маршрутизиращи протоколи със състояние на връзките (Link State).
11. Протокол OSPF.

**Ниво 3 – Scaling Networks** – Разглеждат се архитектурата, компонентите и принципа на работа на маршрутизаторите и комутаторите в големи офис мрежи. Курсистите се обучават как да извършват сложно конфигуриране на необходимата мрежова функционалност при големи мрежови топологии. След успешно завършване на семестъра курсистите могат да конфигурират и отстраняват проблеми, свързани с OSPF, EIGRP, STP, VTP за IPv4 и IPv6. Също така курсистите имат знания и умения за конфигуриране на DNS и DHCP.

Теми:

1. Проектиране на локални мрежи.
2. Основни концепции и конфигуриране на комутатори.
3. Виртуални локални мрежи (VLAN).
4. Базов протокол за виртуални локални мрежи (VTP).
5. Протокол на минималното дърво (Spanning-Tree Protocol).
6. Маршрутизация между виртуални локални мрежи (Inter-VLAN Routing).
7. Основни концепции и конфигуриране на безжични мрежи.

**Ниво 4 – Connecting Networks** – В този семестър се разглеждат теми, свързани с WAN мрежите, използването на приложения в сложни мрежови инфраструктури. Курсистите се запознават с актуалните WAN технологии, както и техните предимства и недостатъци. Практическите знания са свързани с конфигуриране на WAN протоколи, VPN, NAT, наблюдение и отстраняване на проблеми при WAN.

Теми:

1. Въведение в глобалните мрежи.
2. Протокол за съединения точка-точка PPP.
3. Технология Frame Relay.
4. Мрежова сигурност.
5. Списъци за управление на достъпа (ACL).
6. Услуги за отдалечени потребители.
7. Услуги за IP адресиране.
8. Диагностика на компютърни мрежи.

Допълнителна информация можете да получите на [cisco.bfu.bg](http://cisco.bfu.bg)

За контакти:

**проф.д-р Ангел Тошков**  
Ръководител  
тел.: 056 900 591  
БСУ, стая Б-1  
[angel@bfu.bg](mailto:angel@bfu.bg)

**гл. ас. д-р Димитър Минчев**  
Инструктор  
Тел.: 056 900 477  
БСУ, стая 417  
[mitko@bfu.bg](mailto:mitko@bfu.bg)

**проф.д-р Андон Лазаров**  
Инструктор  
Тел.: 056 900 485  
БСУ, стая Б-1  
[lazarov@bfu.bg](mailto:lazarov@bfu.bg)

**гл. ас. Атанас Димитров**  
Инструктор  
Тел.: 056 900-432  
БСУ, стая 32  
[atanas@bfu.bg](mailto:atanas@bfu.bg)

За информация относно заплащането, преподавателите, графици и текущи въпроси можете да се обръщате към:

**Златина Николова**  
Инспектор в Учебен отдел  
тел.: 056 900 454  
БСУ, стая 24  
[nikolovazl@bfu.bg](mailto:nikolovazl@bfu.bg)

## ENHANCING THE SECURITY OF MOBILE BANKING THROUGH THE IMPLEMENTATION OF AUTOMATED CHECKS ON THE MOBILE DEVICE

*Penchev Bonimir, University of Economics – Varna, PhD student at Institute of Mathematics  
and Informatics - Bulgarian Academy of Sciences, [b.penchev@ue-varna.bg](mailto:b.penchev@ue-varna.bg)*

**Abstract:** Despite the advantages that mobile banking has for both banks and customers, there are also certain barriers that have a negative influence on its large-scale adoption. One of these barriers is its security level. In our previous research we have identified a certain number of security attacks against mobile banking security. Along with them, we have found out that not all of the protection strategies and best practices are effective enough. In terms of mobile banking application an area of improvement is associated with the failure in training the user regarding certain recommended security actions offered by mobile banking service providers. Therefore the objective of the report is to design a tool to facilitate users by implementing a set of automated checks in order to examine certain parameters of the mobile device directly related to the mobile banking security.

**Keywords:** mobile banking, mobile security, mobile device, mobile applications

## ПОВИШАВАНЕ НА СИГУРНОСТТА ПРИ МОБИЛНОТО БАНКИРАНЕ ЧРЕЗ РЕАЛИЗИРАНЕТО НА АВТОМАТИЗИРАНИ ПРОВЕРКИ НА МОБИЛНОТО УСТРОЙСТВО

*Бонимир Пенчев, Икономически университет – Варна, докторант към институт по  
математика и информатика при БАН, [b.penchev@ue-varna.bg](mailto:b.penchev@ue-varna.bg)*

**Абстракт:** Въпреки предимствата, които мобилното банкиране предоставя на банките и на техните клиенти, съществуват определени фактори, които оказват негативно влияние при възприемане му. Един от тези фактори е нивото на неговата сигурност. По отношение на мобилното приложение за мобилно банкиране насока за подобрене на сигурността е справянето с неуспехите при обучение на потребителя, свързано с реализирането на определени препоръчителни действия, предлагани от доставчиците на услуги за мобилно банкиране. Затова и целта на настоящата разработка е да се проектира инструмент, който да улесни потребителите, като реализира набор от автоматизирани проверки, които да изследват определени параметри на мобилното устройство, пряко свързани със сигурността на мобилното банкиране.

**Ключови думи:** мобилно банкиране, мобилна сигурност, мобилни устройства, мобилни приложения

### 1. Въведение

В продължение на повече от 40 години една от основните цели на финансовите институции е свързана с осигуряването на лесен достъп и удобство за своите клиенти при реализирането на банкови операции. Въпреки че АТМ устройствата и интернет

банкирането представляват ефективни канали за предоставяне на традиционни банкови продукти, един сравнително нов вид банкиране - мобилното банкиране - има значителен ефект върху пазара. За неговата актуалност и непрекъснато развитие свидетелстват проучвания, проведени в различни региони на света и обхващащи както развитите, така и развиващите се страни [1].

Постоянното развитие в посока по-широко разпространение на мобилното банкиране се дължи и на предимствата, които то предоставя както на банките, така и на техните клиенти [2]. Този канал позволява на потребителите да изпълняват финансови операции навсякъде, по всяко време, на по-ниска цена и без да е необходимо да посещават банков офис. От друга страна мобилното банкиране предлага стратегически предимства и на банките. То може да се използва като възможност за достигането до нови клиенти, може да подобри репутацията на организацията и нейните продукти или да послужи за провеждането на маркетингови кампании.

Въпреки тези предимства, използването на мобилни устройства с цел реализирането на банкови транзакции или получаването на достъп до финансова информация, не е толкова широко разпространено, както се очаква [3]. Това от своя страна свидетелства за съществуването на определени фактори, които оказват негативно влияние върху по-мощното възприемане на мобилното банкиране. С цел да идентифицираме кои са те, проведохме допълнително изследване. Неговите резултати не само ясно показаха, че в действителност съществуват различни фактори, които оказват негативно влияние върху потребителите при възприемане на мобилното банкиране, но и потвърдиха, че различните рискове, свързани с неговата сигурност, съществено въздействат при вземане на решение за неговото използване [4].

Представените по-горе резултати провокираха провеждането на следващо изследване, чиято основна цел беше да се проучат най-често проявяващите се уязвимости и заплахи за сигурността на мобилното банкиране. Фокусът на изследването беше насочен към потребителя, тъй като той много често се посочва като най-слабото звено по отношение на сигурността. В резултат на това, при него бяха идентифицирани четири основни проблемни области, засягащи сигурността - мобилно устройство, мобилен уеб браузър, мобилна операционна система и мобилно приложение за мобилно банкиране. Във всяка една от тях бяха проучени уязвимостите и произтичащите от тях заплахи, което доведе до определянето на най-често използваните атаки при мобилното банкиране: подслушване на преносната среда (eavesdropping атака, man in the middle атака), cross site request forgery атака, неупълномощен физически достъп до устройството, phishing атаки (vishing атака, smishing атака, tabnabbing атака и използване на phishing приложения) и злонамерен софтуер [5].

В научната литература за всяка една от посочените атаки съществува широк набор от добри практики и стратегии за защита. Установихме обаче, че не всички от тях са достатъчно ефективни и това налага внасянето на някои подобрения, които да повишат сигурността на мобилното банкиране във всяка една от проблемните области при потребителя.

По отношение на мобилното приложение за мобилно банкиране една от насоките за подобрение е справяне с неуспехите при обучение на потребителя, което е свързано с реализирането на определени препоръчителни действия, предлагани от доставчиците на услуги за мобилно банкиране.

От тук можем да дефинираме и целта на настоящата разработка - да се проектира инструмент, който да улесни потребителите, като реализира набор от автоматизирани проверки, които да изследват определени параметри на мобилното устройство, пряко свързани със сигурността на мобилното банкиране.

## **2. Повишаване на сигурността при мобилното банкиране чрез реализирането на автоматизирани проверки на мобилното устройство.**

За реализирането на целта сме проектирали софтуерен модул, който следва да се интегрира в мобилното приложение за мобилно банкиране. Въз основа на представените във въведението четири основни проблемни области за сигурността на мобилното банкиране сме съставили следния списък с автоматизирани проверки, които могат да бъдат включени в софтуерния модул:

- За реализиране на защита на мобилното устройство:
  - проверка за използването на некриптирана публична безжична мрежа;
  - проверка за реализирано криптиране на данните на мобилната операционна система;
  - проверка за използване на механизъм за удостоверяване преди използване на мобилното устройство;
  - проверка за включено автоматично заключване на мобилното устройство;
  - проверка за включена функция за изтриване на данните след определен брой пъти неуспешно удостоверяване;
  - проверка за включена функция за дистанционно заключване на мобилното устройство или за дистанционно изтриване на съдържанието му.
  - проверка за включените неизползваеми комуникационни интерфейси на мобилното устройство;
- За реализиране на защита на мобилната операционна система:
  - проверка за определяне дали мобилната операционна система е актуализирана;
  - проверка за определяне дали мобилната операционна система е модифицирана;
  - проверка за определяне наличието на мобилно антивирусно приложение;
  - проверка за определяне успешното засичане на модифициран злонамерен софтуер.
- За реализиране на защита на мобилното приложение за мобилно банкиране:
  - проверка за определяне дали мобилното приложение използва TLS протокол за предаване на данните към сървъра и коя версия се използва;
  - проверка за актуалността на версията на мобилното приложение за мобилно банкиране.

Представеният списък поражда някои съображения по отношение проектирането на софтуерния модул. Реализирането на толкова широк набор от проверки може да предизвика неудобство за потребителя, а това да доведе до отказ от използването на съответната услуга. От друга страна различните доставчици на тази услуга предоставят различни препоръчителни действия, които изискват от своите потребители. Затова при проектирането на модула е необходимо на банките, предоставящи мобилно банкиране да се даде възможност да определят кои проверки следва да бъдат задължителни, кои препоръчителни, както и възможност на един по-късен етап да се реализират промени като добавяне, премахване или модифициране на съответната проверка.

Въз основа на представените съображения, може да дефинираме, че софтуерният модул следва да бъде разработен като инструмент, който осъществява определен набор от автоматизирани проверки, дефинирани от доставчиците на услуги за мобилно банкиране, в резултат на което да помага на потребителите да предприемат определени действия, които да доведат до повишаване на нивото на сигурността при мобилното банкиране.

От архитектурна гледна точка софтуерният модул следва да бъде разделен на две основни части. Едната следва да бъде реализирана като компонент на мобилното приложение за мобилно банкиране, като по този начин в него следва да бъдат интегрирани допълнителни функционалности. Другата част следва да бъде разположена на сървър, където ще се поддържа базата от данни и където ще бъдат дефинирани проверките, които следва да бъдат реализирани.

За да осъществим неговата основна функционалност е необходимо да определим основните процеси, които трябва да реализира модулът. Те са:

- съставяне на списък от автоматизирани проверки;
- съхраняване на дефинирания списък в база от данни;
- реализиране на дефинираните автоматизирани проверки;
- представяне на резултатите на потребителя.

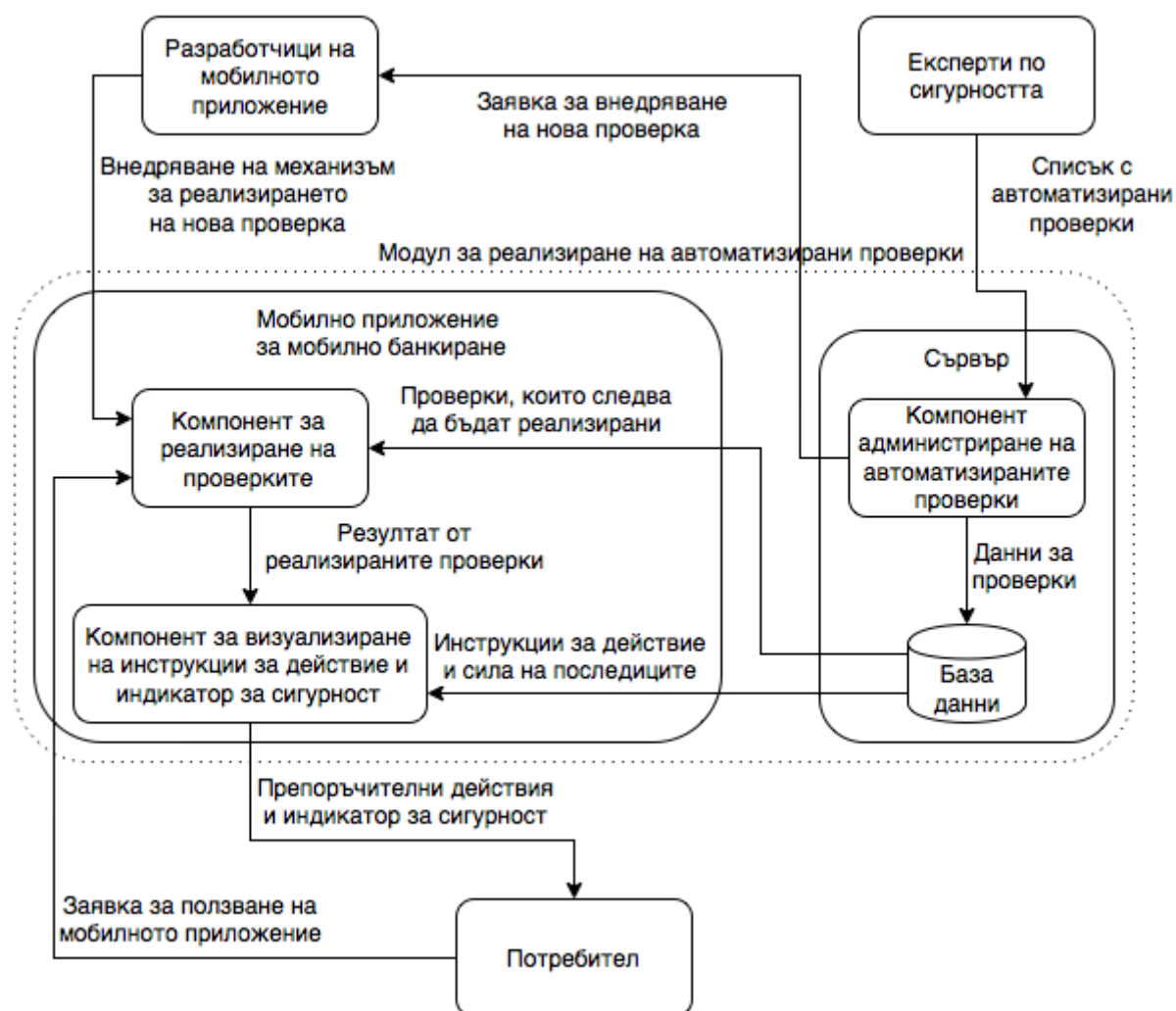
Процесът по съставяне на списъка от автоматизирани проверки следва да се извърши от експертите по сигурността на доставчика на услуги за мобилно банкиране. Този процес следва да включва редица дейности и да започва с анализ на сигурността, въз основа на който могат да бъдат определени съответните автоматизирани проверки, които следва да реализира модула. Следващата стъпка е свързана с реализирането на оценка на риска и по-специално дефиниране на силата на последиците ако някоя от определените проверки не бъде реализирана. По този начин ще се определи кои от тях са ключови и следва да бъдат задължителни и кои ще бъдат само препоръчителни.

След съставянето на списъка с автоматизирани проверки, те следва да бъдат въведени в база от данни, като основната цел тук е да се осигури тяхното повторно използване и ефективно управление. При реализирането на това за всяка проверка е необходимо да бъде съхранена информация за нейното име, нейния вид (задължителна или препоръчителна), инструкциите за действие, както и силата на последиците, ако тя не премине успешно. За всяка от нововъведените проверки е необходимо да се изпрати заявка до разработчиците на мобилното приложение, тъй като те трябва да интегрират нужната функционалност.

Процесът по реализиране на дефинираните автоматизирани проверки следва да се осъществи, когато потребителят стартира мобилното приложение за мобилно банкиране. При това ще се осъществи връзка с базата от данни, която се намира на сървъра, от където ще се установи броят и видът на проверките, които следва да бъдат реализирани. Първоначално следва да се започне със задължителните проверки. Само ако те преминат успешно, ще се премине към реализирането на препоръчителните проверки. За осъществяването на проверките е необходимо да се използва помощта на приложно програмния интерфейс (API) на съответната мобилна операционна система. Резултатите от всички проверки следва да бъдат предадени към следващия процес, който следва да ги представи на потребителя.

Ако резултатът от всяка от задължителните проверки е положителен потребителят следва да получи достъп до услугите за мобилно банкиране. В противен случай той ще получи инструкции какво трябва да направи, за да използва функционалностите на мобилното приложение. По отношение на препоръчителните проверки, както говори името им, отрицателният им резултат не следва да задължава по никакъв начин потребителя да реализира определени действия. От друга страна тяхното състояние следва да участва във формирането на стойност на индикатор на сигурността на мобилното устройство по отношение на мобилното банкиране. Ако потребителят желае да повиши тази стойност, е необходимо той да изпълни определени инструкции свързани с неуспешно преминалите препоръчителни проверки.

Въз основа на разгледаните процеси сме съставили следната архитектура на софтуерния модул за реализиране на автоматизирани проверки (вж. фиг. 1).



Фиг. 1. Архитектура на модула за реализиране на автоматизирани проверки

Както се вижда от представената на фиг. 1 архитектура, за осъществяването на софтуерния модул за реализиране на автоматизирани проверки е необходимо изграждането на три основни софтуерни компонента: компонент за администриране на автоматизираните проверки, компонент за реализиране на проверките, компонент за визуализиране на инструкции за действие и индикатор за сигурност.

### **3. Заключение**

В настоящата разработка представихме софтуерен модул за реализиране на автоматизирани проверки, чиято основна цел е повишаване на сигурността при мобилното банкиране. Акцентът беше поставен върху някои съображения, свързани с неговото проектиране, представяне на функционалните му възможности, както и общата му архитектура. Като насока за бъдеща работа може да очертаяме внедряване на представения софтуерен модул в дадено приложение за мобилно банкиране, в следствие на което и реализирането на проверка на неговата приложимост и ефективност.

### **References**

- [1] Global Mobile Statistics 2014 Section G: Mobile Banking and M-money; Section H: Venture Capital (VC) Investment in Mobile. <http://mobiforge.com/research-analysis/global-mobile-statistics-2014-section-g-mobile-banking-and-m-money-section-h-venture-capital-vc-inve>. Достъп до данните: 31.03.2016.
- [2] Esmaili, E., Desa M., Moradi H., Hemmati A. The Role of Trust and Other Behavioral Intention Determinants on Intention toward Using Internet Banking. International Journal of Innovation, Management and Technology, 2-1, 2011, p. 95-100.
- [3] Mobile Banking Handset & Tablet Market Strategies 2013–2017. [http://www.juniperresearch.com/reports/mobile\\_banking](http://www.juniperresearch.com/reports/mobile_banking). Достъп до данните: 31.03.2016.
- [4] Пенчев, Б. Фактори, оказващи негативно влияние върху потребителите при възприемане на мобилното банкиране. Известия на Съюза на учените – Варна, Серия „Икономически науки“, Варна, 2015, с. 150-155.
- [5] Penchev, B. Security Issues in Mobile Banking. In: Proceedings of International Conference Human Systems Integration Approach to Cyber Security, Sofia, 2016, p. 135-144.

## **MOBILE BROADBAND NETWORKS - EFFECTIVE WAY OF BRIDGE THE DIGITAL SEPARATION AND ENCOURAGE THE USE OF SERVICES FOR E-GOVERNANCE**

Zaharieva Janet, New Bulgarian University - janet.zaharieva@vivacom.bg

**Abstract:** The article examines "digital segregation" of the population in small and remote settlements in access to high speed internet and use of eGovernment services and services online. It offers a way to overcome this problem through measures by the government to stimulate the construction of mobile broadband networks in rural areas through public-private partnerships, investment funds under EU programs and complete release of spectrum in the band 790-862 MHz.

**Keywords:** e-government, high speed internet, mobile data, digital segregation, broadband networks

## **МОБИЛНИТЕ ШИРОКОЛЕНТОВИ МРЕЖИ – ЕФЕКТИВЕН НАЧИН ЗА ПРЕОДОЛЯВАНЕ НА ЦИФРОВТО РАЗДЕЛЯНЕ И СТИМУЛИРАНЕ ИЗПОЛЗВАНЕТО НА УСЛУГИТЕ НА Е- УПРАВЛЕНИЕ**

*Жанет Захариева, Нов Български Университет - janet.zaharieva@vivacom.bg*

**Абстракт:** Статията разглежда „цифрово разделяне“ (digital divide) на населението в малките и отдалечени населени места по отношение достъпа до високоскоростен интернет и ползването на услугите на електронното управление и услуги онлайн. Предлага начин за преодоляване на този проблем чрез мерки от страна на държавата за стимулиране изграждането на мобилни широколентови мрежи в тези райони посредством публично-частни партньорства, влагане на средства по европейски програми и цялостно освобождаване на спектъра в обхват 790–862 MHz.

**Ключови думи:** електронно управление, високоскоростен интернет, мобилни данни, цифрово разделяне, широколентови мрежи

### **I. ВЪВЕДЕНИЕ**

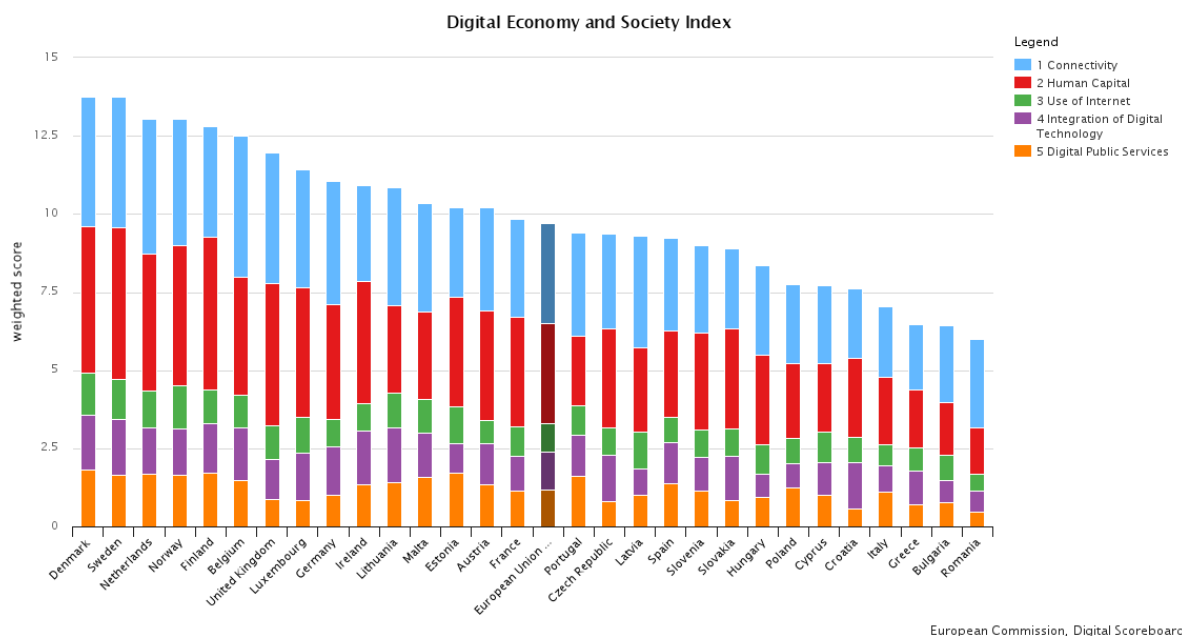
Цифровото разделяне е термин, който илюстрира неравенството в достъпа, използването на услугите на информационните технологии, включително интернет, между социалните групи в урбанизираните територии и тези в малките и отдалечени населени места.

България се нарежда на 27-мо място сред 28 държави на ЕС, според индекса за навлизането на цифровите технологии в икономиката и обществото (DESI)<sup>1</sup> на Европейската комисия за 2016 г. България попада в групата на изоставащите държави, които показват резултати под средното за ЕС и които напредват по-бавно.<sup>2</sup> [1]

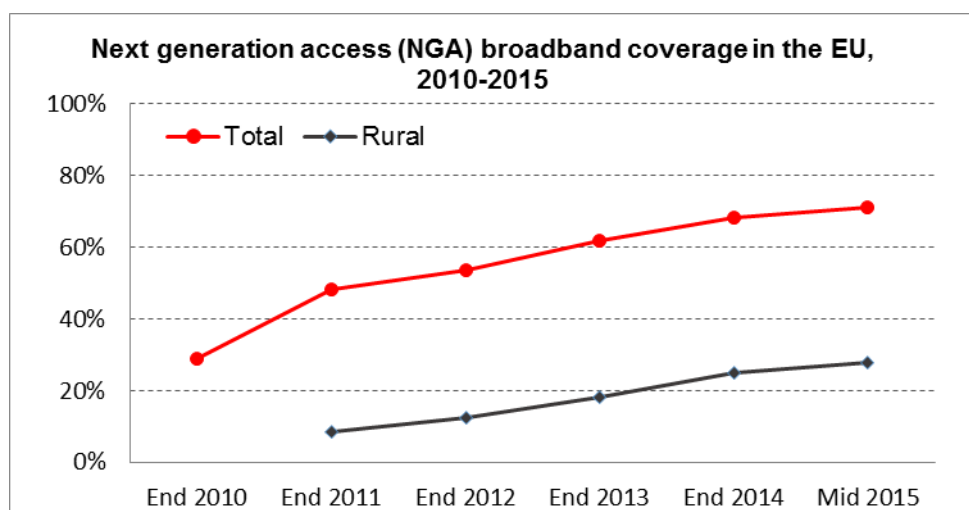
<sup>1</sup> Индексът за навлизането на цифровите технологии в икономиката и обществото (DESI) е сложен съставен показател, разработен от Европейската комисия за оценяване на развитието на държавите от Европейския съюз (ЕС) в посока към цифрова икономика и цифрово общество. Той обединява набор от съответни показатели, структурирани по 5 измерения: свързаност, човешки капитал, използване на интернет, внедряване на цифрови технологии и цифрови обществени услуги.

<sup>2</sup> Профил на държавата според DESI за България:

По отношение на показателя „Свързаност“ представянето на България е под средното за ЕС, отчита се изоставане в развитието на широколентовите мрежи в България. Общото покритие от фиксирани мрежи с широколентов достъп е 95 % от домакинствата (97% в ЕС), но в селските райони е значително под средното за ЕС (60% от домакинствата в сравнение с 91% в ЕС). Покритието на мрежи за достъп от следващо поколение (NGN) е 72% от домакинствата, подобно на средното за ЕС, но е само 3% в селските райони.



Фиг.1. Основни показатели по индекс DESI за държавите-членки за 2015 г., ЕК, Digital Scoreboard



Фиг. 2. Покритие с мрежи от следващо поколение в ЕС за периода 2010-2015

Впрочем, изоставането в отдалечените територии не е проблем само в България, а като цяло за ЕС България продължава да бъде сред държавите с най-нисък процент на домакинствата, абониращи за фиксирани широколентови услуги (55% от домакинствата в сравнение със 72% средна стойност за ЕС). Европейската комисия сочи, че това може

да се дължи както на недостатъчни умения на населението за ползване на цифрови технологии - едва 31 % от населението имат основни умения в тази област, така и на слабо развитата широколентова инфраструктура извън основните градове, което води до цифровото разделение между градските и селските райони. В допълнение към това, продължителната процедура за получаване на разрешения за изграждане на съобщителни мрежи и слабото публично финансиране ограничават инвестициите в сектора. Планинският релеф на България и съществения процент територии в НАТУРА (около 40%) създава допълнителни затруднения в изграждането на широколентови мрежи.

Стратегия “Европа 2020” и по-конкретно една от нейните водещи инициативи програма “Цифров дневен ред за Европа” поставя амбициозни цели пред държавите-членки, свързани с ускоряване на развитието на високоскоростния достъп до интернет.

- ✓ до 2020 г. всеки гражданин на ЕС да има достъп до високоскоростен широколентов достъп (fast broadband >30 Mbps)<sup>3</sup>
- ✓ до 2020 г. 50% от домакинствата в ЕС да са абонирани за свръх-високоскоростен широколентов достъп (ultra-fast broadband >100 Mbps)

Визията за постигането тези цели на национално ниво е намерила своето отражение в Националната стратегия за развитие на широколентовия достъп в Република България, която акцентира върху дефинирането на мерки за насърчаване изграждането на широколентова инфраструктура в отдалечените и слабо населените места/райони. Съгласно последната, инвестиционните намерения на държавата се ограничават до проекти, свързани с разгръщането на инфраструктура в тези райони, но при условие, че такава не била изградена до този момент. Това е и критерий за съфинансиране на ЕС, тъй като пазарната логика при предоставянето на широколентови услуги не винаги оправдава инвестициите в мрежа. Такова е фактическото положение в слабо населените райони, в които особеностите на релефа и/или отдалечеността предполагат високи разходи за изграждане на мрежи и в тази връзка предоставянето на широколентови услуги на достъпни цени не би било възможно без намеса на държавата. Европейската комисия (ЕК) е разработила “Насоки на Общността за прилагане на държавна помощ във връзка с бързото разгръщане на широколентови мрежи” (Насоки на ЕК) [2], в рамките на които ясно са дефинирани критериите за идентифициране на населените места/райони, за които е допустима държавна намеса при изграждането на широколентови мрежи.

Дефинирането на правителствени мерки по отношение разгръщането, надграждането и модернизирането на широколентова инфраструктура следва да има специален фокус върху отдалечените и слабо населени райони, в които не е налице комуникационна инфраструктура и пазарната логика не определя като икономически изгодно нейното изграждане. Досега в България са реализирани два проекта чрез европейско финансиране по ОП за развитие на селските райони, като и при двата акцентът се поставя върху изграждането на фиксирана инфраструктура.

В Европа разходът на операторите за свързване на едно домакинство към Интернет чрез изграждане на фиксирана инфраструктура в урбанизираните райони варира между 150 и 540 евро. За отдалечените райони обаче този разход достига до 2 700 евро.[3]

---

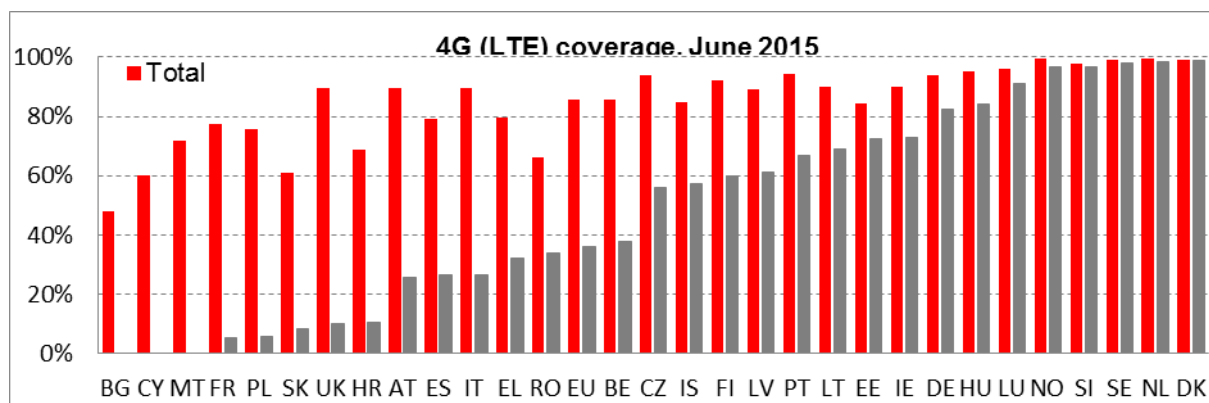
<sup>3</sup> Broadband е телекомуникационен термин, който се използва за обяснение на трансмисионния капацитет и по-високи скорости на предаване на данни чрез интернет в сравнение с използвания преди това dial-up чрез телефонната мрежа. Мерната единица, която обичайно се използва е средното число от битове (съкр. от **binary digit** - двоична единица информация) за секунда.

Очевидно, от гледна точка на икономическа жизнеспособност и възвръщане на инвестициите, операторите нямат стимул да инвестират във фиксирана инфраструктура в тези райони. Поради това частните инвестиции в комуникационна инфраструктура след началото на икономическата криза през 2008 г. са спаднали от 209 милиарда долара/годишно до приблизително 190 милиарда долара за следващите три години. [4]

Същевременно високоскоростните мрежи се определят като един от важните фактори за стимулиране на социалното включване на населението, което живее в отдалечени или слабо-населени места. Те осигуряват възможност за работа онлайн и така привличат млади хора, които да се заселват в тези райони. За по-възрастното население, което има ограничения в придвижването са възможност за повишаване качеството на живота и ползване на услуги, които са типични само за големия град. Например чрез теле-медицината се извършват консултации и дори интервенции от медицински специалисти без да се налага възрастният или трудноподвижен човек да изминава големи разстояния

## II. АНАЛИЗ

Инвестирането на обществени средства за изграждане на високоскоростни мрежи в отдалечените райони е наложително, за да се избегне цифровото разделяне на част от обществото. Мобилните мрежи от ново поколение са един от начините за постигане на достъп до широколентов интернет. В България поради липсата на свободен спектър за граждански нужди в обхвата 700-800 MHz и липсата на мерки за стимулиране на публично-частни партньорства, покритието с мобилни мрежи от ново поколение в селските райони не е добре развито.

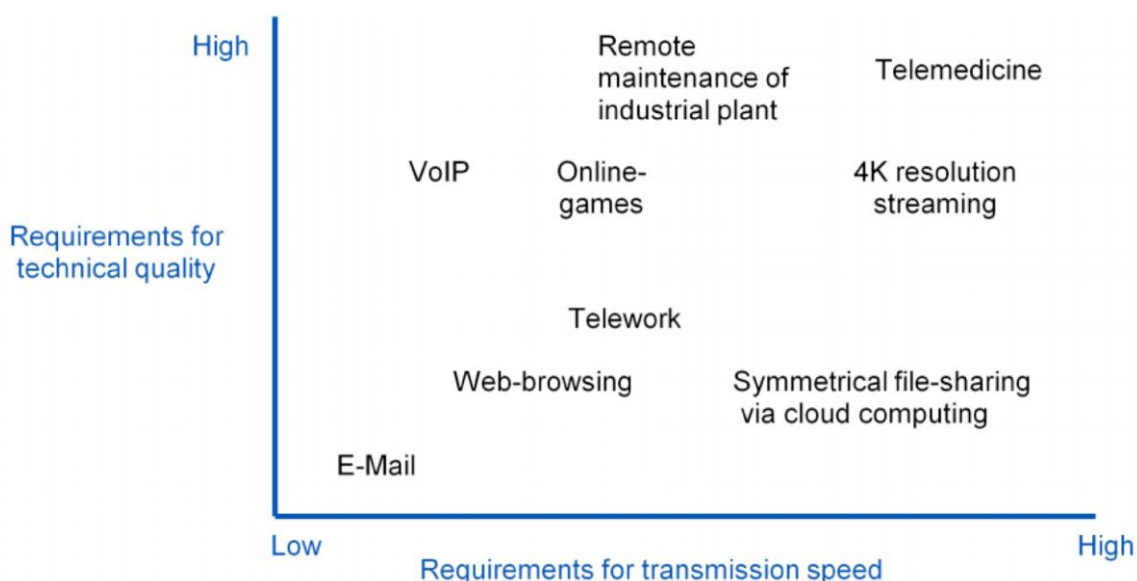


Фиг. 3. LTE-покритие в държавите-членки, юни 2015, Digital Agenda Scoreboard

Същевременно данните за потребителското поведение в световен мащаб показват траен интерес към мобилния интернет. Абонаментите за мобилни услуги се очаква да се удвоят до 2019 г. като смартфоните вече са половината от продадените мобилни телефони. Месечната консумация на трафик от потребител със смартфон се очаква да достигне 4.9 gigabytes през 2020 [5]. Свляянето на видео-съдържание нараства като процент от интернет трафика и съответно изисква по-голям капацитет и по-високи скорости на мрежите.

Очакванията на потребителите за качеството на достъпа се повишават значително. Изследване, проведено във Великобритания относно навиците на потребителите

пазаруващи онлайн, посочва, че 36% от анкетираните биха сменили сайта за пазаруване, ако той не зареди в рамките на 2-3 секунди.



Фиг. 4. Изисквания за качество и скорост на онлайн-апликациите

Пазарната ситуация в България се характеризира със засилено търсене на услуги за достъп до интернет, като едновременно с това се повишават и изискванията на потребителите към качеството на тези услуги. Удовлетворяването на потребителското търсене в съответствие със заложените стратегически цели на Общностно равнище не се обуславя единствено от изграждането на фиксирана инфраструктура за ширококолов достъп.

Тенденциите в развитието на пазара и устойчивият ръст в търсенето на услуги за достъп до интернет обуславят наличието на инвестиционен интерес от страна на операторите за изграждане и модернизация на мобилните мрежи за периода до 2020 г. Плановите на компаниите, участници на българския пазар, включват осигуряването на ширококолов достъп до интернет чрез въвеждане на LTE технология за преобладаваща част от населените места, попадащи към настоящия момент в категории “бели” и “сиви” райони. Информация за плановите на пазарните участници до 2020 г. по населени места е предоставена на МТИТС през м. март 2015 г. и следва да се вземе под внимание при актуализиране на районите, в които е допустимо разгръщането на ширококолтова инфраструктура в необходимите мащаби да се осъществи чрез публична подкрепа. Прилагането на такъв подход е в съответствие с Общностните правила, доколкото безжичните мрежи също се обхващат от дефиницията за “мрежи за достъп от следващо поколение” (NGA) по аргумент от т. 57 от Насоките на ЕС.

Идентифицирането на зоните, отговарящи на изисквания за публична подкрепа при разгръщането на мрежи за ширококолов достъп е предпоставка, но не и гаранция за изпълнение на заложените стратегически цели. Това е така, тъй като изграждането на инфраструктура изисква определено време. Предвид броят на населените места у нас, попадащи в момента в т.нар. “бели зони”, залагането на модел, базиран единствено на разгръщането на жични мрежи за ширококолов достъп на практика ограничава

възможностите за навременно постигане на набелязаните цели. С развитието на технологиите като подходяща алтернатива се очертава организирането на широколентов достъп до интернет посредством мобилни мрежи. Основно преимущество на тези мрежи е изграждане на покритие, което позволява ползване на същите услуги без фиксирано местоположение в дадения район. Същевременно изграждането на мобилни мрежи изисква съществени по размер инвестиции, с оглед изискванията на законодателството по отношение на строителството, качествено изграждане на съоръженията и надеждното и безопасно ползване на последните. Чрез предприемането на подходящ минимален набор от мерки в проекта на Закон за електронните съобщителни мрежи и физическа инфраструктура<sup>4</sup>, държавата може да окаже благоприятно влияние върху формирането на инвестиционни намерения от страна на пазарни участници и съответно да облекчи роля си във връзка с реализирането на конкретни проекти в тази област и осигуряване на необходимото финансиране.

Мерки, които ресорните държавни органи следва да предприемат

- *Да бъде осигурена възможност за ползването на спектър в обхват 800 MHz за граждански нужди във възможно най-кратки срокове.*

Разгръщането на мобилни мрежи чрез внедряване на LTE технология е в пряка зависимост от възможността за ползване на целия спектър в обхват 800 MHz. В случай че този спектър бъде предоставен за ползване за граждански нужди, пазарната ситуация ще провокира интерес и от страна на останалите пазарни участници за ориентиране на бизнес стратегии по предоставяне на услуги за достъп до интернет посредством разгръщането на безжичните им мрежи.

В съответствие с постигнатите на Общностно равнище договорености държавите-членки следваше да осигурят предоставянето на радиочестотния обхват 800 MHz (радиочестотна лента 790–862 MHz) за електронни съобщителни услуги в съответствие с хармонизираните технически условия, установени съгласно Решение № 676/2002/ЕО [6] и по специално в съответствие с разпоредбите на Решение 2010/267/ЕС [7]. България е една от държавите-членки, която среща трудности при осигуряването на разглежданата честотна лента, като и към момента този ресурс се използва преимуществено за целите на националната сигурност.

В доклада си за 2016 [8] ЕК сочи: „Независимо от това, въпреки че безжичният широколентов достъп има потенциал да намали разделението между градските и селските райони, липсата на ясни и конструктивни планове за промяна в използването на радиочестотни ленти за мобилни широколентови комуникации (лентите 800 MHz и 700 MHz) утежнява проблема. ... Недостигът на свободен радиочестотен спектър под 1 GHz (по-специално в лентите 800 MHz и 700 MHz) в България е критичен за разгръщането на национално ниво на висококачествени безжични широколентови услуги за икономиката и обществото, както и за разширяването на интернет на нещата по пътя към пето поколение мобилни мрежи (5G) и изпълнението на целите на Съюза относно широколентовите мрежи и радиочестотния спектър.“

Държавата следва да предприеме своевременни действия и в краткосрочен план да осигури възможност за ползването на целия свободен спектър от 2x30 MHz в обхват 800 MHz за граждански нужди с цел разгръщането на мрежи за безжични широколентови услуги. Частичното освобождаване на отделни ленти в обхват 800 MHz

---

<sup>4</sup> Към датата на съставяне на статията, внесен за разглеждане и приемане от НС.

и предоставянето им само на ограничен брой оператори чрез търг би довело до изкривяване на конкуренцията, изкуствено завишаване цената на този спектър и като краен ефект - до забавяне на инвестициите в мрежите и в развитието на нови потребителски услуги. Такъв подход би бил в противоречие със Стратегията за единен цифров пазар, която се очаква да въведе общеевропейски критерии за управление на спектъра, така че да бъдат стимулирани инвестициите в широколентови мобилни мрежи [9].

- *Да бъдат предприети определени законодателни инициативи за стимулиране на частните инвестиции за изграждане на мрежи.*

Съгласно Насоките на ЕС, осъществяването на държавна намеса включва основно законодателни мерки - облекчаване на регулаторните режими за изграждане на мрежи, като не се прави разлика между технологията за предоставяне на услуги – жична или безжична. Към момента една от основните причини за ограничаване на частните инвестиции за изграждане на мрежи е наличието на тромави административни процедури, следването на които изисква значително време и финансов ресурс. Посочените практически проблеми за изграждане на мрежи за широколентов достъп са свързани със законодателните решения и процедури и могат да се обобщят в следните основни категории:

- ✓ Изграждането на електронно съобщителна инфраструктура (базови станции, мачти, канална мрежа и др.) се осъществява въз основа на общото законодателство за строителство, с всички изискуеми в тази връзка документи и разрешения, без да има специфична уредба за електронни съобщителни мрежи;
- ✓ Изграждането на електронна съобщителна инфраструктура попада в една от най-високите категории строителство (трета категория) – по аналогия с промишлени инсталации, производствени сгради, фабрики, електрически централи;

В резултат, процесът по изграждане на всяка отделна базова станция отнема приблизително 1 година при липса на усложнения в разрешителните процедури.

- ✓ Строителните разрешения, свързани с изграждането на мрежи се издават в условията на децентрализация от всяка от 265-те общини в страната и при липса на единни правила. Всяка община прилага собствени процедури, условия и цени, което пречи за въвеждане на унифициран подход при едни и същи строежи.

На практика е налице и разлика в подхода от страна на администрацията при разглеждане на документите на различните оператори (инвеститори), което пречи на конкурентната среда. При поизнасяне на административните органи и други институции, участващи в процеса по издаване на строителни документи, в много от случаите се отчита голямо забавяне. Не се редки случаите, при които, поради такова забавяне се губи интерес от реализиране на инвестиционното намерение. Всяка промяна в оборудването на съществуваща базова станция, както и замяната на антени поради технологична модернизация се приемат за нов строеж и за тях се изисква ново разрешение за строителство - процедура, която е свързана със значителен допълнителен разход на средства и време от страна на операторите.

Определените в Директива 2014/61/ЕС [10] мерки създават предпоставки за облекчаване на приложимите регулаторни режими и стимулиране на частния инвестиционен интерес. По отношение на развитието и модернизирането на широколентовите мобилни мрежи, новият закон или евентуално изменение на ЗУТ

трябва да предоставят възможност на операторите да подменят оборудване в мрежите си без ново строително разрешение, когато съответната подмяна не води до конструктивни изменения на съществуващия строеж. Последното може да бъде проверено и удостоверено от регистриран инженер-конструктор. Важно е да се подчертае, че спазването на нормите относно електромагнитните излъчвания няма да се промени и контролът на районните здравни инспекции, предвиден в Закона за здравето остава непроменен. Едно възможен подход, който ще реши много проблеми в осъществяването и забавеното изграждане на мобилни мрежи от ново поколение е

- ✓ Преоборудването на съществуващи покривни базови станции в резултат на модернизация, да не бъде считано за нов строеж и за него да не се изисква разрешение за строеж, когато не засягат конструкцията на сградата и не се повишава натоварването;

Предприемането на законодателни инициативи, включващи прилагането на изложените по-горе мерки, значително ще облекчи следването на процедури, свързани с развитието, модернизацията и поддръжката на мобилните електронни съобщителни мрежи. Административната тежест и разходите за изготвяне, представяне и одобряване на строителни книжа ще бъдат редуцирани. Облекчаването на регулаторните режими като цяло ще окаже благоприятно въздействие върху развитие на конкуренцията и ще осигури достъп до качествени услуги за повече потребители.

- *Да се предвидят облекчения за изграждане на мрежи в отдалечени и труднодостъпни райони*

Един от основните проблеми, пред които са изправени операторите е свързан с разгръщането на мрежите им в отдалечени и труднодостъпни райони. В тези случаи, дори и да е налице прилагането на по-либерални режими за изграждане на мрежи, необходимостта от значителни по размер инвестиции се явява бариера пред реализирането на такива планове. Добрата европейската практика дава примери за осъществено взаимодействие на ниво държава-оператори, което в значителна степен решава проблема с изграждането на инфраструктура в отдалечени и труднодостъпни райони. Словакия например, като част от проекта си за осигуряване на ширококолов достъп в “бели” райони, е счела за необходимо изгражданата инфраструктура в отдалечени и труднодостъпни райони да бъде ползвана както в помощ на жична, така и в помощ на ползване на безжична технология при предоставянето на ширококолов достъп. По силата на този проект, който представлява и одобрена държавна помощ [11], операторите имат възможност да наемат изградената от държавата инфраструктура (мачти за мобилни станции), да монтират оборудване и съответно осигурят покритие на мобилните си мрежи, при разумно ниво на инвестициите.

По аналогия със Словакия, в България районите с потенциал да бъдат категоризирани като “бели” зони обхващат също територии с труден планински терен. В тези райони възникването на частен инвестиционен интерес е малко вероятно, предвид размерът на необходимите инвестиции, особено в случай, че се касае за изграждане на жични мрежи. Ето защо прилагането на опита на Словакия при изграждането на инфраструктура (мачти за мобилни станции) в отдалечени и труднодостъпни райони ще насърчи оператори да осигурят покритие на мобилните си мрежи в тези райони. От потребителска гледна точка навлизането на повече оператори в засегнатите райони е предпоставка за повишаване на качеството на предлаганите услуги, а като цяло това ще спомогне за постигане на заложените стратегически цели на национално ниво.

В таблицата по-долу са посочени сравнителни параметри на одобрени държавни помощи в няколко страни-членки [12]. Видно от опита на Гърция и Словакия, изграждането на мачти и кули с обществени средства и последващото им предоставяне на комуникационни оператори е политика, която среща одобрението на Европейската комисия.

|                                              | <b>Италия</b>                                     | <b>Гърция</b>                                                                                        | <b>Словакия</b>                                                                                                              | <b>Полша</b>                                   | <b>Румъния</b>                                    | <b>България</b>                                                                           |
|----------------------------------------------|---------------------------------------------------|------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|---------------------------------------------------|-------------------------------------------------------------------------------------------|
| Година на одобрение                          | 2009                                              | 2011                                                                                                 | 2011                                                                                                                         | 2011                                           | 2013                                              | 2013                                                                                      |
| Цел на държавната помощ                      | Осигуряване на свързаност за гражданите и бизнеса | Осигуряване на свързаност за гражданите и бизнеса                                                    | Изграждане на регионална оптична мрежа (Backhaul)                                                                            | Изграждане на регионална ширококолентова мрежа | Осигуряване на свързаност за гражданите и бизнеса | Изграждане оптична мрежа на държавната администрация; частично за ползване от операторите |
| Брой населени места в „белите зони“          | 2 000                                             | В рядко населени зони с повече от 400 жители                                                         | 729 общини                                                                                                                   | Рядко населени зони в източна Полша            | 2287                                              | 53                                                                                        |
| Бюджет (mm, EUR)                             | 154.5                                             | 250                                                                                                  | 113.2                                                                                                                        | 352.3                                          | 84                                                | 20                                                                                        |
| Продължителност                              | 2009-2015                                         | 2012-2015                                                                                            | 2012-2015                                                                                                                    |                                                |                                                   | 2013-2015                                                                                 |
| Задължения за предоставяне на достъп на едро | При справедливи и недискриминационни условия      | Достъп до пасивна инфраструктура и тъмно влакно<br>Достъп до кули за монтиране на антенни съоръжения | Достъп до пасивна инфраструктура и тъмно влакно<br>Наемане на мачти от общините за изграждане и използване на безжични мрежи | Активен и пасивен достъп                       |                                                   | Активен и пасивен достъп                                                                  |

Табл. 1. Сравнителни параметри на одобрени държавни помощи

### III. ИЗВОДИ

Цифровото разделяне в България може да бъде преодоляно чрез комплекс от мерки, които да стимулират инвестициите в мрежи за мобилни данни от четвърто поколение като:

1. Освобождаване на целия радиочестотен спектър в обхват 800 MHz, който да бъде предоставен за ползване на действащите мобилни оператори за изграждане на покритие на мрежите им за мобилни данни от четвърто поколение (LTE) в рамките на 2-3 годишен период.
2. Наред с изграждането на фиксираната инфраструктура, ЕСМИС или отделни общини да изградят мачти за мобилни станции в отдалечени и труднодостъпни

райони, които впоследствие да отдават под наем на операторите. Това е сериозен стимул, който ще насърчи частните инвеститори да осигурят покритие на мобилните си мрежи в тези райони и така ще гарантира на населението в тези райони достъп до интернет със скорости, съответстващи на целите на програмата „Цифров дневен ред за Европа“.

3. При въвеждането на нормите на Директива 2014/61/ЕС в националното законодателство, чрез проектозакона за електронните съобщителни мрежи и физическа инфраструктура, да бъдат предвидени ефективни мерки за бърза подмяна на оборудването в мобилни широколентови мрежи за достъп до интернет.

#### References:

- [1] Индекс за навлизането на цифровите технологии в икономиката и обществото (DESI), профил за България: <https://ec.europa.eu/digital-single-market/en/scoreboard/bulgaria>
- [2] Насоки на Общността за прилагане на държавна помощ във връзка с бързото разгръщане на широколентови мрежи, Съобщение на ЕК (2013/С 25/01), Официален вестник на Европейския съюз С 25/1, 26.1.2013 г. BG
- [3] Broadband for all: the state of broadband, ITU/Unesco, 2014
- [4] OECD Communications Outlook, 2013
- [5] Ericsson's estimate is reported in D. Thomas, S. Bond, Smartphone poised for revolution in media access, Financial Times, 3 June 2015
- [6] *Решение № 676/2002/ЕО на Европейския парламент и на Съвета относно регулаторната рамка за политиката на Европейската общност в областта на радиочестотния спектър*
- [7] Решение 2010/267/ЕС на Европейската комисия относно хармонизирани технически условия за използването на радиочестотната лента 790-862 MHz за наземни системи, позволяващи предоставяне на електронни съобщителни услуги в Европейския съюз
- [8] Digital Agenda Scoreboard, European Commission 2016
- [9] European Commission, A Digital Single Market strategy for Europe, 06 May 2015. COM(2015) 192)
- [10] Directive 2014/61/EU of the European Parliament and of the Council of 15 May 2014 on measures to reduce the cost of deploying high-speed electronic communications networks
- [11] State aid SA.33151 (2011/N) – Slovakia Basic broadband deployment in white areas of Slovakia
- [12] State aid SA.33324 (2011/N) – Latvia, State aid SA.32866 (2011/N) – Greece, State aid SA.3623 (2013/N) – Bulgaria, State aid N-646 (2009) – Italy
- [13] Broadband infrastructure. Supporting the digital economy in the European Union. EPRS, European Parliamentary Research Service, Author: Ron Davies, Members' Research Service, September 2015 — PE 565.891

## A METHOD FOR MATHEMATICAL OPTIMIZATION OF THE TERMS FOR PROPHYLAXES OF COMPLEX TECHNICAL SYSTEMS IN ACCORDANCE WITH THE LEVEL OF THEIR RELIABILITY REQUIRED

Georgiev Anton, Technical University of Varna, [georgiev\\_an@tu-varna.bg](mailto:georgiev_an@tu-varna.bg)

Nikolov Nikolay, Technical University of Varna, [nikolay.nikolov@tu-varna.bg](mailto:nikolay.nikolov@tu-varna.bg)

Toncho Papanchev, Technical University of Varna, [t.papanchev@tu-varna.bg](mailto:t.papanchev@tu-varna.bg)

**Abstract:** This article suggests and mathematically founds a new method for complex technical systems prophylaxes terms optimization in accordance with the level of reliability that they have to perform. For presenting new ideas are derived analytical dependencies suitable for practical application. On the basis of the analytical expressions proposed experimental studies are performed, the findings of which are located in the last section of the article.

**Keywords:** operational reliability; prophylaxes of technical systems; maintenance of electronic devices.

## МЕТОД ЗА ОПТИМИЗИРАНЕ НА СРОКОВЕТЕ ЗА ПРОФИЛАКТИКА НА СЛОЖНИ ТЕХНИЧЕСКИ СИСТЕМИ В СЪОТВЕТСТВИЕ С НЕОБХОДИМОТО РАВНИЩЕ НА ТЯХНАТА НАДЕЖНОСТ

Антон Славчев Георгиев, Технически университет – Варна, [georgiev\\_an@tu-varna.bg](mailto:georgiev_an@tu-varna.bg)

Николай Иванов Николов, Технически университет – Варна, [nikolay.nikolov@tu-varna.bg](mailto:nikolay.nikolov@tu-varna.bg)

Тончо Христов Папанчев, Технически университет – Варна, [t.papanchev@tu-varna.bg](mailto:t.papanchev@tu-varna.bg)

**Абстракт:** В статията е предложен и математически аргументиран нов метод за оптимизиране сроковете на профилактика на сложни технически системи в съответствие с равнището на надеждност, което те трябва да притежават. За представяне на новите идеи са изведени аналитични зависимости, удобни за практическо приложение. Въз основа на предложените аналитични изрази са направени експериментални изследвания, резултатите от които са поместени в последния раздел на статията.

**Ключови думи:** експлоатационна надеждност, профилактика на технически системи, техническо обслужване на електронни апаратури.

### Специфика на проблема

В процеса на техническо обслужване би трябвало субективният фактор да въздейства на техническите системи, пропорционално на равнището на тяхната деградация. Възстановителните въздействия върху техническите обекти по принцип са също толкова разнообразни, колкото и факторите, причиняващи /ускоряващи/ деградацията им. Разнообразни са и критериите, по които възстановителните въздействия биха могли да бъдат диференцирани. За целите на направения в тази статия анализ, по-съществено значение има класифицирането им според момента, в който биват стартирани възстановителните процедури. От тази гледна точка те са сепарирани в две обобщаващи групи – профилактични възстановявания (със субективно установена нужда от намеса) и аварийни възстановявания (с обективно съществуваща, видима нужда от ремонт).

Профилактиката на техническите системи е съвкупност от предварителни (превантивни) прегледи на отделни елементи и блокове, контрол и регулиране на променените па-

раметри, замяна и ремонт на отказалите компоненти и редица други мероприятия, целящи повишаване нейната експлоатационна надеждност. Профилактичните дейности се прилагат в строго определена последователност (която може да се опише чрез многократно разклонен алгоритъм), специфична за различните технически системи, като например: изключване от експлоатация на системата, оглед на нейните модули и елементи, измерване на контролираните параметри - ако всички параметри са в допустимите граници - включване на системата в експлоатация; ако някой/някои от параметрите са извън допустимите граници - провеждане на допълнителни измервания [1], [2] (преди и/или след демонтажа на съответните модули), диагностика, локализация на отказалия блок/елемент, демонтаж, ремонт на отказалия блок или подмяната му с нов, монтаж, регулиране и настройка на параметрите до достигане на допустимите граници, включване на системата и функционален контрол. За съжаление натрупаният практически опит показва, че профилактичните възстановявания са съпроводени с поне три нежелани ефекта:

- значителни материални разходи, поради необходимостта от използване на висококвалифициран труд и скъпа специализирана техника;
- влошаване на коефициента на готовност<sup>1</sup>, поради намаляване на времето, в което техническата система функционира;
- поява на “следпрофилактични” откази.

За да се намали влиянието на изброените негативни явления е необходимо да бъдат оптимизирани както организацията и сроковете за профилактика, така и съдържанието и последователността на профилактичните дейности. Изброените дейности са основните атрибути, характеризиращи стратегията за техническо обслужване.

Въведеното понятие „стратегия за техническо обслужване” може да бъде формулирано като регламентирана система от правила, включена в състава на техническото обслужване, съгласно която се вземат решения, касаещи: обема и състава на профилактичните и аварийните възстановявания на техническите системи, големината на срока за профилактика, началния момент за отчитане на срока за профилактика, начинът за редуване на профилактичните и аварийните възстановявания, доминиращия критерий за вземане на решения относно вида и обема на профилактичните дейности и др. За съжаление, в теорията на надеждността не се поставя необходимият акцент върху проблемите, касаещи профилактичните дейности, а проблемите, свързани с обема и състава на профилактичните и аварийните възстановявания, срока за профилактика и началния момент за отчитането му, подходът при редуването на профилактичните и аварийните възстановявания, както и критериите за вземане на решения относно обхвата на възстановяванията, се решават интуитивно - според субективната преценка на екипа, извършващ техническото обслужване, решения, базирани почти винаги на априорен емпиричен опит. Информацията, натрупана от априорен емпиричен опит има конкретен, силно индивидуален характер, поради разнообразието на техническите системи (по отношение на приложение, структура, елементна база, степен на резервиране на елементи и модули в нея, ролята ѝ за съхраняване на човешки живот и др.). Ето защо тази информация няма универсална приложимост, което е основната причина да бъдат допускани грешки при техническото обслужване на сложните технически обекти. Грешки, предизвикващи сериозно понижаване на тяхната експлоатационна надеждност.

### **Същност на метода**

Съществуват различни методи за определяне на сроковете за провеждане на периодични превантивни възстановителни дейности на техническите системи [3], които си основават на оптимизиране на един или друг надеждностен показател. Тъй като постигането

<sup>1</sup> при системи с висока експлоатационна надеждност и необосновано малки срокове на профилактика.

на оптимален срок на профилактика<sup>2</sup> е многоцелева задача, критериите за оптималност биха могли да бъдат различни: максимална стойност на коефициента на готовност, минимални разходи за профилактично обслужване при осигуряване на необходимото ниво на експлоатационната надеждност, минимална вероятност за възникване на следпрофилактични откази [4], максимален профит [5], [6] от експлоатацията на техническата система и др. Всеки един от методите, основаващи се на определен частен критерий има своите предимства, но общият им недостатък е, че оптималната профилактика по един частен критерий се оказва нецелесъобразна по друг/други частни критерии. В настоящата статия се предлага нов изчислителен метод за определяне на оптималния срок за профилактика, основаващ се на данни за възникналите откази в процеса на експлоатация на конкретната техническа система, при конкретните условия на експлоатация и режими на работа. Разработеният метод гарантира такъв срок на профилактика, при който се осигурява необходимото (предварително зададено) равнище на експлоатационната надеждност. Новият метод осигурява отличен баланс между разходите за профилактично обслужване и високата надеждност, с други думи - гарантира нужното ниво на експлоатационната надеждност, при минимални разходи за техническо обслужване.

Натрупаният опит [7], [8], [9], [10], [11] в изследването на експлоатационната надеждност на сложни технически системи ни дава основание да обобщим два детерминиращи принципа, прилагани при фиксирането на сроковете на профилактика. В съответствие с техните характеристики, тук те са наречени „регламентен” и „календарен”.

При регламентен принцип за определяне на сроковете на профилактика, профилактичните дейности се провеждат след точно определено време на експлоатация.

При прилагане на календарен принцип, отработеното време между две съседни профилактики не е от значение (профилактичните дейности се провеждат след точно определен календарен период от време - примерно на всеки 6 месеца). Практиката показва [7], [8], че този подход е целесъобразен при наличие на голям брой параметрични откази. Определящи за надеждността на съвременните електронни системи (както и за надеждността на преобладаващата част от съвременните сложни технически системи като цяло) се явяват внезапните откази. Това прави регламентния принцип за определяне сроковете на профилактика, по-подходящ при реализирането на техническото обслужване на съвременните електронни системи. Прецизното изчисляване на сроковете изисква внасяне на определени корекции в резултата, получен при прилагането на регламентния принцип. Корекциите се налагат поради наличието на временни прекъсвания на експлоатацията на техническата система, дължащи се на краткотрайната неработоспособност поради възникване на внезапни откази в периода между две поредни профилактики. При определяне стойността на коригиращата компонента са взети под внимание както статистическата точкова оценка  $T_B^*$  на средното време за аварийно възстановяване  $T_B$  и статистическата точкова оценка  $\omega(t)^*$  на параметъра на потока на отказите<sup>3</sup>  $\omega(t)$ , така и големината на предварително изчисления (съгласно регламентния принцип) срок на профилактика. Статистическите точкови оценки  $T_B^*$  и  $\omega(t)^*$  се изчисляват с помощта на статистическите данни за отказите, натрупани и обработени за периода на

<sup>2</sup> В настоящата статия, съвкупността от периодични превантивни възстановителни дейности на техническите системи е обобщена чрез добилия популярност термин „профилактика” на техническите системи. Коректно е все пак да се отбележи, че превантивните възстановителни дейности включват твърде широк кръг дейности. Тук ще бъдат дискутирани проблеми, касаещи само тази част от тях, които се провеждат през определен период от време.

<sup>3</sup> Параметърът на потока на отказите  $\omega(t)$  е основен показател, оценяващ безотказността на възстановимите електронни изделия. По своята физическа същност той е близък до показателя интензивност на отказите, използван при оценяването на невъзстановимите изделия. Изразява се чрез границата на отношението на вероятността за появата дори и само на един отказ през разглеждания период от време, към големината на този период от време, при условие, че периодът от време е безкрайно малък  $\omega(t) = \lim_{\Delta t \rightarrow 0} \frac{P(t, t + \Delta t)}{\Delta t}$ .

нормална експлоатация.

Предявените изисквания по отношение на надеждността на техническите системи най-често се формализират чрез нормиране на вероятността за безотказната им работа - поставя се изискване, в процеса на експлоатация тяхната вероятност за безотказна работа да не бъде по-малка от определена, предварително зададена стойност  $P(t)_{\text{ЗАД}}$ .

Основната идея на разработения метод е, че като се има предвид конкретната стойност на  $P(t)_{\text{ЗАД}}$  и се използва изчислената статистическа точкова оценка на параметъра на потока на отказите  $\omega(t)^*$  за конкретната техническа система, при конкретните условия на експлоатация и режими на работа, може да се определи оптималната стойност на срока на профилактика. За реализиране на тази идея е използван постулата, че профилактичните възстановявания водят до пълно възстановяване на изправността, т.е. след завършване на поредното профилактично възстановяване, техническата система възстановява изцяло своята работоспособност. Това означава, че вероятността техническата система да бъде в изправно състояние, в периода от време  $T_{\text{ПР}}$  между две поредни профилактики, може да се моделира математически чрез израза

$$P(t_n + T_{\text{ПР}}) = e^{-\int_0^{t_n + T_{\text{ПР}}} \omega(t) dt}. \quad (1)$$

Вероятността техническата система да бъде в технически изправно състояние, в периода от време между две поредни профилактики, може да се изрази и чрез произведение на една пълна и една условна вероятност

$$P(t_n + T_{\text{ПР}}) = P(t_n) \cdot P(T_{\text{ПР}} | t_n). \quad (2)$$

Десните части на последните два израза могат да бъдат приравнени, при което да се запише равенството

$$P(t_n) \cdot P(T_{\text{ПР}} | t_n) = e^{-\int_0^{t_n + T_{\text{ПР}}} \omega(t) dt}. \quad (3)$$

От равенство (3) лесно може да се изрази условната вероятност

$$P(T_{\text{ПР}} | t_n) = e^{-\int_{t_n}^{t_n + T_{\text{ПР}}} \omega(t) dt}. \quad (4)$$

На практика изразената условна вероятност би трябвало да отговаря на предявените изисквания по отношение на надеждността за конкретната техническата система. Това означава, че трябва да бъде изпълнено условието „в процеса на експлоатация вероятност за безотказна работа на апаратурата да не бъде по-малка от желаната, предварително зададена стойност  $P(t)_{\text{ЗАД}}$ ”, т.е.

$$P(T_{\text{ПР}} | t_n) \geq P(t)_{\text{ЗАД}}. \quad (5)$$

Оптимизационният принцип „минимални разходи за профилактично обслужване при осигуряване на необходимото ниво на експлоатационната надеждност на техническата система” изисква при определянето на срока на профилактика да бъде разгледан случаят, при който се изпълнява равенството

$$P(T_{\text{ПР}} | t_n) = P(t)_{\text{ЗАД}}. \quad (6)$$

Очевидно, десните части на изведените аналитични изрази (4) и (6) биха могли да се приравнят, при което да се запише, че

$$P(t)_{\text{ЗАД}} = e^{-\int_{t_n}^{t_n + T_{\text{ПР}}} \omega(t) dt}. \quad (7)$$

Което от своя страна означава, че

$$\int_{t_n}^{t_n+T_{\text{ГП}}} \omega(t) dt = -\ln P(t)_{\text{ЗАД}}. \quad (8)$$

Изведената аналитична зависимост е ценна с това, че тя показва, че оптималната големина на сроковете за профилактика на сложни технически системи може да се променя в зависимост от тяхната надеждност. Благодарение на нея, сроковете за профилактика за показани в пряка зависимост от параметъра на потока на отказите на конкретната техническа система, за конкретния период от време предхождащ профилактичното обслужване, при конкретните условия на работа и режими на експлоатация.

Изменението на параметъра на потока на отказите, в общия случай, може да се моделира чрез разпределението

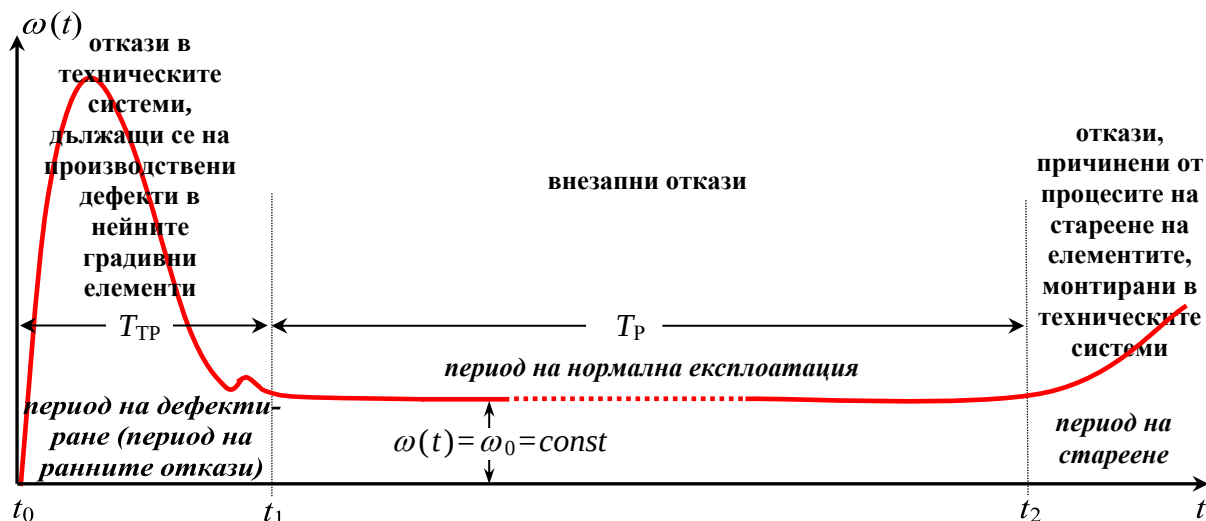
$$\omega(t) = a + b \cdot t. \quad (9)$$

Ако разпределението (9) бъде отразено в изведената зависимост (8) и полученият израз бъде интегриран, ще се получи аналитичен израз, по който биха могли да се изчисляват сроковете за профилактика

$$T_{\text{ГП}} = \frac{a + b \cdot t_n}{b} \left[ \frac{(a + b \cdot t_n)^2}{b^2} - \frac{2}{b} \ln P(t)_{\text{ЗАД}} \right]^{1/2}. \quad (10)$$

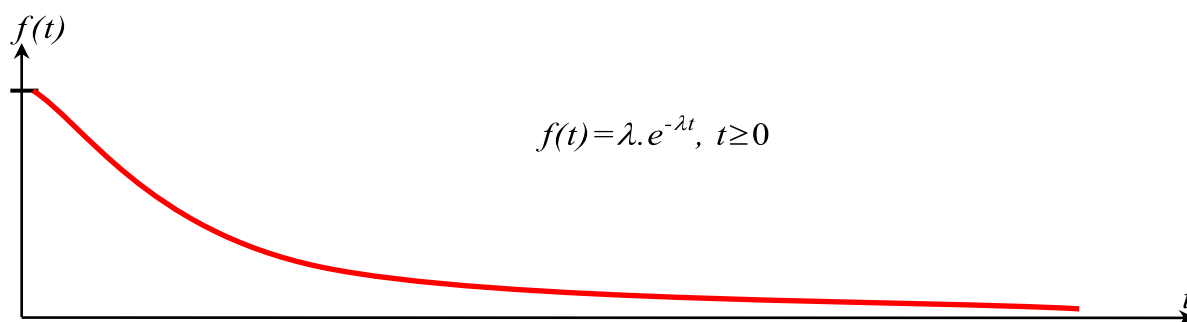
Чрез метода на максималното правдоподобие или чрез метода на най-малките квадрати могат да се конкретизират параметрите  $a$  и  $b$ , на разпределението (9). За целта се ползват статистическите данни, получени в периода на реалната експлоатация на конкретната техническа система.

Съгласно един от основните постулати в теорията на надеждността [12], в етапа на нормална експлоатация (фиг.1) времената между отказите на елементите, изграждащи сложните технически обекти, се моделират чрез експоненциален закон на разпределение<sup>4</sup> (фиг. 2).



Фиг.1. Позициониране на отказите в отделните етапи от експлоатационния цикъл на електронните системи (обобщено представяне на параметъра на потока на отказите на техническите системи)

<sup>4</sup> експоненциалното разпределение е еднопараметрично разпределение, което се използва при моделирането на времената за безотказна работа при внезапните откази (времената до отказ при невъзстановимите изделия и времената между отказите при възстановимите изделия)  $P(t) = e^{-\lambda t}$ . Това разпределение се използва още и в случаите, когато явленията износване и стареене са слабо изразени и тяхното влияние върху надеждността може да се пренебрегне; времената за завършване на ремонта (времената за възстановяване); времената до отказ при съхранение. В тази връзка, експоненциалният закон е най-използвания закон при оценяване на надеждността на електронните изделия [3], [12].



Фиг.2. Плътност на разпределението при експоненциален закон

Получените експериментални резултати в периода на нормална експлоатация (фиг.1) на различни по тип и предназначение електронни апаратури, потвърждават този теоретичен постулат [7], [8], [9], [10], [11]. Това означава, че в периода на нормална експлоатация на сложните технически обекти, е в сила равенството

$$\omega(t) = \omega_0 = \text{const.} \quad (11)$$

След интегриране на израз (8), при допускането (11), се получава израз, удобен за практическо приложение

$$\omega_0 \cdot T_{\text{ПР}} = -\ln P(t)_{\text{ЗАД}}, \quad (12)$$

т.е.

$$T_{\text{ПР}} = -\frac{\ln P(t)_{\text{ЗАД}}}{\omega_0}. \quad (13)$$

Трябва да се отбележи обаче, че чрез полученият израз (13) може да се определи срока на профилактика само в случаите, когато техническата система е работила без прекъсване от момента на приключване на предходното пълно (аварийно или превантивно [4], [5], [6]) възстановяване  $t_n$ , до момента на стартиране на следващата профилактика. Или изчислената с помощта на израз (13) стойност на срока на профилактика не отчита времето на неработоспособност на техническата система (времето за престой, изразходвано за извършване на възстановителни дейности при отстраняването на възникнали,  $j$  на брой откази) в периода от време между две поредни профилактики. Коректното и прецизно изчисляване на срока между две поредни профилактики (между  $i$ -тата и  $i+1$ -вата) изисква да бъде взето под внимание времето за престой. При липса, или при не ефективно работеща система за непрекъснат контрол на състоянието на техническата система, времето за престой е величина която не може и не бива да бъде пренебрегвана. Това налага добавянето на коригираща компонента в израз (13)

$$T'_{\text{ПР}} = -\frac{\ln P(t)_{\text{ЗАД}}}{\omega_0} + \sum_{j=1}^r \left( T_{B_{i,i+1}} \right)_j. \quad (14)$$

Стойността на коригиращата компонента в израз (14) би могла лесно да се изчисли с помощта на статистически данни за надеждността, натрупани в периода на нормална експлоатация на техническата система (фиг.1). Тази стойност е пропорционална на големината на срока на профилактика, на честотата с която възникват отказите (т.е. на статистическата точкова оценка на параметъра на потока на отказите) и на статистическата точкова оценка на средното време за аварийно възстановяване

$$\sum_{j=1}^r \left( T_{B_{i,i+1}} \right)_j = \omega(t) \cdot T_{\text{ПР}} \cdot T_B^*. \quad (15)$$

Но тъй като за периода на нормална експлоатация е валидно равенството (11), последният израз може да се запише във вида

$$\sum_{j=1}^r \left( T_{B,i,i+1} \right)_j = \omega_0^* \cdot T_{PP} \cdot T_B^*, \quad (16)$$

при което израз (14) добива вида

$$T'_{PP} = T_{PP} + \omega_0^* \cdot T_{PP} \cdot T_B^*, \quad (17)$$

или

$$T'_{PP} = -\ln P(t)_{ЗАД} \cdot \left( \frac{1}{\omega_0^*} + T_B^* \right). \quad (18)$$

При оптимизиране на сроковете за профилактика  $T_{PP}'$  на периферните устройства<sup>5</sup> в дадена сложна техническа система, трябва да се отчита и сумарното време за престой, дължащо се на скрити откази<sup>6</sup>

$$T'_{PPPV} = -\ln P(t)_{ЗАД} \cdot \left( \frac{1}{\omega_0^*} + T_B^* \right) + \sum_{k=1}^{r_{с.о.}} (T_{ПРЕСТОЙ,i,i+1})_k. \quad (19)$$

Чрез изведените изрази (18) и (19), и с помощта на статистическите точкови оценки на времето за аварийно възстановяване  $T_B^*$  и на параметъра на потока на отказите  $\omega(t)^*$ , лесно могат да бъдат оптимизирани стойностите на сроковете за профилактика и на техническите системи, и на техните периферни устройства, при зададена (желана) стойност на вероятността за безотказна работа.

## Експериментални резултати

Изложеният нов подход при определянето на сроковете за профилактика е експериментиран при провеждане на техническото обслужване на различни по тип, структура и предназначение сложни електронни системи [7], [8], [9], [10], [11]. Получените резултати показват, че прилагането му понижава силно броя на следпрофилактичните откази, редуцира разходите за техническо обслужване на системите и в крайна сметка - подобрява чувствително профитът [5], [6] от експлоатацията на системите. Така например, при изследваните мултиплексни телекомуникационни системи [7], [8], при които зададената вероятност за безотказна работа е  $P(t)_{ЗАД} = 0,94$ ,  $T_B^* = 0,14$  h, а параметъра на потока на отказите за канал от системата е  $\omega(t)^* = 8,81 \cdot 10^{-6}$ ,  $h^{-1}$ , бе установено, че оптимизацията на сроковете на профилактика по изложения тук начин, в съчетание с въведената нова стратегия за техническо обслужване<sup>7</sup> [5], [6] повиши времето между две съседни профилактики от 4320 h, на 9075 h. На *фиг. 3* са съпоставени експериментално

<sup>5</sup> от гледна точка на надеждността, за периферни устройства в дадена сложна техническа система, тук се приемат тези устройства, чиято надеждност води до редуциране на крайния ефект от работата на системата, но не влияе на надеждността на системата като цяло, т.е. това са устройства, чийто отказ предизвиква единствено понижаване на производителността (ефективността) на системата.

<sup>6</sup> при голяма част от сложните технически системи, дори и при тези в които функционира система за непрекъснат контрол на състоянието, състоянието на периферните устройства не се контролира; това означава, че скритите откази, възникващи в периода от време между две поредни профилактики, се установяват и отстраняват само по време на профилактика - при провеждане на профилактичното замерване на параметрите; времето за престой в състояние на скрит отказ за такъв тип устройства е достатъчно голямо за да бъде пренебрегнато.

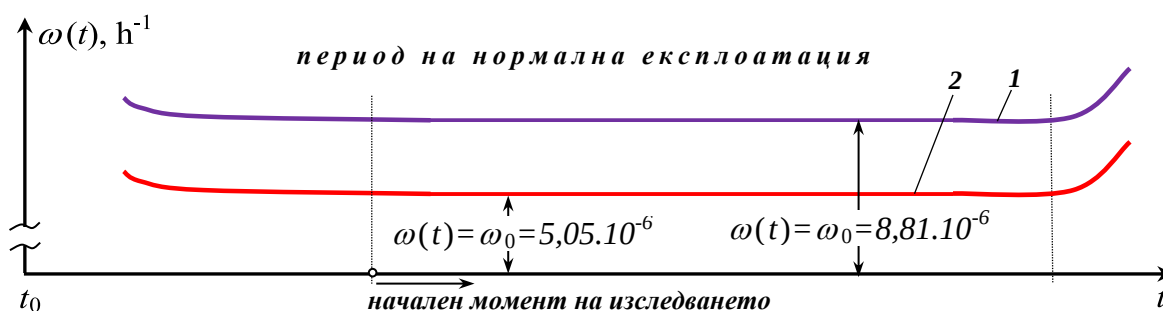
<sup>7</sup> Класифицираната като „Блокова стратегия за техническо обслужване” бе заменена с новосъздадената „Строго периодично стратегия за техническо обслужване” [6] [13].

получените криви за  $\omega(t)$  при прилагания преди това срок за профилактика и Блокова стратегия за техническо обслужване, и при оптимизирания, чрез новата методика, срок за профилактика.



Фиг.3. Апозиция на експериментално получените криви за  $\omega(t)$  преди (крива 1) и след (крива 2) оптимизирането на срока на профилактика

Съчетаването на изложената тук нова методика с разработената за целта нова Строгопериодична стратегия за техническо обслужване [6] [13], повиши допълнително надеждностните показатели на изследваните мултиплексни системи (фиг.4). Оптимизирането само на срока на профилактика, редуцира параметъра на потока на отказите около 1,2 пъти - от  $8,81 \cdot 10^{-6}$ ,  $h^{-1}$  до  $7,34 \cdot 10^{-6}$ ,  $h^{-1}$ . Съчетаването на предложените промени (оптимален срок на профилактика и нова стратегия за техническо обслужване) редуцираха параметъра на потока на отказите около 1,74 пъти – от  $8,81 \cdot 10^{-6}$ ,  $h^{-1}$  до  $5,05 \cdot 10^{-6}$ ,  $h^{-1}$ .



Фиг.4. Апозиция на експериментално получените криви за  $\omega(t)$  преди (крива 1) и след (крива 2) оптимизирането на срока на профилактика и въвеждането на нова стратегия за техническо обслужване

Изследванията, представени в тази статия, са проведени в рамките на проект ПД11/2016 „Изследване надеждността на електронна система с мрежова структура“, финансиран целево от държавния бюджет, чрез фонда за научни изследвания на Технически университет – Варна.

## References

- [1] Йорданов Ст., Р. Василев, "Възможности за управление на обекти от електроразпределителната мрежа чрез интелигентни измервателни системи", Международна научно-техническа конференция "Електроенергетика 2014", 11-13 септември 2014, Варна, България.
- [2] Василев Р., Й. Неделчев, Прецизният измервателен анализ - основен фактор за постигане на максимална енергийна ефективност, УНИТЕХ'06, Международна научна конференция. Сб. т. I, стр. 55÷57, ТУ-Габрово, 24-25 ноември, 2006.

[3] Беляев Ю. Надежность технических систем. Справочник под редакциата на И. Ушаков. М., Радио и связь, 1985.

[4] Георгиев А. С. Нова концепция за повишаване на експлоатационната надеждност на електронни системи. “Аквапринт” ООД, ISBN 978-954-92824-6-7, Варна, 2013. 96 с.

[5] Георгиев А.С. Стратегия за техническо обслужване на електронни системи чиито обем и съдържание зависят от усвоената част от техническия ресурс Електронно списание „Компютърни науки и комуникации” брой 1, 2014 г. ISSN: 1314-7846.

[6] Георгиев А.С. Стратегии за техническо обслужване на електронните системи. Електронно списание „Компютърни науки и комуникации” брой 1, 12.2012 г. стр.58-66. ISSN: 1314-7846 <http://ojs.bfu.bg/index.php/knk/article/view/37/70> <http://ojs.bfu.bg/index.php/knk/article/view/37>

[7] Пранчов Р.Б, А.С.Георгиев, П.Славейков. “Изследване надеждността на уплътнителни телефонни системи UTC100”, Отчет по проект №353/88 с ръководител доц. д-р Р. Б. Пранчов, заявител Комитет по съобщения и информатика, НИС ТУ-София, 1989.

[8] Пранчов Р.Б, А.С.Георгиев, Н.Г.Георгиева. “Оценка на експлоатационната надеждност на уплътнителни телефонни системи UTC100”, Отчет по проект №184-11/90 с ръководител доц. д-р Р. Пранчов, заявител Комитет по съобщения и информатика, НИС ТУ-София, С. 1991.

[9] Георгиев А.С., Нели Г. Георгиева, Т. Папанчев, и др. „Изследване надеждността и изготвяне на съответната надеждностна документация за система за мониторинг на състоянието и за оповестяване”, Научноизследователски проект с ръководител доц. д.т.н. Георгиев А.С, заявител ДИКС Интъртрейд ООД гр. София, 25.10.2010.

[10] Георгиев А.С., Н.Г.Георгиева, Т.Папанчев и др. „Изследване на възможностите за подобряване надеждността на електронни изделия”, Научноизследователски проект НПЗ/2011 с ръководител доц. д.т.н. Георгиев А.С.

[11] Георгиев А.С. и Т.Папанчев, Изследване на надеждността на електронни изделия”, Докторантски научноизследователски проект №ПДЗ „с ръководител доц. д.т.н. инж. Георгиев А.С.

[12] Гиндев Е.Г. Увод в теорията и практиката на надеждността - част 1: Основи на приложната надеждност. София, Акад. издателство Марин Дринов, 2000.

[13] Anton Sl.Georgiev and Toncho H.Papanchev. Strictly periodic maintenance strategy for electronic systems. „Electrotechnica & Electronica” (E&E), стр. 18-23, ISSN: 0861-4717, Vol. 48.Number 3-4, 2013.

## TESTBED FOR ONE-WAY IP PACKET DELAY MEASUREMENT IN SMART GRID WAMS APPLICATIONS BASED ON IEEE C37.118

*Martin Ivanov, Technical University of Varna, martinivanov@tu-varna.bg*

*Rozalina Dimova, Technical University of Varna, rdim@tu-varna.bg*

**Abstract:** With the emergence of Smart Grid technologies, the wide area measurement systems show potential in securing the reliability of the power grids by using real-time centralized data collection over hundreds or thousands of kilometers. The strict requirements for sub-20 ms one-way delay of these systems impose numerous challenges to the process of accurate network delay measurement. In this paper, a testbed for one-way delay measurement in wide area measurement systems is proposed. The testbed is based on system clock synchronization to the Coordinated Universal Time (UTC) via Global Positioning System (GPS) receivers and Network Time Protocol (NTP) servers. In order to evaluate and bound the measurement error, two experiments have been performed in accordance with the IETF RFC 2679 standard. The results show low relative errors and allow accurate reporting of the one-way delay measurements.

**Keywords:** one-way packet delay, testbed, wide area measurement systems, synchrophasor communications.

## ЕКСПЕРИМЕНТАЛНА ПОСТАНОВКА ЗА ИЗМЕРВАНЕ НА ЕДНОПОСОЧНИ ПАКЕТНИ ЗАКЪСНЕНИЯ В SMART GRID ШИРОКООБХВАТНИ СИСТЕМИ ЗА НАБЛЮДЕНИЕ БАЗИРАНИ НА IEEE C37.118

*Мартин Иванов, Технически университет - Варна, martinivanov@tu-varna.bg*

*Розалина Димова, Технически университет - Варна, rdim@tu-varna.bg*

**Резюме:** С появата на Smart Grid технологиите, широкообхватните системи за наблюдение показват потенциал за осигуряване на надеждността на електроенергийните системи чрез централизирано събиране на данни в реално време на стотици или хиляди километри. Строктните изисквания на тези системи за еднопосочни закъснения в рамките на 20 ms налагат редица предизвикателства пред точното им измерване. В тази статия е предложена експериментална постановка за измерване на еднопосочни пакетни закъснения в широкообхватни системи за наблюдение. Постановката е базирана на синхронизация на системни часовници посредством GPS приемници и NTP сървъри. С цел да бъде оценена и ограничена грешката при измерване са проведени два експеримента в съответствие със стандарта RFC 2679 на IETF. Резултатите показват ниски относителни грешки и позволяват точно докладване на измерените стойности за еднопосочни закъснения.

**Ключови думи:** еднопосочни пакетни закъснения, експериментална постановка, широкообхватни системи за наблюдение, синхрофазорни комуникации.

## I. INTRODUCTION

The IP-based network technologies are rapidly gaining popularity with the power utilities and operators due to the recent advancements in the paradigm shift towards information- and communication-enabled power grids (widely known as Smart Grids, SG). The critical nature of the SG applications imposes stringent requirements toward network delay in order to achieve real-time centralized data collection over hundreds or thousands of kilometers.

The widespread approach for measuring IP packet delay is the round-trip time (RTT) between two network hosts, defined as the sum of the forward and the reverse delay. In the context of SG reference and architectural models [1]-[3], the centralized northbound data collection from end devices (smart meters, phasor measurement units, energy management systems, etc.) is characterized by large network traffic volumes, exceeding numerous times the southbound traffic which consists mainly of configuration messages and polling requests. From this perspective, measuring RTT for network performance evaluation leads to increased uncertainty due to the discrepancy in northbound and southbound traffic volumes, as well as the possibility of using different paths in each direction. Instead, the approach of one-way delay (OWD) measurement is more suitable solution, differentiating both traffic directions and enabling more precise one-way path diagnostics. The motivation for OWD measurement instead of RTT is given in RFC 2679 [4]:

- *Asymmetric paths* – different sequences of routers are used for the forward and reverse paths (RTT measurement actually measure the performance of two distinct paths together).
- *Asymmetric queueing* – even when two paths are symmetric, they may have radically different performance characteristics due to asymmetric queueing policies.
- *Application performance* – the overall application performance may depend mostly on the performance in one direction.
- *Quality of Service (QoS) provisioning* – in QoS-enabled networks, provisioning in one direction may be radically different than provisioning in the reverse direction, and thus the QoS guarantees differ.

Furthermore, the packet processing delay in the destination host incurs additional uncertainty when using RTT, as it is regarded as computational and not communication delay, and must not be included in the delay analysis [5].

The de facto standard for synchrophasor communications in WAMS is the IEEE C37.118-2011, consisting of IEEE C37.118.1 for synchrophasor measurements description and IEEE C37.118.2 for data transfers [6], [7]. This paper addresses the second part of the standard with an emphasis on OWD measurement. Being a protocol on the application layer, the IEEE C37.118 does not define a complete communication system and thus it is not bounding the network performance parameters, including OWD: “*If delay in data delivery is critical to applications, the designers need to examine all communication aspects they are incorporating to make sure delivery time meets specifications and there are no unexpected delays*”, [7].

Despite the lack of standardization activities for defining maximum allowable end-to-end OWD in WAMS, several studies have already pinpointed the need of achieving sub-20ms packet OWD while monitoring power systems with nominal frequency of 50 Hz [8]-[10]. The ITU-T recommendation Y.1541 defines 6 main QoS classes with each class creating a specific combination of bounds on the network performance values (Table 1). Clearly, the sub-20ms WAMS delay bounds does not match the established values in Y.1541. Under the most stringent Class 0, the packet delay bound exceeds the WAMS requirement five times, thus also introducing quintuple increase in the relative measurement error.

| Network performance parameter <sup>1</sup> | QoS Classes        |                    |                    |                    |                    |                       |
|--------------------------------------------|--------------------|--------------------|--------------------|--------------------|--------------------|-----------------------|
|                                            | Class 0            | Class 1            | Class 2            | Class 3            | Class 4            | Class 5 (unspecified) |
| IPTD                                       | 100 ms             | 400 ms             | 100 ms             | 400 ms             | 1 s                | U                     |
| IPDV                                       | 50 ms              | 50 ms              | U                  | U                  | U                  | U                     |
| IPLR                                       | $1 \times 10^{-3}$ | $1 \times 10^{-3}$ | $1 \times 10^{-3}$ | $1 \times 10^{-3}$ | $1 \times 10^{-3}$ | U                     |
| IPER                                       | $1 \times 10^{-4}$ |                    |                    |                    |                    | U                     |

Table 1. IP network QoS class definitions as in Y.1541 [11]

The main contribution of the current paper is the development of an experimental OWD measurement testbed for IP-enabled WAMS applications, based on system clock time synchronization between source and destination end nodes. The paper is organized as follows. Section II offers a description of the testbed, discussing the proposed setup, system time sources and clock synchronization as well as the used notions of clock uncertainty. Evaluations of the synchronization and the difference between “host” time and “wire” time are presented in Section III. The work is concluded in Section IV.

## II. EXPERIMENTAL TESTBED OUTLINE

In order to achieve system clock time synchronization and reduce the OWD measurement errors, both source and destination end node network segments are equipped with NTP version 4 compliant servers [12]. Each NTP server is connected to a GPS receiver, enabling accurate time tagging with UTC timestamps. Figure 1 depicts the structure of the proposed testbed.

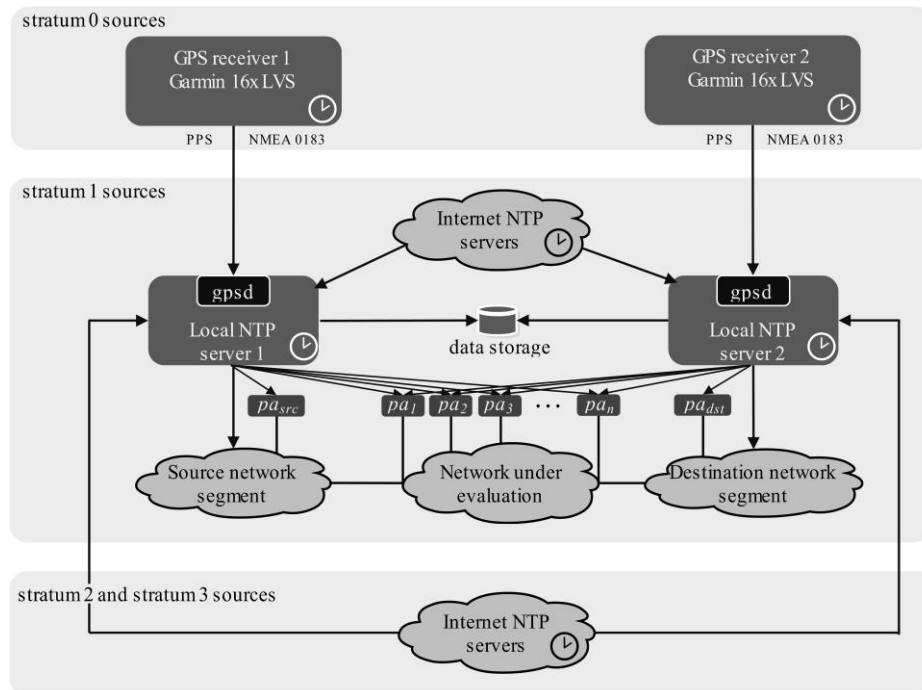


Fig.1. Time sources

<sup>1</sup> Network performance parameters as defined by ITU-T: IPTD – IP packet delay; IPDV – IP packet delay variation; IPLR – IP packet loss ratio; IPER – IP packet error ratio.

The shown stratum 1, 2 and 3 internet NTP servers are only used as secondary (backup) time sources due to the additional uncertainty from the increased hop count and asymmetric delays that NTP assumes to be symmetric. Both source and destination segments are equipped with protocol analyzers,  $pa_{src}$  and  $pa_{dst}$  respectively, in order to document packet generation time and packet reception time. The optional protocol analyzers  $pa_1, pa_2, \dots, pa_n$  are used when packet arrival/departure time measurement is required on the intermediate network nodes. If the operating system of a given device does not support packet capture, the analyzer is connected to that device using a mirrored switch interface. The data storage server consists of MySQL databases and FTP server which are used for the purpose of logging the reference clocks' accuracy.

## A. Used notions of clock uncertainty

The testbed evaluation is performed in accordance to the sources of uncertainty as defined by IETF. Both RFC 2679 and RFC 2681 define four distinct but related notions of clock uncertainty [4], [13]:

- *Synchronization ( $T_s$ )* – measures the extent to which two clocks agree on what time it is.
- *Accuracy ( $T_a$ )* – measures the extent to which a given clock agrees with UTC.
- *Resolution ( $r_{clk}$ )* – measures the precision of a given clock.
- *Skew ( $\varphi(t)$ )* – measures the change of accuracy, or of synchronization, with time.

RFC 2679 provides general guidance for accounting and analysis of various sources of error or uncertainty. The standard also notes the following specifics related to OWD metrics [4]:

- Errors or uncertainties due to uncertainties in the clocks of the source and destination hosts.
- Errors or uncertainties due to the difference between “wire time” and “host time”.

In order to gain an insight on the particularities of the two types of errors or uncertainties in the proposed testbed, both are separately evaluated in section III.

## B. UTC time sources

Two Garmin 16x LVS receivers are used as stratum 0 UTC reference clocks in both source and destination network segments. The format of the sentences is based on the NMEA 0183 standard [14]. The model selection is based on the support of additional output for Pulse Per Second (PPS) synchronization signal with  $T_{a,GPS} = \pm 1 \mu s$  on the rising edge [15]. The receivers are connected to the NTP servers via RS-232 serial interfaces with data rate of 9600 bps.

## C. Clock resolution

The precision of the periodic system clock corrections, issued by NTP, is limited by the time resolution  $r_{clk}$ . Therefore, in order to reduce  $r_{clk}$ , the operating system used for both NTP

servers is Ubuntu Linux 14.04.3 with kernel version 3.16. The compliance with RFC 2783 by using PPSkit allows achieving of  $r_{clk}$  values under  $1 \mu s$  [16], [17]. In comparison, Microsoft Windows offers  $r_{clk} \in [0.5ms, 15.6ms]$  and for most applications, the available resolution is 1 ms. Values of such order result in high instrument errors leading to inaccurate OWD measurement.

#### D. Local NTP servers

As synchronization via remote NTP servers is considered unsuitable for primary time source in the current testbed, the local NTP servers are directly connected to the statum 0 GPS receivers. The presence of two separate GPS receivers aims at excluding the possibility of transmitting NTP packets through the OWD-evaluated network segments in order to reduce the systematic and random errors and allow the testbed deployment over geographically remote locations, i.e. between substations and control centers.

The NTP servers are unable to establish a direct interface with GPS receivers, but have a numerous interfaces for accessing synchronization data through the use of additional system services for processing and placing the NMEA 0183 sentences and PPS in a shared memory segment. Figure 2 shows the data processing procedure of the used GPS service daemon [18].

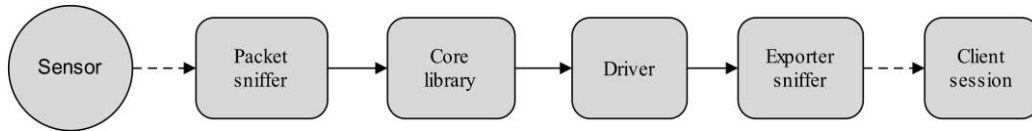


Fig.2. Dataflow architecture between GPS receiver and NTP server

### III. EXPERIMENTAL TESTBED EVALUATION AND RESULTS

RFC 2679 states the error in OWD measurements could be bounded by determining all the individual uncertainties, and adding them together to form the budget [4]:

$$U_{\max} = E_{\text{synch}}(t) + r_{clk,src} + r_{clk,dst} + H_{src} + H_{dst} , \quad (1)$$

where:

- $E_{\text{synch}}(t) \geq |\varphi(t)|$  denotes the upper bound on the uncertainty in synchronization (or accuracy).
- $r_{clk,src}$  and  $r_{clk,dst}$  denote the resolution of the source and destination clocks, respectively.
- $H_{src}$  and  $H_{dst}$  denote the upper bounds on the host-related uncertainties due to the differences between “wire time” and “host time”.

As  $r_{clk,src}$  and  $r_{clk,dst}$  are known, the main uncertainty sources considered in this paper are synchronization and differences between “wire time” and “host time”. Their evaluation is conducted in sections III.A and III.B respectively.

#### A. Synchronization evaluation

The testbed design is aimed for OWD measurement in IP-based WAMS that are inherently digital communication networks and allow differentiation of random and

systematic errors. Let  $d_m^{[p]}$  be the OWD of Type-P IP packet “ $p$ ”, defined in RFC 2330 [5], that is measured between two endpoint network devices  $\kappa_i$  and  $\kappa_j$  that are being synchronized by the NTP servers. Assuming that the GPS receivers and NTP servers operate in a stable state and system clocks of the respective devices are synchronized to UTC, the measured value of OWD is given by:

$$d_m^{[p]} = T_{ij, dst}^{[p]} - T_{ij, src}^{[p]}, \quad (2)$$

where  $T_{ij, src}^{[p]}$  and  $T_{ij, dst}^{[p]}$  are the timestamps of sending  $p$  by  $\kappa_i$  and receiving  $p$  by  $\kappa_j$ . Let  $d_{ete}^{[p]}$  be the true OWD value that cannot be directly determined due to the presence of systematic  $e_s$  and random  $e_r$  errors [19]:

$$d_m^{[p]} = e_s^{[p]} + e_r^{[p]} + d_{ete}^{[p]} \quad (3)$$

When multiple OWD measurements are performed (packet flow  $p_1 \dots p_n$ ), the changes in  $e_s$  and  $e_r$  in time must be bounded, as they characterize the skew  $\varphi(t)$  of the time sources. The systematic errors remain constant or vary in predictable matter [19]. The known or estimated systematic error can be compensated by the correction  $c_s = -e_s$ , with the corrected value of a single measurement being  $d_c^{[p]} = d_m^{[p]} + c_s^{[p]}$ . In the proposed testbed, the known systematic errors are considered to be instrumental, the bounds of which can be determined by a large number of measurements under the same conditions.

In terms of deploying the testbed over geographically distant locations, the most appropriate approach is to evaluate the accuracy  $T_a$  instead of synchronization  $T_s$  for the determination of  $\varphi(t)$ , avoiding the need for further exchange of synchronization data over long distances. The degree of synchronization can be determined by the accuracy of the NTP servers at each time point using  $T_s = |T_{a, NTP1}| + |T_{a, NTP2}|$ .

When performing multiple measurements, the random error  $e_r$  varies in an unpredictable manner [19]. As the number of measurements increase, the mean value approaches the probability density function of  $e_r$  and can be eliminated by performing large number of measurements under the same conditions.

In order to evaluate  $\varphi(t)$ , an experimental measurement of  $T_a$  with 1800 measured samples for each NTP server is conducted under the same conditions. The duration is 8 hours (28800 seconds). Given in UTC format, it represents the period 25200 – 54000 seconds. The input of the GPS service daemon is used for reference timing data acquisition which is accessed by gpspipe application [20]. The results are depicted on figure 3 and figure 4.

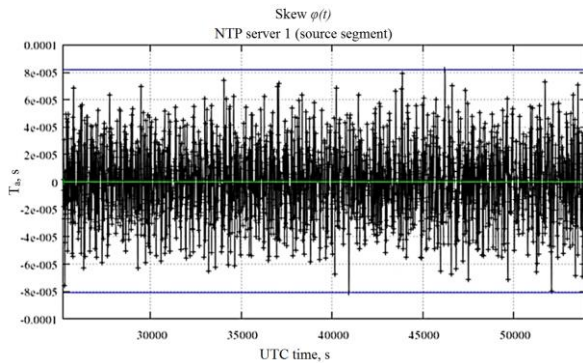


Fig.3. Skew  $\varphi(t)$  of NTP server 1

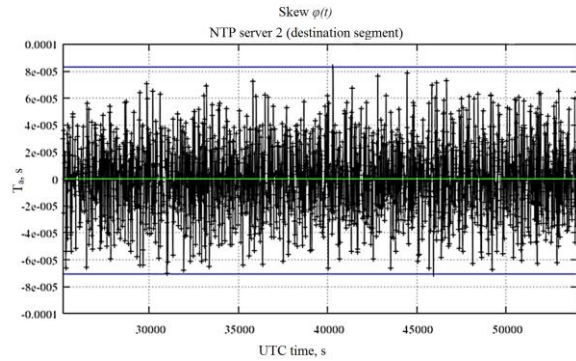


Fig.4. Skew  $\varphi(t)$  of NTP server 2

The results show similar characteristics in the change of  $T_a$  over the evaluation period. A statistical summary is shown in table 2.

|                                               | NTP server 1 | NTP server 2 |
|-----------------------------------------------|--------------|--------------|
| Minimum ( $\mu\text{s}$ )                     | -80.9        | -70.9        |
| Maximum ( $\mu\text{s}$ )                     | 82.2         | 83.2         |
| Range ( $\mu\text{s}$ )                       | 163.1        | 154.1        |
| Median ( $\mu\text{s}$ )                      | 0.101        | 0.088        |
| Mean $\bar{T}_a$ ( $\mu\text{s}$ )            | -0.029       | 0.042        |
| Standard deviation $\sigma$ ( $\mu\text{s}$ ) | 28.55        | 28.61        |
| Skewness                                      | 0.0196       | 0.0467       |
| Kurtosis                                      | -0.48        | -0.50        |

Table 2. Statistical summary of the experimental results

The skewness and kurtosis are close to 0, suggesting the normal distribution of the measured samples. With confidence level of 95%, the true mean value of NTP server 1 falls within the range between  $-1.35 \mu\text{s}$  and  $1.29 \mu\text{s}$  (with confidence interval of  $\pm 1.32 \mu\text{s}$ ). For NTP server 2, the true mean falls between  $-1.28 \mu\text{s}$  and  $1.36 \mu\text{s}$  (with the same confidence interval). The results indicate very small systematic errors due to the high resolution of the system clocks. However, the random errors remain as a main source of synchronization uncertainty. This is confirmed by the conformity of the sample data with the three sigma-rule (table 3) and the histogram distributions for the two data sets (figure 5). The lack of large variations from the true value of  $\bar{T}_a$  exclude the presence of errors due to loss of system clock synchronization.

|              | $[\bar{T}_a - \sigma ; \bar{T}_a + \sigma]$ | $[\bar{T}_a - 2\sigma ; \bar{T}_a + 2\sigma]$ | $[\bar{T}_a - 3\sigma ; \bar{T}_a + 3\sigma]$ |
|--------------|---------------------------------------------|-----------------------------------------------|-----------------------------------------------|
| NTP server 1 | 67.45%                                      | 96.95%                                        | 100%                                          |
| NTP server 2 | 66.89%                                      | 95.94%                                        | 100%                                          |

Table 3. Conformity of the sample data with the three-sigma rule

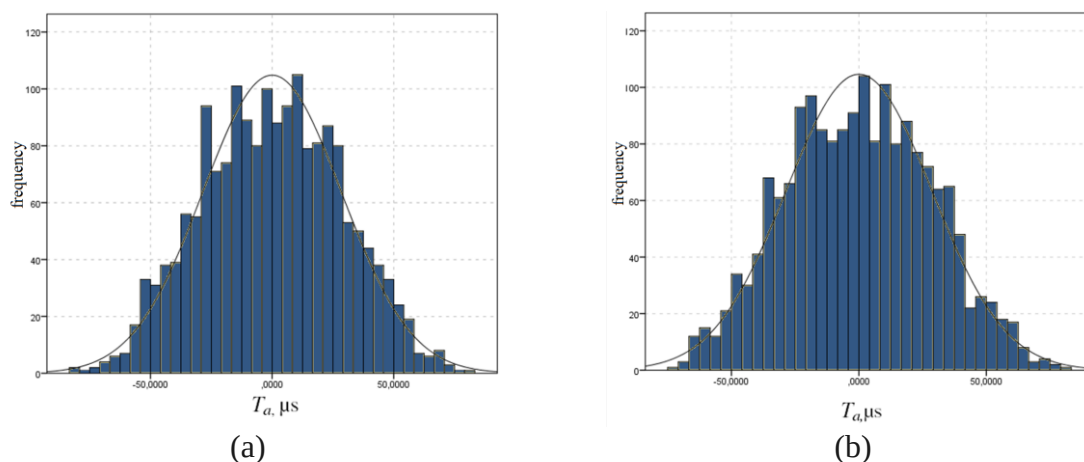


Fig.5. Histogram distribution for NTP server 1 (a) NTP server 2 (b)

The total uncertainty from the synchronization process can be defined as the maximum measured deviation from UTC for both servers and the uncertainty introduced by the GPS receivers:

$$E_{synch}(t) = |T_{a,max,NTP1}| + |T_{a,max,NTP2}| + T_{a,GPS} = 166.4\mu s \quad (4)$$

The notion  $E_{synch}(t)$  represents the upper bound on the uncertainty in the system clock synchronization.

## B. Evaluation of the difference between “host” and “wire” times

The timestamp  $T_{src}$  represents the sending of the first frame bit from the source interface and  $T_{dst}$  represents the time of receiving the last frame bit in the destination interface – defined in RFC 2679 as “wire” time ( $h_{wire}$ ). In real network conditions, the timestamping of an outgoing network packet is often performed before it is handed to an interface driver. Similarly, the timestamping of an incoming network packet in the destination device is performed after the reception from the interface driver – referred to as “host” time ( $h_{host}$ ). The difference between the two types of timestamping  $H = h_{host} - h_{wire}$  is considered difficult to measure or predict [21]. RFC 2679 states that the difference must be included in the uncertainty analysis but does not provide a methodology to measure it.

The experiment from [22] is reproduced in order to obtain the magnitude of the introduced error  $H$  by the host-related uncertainty. By using Internet Control Message Protocol (ICMP) echo requests between two network hosts in a local area network segment, the authors successfully determine the difference between “host” time and “wire” time.

In the current experiment, an Ethernet frame of 116 bytes carrying the ICMP packets is chosen to comply with the length of the IEEE C37.118 messages, used for evaluation of phasor data bandwidth requirements in [23]. The experiment is based on 1500 ICMP echo requests/replies, generated once every second. The two hosts being evaluated are used in the testbed as source and destination network nodes for measuring  $T_{ij,src}^{[p]}$  and  $T_{ij,dst}^{[p]}$  in order to calculate the OWD values. The hosts can be used for OWD evaluation between substations and control centers by using the iPDC platform [24].

Figure 6 and figure 7 depict the results for the source network segment host and the destination network segment host, respectively.

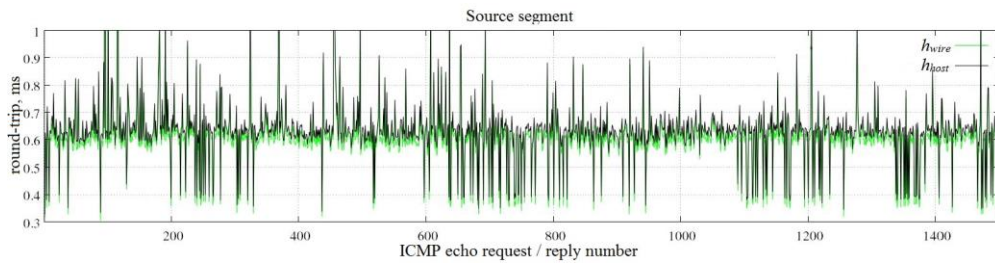


Fig.6. Round-trip measurement results for  $h_{wire}$  and  $h_{host}$  in the source segment

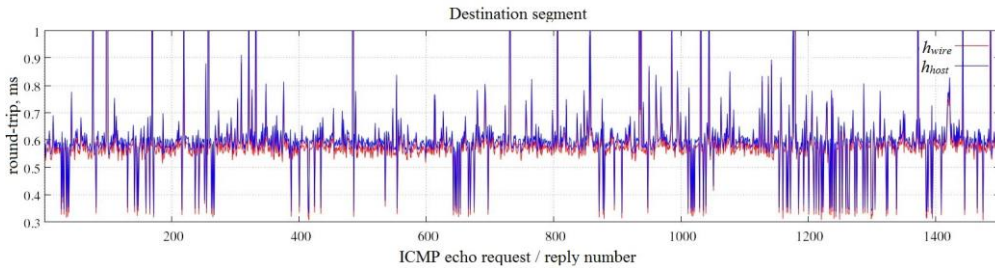


Fig.7. Round-trip measurement results for  $h_{wire}$  and  $h_{host}$  in the destination segment

In both segments, the round-trip values always satisfy  $h_{host} > h_{wire}$  which indicate the correctness of the obtained results. The difference  $H$  for the source segment varies in the range between 9  $\mu$ s and 53  $\mu$ s. For the destination segment,  $H \in [8 \mu$ s, 36  $\mu$ s]. Table 4 shows a summary of the obtained results during the experiment.

|                     | Source segment |            | Destination segment |            |
|---------------------|----------------|------------|---------------------|------------|
|                     | $h_{wire}$     | $h_{host}$ | $h_{wire}$          | $h_{host}$ |
| Minimum (ms)        | 0.304          | 0.328      | 0.305               | 0.328      |
| Maximum (ms)        | 3.034          | 3.06       | 4.408               | 4.42       |
| Range (ms)          | 2.73           | 2.723      | 4.103               | 4.092      |
| Median (ms)         | 0.606          | 0.63       | 0.571               | 0.592      |
| Mean (ms)           | 0.606          | 0.63       | 0.585               | 0.606      |
| Std. deviation (ms) | 0.130          | 0.130      | 0.203               | 0.202      |

Table 4. Summary of the experimental round-trip time results

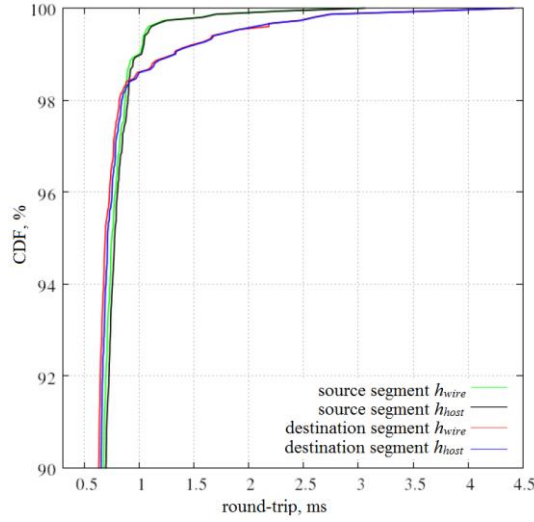


Fig.8. Cumulative distribution function

Figure 8 depicts the cumulative distribution function of  $h_{wire}$  and  $h_{host}$ . The values of  $h_{host}$  closely follow those of  $h_{wire}$  for both segments, showing very low difference variations. The majority of the measured values fall within the range from 500  $\mu$ s to 700  $\mu$ s: 83.8% for  $h_{wire}$  and 82.13% for  $h_{host}$  in the source segment, and 88.6% for  $h_{wire}$  and 87.6% for  $h_{host}$  in the destination segment. The sample distributions are characterized by similar standard deviations, as the differences between the mean values for the source and destination segments are 24  $\mu$ s and 21  $\mu$ s, respectively. The obtained results show the successful provision of similar host-related conditions in the source and destination segments of the testbed. As the differences  $H$  are accurately known, they can be bounded by  $H_{src} = 53 \mu$ s and  $H_{dst} = 36 \mu$ s in accordance with RFC 2679.

### C. Bounded total error in OWD measurements

Based on the obtained results in sections III.A and III.B, the total bounded error in the OWD measurement process with the testbed is calculated using (1). Table 5 gives the values depending on the method used to report the errors and the chosen timestamping procedure in the source and destination segment hosts.

| Reporting results            | Measuring<br>with $h_{host}$ , $\mu s$ | Relative error <sup>2</sup><br>( $h_{host}$ ), % | Measuring<br>with $h_{wire}$ , $\mu s$ | Relative error <sup>2</sup><br>( $h_{wire}$ ), % |
|------------------------------|----------------------------------------|--------------------------------------------------|----------------------------------------|--------------------------------------------------|
| Maximum range                | $\pm 257.4$                            | 1.287                                            | $\pm 168.4$                            | 0.842                                            |
| 95% confidence<br>(RFC 2679) | $\pm 148.2$                            | 0.741                                            | $\pm 59.2$                             | 0.296                                            |

Table 5. Values of errors during OWD measurement with the testbed

#### IV. CONCLUSION

The work presented in the paper addresses the OWD measurement in IEEE C37.118-enabled WAMS. A testbed for measuring sub-20ms packet OWD is presented, based on system clock time synchronization with UTC via GPS receivers and NTP servers. The extensive measurement error evaluation, performed in accordance with RFC 2679, shows very low relative errors and allows accurate results reporting. Future work could explore the possibilities of improving the accuracy of the testbed by using the Precision Time Protocol version 2 (PTPv2), defined in the standard IEEE 1588-2008.

#### References

- [1] National Institute of Standards and Technology (NIST), “NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0”, NIST Special Publication 1108r3, Jan. 2014.
- [2] International Telecommunication Union - Telecommunication Standardization Sector (ITU-T), “Deliverable on Smart Grid Architecture”, Smart-O-33 Rev.6, Dec. 2011.
- [3] European Telecommunications Standards Institute (ETSI), “Applicability of M2M architecture to Smart Grid Networks; Impact of Smart Grids on M2M platform”, TR 102 935 V2.1.1, Sept. 2012.
- [4] Almes G., S. Kalidindi and M. Zekauskas, “A One-way Delay Metric for IPPM”, IETF RFC 2679, Sept. 1999.
- [5] Paxson V., G. Almes, J. Mahdavi and M. Mathis, “Framework for IP Performance Metrics”, IETF RFC 2330, May 1998.
- [6] IEEE Standard for Synchrophasor Measurements for Power Systems, IEEE Std. C37.118.1-2011, Dec. 2011.
- [7] IEEE Standard for Synchrophasor Data Transfer for Power Systems, IEEE Std. C37.118.2-2011, Dec. 2011.
- [8] Paolone M., M. Pignati, P. Romano, S. Sarri, L. Zanni and R. Cherkaoui, “A Hardware-in-the-Loop Test Platform for the Real-Time State Estimation of Active Distribution Networks using Phasor Measurement Units”, *Proc. 2013 Cigre SC6 Colloquium*, pp.92-97, Yokohama, Japan, 6-9 Oct. 2013.
- [9] Khan R., J. Khan, “Wide Area PMU Communication over a WiMAX Network in the Smart Grids”, *Proc. 3rd Int. Conference on Smart Grid Communications (SmartGridComm'2012)*, pp.187-192, Tainan, Taiwan, 5-8 Nov. 2012.
- [10] Katsaros K. V., B. Yang, W. K. Chai and G. Pavlou, “Low Latency Communication Infrastructure for Synchrophasor Applications in Distribution Networks”, *Proc. 5th*

<sup>2</sup> For  $d_{ete} = 20\text{ ms}$  ( $f_{AC}=50\text{ Hz}$ )

- IEEE Int. Conference on Smart Grid Communications (SmartGridComm'2014)*, pp.392–397, Venice, Italy, 3-6 Nov. 2014.
- [11] ITU-T Rec. Y.1541 “Network performance objectives for IP-based services”, Dec. 2011.
- [12] Mills D., U. Delaware, J. Martin, J. Burbank and W. Kasch, “Network Time Protocol Version 4: Protocol and Algorithms Specification”, IETF RFC 5905, June 2010.
- [13] Almes G., S. Kalidindi and M. Zekauskas, “A Round-trip Delay Metric for IPPM”, IETF RFC 2681, Sept. 1999.
- [14] National Marine Electronics Association (NMEA), NMEA 0183 Standard v.4.0, Nov. 2008.
- [15] Garmin International, Inc, “GPS 16x Technical Specifications”, 190-00228-08, Revision B, Sept. 2008, online: [http://static.garmincdn.com/pumac/GPS16x\\_TechnicalSpecifications.pdf](http://static.garmincdn.com/pumac/GPS16x_TechnicalSpecifications.pdf)
- [16] Mills D., “A Kernel Model for Precision Timekeeping”, RFC 1589, Mar. 1994.
- [17] Mogul J., D. Mills, J. Brittonson, J. Stone and U. Windl, “Pulse-Per-Second API for UNIX-like Operating Systems, Version 1.0”, RFC 2783, Mar. 2000.
- [18] gpsd — a GPS service daemon, online: <http://www.catb.org/gpsd/>.
- [19] Bureau International des Poids et Mesures, *International vocabulary of metrology - Basic and general concepts and associated terms (VIM)*, JCGM 200:2012, Beuth Verlag, 3<sup>rd</sup> ed., 2008.
- [20] gpspipe.1 client, <http://www.catb.org/gpsd/gpspipe.html>
- [21] Hens F. J., J. M. Caballero, *Triple Play: Building the converged network for IP, VoIP and IPTV*, Wiley Press, 2008.
- [22] Cottrell L., W. Matthews, “PingER Calibration and Context”, Stanford University, Apr. 1999, online: <https://www.slac.stanford.edu/comp/net/wan-mon/error.html>
- [23] Dart E., “Increasing Information Flow between PDCs”, white paper, Sandia National Laboratories, Dec. 2000.
- [24] Pandit N., and K. Khandeparkar, “Design and Implementation of IEEE C37.118 based Phasor Data Concentrator & PMU Simulator for Wide Area Measurement System”, Technical Report, May 2012, online: <http://ipdc.codeplex.com/>

## INFORMATION SECURITY IN XXI CENTURY – CONCEPTUAL ISSUES

*Prof. Bojidar Violinov Bojinov, PhD, Tsenov Academy of Economics, Svishtov, Bulgaria,  
[b.bojinov@uni-svishtov.bg](mailto: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, information society

## ИНФОРМАЦИОННАТА СИГУРНОСТ ПРЕЗ ХХІ ВЕК – КОНЦЕПТУАЛНИ АСПЕКТИ

*Проф. д-р Божидар Виолинов Божинов, Стопанска академия „Д.А. Ценов“,  
[b.bojinov@uni-svishtov.bg](mailto: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 ХХІ ВЕК – КОНЦЕПТУАЛНИ АСПЕКТИ

Проф. д-р Божидар Виолинов Божинов, [b.bojinov@uni-svishtov.bg](mailto: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 тези технологии“<sup>1</sup>. 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)<sup>2</sup>. 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“<sup>3</sup>, „мрежова“<sup>4</sup>, „Интернет“<sup>5</sup>, „кибер“<sup>6</sup> икономика.<sup>7</sup> Особено важен аспект във функционирането на тази нова

<sup>1</sup> **Перес, К.** Технологические революции и финансовый капитал (Динамика пузырей и периода процветания). Издателство „Дело“, Москва, 2011, с. 31.

<sup>2</sup> **Макарова, Н.В., Волков, В.Б.** Информатика. Питер, Москва, 2011, с. 50.

<sup>3</sup> 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.

<sup>4</sup> 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.

<sup>5</sup> 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](https://bg.wikipedia.org/wiki/Интернет_икономика) (последен достъп 19.08.2016 г.).

<sup>6</sup> Думата **cyber** произхожда от гръцката дума **κυβερνέω** (kyberneo) – направлявам, ръководя, контролирам. Уилям Гибсън използва термина **кибер пространство** в научно-фантастичната новела Neuromancer за описание на глобална компютризирана 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 настоящето 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.<sup>8</sup> 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.

Някои автори обособяват четири ери в развитието на заплахите пред компютърната и информационна сигурност:<sup>9</sup>

- „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

---

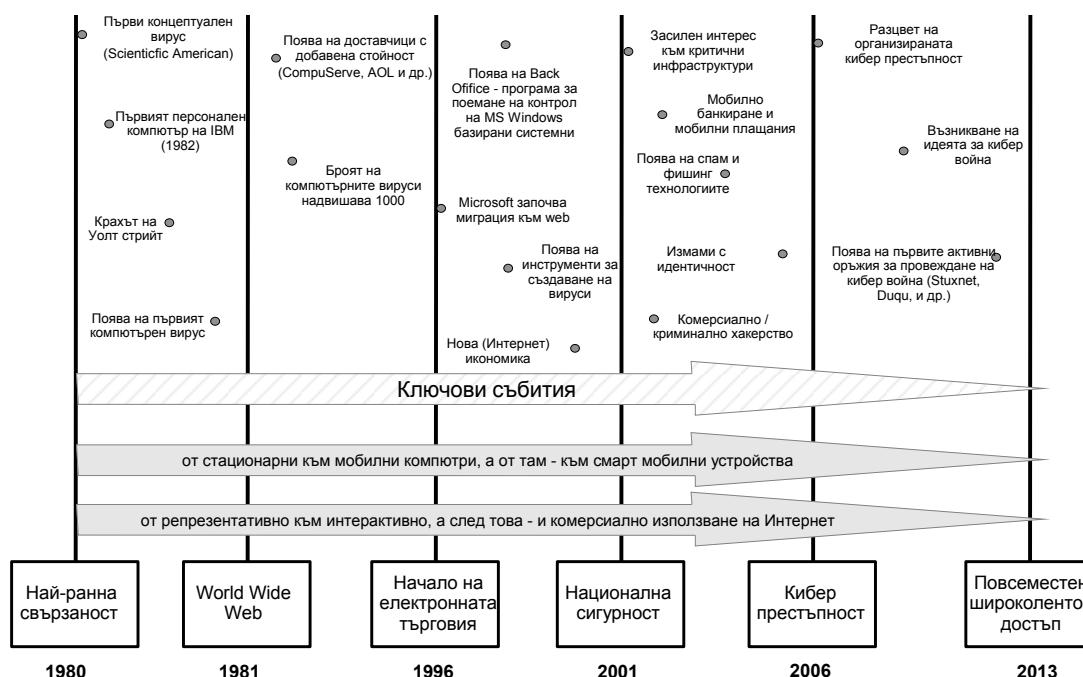
Security: Analysis, Thechnology and Automation, Intelligent Systems, Control and Automation: Science and Engineering 78, Springer International Publishing, Switzerland, 2015, p. 4.

<sup>7</sup> **Бургоский, В.Н.** Сетевая экономика. Финанси и статистика, Москва, 2008, с. 11.

<sup>8</sup> **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.

<sup>9</sup> 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.<sup>10</sup> 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 заплахата“<sup>11</sup> 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<sup>12</sup>:

<sup>10</sup> Transforming cybersecurity using COBIT®5, 2013, с. 14; ISACA, Reporting to Targeted Cyberattacks, USA, 2013 .

<sup>11</sup> 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 Engineering, Vol. 78, Springer, 2015, с. 9.

<sup>12</sup> Белов, Е.Б., Лосъ, 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<sup>13</sup>:

- *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: <sup>14</sup>

- *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: <sup>15</sup>

- *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:

---

<sup>13</sup> Белов, Е.Б., Лосъ, В., Меюеряков, Р.В., Шелупанов, Д.А. Основы информационной безопасности. Москва, Горячая линия – Телеком, 2006, с. 139-140.

<sup>14</sup> Белов, Е.Б., Лосъ, В., Меюеряков, Р.В., Шелупанов, Д.А. Основы информационной безопасности. Москва, Горячая линия – Телеком, 2006, с. 140.

<sup>15</sup> 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:<sup>16</sup>

- *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 заплахы за държавата и обществото*, които се проявяват в следните направления<sup>17</sup>:
  - *заплахы 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;
  - *заплахы 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;
  - *заплахы 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;
  - *заплахы 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,

<sup>16</sup> Cavelti, M. The reality and future of cyberwar. [http://mercury.ethz.ch/serviceengine/Files/ISN/115230/chaptersection\\_singledocument/d9c3a284-0167-4492-aaa9-45b2176d2eee/en/Reality\\_and\\_Future\\_of\\_Cyberwar.pdf](http://mercury.ethz.ch/serviceengine/Files/ISN/115230/chaptersection_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 and Engineering, 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.

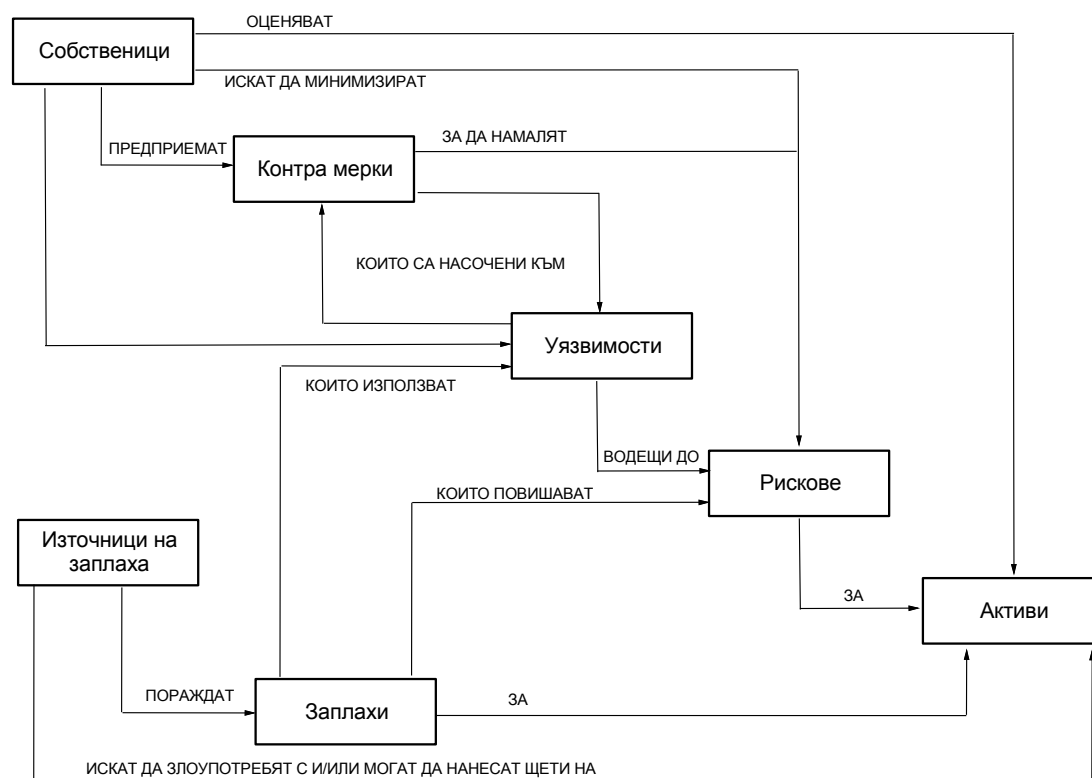
<sup>17</sup> Макарова, Н.В., Волков, В.Б. Информатика. Питер, Санкт-Петербург, 2011, с. 237-239.

нарушаващи нормалното функциониране на системите, прихващане на информация в мрежите за предаване на данни, дешифрирането на тази информация, и замяната ѝ 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.<sup>18</sup> 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.<sup>19</sup>



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:<sup>20</sup>

- 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:<sup>21</sup>

<sup>18</sup> Макарова, Н.В., Волков, В.Б. Информатика. Питер, Санкт-Петербург, 2011, с. 236.

<sup>19</sup> Белов, Е.Б., Лось, В., Меюеряков, Р.В., Шелупанов, Д.А. Основы информационной безопасности. Москва, Горячая линия – Телеком, 2006, с. 9.

<sup>20</sup> 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 заплахата 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:<sup>22</sup>

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

---

<sup>21</sup> 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

<sup>22</sup> 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 своя 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”<sup>23</sup>.

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),

---

<sup>23</sup> 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.<sup>24</sup>

## References:

1. Алавердов А.Р. Организация и управление безопасностью в кредитно-финансовых организациях. Московская финансово-промышленная академия. Москва, 2004.
2. Арnaudов, 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. Народно стопански архив, бр. 3, 2016.
5. Бугорский, В.Н. Сетевая экономика. Финанси и статистика, Москва, 2008.
6. Визгунов, А., Визгунов, Ар. Уровень защищенности от несанкционированного доступа как ключевой показатель качества систем дистанционного банковского обслуживания. Информационные 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. Семерджиев, 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 писменехъ, 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. Cavelt, 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](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

---

<sup>24</sup> 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](https://bg.wikipedia.org/wiki/Интернет_икономика) (последен достъп 19.08. 2016).

## A MATHEMATICAL METHOD FOR INTEGRATION OF INFORMATION, WHICH IS SIMILAR IN NATURE, FOR THE PURPOSE OF MEDICAL RESEARCH

*Tsvetoslav Antonov Georgiev, Medical University of Sofia, University Hospital "St. Ivan Rilski",  
[tsetso@medfaculty.org](mailto:tsetso@medfaculty.org)*

**Abstract:** In this article is looking for adequate solution of the task to the unification of uniform information from diverse sources for purposes of medical analysis of the research of various diseases or the impact of new drugs on the state of patients.

**Keywords:** reconciliation of uniform information with medical essence, pooling of uniform information from various sources, synchronizing of data of a medical nature.

## МЕТОД ЗА СИНХРОНИЗИРАНЕ НА ЕДНОРОДНА ИНФОРМАЦИЯ ЗА ЦЕЛИТЕ НА МЕДИЦИНСКИТЕ ИЗСЛЕДВАНИЯ

*Цветослав Антонов Георгиев, Медицински университет – София, Университетска  
МБАЛ "Св. Иван Рилски" [tsetso@medfaculty.org](mailto:tsetso@medfaculty.org)*

**Абстракт:** В статията се търси адекватно решение на проблема с обединяването на еднородна информация от диверсифицирани източници, за нуждите на медико-диагностичните изследвания, за целите на медицинския анализ на различни заболявания или при проучване въздействието на нови медикаменти върху състоянието на пациенти.

**Ключови думи:** съвместяване на еднородна информация с медицински характер, обединяване на еднотипна медицинска информация от различни източници, синхронизиране на информация от медицинско естество.

### Въведение

Математизирането на човешките познания в глобален мащаб е задача върху която се работи от векове, но през последните десетилетия интензитета на изследванията в тази област рязко нарасна. За съжаление, поради своята уникална специфика, медицинската наука е и ще остане най-трудният и най-деликатният дял за математизиращото се човешко познание. Независимо от обективните трудности, трябва да се стимулира и насърчава, търсенето на релевантни математически модели, както и разработването на нови такива, подходящи за интерпретиране на наличните данни и за прогнозиране на очакваните ефекти от лечението. В тази връзка трябва да се отбележи, че точните и адекватни математически модели могат да се окажат ключът към разрешаването на множество сериозни и значими казуси в медицината.

### Същност на проблема

Независимо от епизодичната поява на публикации, свързани с приложението на условните вероятности в математическата статистика [5], [6], все още неизяснен и енигматичен остава въпросът за мястото на Бейсовските методи при моделирането на реални процеси - като цяло [7], и в частност - в медицинската теория и практика. Това е основната причина, поради която все още няма еднозначен отговор на въпроса за мястото, ролята и позициите на тези методи в хуманитарните науки. Спорът за състоятелността и научността на Бейсовския подход се води повече от двеста и петдесет години (от 1763 г. до наши дни). Основният аргумент, изтъкван в научния спор, от противниците на Бейсовската теория е факта, че авторът сам не е публикувал своите идеи, изводи и на-

учни постулати. Част от тях са били публикувани едва три години след неговата смърт. Противниците на тази теория, сочат този факт като сериозен аргумент за съмненията на автора в състоятелността на изказаните идеи и обективността на направените изводи. Друга група автори, като Айвазян, Мхитарян [8] Енюков, Мешалкин, Бухштабер [9], Ледерман и Лойд [10], въпреки че не отхвърлят изцяло идеята за "субективната" условна вероятност, догматично ограничават периметъра на нейното приложение. „Съмненията” на Бейс обаче, не са попречили на гениален математик като Лаплас да доразвие първоначално оформилата се теория, и да възприеме постулата му за еднородната априорна информация като аксиома, в която вероятността се тълкува като логическа величина. Трябва да се спомене, че последователи на тази енигматична теория са дори великите Гаус и Поасон, които само няколко десетилетия след публикуването на трудовете на Бейс, ги оценяват по достойнство и дават своя принос в развитието на условните вероятности.

Възраждането на Бейсовските идеи днес е свързано с ярките и оригинални публикации на Фишер, Де Грот, Де Финети, Севиджа и Гуд, Стюдент и други именити съвременни статистици. Въпреки известните си резерви и съмнения по въпроса, Ледерман и Лойд акуратно систематизират теоремите, лемите и следствията на Бейсовската теория за дискретни и непрекъснати случайни величини при един и при два неизвестни параметъра [10]. Авторите акцентират на приложенията, свързани с апроксимационния анализ при наличие на голяма априорна неопределеност. Изследват и анализират състоятелността на Бейсовския подход: при точковото и интервалното статистическо оценяване на случайните величини, при проверката за значимост на хипотезите и при прогнозирането на бъдещи състояния на случайни събития, като за целта прилагат принципа на правдоподобие. Вентцел, Овчаров [11], Вуколов, Ефимов, Земсков, и Поспелов [12] изясняват приложението на Бейсовските способности и условните вероятности посредством решени примери и задачи. Многобройните доводи "за" и "против" приложимостта на субективните вероятности, могат да се намерят систематизирани в научния трактат на Дзин Лин, Матиас Асплънд и Адития Парида [13].

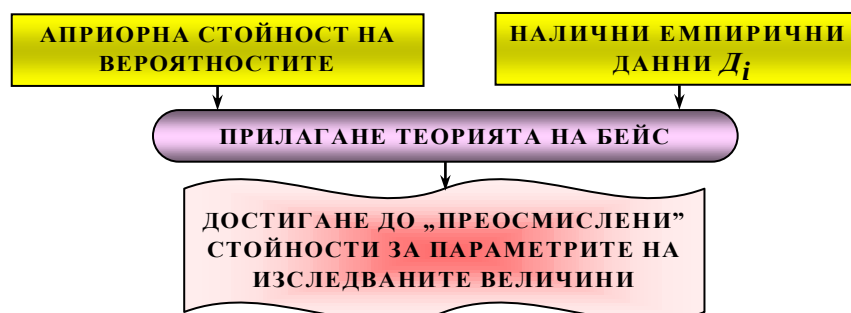
Съществен принос за сериозните позиции на Бейсовската теория в съвременната практика, има руският математик Савчук [14]. Авторът изследва основните аспекти на йерархичната Бейсовска методология; методите за параметрично Бейсовско оценяване по цензурирана извадка; непараметричното Бейсовско оценяване; квазипараметричните Бейсовски оценки; оценките на вероятността за безотказна работа в условията на частична априорна определеност; априорните, апостериорните и емпиричните Бейсовски оценки и др. Авторът предлага интересни решения на задачите за Бейсовско оценяване, като използва априорната средна стойност на изследвания параметър и на резултатите от биномните изпитвания, при отсъствие на априорно разпределение.

Изводът до който достигат Джеймс Прес и Джудит Танур [15] е, че е на лице пълно разминаване в аргументите, и очевидно отсъствие на пресечни точки във възгледите на застъпниците на двете противоположни тези. И като краен резултат авторите констатира методологическа безполезна водената дискусия за приложимостта на условните вероятности в теорията и практиката.

### **Същност на метода**

Постулатите на Бейс се явяват методологическа база за моделиране на прехода от априорна информация (формализирана във вид на априорно разпределение) към апостериорната информация. Това моделиране се основава на последователното натрупване на информация. В началния етап се изследва натрупаният опит (информация от направени в миналото, аналогични изследвания и систематизирани в резултат на това данни) и приложимостта му при моделирането на свойствата и поведението на изпитвания в мо-

мента обект (конкретно медико-диагностично изследване, конкретно лечение или въздействие на конкретен медикамент). В хода на тестването на обекта се получава нова информация, във вид на емпирични данни, която в общия случай се различава от априорната информация. Това налага перманентно поетапно преосмисляне и преоценка на апостериорното представяне. При това, във всеки един момент е възможно да бъде даден обобщаващ отговор на свойствата и параметрите на обекта, и този отговор ще бъде изчерпателен и пълен, тъй като се базира на цялата съществуваща до момента информация. Този процес е непрекъснат - продължава след получаването на поредния пакет от данни за провеждания експеримент. Процесът на поетапна преоценка на вероятността за състоятелност на дадена медицинска хипотеза, след получаване на новите данни, е в унисон с обобщената схема на Ледерман и Лойд [10] (фиг. 1).



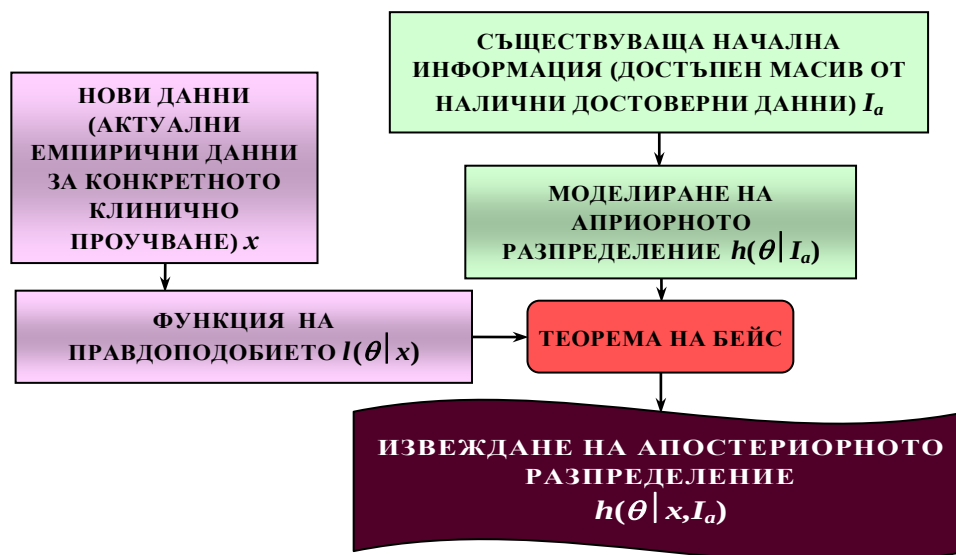
фиг.1 Обобщена схема на Ледерман и Лойд

По подробна схема на процеса, преосмисляне и преоценка на априорната информация, с оглед на постъпващата „свежа” информация, е предложена от Зелнер [16]. Свойствата на моделирания обект са изразени чрез параметъра  $\theta$ . В общия случай този параметър се представя във векторен вид. Предварителната представа за свойствата на обекта се основава на масив от конкретни, вече налични данни  $I_a$ . Формалният запис на тази предварителна (априорна) информация се извършва помощта на априорното разпределение на параметъра  $\theta$ , което, от своя страна е условно по отношение на наличните данни  $I_a$ , т.е.  $h(\theta|I_a)$ . Получените в процеса на изпитване „свежи” емпирични данни  $x$  се записват във формализиран вид чрез функцията на правдоподобие  $l(\theta|x)$ . Функцията на правдоподобие интерпретира вероятността (или плътност на вероятностите) за получаване на емпирическите данни и се изразява като условна функция на параметъра. За получаването на  $l(\theta|x)$  е необходимо да се познава модела на обекта, изразен най-често във вид на условно разпределение за основната случайна величина  $\theta$ .

В схемата на Зелнер (фиг. 2) свойствата на обекта се изразяват чрез параметъра  $\theta$ . Този параметър в общия случай се изразява във векторна форма. Предварителната представа за свойствата на обекта се основава на някаква известна вече информация  $I_a$ . Формализирането на тази предварителна (априорна) информация се извършва чрез запис на априорното разпределение на параметъра  $\theta$ , което, от своя страна е условно по отношение на  $I_a$ , т.е.  $h(\theta|I_a)$ . Получените в процеса на изпитване емпирични данни  $x$  се записват във формализиран вид чрез функцията на правдоподобие  $l(\theta|x)$ . Функцията на правдоподобие изразява вероятност (или плътност на вероятностите) за получаване на емпирическите данни и се записва във вид на условна функция на параметъра. За получаването на  $l(\theta|x)$  е необходимо да се познава модела на обекта, изразен най-често във вид на условно разпределение за основната случайна величина  $\theta$ . След прилагане на теоремата на Бейс:

$$h(\theta|x, I_a) = \frac{h(\theta|I_a)l(\theta|x)}{\int h(\theta|I_a)l(\theta|x)d\theta}, \quad (1)$$

се получава апостериорното разпределение  $h(\theta|x, I_a)$  за параметъра  $\theta$ . Това разпределение е условно по отношение на първоначалната информация  $I_a$  и емпиричните данни  $x$ . В процеса на натрупване на извадкова информация във вид на емпирични данни, тегловния и коефициент, изразяващ влиянието и върху апостериорното разпределение, непрекъснато нараства. Плътността на апостериорното разпределение все повече се концентрира около действителната стойност на параметъра.

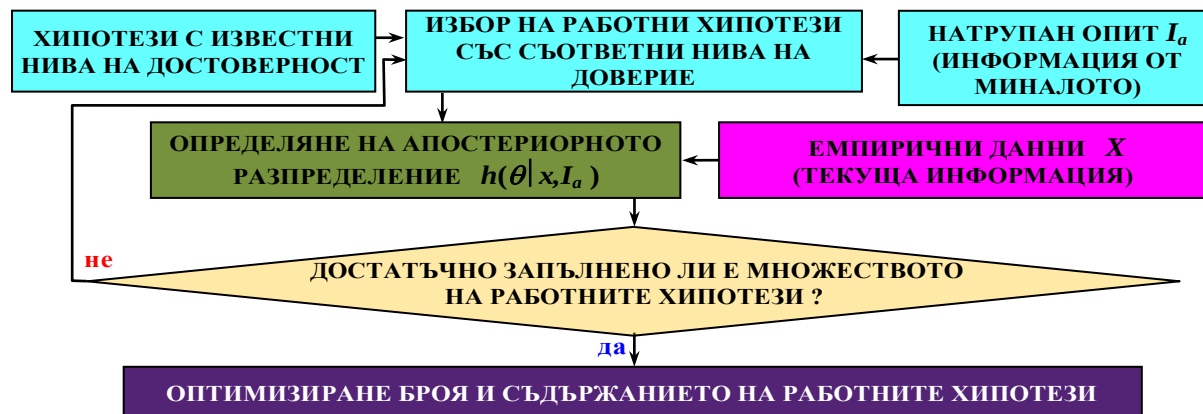


фиг.2 Схема на Зелнер

Описаната на *фиг. 2* схема илюстрира ортодоксалната Бейсовска процедура. За разлика от повечето свои модификации, тя запазва априорното разпределение неизменно в процеса на натрупване на емпирични данни. Логичното обяснение на такъв подход в Бейсовската теория е формулирано от Удуърд [17], който твърди, че нито една съвкупност от вероятности не може да се приеме за по-фундаментална от друга съвкупност от вероятности. Авторът предлага по-детайлизирана и усъвършенствана модификация (*фиг. 3*) на ортодоксалната схема. Тя дава възможност за коригиране на "априорното ниво на доверието" [17]. Удуърд се базира на философското разбиране, че човек по рождение притежава неизброимо многообразие от подсъзнателни съждения, на всяко от които съответства някаква вродена степен на доверие. От множеството подобни съждения авторът отделя неговолямо подмножество от осъзнати съждения, към които добавя новополучените по време на експеримента съждения. Въз основа на последните две подмножества от съждения формира множеството на работните хипотези със съответстващото на всяка от тях ниво на доверие. Процедурата приключва с формиране на нивото на доверие към всяка от възприетите хипотези. С помощта на теоремата на Бейс се определят нивата на доверие на емпирични данни, постъпващи от различните източници на информация (оценява се достоверността, прецизността и коректността на всеки от каналите за постъпване на емпирични данни, и тази оценка се взема под внимание при определянето на апостериорното разпределение).

Кондън достига и по-далеч като предлага при всяко поредно постъпване на нови емпирични данни Бейсовската процедура да включва задължителна корекция на априорните вероятности [18]. Нещо повече, авторът счита, че след обединяването на априорното разпределение с емпиричните данни, Бейсовското апостериорно и субективното априорно разпределение е необходимо да се съгласуват изцяло. При такава специфика на Бейсовската процедура Кондън стига до логичния извод, че ефектът би бил максимален, ако съществуват няколко работни априорни разпределения и изследователят избира едно от тях, което най-пълно съвпада с емпиричните данни. Идеята в случая е, да се

премахнат изцяло субективните вероятности в Бейсовската теория. Модификациите предлагани от Денисън, Холмс, Малик и Смит [19] могат да се причислят в групата на рационалните Бейсовски процедури.



фиг.3

Ледерман и Лойд разглеждат възможността за получаване на апостериорна информация въз основа на няколко пакета от данни. За целта авторите прилагат Бейсовския подход за съвместяване на сходна по характер информация [10]. Те разглеждат крайно множество от взаимноизключващи се статистически модели  $\{M_1, M_2, \dots, M_k\}$ , всеки от които притежава определена априорна вероятност  $P\{M_1\}, P\{M_2\}, \dots, P\{M_k\}$ , където  $0 \leq P\{M_i\} \leq 1, i=1 \div k$ . Авторите използват още факта, че сумата от вероятностите за едновременно настъпване на пълна група от взаимно изключващи се случайни събития е:  $P\{M_1\} + P\{M_2\} + \dots + P\{M_k\} = 1$  и анализират схема на "поетапното" постъпване и използване на пакетите от данни. За оценяване на възможността да бъде съчетана наличната априорна информация с емпиричните данни (с „новите данни“), те предлагат схема за получаване на Бейсовски оценки, основаваща се на ортодоксалната Бейсовска процедура. Разработената от тях схема съдържа три етапа:

**I етап.** Съставяне на функцията на правдоподобие  $l(\theta | I_e)$ . За целта се използва подходящ статистически модел, основаващ се на разпределението на основната случайна величина  $F(t; \theta)$  и експерименталните данни  $I_e$ , получени в резултат от реализацията на плана за изпитване  $\Pi$ .

**II етап.** Установяване на апостериорното разпределение  $h(\theta | I_a, I_e)$ . За целта се използва формулата на Бейс (1), във вида:

$$h(\theta | I_a, I_e) = \frac{h(\theta | I_a) l(\theta | I_e)}{\int_{\Omega} h(\theta | I_a) l(\theta | I_e) d\theta}, \quad (2)$$

където  $\Omega$  е областта на изменение на параметъра  $\theta$ .

**III етап.** Получаване на Бейсовските оценки. Бейсовският доверителен интервал се определя от условието:

$$P\{\underline{R} \leq R \leq \bar{R}\} = \delta, \quad (3)$$

или

$$\int_{\underline{R} \leq R(\theta) \leq \bar{R}} h(\theta | I_a, I_e) d\theta = \delta. \quad (4)$$

За определяне на Бейсовската точкова оценка  $\hat{R}^*$  се използва функцията на апостериорния риск:

$$G(\hat{R}) = \int_{\Omega} L(\hat{R}, R(\theta)) h(\theta | I_a, I_e) d\theta, \quad (5)$$

и от всички оценки  $\hat{R}$  се избира тази, която минимизира функцията (5):

$$\hat{R}^* = \arg \min_{\hat{R} \in [0;1]} G(\hat{R}) . \quad (6)$$

Ако избраната функция на загубите е квадратична функция от вида:

$$L(\hat{R}, R) = (R - \hat{R})^2 , \quad (7)$$

то Бейсовската оценка  $\hat{R}^*$  се определя като средна апостериорна стойност:

$$\hat{R}^* = \int_{\Omega} R(\theta) h(\theta | I_a, I_e) d\theta . \quad (8)$$

Грешката за изчислената стойност  $\hat{R}^*$  се оценява чрез апостериорното средно квадратично отклонение  $\sigma_{\hat{R}^*}$ :

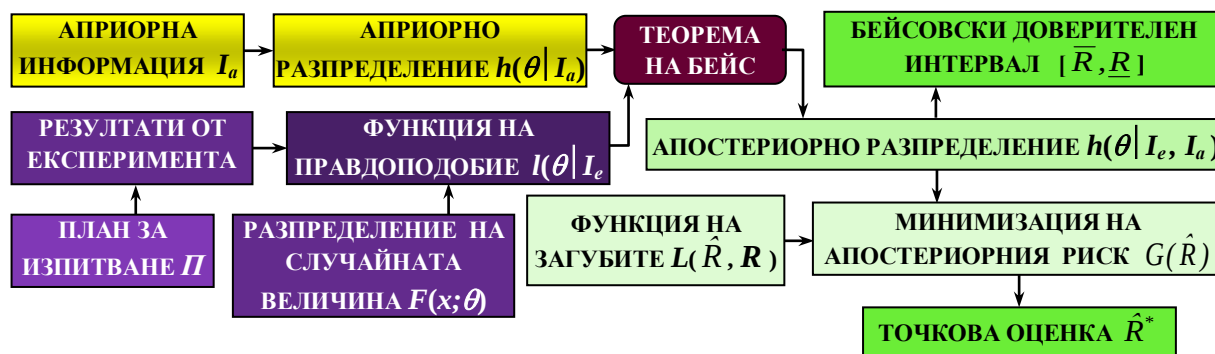
$$\sigma_{\hat{R}^*}^2 = \int_{\Omega} R^2(\theta) h(\theta | I_a, I_e) d\theta - \hat{R}^{*2} . \quad (9)$$

Алгоритъмът за оценяване с помощта на ортодоксалната Бейсовска процедура се основава на четири компонента (фиг. 4):

**I елемент** - план на изпитване  $\Pi$  - посочва начина, по който се получават емпиричните данни;

**II елемент** - разпределение на вероятностите за настъпване на основната случайна величина, характеризираща конкретното медицинско изследване (например, функцията за разпределение на случайната величина  $F(t; \theta)$ , където  $\theta$  е вектора на параметрите);

**III елемент** - априорно разпределение на вероятностите (например плътността на разпределението  $h(\theta)$  за вектора на параметрите  $\theta$ ), характеризиращо степента на неопределеност на априорната информация  $I_a$ , касаеща направените в миналото медицински изследвания;



фиг.4 Алгоритъм за прилагане на Ортодоксална Бейсовска процедура

**IV елемент** - функция на загубите  $L(\hat{R}, R)$ , характеризираща стойността на загубите на информация, свързани със замяната на действителната стойност на оценявания показател  $R$  с неговата оценка  $\hat{R}$ .

За онагледяване на постулатите, присъщи на емпиричното Бейсовско оценяване тук е показана формулировката на задачата и последователността за получаване на оценка на скаларния параметър  $\theta$  и свързания с него оценяван количествен показател  $R(\theta)$ .

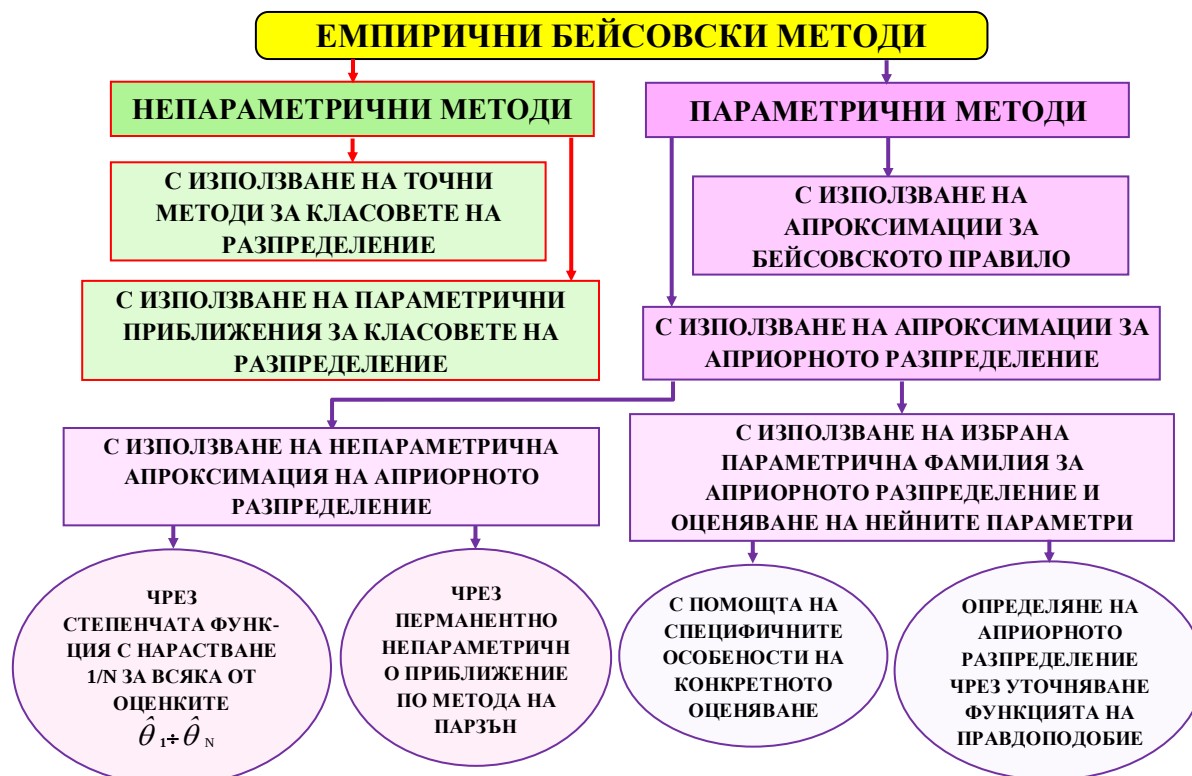
Поради изложените по-горе причини (наличие на необходимата априорна информация от предходни аналогични медицински изследвания) се приема, че съществува и е известно (или, че лесно може да се установи) априорното разпределение на параметъра  $\theta$ , условие, необходимо за прилагането на емпиричния Бейсовски подход. Прилага се основната схема на Бейсовското оценяване (фиг. 1), като се апроксимира или Бейсовското решаващо правило или априорното разпределение, кореспондиращо с данните за пред-

шестващите изследвания. Приема се, че  $T^{(i)} = (T_1^{(i)}, T_2^{(i)}, \dots, T_{N_i}^{(i)})$  са резултатите от тестването (изпитването), получени при  $i$  на брой серии експерименти. Приема се също, че експерименталните данни (за действието на лекарствените средства, или за сходни клинични проучвания, или за медико-диагностични тестове, или за конкретни медицински практики при лечения на конкретно заболяване и т.н.), натрупани за в I-вата, II-рата, ... (N-1)-та серия, са за аналогични, достатъчно близки по характер до емпиричните данни (тези за текущото медицинско проучване, съставляващо в N-тата серия). Следвайки формализираното описание на емпиричния Бейсовски подход се допуска съществуването на устойчив статистически механизъм, който довежда до неизвестното в общия случай априорно разпределение  $h(\theta)$ . Така задачата може да се сведе до намиране на Бейсовска оценка на параметъра или показателя  $R(\theta)$ , с помощта резултатите от N-тата серия експерименти, като се отчитат резултатите от изпитванията, получени при предшестващите N-1 серии.

За оценяването на скаларния параметър  $\theta$  биха могли да се използват: точковата оценка  $\hat{\theta}_R^*$ , апостериорното средноквадратично отклонение  $\sigma_{\hat{\theta}_R^*}$  или Бейсовският доверителен интервал  $[\theta, \bar{\theta}]$ . Оценяването на вероятността за безотказна работа ще бъде извършено с помощта на: точкова оценка  $\hat{R}_e^*$ , апостериорно средноквадратично отклонение  $\sigma_{\hat{R}_e^*}$ , долна доверителна граница  $\underline{R}_{de}^*$ . Емпиричните Бейсовски методи дават възможност за постигане на необходимите оценки.

Съществуващите емпирични Бейсовски методи, които биха могли да намерят приложение при обединяване на априорната информация с получените „свежи” емпирични данни от конкретното медицинско изследване, могат да бъдат разделени в две групи (фиг. 5):

- параметрични емпирични методи, които могат да се използват в случаите, когато са известни параметричните разпределения на натрупаните статистически данни;
- непараметрични емпирични методи, които са приложими при неизвестни параметричните разпределения на наличните статистически данни, но при които може да се докаже принадлежността им към по-голям или по-малък непараметричен клас  $S$ .



фиг. 5 Класификация на Емпиричните Бейсовски методи

## Констатации и изводи

При разработването на нови методи за лечение, на нови медицински практики или на нови лекарствени средства (или модификации на вече съществуващите такива), екипите провеждащи изследването, по правило разполагат необходимата им информация за провеждани преди това аналогични проучвания, изследвания, тестове или експерименти. Голяма част от данните за тези аналогични изследвания, са били натрупвани продължително време, от различни, независими един от друг екипи, което на практика редуцира до минимум субективното влияние върху натрупаните научни факти и доказателства, и по този начин гарантира високата степен на достоверност на събраната информация. Като прототипи на конкретното медицинско изследване могат да бъдат използвани емпирични данни от изследвания, притежаващи аналогично предназначение и характеристики и отличаващи се него по някои специфични, второстепенни, маловажни и несъществени параметри, непроменящи характера и същността на актуалното емпирично изследване. За прототипи могат да послужат и изследвания от същия тип, но проведени по друг метод или базирани на различна технология за обработка на резултатите, или на концепция с различно предназначение. Подходящи за използване са и данни от емпирични изследвания, напълно сходни по функция и цели, но проведени при различни условия на изпитване.

Изложените в статията аргументи и констатации потвърждават необходимостта от търсене и намиране на релевантен отговор на изброените по-горе проблеми. В заключение може да се констатира безспорната е нуждата от:

- решаването на проблеми, свързан с синхронизирането на наличната априорна информация от медицинско естество с поучаваната нова, актуална информация от текущото към конкретния настоящ момент медицинско изследване [5], [6].
- разработването на нови достатъчно точни и надеждни методи, които да направят възможно това синхронизиране, и така да подпомогнат и ускорят практическите дейности, свързани със събирането, обработката, класифицирането и анализа на резултатите от медико-диагностичните изследвания.

Идеите представени в тази статия, са резултат от работата по докторантски проект 353/15.01.2015 (договор #22-Д/2015 г.), финансиран целево от държавния бюджет, чрез фонда за научни изследвания на Медицински университет – София.

## References

- [1] Vladimira I. Boyadzhieva, Nikolai Stoiov, Tsvetoslav A. Georgiev, Guenka Petrova. How to treat patients with rheumatoid arthritis? Opportunities and benefits of the implementation of a pharmacoeconomic cost-effectiveness analysis. January 2015.
- [2] Tsvetoslav A. Georgiev, M. Ivanova, R. Stoiov. Recent trends in the pathogenic mechanism of osteoarthritis, *Revmatologia*. October 2013.
- [3] Tsvetoslav A. Georgiev, R. Stoiov, Vladimira I. Boyadzhieva, M. Ivanova. Hyaluronic acid - Historical data, classification, mechanism of action and recommendations. January 2014.
- [4] Tsvetoslav A. Georgiev, R. Stoiov, M. Ivanova. Biomarkers in osteoarthritis. January 2013.
- [5] Douglas S. McNair, Roy L. Simpson. Bayesian Cost-effectiveness Analysis of Falls Risk Assessment Tools: Falls. *Nursing administration quarterly*, Oct 2016.
- [6] F. Cronin, S. Loughran, E. O'Connell, R. O'Connell. Comparison of two Multifactorial Fall Risk assessment Tools in an Irish Day Care Centre setting: A Modified Version of the "Quick Screen" and the HSE "Multi-factorial Falls Risk Assessment in Primary Care".

Irish Journal of Medical Science 182:S269-S269. September 2013.

- [7] Харалампиев К. Парадигмите в статистиката - Бейсовска статистика. Сб. доклади от НК „Актуални проблеми на статистическата - теория и практика”. Университетско изд. „Стопанство“, С. 2007. <http://kaloyan-haralampiev.info/wp-content/uploads/2010/03/doklad-1.pdf>
- [8] Айвазян С. А., В. С. Мхитарян. Теория вероятностей и прикладная статистика. UNITY, Москва, 2001.
- [9] Айвазян С., В. Бухштабер, И. Енюков, Л. Мешалкин. Прикладная статистика. Классификация и снижение размерности. Москва, Финансы и статистика, 1989. - 607 с.
- [10] Ledermann W., E. Lloyd. Handbook of applicable mathematics: Volume VI: Statistics, Part A./Part B. Chichester-New York-Brisbane-Toronto-Singapore John Wiley & Sons Ltd, 1984. - p. 544.
- [11] Вентцель Е.С., Овчаров Л.А. Теория вероятностей и ее инженерные приложения М.: Высшая школа, 2000. - 480 с.
- [12] Вуколов Э.А., Ефимов А.В., Земсков В.Н., Поспелов А.С. Сборник задач по математике для втузов Т. 4. Москва, Физматлит, 2004. - 432 с.
- [13] J. Lin, M. Asplund and A. Parida. Reliability Analysis for Degradation of Locomotive Wheels using Parametric Bayesian Approach. DOI: 10.1002. Copyright © 2013 John Wiley & Sons, Ltd. Qual. Reliab. Engng. Int. 2013.
- [14] В. Савчук. Байесовские методы статистического оценивания. Москва, Наука, 1989, ISBN 5-02-014103-8. - с. 328.
- [15] S. James Press Subjective and Objective Bayesian Statistics: Principles, Models and Applications, John Wiley & Sons, Inc., 2001., ISBN: 978-0-471-34843-6. - p. 600.
- [16] Arnold Zellner. An Introduction to Bayesian Inference in Econometrics. Chichester-New York-Brisbane-Toronto-Singapore John Wiley & Sons Ltd, 1996. ISBN: 978-0-471-16937-6. p. 448.
- [17] George G. Woodworth. Biostatistics: A Bayesian Introduction. Wiley Series in Probability and Statistics. 2004. ISBN 9780471468424. p. 384.
- [18] Peter Congdon. Applied Bayesian Modelling. Wiley Series in Probability and Statistics, March 2003, ISBN: 978-0-471-48695-4. - p.478.
- [19] David G. T. Denison, Christopher C. Holmes, Bani K. Mallick, Adrian F. M. Smith. Bayesian Methods for Nonlinear Classification and Regression. Wiley Series in Probability and Statistics. March 2002, ISBN: 978-0-471-49036-4. - p. 296.