On Experience of Using Distance Learning Technologies for Teaching Cryptology

Sergey Zapechnikov, Natalia Miloslavskaya, Vladimir Budzko

On Experience of Using Distance Learning Technologies for Teaching Cryptology

Zapechnikov Sergey, Miloslavskaya Natalia and Budzko Vladimir

The National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), 31 Kashirskoye shosse, Moscow, Russia

{SVZapechnikov, NGMiloslavskaya}@mephi.ru

Abstract. The necessity of using Distance Learning (DL) for teaching cryptology is analyzed. The modern features of applying different DL approaches to solve this task are extracted. The NRNU MEPhI's experience in creating mass-oriented DL project called Cryptowiki.net is described; its structure and assignments implemented by the students of cryptologic courses are shown. The related works are presented. Cryptowiki.net's difference from the analogs is stressed out. The main findings of the research are formulated in conclusion.

Keywords: Cryptology, Teaching cryptologic courses, Mass-oriented Distance Learning Technologies

1 INTRODUCTION

Distance learning (DL) can be defined as a teachers-students interaction at a distance that reflects all the typical learning process's components (objectives, contents, methods, organizational forms, and learning tools) and is realized by the specific means of the Internet technologies or another tools providing interactivity [1, 2]. Even a new cryptology concept was formed: "Modern cryptography is concerned with the construction of information system that is robust against malicious attempts to make these systems deviate from their prescribed functionality" [3].

The comprehensive DL technologies' (DLT) development is one of the global trends widely supported by almost all universities being at the first places in the world rankings like THE (Times of Education), Quacquarelli Symonds (QS) World University Rankings, Shanghai ranking and others. This trend also affects teaching of different subjects in the field of information security and cryptology in particular. However, the widespread DLT usage for teaching cryptology observed today is due to not only the "spontaneous" world trends, but it is also prepared by a number of objective conditions discussed below.

The subject area of cryptology has significantly expanded over the past two decades. Many new applications and corresponding new scientific and methodological apparatus have appeared. At the same time there is a stabilization (or even some decrease) of scientists' and practitioners' interest to the specific sections of classical

adfa, p. 1, 2015.

cryptology or relatively new sections which were developed dynamically up to this moment. Such significant changes are due to, on the one hand, the rapid information technologies (IT) development and the growing needs of society in ensuring IT security, and on the other hand, new scientific discoveries in cryptology and related fields of applied mathematics. The universities teaching cryptologic disciplines were faced the problem of adequately addressing the extraordinary changes, taking place in the field of computer science in general and in cryptology in particular, in their curricula and educational practice.

The steady and rapid growth of scientific publications in the field of cryptology is observed around the world in recent years. The publications' statistics in the electronic preprint archive of the International Association for Cryptologic Research (IACR) for 1996–2014 (Fig. 1) is a vivid evidence of this fact [4].

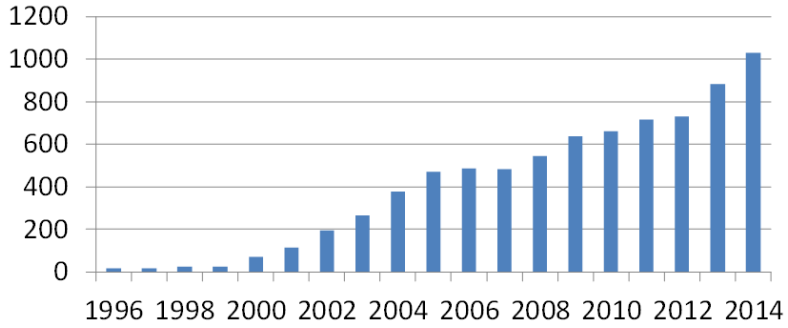

Fig. 1. Publications' statistics in the IACR's electronic preprint archive

In addition the fact that the scientific and technical information search capabilities were fundamentally changed with the advent of the Internet search services like Google, Yahoo!, Yandex, etc., Electronic encyclopedias such as Wikipedia, the archives of electronic publications and preprints (for example, CiteSeer, IEEExplore, eprint.iacr.org et al.) cannot be ignored. As our practice shows these services are actively used by the students and teachers to find a proper term, article, book, algorithm, protocol, method or application description, etc.

A teacher's role is fundamentally changing in the context of this "information explosion". In the past he/she was almost the only affordable student's authoritative source of knowledge. Now he/she turns in some sense into a certain filter that should save the students from the huge flow of superfluous, insignificant or frankly false information and give them only high-quality and systematically organized knowledge. In these circumstances the teacher's task is to organize an educational process in such a way that will maximize the effectiveness of learning and acquisition of the necessary competencies (knowledge, skills and abilities) by the students.

The remainder of the paper is organized as follows. Section 2 includes an overview of related works. Different DLT applications are analyzed in Section 3. Section 4 introduces the NRNU MEPhI's experience in applying the mass-oriented

DLT in the form of the Cryptowiki.net site. The main findings of the project are formulated in conclusion.

2 RELATED WORKS

Of course our idea to create a specialized DL site in not novel. The sharply increasing interest to DL has led to the emergence of a number of DL courses on cryptology in English (with rare exceptions) at present. The courses offered by the MOOC systems (from *Massive Open Online Courses*) should be noted among them first of all.

The "Cryptography I" course is already available and the "Cryptography II" course is going to start from June 2015 in the Coursera system; both courses are authored by the famous Stanford University's Professor Dan Boneh [5].

The Udacity portal offers the "Applied Cryptography" online course conducted by the University of Virginia's Professor Dave Evans [6].

Three courses ("Cryptography and Cryptanalysis", "Advanced Topics in Cryptography", and "Selected Topics in Cryptography") are available at the online educational portal of the Massachusetts Institute of Technology (MIT) [7].

In addition to the online courses a number of carefully designed offline courses on cryptography well suited for self-training can be found on the Internet (not only in the form of lectures' video records and forums that allow to meet with a teacher, but also as notes, lectures, tutorials, home works and their solutions, sample exam assignments, etc.). For example, the courses such as "Modern Cryptography" and "Advanced Cryptography" by Professor Mihir Bellare and Professor Phillip Rogaway from the University of California at San Diego [8], "Cryptographic Protocols" by Ueli Maurer from the ETH Zurich University [9], and "Introduction to Cryptography" by Rafael Pass from the Cornell University [10] can be mentioned here.

It is often recommended for the students to use a wiki as a reference tool in some online courses. That mainly affects the sections not included in the curriculum body (typically the wiki textbooks are additional, not obligatory parts of a taught course) and submitted to their independent study. For example, D.Boneh recommends using the wiki tutorial on the basics of discrete mathematics and discrete probability posted on the popular Wikibooks site as a complement to the above courses [11]. The wiki book on cryptography can be found at the same site [12], but it still looks unfinished.

The given brief analysis shows the necessity of developing a consolidating bilingual (English-Russian) Internet resource in the form of web site containing systematized information on cryptology.

3 DISTANCE LEARNING TECHNOLOGIES' APPLICATION SCENARIOS

Since cryptology itself is a part of computer science for a long time, the IT role in teaching cryptologic disciplines is dual in modern conditions: they are both a study

subject and the tools for organizing an educational process. DLT have the leading role among these tools [13].

At present DLT are quite clearly divided into two sectors: mass-oriented "stream" (large-scale) learning and individual-oriented "chamber" learning.

The first type of technologies is called MOOC. There are the completely-ready-to-use educational products including both learning tools and information resources available online to a potentially unlimited number of trainees via the web interface. In addition to the traditional courses the MOOC's users may have an access to the new educational resources (videos, interactive tasks' sets and assignments in programming, as well as users' forums), enabling to establish an original community of students, professors and teachers being involved in the educational process [14].

The main MOOC idea is realized most completely in the DL Networks (DLN) available via portals, accumulating extensive themed sets of courses in various subject areas. The characteristics of the most-known and popular DLN are shown in Table 1.

Table 1. Most-known DLN on the Internet

DLN Name	**Internet Address**	**Founders**	**Number of available courses**			**Price; Certificate Issuance**
			2012	**2013**	**2014**	
Coursera	coursera.org	Universities: Stanford, Princeton, Berkley, Ohio, Pittsburg, Illinois, Toronto, Georgia, Virginia	207	553	1127	Free; certificates are issued at the end of some courses
edX	edx.org	Universities: Harvard, Massachusetts, Berkley, since 2013 – Texas	9	110	429	Resources – free; certificates are now free; will be paid in future
UM Global Academy	umga. miami.edu	University of Miami	Middle school (MS) – 39, High school (HS) – 91	MS – 39, HS – 73	MS – 39, HS – 74	Access to all resources and courses – $70 registration fee
Udacity	udacity.com	Private company	18	33	60	Free
MIT Open Coursware	ocw.mit.edu	Massachusetts Institute of Technology	2100	2150	2150	Resources – free; certificates are not issued

The high quality of all DLN educational resources and significant increase in the number of available courses should be marked. The number of trainees for the most successful courses is measured by tens and hundreds of thousands worldwide. For example, the "Artificial Intelligence" course from the Coursera network is a leader with more than 180,000 people signed up all over the world at the same time. Such courses being once "put on a stream" are as a rule repeated periodically in the future.

Focusing on such a large audience determines the MOOC's characteristics:

- lack of the students' online feedback to a teacher during the sessions (as the main educational form is a video lecture);
- home works' and long-term projects' check implementation: knowledge progress testing is carried out either by choosing a correct answer from the given set and filling out some online form with automatic check of formats and value meanings entered, or by mutual check and review performed by the students themselves.

In almost all DLN listed in Table 1 the courses in cryptology are presented, for example: "Cryptography I" and "Cryptography II" (D.Boneh) in the Coursera network, "Applied Cryptography" (D.Evans), "Computer Security" conducted by the Stanford University together with the University of California, Berkley (USA) in the same network and several courses on network security and cryptography (both more general and more specialized) in the MIT Open Courseware network (USA).

According to the authors' opinion the obvious advantages of the DLN courses are their high quality and minimum price. That allows to recommend them for self-training to the universities' teaching staff as well as to the students studying on different degrees. The DLN courses being taken together cover all the stages of education – from undergraduate to postgraduate, from Bachelors to Masters and PhD.

However the technologies oriented on massive training do not limited to DLN. They are based on the web technologies as it has been already mentioned. Therefore the creation of multifunctional web sites supporting the educational process and implementing various forms of teachers-students interaction can also benefit.

Technologies of the second type (oriented on individual learning) are essentially different types of videoconferencing with one or more leading (professor/instructor) and a small number of participants actively involved in the process of interaction with the leading. They have a special name – webinars, resulting from compound of the words "web" and "seminar", i.e. a seminar conducted using the web technologies (another names are online seminars, web conferences). All the webinar's participants should either install the special software on their computers or use the special web services provided by several service providers on the Internet. The best-known examples are the services such as Cisco WebEx, Citrix Online, Microsoft Office Live Meeting, HP video conferencing & HP Halo telepresence solutions. However, the number of solutions is increasing every day.

As practice shows the webinars are well suited for the lectures and seminars on different subjects, in particular, a wide range of IT-related disciplines. Currently, some Russian training centers and universities (like the NRNU MEPhI since 2012) implement a few training courses in "Information Security" in the form of webinars.

We would like to point out another model of IT application, having great potential for teaching the cryptologic disciplines. It is no secret that the universities have a very strong and old tradition of "theorizing" (sometimes too redundant) many subjects being taught at the higher school. The reason is the pronounced orientation toward the mass training of scientific and pedagogical personnel required in the past. However, a significant increase in demand for developing the students' practical skills and abilities in using the latest hardware and software and acquisition of practical experience in chosen speciality is observed due to the changes in economic and social life taking place over the past two decades all over the world. The laboratory facilities of many universities and their funding level are not always fully prepared to meet these requirements. At the same time open source software usage is significantly expanding all over the world. In most cases the license agreements for such software allow either its completely free usage for any purpose or at least free usage for non-commercial and educational projects. Free software emerging in the Internet and having a lot of potential applications in cryptology training and its mastering (in particular the development of new labs and practical assignments) can significantly enhance the practical focus of the updated cryptologic courses. The specific examples of such open source software are the libraries of cryptographic algorithms Crypto++, PyCrypto, the prototyping tool for cryptographic constructions Charm, the theoretical and numerical library NZmath and many others.

4 Experience of Mass-Oriented Distance Learning Technologies' Application

The creation of the Cryptowiki.net site supporting educational process for the cryptologic disciplines at the "Information Security of the Banking Systems" Department of the NRNU MEPI is an example of the first type of DLT application.

The site available at http://cryptowiki.net is used as a reference and information resource for professionals in the field of cryptography and for all kinds of students' home and independent works in their study of the "Cryptographic Protocols and Standards" and "Cryptography in Banking" courses. The site contains various materials for the students' work, rules description for the progress testing rating system and records of webinars previously conducted by the courses' author (Professor S. Zapechnikov).

The site operates under OS Windows on the commercially available hosting with a free content management system (engine) MediaWiki, version BitNami.

Cryptowiki.net's interface is similar to the Wikipedia interface, well known to the absolute majority of users (Figure 2).

The central place on the site is allocated to the reference and information system called the "Encyclopedia of Theoretical and Applied Cryptography" (further Encyclopedia). This is a comprehensive information resource created by the joint efforts of the teachers and students, which includes all content types available for posting: text, graphics, video, demo programs, mathematical expressions, program fragments' listings and others.

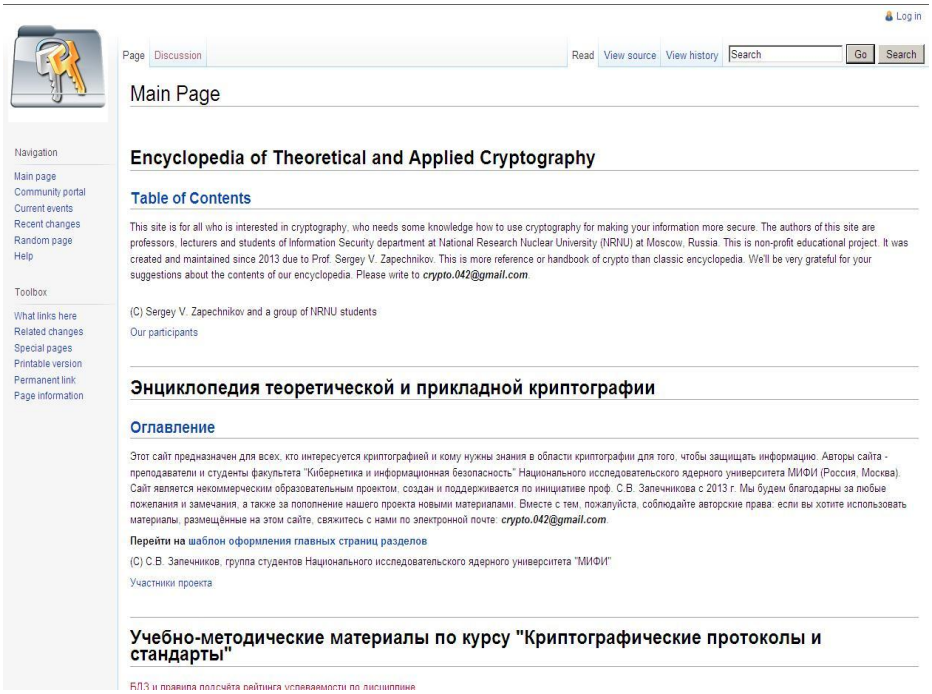

Fig. 2**.** Cryptowiki.net home page

The Encyclopedia consists of 56 substantive sections, each of which is dedicated to one of the major areas of modern cryptography and is available both in English and Russian languages. The Encyclopedia currently includes the following sections.

Part I "Foundations of Cryptography (Cryptographic Primitives)" consists of 25 sections covering all the main sections of the mathematical apparatus used in modern cryptography and the main types of cryptographic constructions such as block and stream ciphers, hash functions, open encryption schemes, digital signature scheme, as well as numerous supporting questions.

Part II "Applications of Cryptography (Cryptographic Protocols)" includes 31 chapters and is devoted to the cryptographic protocols' design and analysis. It gives knowledge on Zero-knowledge proofs, identification protocols, key distribution protocols, Secret sharing schemes, Threshold cryptography, Byzantine agreement protocol, Fair exchange, Protocols for secure communication channels, Protocols for secure databases retrieval, Protocols for secure cloud computing and secure cloud storage, Protocols for mobile security, Secure multi-party computations and many other cryptographic applications.

Detailed Encyclopedia's content is presented in Table 2.

Table 2. Cryptowiki Encyclopedia's content

Part I "Foundations of Cryptography (Cryptographic Primitives)"	***Part II "Applications of Cryptography (Cryptographic Protocols)"***
(1) Brief overview of cryptography; (2) Mathematical background; (3) Classical cryptography: experience and lessons; (4) Perfectly-secret ciphers and Shannon's theory; (5) Cryptographic generators. Stream ciphers and their cryptanalysis; (6) Block ciphers and their cryptanalysis; (7) Symmetric encryption schemes; (8) Symmetric message authentication schemes based on block ciphers; (9) Cryptographic hash functions; (10) Symmetric message authentication schemes based on cryptographic hash functions; (11) Symmetric authenticated encryption schemes; (12) Symmetric encryption schemes with special features or additional functionality; (13) Symmetric key management; (14) More mathematical background for asymmetric cryptography; (15) Computationally hard problems used in asymmetric cryptography; (16) Algorithms used in asymmetric cryptosystems; (17) Public key exchange; (18) Asymmetric encryption schemes; (19) Digital signature schemes; (20) Pairing-based asymmetric cryptosystems; (21) Digital signatures with special features or additional functionality; (22) Asymmetric key management; (23) Physically unclonable functions; (24) Standardization of cryptographic methods; (25) Overview of cryptographic primitives: Roadmap for cryptographers.	(1) The basics of cryptographic protocol construction and analysis; (2) Zero-knowledge proofs; (3) The framework for identification protocols; (4) The framework for key distribution protocols; (5) Secret sharing schemes. Threshold cryptography; (6) Byzantine generals' problem. Byzantine agreement protocol. Security of distributed computing; (7) Fair exchange; (8) Privacy-preserving collaborative optimization; (9) Hardware and embedded cryptography; (10) Cryptographic libraries for software developers; (11) Vulnerabilities and security of software cryptography; (12) Remote authentication protocols and "single sign-on" mechanisms; (13) Protocols for secure communication channels; (14) Wireless networks security; (15) Secure e-mail; (16) Secure instant messaging; (17) Anonymity networks; (18) Protocols for secure databases retrieval; (19) Protocols for secure cloud computing and secure cloud storage; (20) Protocols for mobile security; (21) RFID security; (22) Grid security; (23) Peering networks security; (24) Secure payment systems; (25) Secure broadcasting. Digital content copyright protection; (26) Secure multi-party computations; (27) Steganography; (28) Quantum cryptography; (29) Post-quantum cryptography; (30) Beyond the post-quantum cryptography; (31) Unsolved crypto problems and the future of computer security.

The site's sections essentially differ from the majority of online information resources by their content's volume and depth. It should be noted that the site is a joint textbook on theoretical and applied cryptography, co-written by students and teachers. However, its content is more focused at people experiencing practical needs in cryptography usage at their workplace, rather than cryptographers–theorists. Most sections do not present the formulations and rigorous proofs of theorems and propositions, but each section contains extensive information on the best-known methods and algorithms for solving the corresponding cryptographic tasks, especially their implementation, allowing to ensure high performance, to avoid vulnerabilities and to achieve ease of use of cryptographic mechanisms by their customers.

In comparison with the traditional textbooks the site's content can be replenished quicker, but of course it is not edited so carefully as for "paper" publishing.

There are some sections, which cannot be found in traditional textbooks. For example, the "Overview of cryptographic primitives: Roadmap for cryptographers" section provides a roadmap of cryptography primitives usage for security tasks' decision. That allows the readers to easily navigate the variety of available cryptographic constructions, to choose the most suitable among them for solving their problems and to correctly use it in building their own cryptographic protocol.

Completing assignments, their mutual reviewing by the students and commenting by the teachers on the site create an open and transparent environment for all parts of the educational process, and promote the publicity of students' work results and their objective assessment by the teachers.

An assignment given to the students using the site in the educational process consists of three parts:

1. *content creation for the selected site's section in Russian*. To complete this part of the work it is necessary to create a working team of 2 students (it is allowed to do the work of the whole team alone if a student wants that). The accomplished work is evaluated by the teachers using the 50-points' scale, and the resulting points are distributed among the members of the working team according to their real contribution to the work performed (but not more than 25 points for each member of the working team);
2. *content creation for the selected site's section in English*. The previously formed working teams are kept to perform this work. The site's section content in English should be adequate to the corresponding section in Russian. The slight reductions are allowed in the event of difficulty of the text interpreting in English. The accomplished work is evaluated by the teachers using the same 50-points' scale, and the resulting points are distributed among the members of the working team according to their real contribution to the work performed (but not more than 25 points for each member of the working team). If very many questions to the work performed appear, the team can be called for the oral defense of their work results;
3. *software demo creation demonstrating in practice the execution of one of the cryptographic protocols (algorithms) described in this site's section (or one of the sections created in previous years).* The protocol initial data input (for example long-term and (or) one-time keys, parameters, identifiers, etc.) from files or keyboard

and program output to the screen and file should be provided in the program. All arithmetic and logical operations performed by the protocol's parties should be implemented. It is enough to make the program run on one computer and to execute sequentially data input for each of the protocol's parties. Similarly to the output data. Default data input should be provided in case of users' refusal of entering their data. The choice of programming tools and libraries is not limited. The user interface can be arbitrary, but it should be clear to a program's user (for example, the protocol implementation can be presented as a table, similar to those discussed during the lectures). It is desirable, but not required, that the interface will be graphical rather than textual. The program should be run under OS Windows. The program's source code and executables will be available on the corresponding pages of Cryptowiki.net after work will be finalized.

In addition to the Encyclopedia the traditional functionality for educational and methodical sites is implemented on the site: there are a lot of information materials, bulletin board, additional materials for lectures, etc.

5 CONCLUSION

Summarizing the discussion on applying DLT to teaching cryptology, we would like to note the following.

1. The existing DLT's analysis and the authors' personal experience of their application in teaching cryptology testify that DLT can significantly upgrade all kinds of training – lectures, seminars, and laboratory works. The main positive effect in this case is an increase of educational process's effectiveness, as well as the convenience of teachers-students interaction when performing the home works, course projects, organizational issues and mastering of elective discipline sections.

2. Two pronounced current trends of DLT development are DLN (as well as the related multifunctional web resources that address more narrow audience) and webinars. DLN is the most striking manifestation of emerging global educational space and global competition of the world's leading universities in the educational field. A webinar is the most effective form of classes' organization for the small groups of students. DLT combining both approaches are equally applicable in cryptology training.

3. Our gained experience in applying DLT in teaching cryptology can be extended to the other specialized disciplines taught to the students and trainees of short-term training and long-term professional retraining courses in the "Information Security" direction as well as to supervising the students' educational and scientific research, practical and final qualifying works.

4. The main difference between our CryptoWiki project and its analogs is that it organically complements the lectures and practical works in the cryptologic disciplines, supporting the interactive forms of students' teaching. They feel themselves involved in the process of creating a large-scale Encyclopedia, launched by their predecessors – the students of previous graduation years and planned to continue in the coming years. After graduating from the NRNU MEPhI the former students continue

to access the Encyclopedia, in developing which they have contributed, to recommend it to their colleagues and thus spread the cryptologic knowledge.

The project's success is confirmed by the facts that more than 17,000 users have visited the site during the first year of its operation and totally more than 28,000 since 2013.

6 REFERENCES

1. Michael W. Allen. Michael Allen's Guide to E-Learning: Building Interactive, Fun, and Effective Learning Programs for Any Company. February 2003. 360 p. ISBN: 978-0-471-20302-5.
2. Termini i opredelenija distanchionnogo obuchenija. Laboratorija distanchionnogo obuchenija Rossiyskoy Academii Nauk. URL: http://distant.ioso.ru/do/termin.htm (access date 24.02.2015) (in Russian).
3. Goldreich O. Foundations of cryptography – a primer. URL: http://www.wisdom.weizmann.ac.il/~oded/PS/foc-sur04c.ps (access date 27.02.2015).
4. Cryptology ePrint Archive. URL: http://eprint.iacr.org (access date 27.02.2015).
5. Cryptography I. URL: https://www.coursera.org/course/crypto (access date 27.02.2015).
6. Applied Cryptography. URL: https://www.udacity.com/course/cs387 (access date 27.02.2015).
7. MIT Open Courseware. URL: http://ocw.mit.edu/courses/find-by-topic (access date 27.02.2015).
8. Courses. URL: https://cseweb.ucsd.edu/~mihir/courses.html (access date 27.02.2015).
9. Information Security & Cryptography. URL: http://www.crypto.ethz.ch/teaching (access date 27.02.2015).
10. Cornell University. Computer Science. Introduction to Cryptography. URL: http://www.cs.cornell.edu/courses/cs4830/2010fa (access date 27.02.2015).
11. High School Mathematics Extensions. URL: http://en.wikibooks.org/ wiki/ High_School_Mathematics_Extensions/Discrete_Probability (access date 27.02.2015).
12. Cryptography. URL: http://en.wikibooks.org/wiki/Cryptography (access date 27.02.2015).
13. The Theory and Practice of Online Learning, 2nd ed. / ed. Anderson T. AU Press, 2008. 484 p.
14. Waldrop, M. Massive Open Online Courses, aka MOOCs, Transform Higher Education and Science. Scientific American. April 2013. URL: http://www.scientificamerican.com/ article.cfm?id=massive-open-online-courses-transform-higher-education-and-science (access date 27.02.2015).