UDC 681.3

Gajsha A.
Physics Department,
National University of Shipbuilding,
Prospekt Geroyv, 9, Mykolayv, 54025, Ukraine,
E-mail: physics2005@mail.ru

THE MENACES ANALYSIS OF THE DISTANCE EDUCATION PROCESS

The menaces of the distance education process are analyzed, described and classified. The recommendations to build strong and safe distance learning protection system are presented. The well-known methods to neutralize the menaces of view are analyzed and also there are short descriptions and references to proper author's works.

Keywords – distance education, E-learning, protection of information, information security, process menaces, piracy, biometry.

1. Introduction

The computer technologies have become a part of our everyday life. Mass availability of personal computers influences on different branches, particularly on education. It allows to realize new highly technological education methods such as E-Learning or distance education.

Distance education has many advantages that's why it becomes more and more popular. At the same time there are some problems that must be solved to get high quality of the distance learning process. The most complex one is the development of an appropriate protection system. Really there are some menaces to the distance learning process that follow.

2. The First Universal Menace – E-Learning Software Piracy

Firstly as the modern distance education is provided by personal computer software, there is a menace of its unauthorized using (software piracy). It is the universal menace to all commercial software so it is very important not only for E-learning branch but for all IT sector.

As it is adopted in information protection branch all protective measures are divided into three classes: legislative enactments, managerial procedures and program-technical actions. Unfortunately two first measures are not wealthy to solve such serious problem as piracy. That is why software developers have to use stronger protection systems. Taking into account this circumstance you can find many different protection systems to prevent unauthorized using. In spite of this most of them close down some one cracking method and do not take into account others. For example protection system controls entered by user serial number but does not control its own checksum. Of course malefactor changes some program code in low level (using disassembler and hex-editor) and cracks the program. Or sometimes protective system carefully controls its physical consistency, but has not appropriate mechanism to prevent installation of one legal (purchased) copy to many computers (what is of course unlawfully).

This situation is caused by the absence of appropriate software menaces classification. The task is insufficiently formalized and the developers do not take into account all the methods of cracking, and make the protection only from some of them. The author has developed such classification and has given recommendations to build strong protection systems [1]. Basing on those recommendations author has worked out universal software protection method [2]. Of course it may be used as the part of complex distance learning protection system.

3. The Menace of the Student Substitution

The next menace to the E-learning process is the student substitution. It means that exercises may do not a student but his agent (some competent person). At first sight this problem has no solution, as it is underlined in many sources (for example, in [3]). In reality there are some methods to recognize personal computer's user. Such systems could be built using some biometrical hardware devices (that is expensive and complex way but having high reliability level), and also it may be purely software product.

To most specialists' mind software biometry systems using is the most preferable to the mass education system. Really all the E-learning is based on the computer software using. The user continually must interact with the PC by input-output devices. So computer can gather the type and the characteristics of interaction that are more or less individual to the end user. Then PC compares collected data with the standard that was created in the trusted environment. It is the software behaviour biometrical systems that usually consider only keyboard characteristics (such as time intervals between two successive keystrokes). Author propose to take into consideration also mouse characteristics, such as cursor moving speed and acceleration, scrolling characteristics, typical mouse moves, etc.

Author's mathematical model of behaviour biometrical system was developed in [4]. This model was realized in program code for Microsoft Windows OS and uses Windows Hooks Mechanism.

4. The Menace of Works Results Falsification

This menace is characteristic for E-learning systems when the education is passed in asynchronous off-line mode. This means that correct answers are inbuilt into the software which is accessible to the user. Off-line education is suitable if you have no access to Internet. In off-line education systems user gradually executes his exercises and in his computer there is formed small results file. In the end of education period this file is sent to the educational institution where it is analyzed. Logically there is the menace of exercises execution results falsification. In results file there must be some record for every exercise, and student may falsify this record and get good results without tasks execution. Moreover student may give his results file to another one. Also he may copy record1 corresponding to executed work1 so as this copy of record1 signals that work2 also was executed (variety of falsification, basing on existing legal record).

Listed falsification menaces are very highly tailored that is why they were not covered in literature. To solve this specific problem it was developed special cryptographic protocol, that allows to make sure that remote subject has executed some tasks and gives real results of execution [5].

5. Conclusion

Distance learning is a perspective high-technological education method. Due to its complexity there are some menaces that may reduce E-learning process quality or involve commercial damages to educational institutions. To prevent that there must be used adequate protection system. It has to neutralize such general menaces: E-learning software piracy, student substitution, results forming system cracking (Fig.1). To neutralize each menace must be used separate subsystem and all of them will be encapsulated into one integrated distance education protection system.

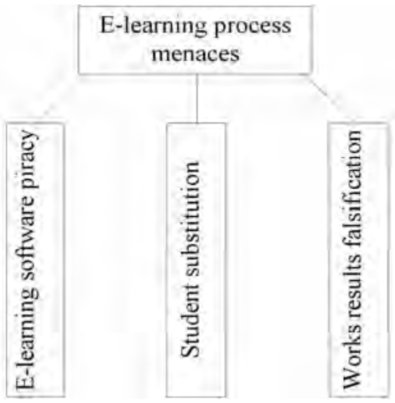
E-learning process menaces
E-learning software piracy
Student substitution
Works results falsification

Fig.1 Menaces tree.

References

[1] Гальчевський Ю.Л., Гайша О.О. «Логічні» та «фізичні» захисти програмного забезпечення від несанкціонованого копіювання // Захист інформації: Науково-технічний журнал. – 2005. - №2(23). - С.34-40.

[2] Мочалов О.О., Гайша О.О. Спосіб захисту програмного забезпечення від несанкціонованого використання. – Заявка на патент України № u 2006 04340 від 15 травня 2006 року.

[3] П.С. Ложников. Распознавание пользователей в системах дистанционного образования // Образовательные технологии и общество: Научно-педагогический журнал. – 2001. № 4(2). – С.211-216.

[4] Гайша О.О. Математичне моделювання методу біометричної поведінкової ідентифікації особи користувача персонального комп'ютера // Защита информации: Сборник научных трудов НАУ. – К.: НАУ, 2006. - С.3-6.

[5] Мочалов О.О., Гайша О.О. Проектування системи захисту програмного комплексу дистанційної освіти // Збірник наукових праць НУК. – Миколаїв: НУК, 2006. – № 2 (407). – С.149-156.