**Begalin A.Sh., senior teacher,**
*Kostanay state university named after A. Baitursynov*

## THE POSSIBILITIES OF CONSTRUCTING THE RELIABLE SYSTEMS BY THE MODERN COMPUTER THREATS

Well-known that it's impossible to create utterly reliable system of protection. We may overcome any protection by the enough time. That's why it can be said only about some sufficient level of security, providing with such level of protection, when the price of its overcome becomes more than the price of information received (reaching effect), or when in time of receiving information it depreciates so that the efforts on its receiving lose the meaning.

What do we need to protect and from what to be protect?

We need to protect all subjects of informational attitudes from possible financial and moral damage which can bring them casual or willful influence on computer system and information.

We should be protected from such undesirable influence as mistakes in actions of serving staff and users of system, mistakes in program security, willful actions of ill-natured people, refusal and breakdown of equipment, spontaneous disasters and crushes. Naturally it is on the base of reasonable analyses of risk. It needs to be prevented not only from non-sanctioned access to information with the aim to its opening or breaking its intact, but there are the attempts of penetration with the aim of infringement of capacity for work of these systems. We need to protect all components of systems: equipment, programs, data and staff.

One of the main aspects of problems of providing the security of computer systems is discover, analyses and classification of possible ways of realization of security's threats, that is possible channels of non-sanctioned access to the system with the aim of infringement its capacity for work or access to critical information and also evaluation of reality of realization of security's threats and causing the damage by the way.

We may prevent the introducing the program bookmarks only by the way of creating closed software environment in which must be excluded the possibility for usage the instrumental programs with the help of which can be implemented the adjustment of data and programs on media and memory.

The main mechanisms of universal threats to security implemented in the specific remedies which are: identification (naming and recognition), authentication (proof of identity) and authorization (assigning authority) subjects, control (concurrent) access to system resources, registration and analysis of events occurring in the system integrity monitoring system resources. Protection system should be constructed in the form of layered concentric rings of security (defense). Outermost ring of security is provided by moral and legal means (the inevitability of retribution for the act committed). The second security ring is represented by physical and organizational means – it is an external system protection (protection against natural disasters and external attacks). Internal protection (protection against false and willful misconduct of the personnel and legitimate users) is provided at the level of hardware and operating system, and represented by a line of defense, which excludes the possibility of outsiders to the system (identification and authentication mechanism), rings protect all system resources from unauthorized use (access





послуг з метою забезпечення єдності й сприятливих умов для розвитку та функціонування ринку фінансових послуг, з врахуванням інтересів споживачів цих послуг та вимог законодавства, що в цілому спрямовано на покращення інвестиційного клімату в країні.

Література:

1. Альошин В. Державне регулювання та нагляд в умовах консолідації діяльності фінансових установ [Текст] / В. Альошин // Фінансовий ринок України. – 2008. – №1(51).

2. Кришевич О. В. Господарське законодавство [Текст]: Навч.-метод. посіб. для самост. вивч. дисц. / О. В. Кришевич, В. В. Мачуський, О. В. Перепадя, В. Є. Постульга. – К.: КНЕУ,2005. – 182 с.

3. Мацелик М.О. Фінансове право [Текст]: навч. посіб. / М.О. Мацелик, Т.О. Мацелик, В.А.Пригоцький ; за ред. В.К. Шкарупи. – К.: Знання, 2011. – 815 с. – (Вища освіта XXI століття).

4. Унинець-Ходаківська В.П. Роль державного регулювання на ринку фінансових послуг [Текст] / В.П. Унинець-Ходаківська // Актуальні проблеми економіки. – 2009. – № 6(96).

**К. т. н. Тихонова О.Б., к. т. н. Русляков Д.В., к. т. н. Калашников А.А.**
*Институт сферы обслуживания и предпринимательства (филиал)*
*Донской государственный технический университет*
*(ИСОиП (филиал) ДГТУ)*

## ПРИМЕНЕНИЕ ВИРТУАЛЬНОГО ОБУЧАЮЩЕГО ТРЕНАЖЕРА В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ

Одной из важных и актуальных задач современного образования является подготовка конкурентоспособной личности. Решение этой задачи невозможно без помощи информационно-коммуникационных технологий. В последнее десятилетие отмечается активное внедрение компьютерных и телекоммуникационных технологий в образовательный процесс, при этом значение информационно-коммуникационных технологий быстро возрастает не только в сфере образования, но и в любой другой сфере деятельности. Новые подходы к решению важных проблем в методике обучения студентов невозможны без применения новых методов и средств, основанных на применении информационно-коммуникационных технологий [1]. Формирование компетентной развитой личности, способной принимать адекватные самостоятельные решения, имеющей желание посто-

3) створення сприятливих умов для розвитку та функціонування ринків фінансових послуг;

4) створення умов для ефективної мобілізації і розміщення фінансових ресурсів учасниками ринків фінансових послуг з урахуванням інтересів суспільства;

5) забезпечення рівних можливостей для доступу до ринків фінансових послуг та захисту прав їх учасників;

6) додержання учасниками ринків фінансових послуг вимог законодавства [3].

Державне регулювання ринку фінансових послуг здійснюється такими уповноваженими органами: щодо ринку банківських послуг – Національним Банком України; щодо ринків цінних паперів та похідних цінних паперів – Державною комісією з цінних паперів та фондового ринку (ДКЦПФР); щодо інших ринків фінансових послуг – Державною комісією з регулювання ринків фінансових послуг України.

В Україні система державного регулювання ринку фінансових послуг пройшла складний шлях становлення та розвитку. Оскільки кожний з ринків, що входить до складу вітчизняного ринку фінансових послуг, формувався як відокремлений елемент, то і становлення системи їх державного регулювання здійснювалося відокремлено.

Слід відмітити, що система державного регулювання ринку фінансових послуг має забезпечувати покращення інвестиційного середовища, захист інтересів споживачів фінансових послуг, справедливе ціноутворення, усунення системних ризиків, функціонування ринку фінансових послуг як механізму економічного розвитку.

На сьогодні сфера фінансових послуг потребує вдосконалення. На довгострокову перспективу в умовах загострення кризових процесів на світових фінансових ринках, а також враховуючи необхідність збереження ліквідності національних фінансової і банківської систем на рівні, здатному забезпечити конкурентоспроможність національної економіки України, держава як регулятор і кредитор останньої інстанції має оптимізувати свою діяльність за такими пріоритетними напрямами модернізації сфери фінансових послуг [4]:

- впровадження механізмів «інтегрованого нагляду» та уніфікація вимог і стандартів фінансової діяльності з метою гармонізації системи управління інститутами сфери фінансових послуг з міжнародними стандартами;

- впровадження систем ризик-орієнтованого нагляду на засадах індивідуального підходу до оцінки ризиків окремих учасників ринку або їхніх активів;

- вдосконалення систем фінансового моніторингу та розкриття інформації фінансових установ для їх клієнтів, а також вдосконалення системи розкриття інформації державних контролюючих установ для всіх учасників фінансового ринку;

- забезпечення високого ступеня інституційної спроможності регулюючих органів та ін.

**Висновки.** Узагальнюючи вищевикладене, під державним регулюванням ринку фінансових послуг України, на нашу думку, слід розуміти взаємопов'язану систему форм, методів та інструментів впливу на учасників ринку фінансових





control mechanism under the authority of the subject). Mechanisms for logging and integrity enhance the reliability of protection, allowing the detection of attempts to overcome other levels of protection and timely to take additional measures as well as to exclude the possibility of losing valuable data due to hardware malfunctions and failures (redundancy mechanisms for tracking transactions). And finally the last ring is represented by means of applied security protection and cryptography.

Experience creating protection systems reveals the following basic principles of computer systems security, which must be considered in their design and development :

systematic approach;

integrated solutions;

-A protection continuity;

-Reasonable sufficiency of security facilities;

-Simplicity and an openness of used mechanisms of protection;

-A minimum of inconveniences to users and a minimum of an overhead charge for functioning of mechanisms of protection.

Daily appear ten thousand new harmful programs and modifications of already existing viruses. Exponential character of growth of an amount of virus programs proceeded in 2010-2011. Thus already by the end of 2011 the total of harmful programs exceeded 15 million Average time of infection of the network unguarded computer makes today less than 20 minutes of Threat become more and more complex. Malicious code writing becomes recently more and more business oriented. Virus writers continue to show hyperactivity in search new in a popular software, first of all in Microsoft Office and Microsoft Windows. The problem of root kits a situation became aggravated becomes complicated that the majority of the anti-virus companies does not give till now proper attention to detection and treatment of the active root kits. Which steels the main source of propagation of spam, DDoS –attacks and mailings of new viruses actively develop. In process of development of systems of Internet banking the further development receive phishing – the Internet swindle type which purpose is success obtaining to confidential data of users – to logins and passwords, and pharming – automatic redirection of the user on the false web site when he tries to enter on the official web site of the financial or commercial organization.

Couple of years the subject of rigid control of access to the Internet on operation back was widely considered. There were many programs, restricting to employees access to the forbidden resources and reducing information leakage threat. Forbidden sites of type «My world», «Schoolmates», «In contact» – in them sit almost all is universal in working and a time off, using and other programs. In a word, social activity of employees grows, and to check, where target, and where no- purpose web access, very difficult. By data «Kaspersky's Laboratory», social network became the main target of attacks in 2012. Social networks contain the personal information which can be used, including malefactors.

References:

1. Millers Ю.Н., Methods and information security facilities.
2. Gajkovich V.Ju, Ershov Д.В. Bases of safety of information technologies., SPb! At ИТМО , 2009.-84 with
3. Log the Computer the Press 11. –M.2009.123 with
4. Log the Computer the Press 6. –M.2009.126 with
5. Log the Computer the Press 5. –M.2009.128 with
6. The environment of existence of viruses/ Red. Kaspersky's laboratory. – M, 2007. – the Access mode: <http://www.securelist.com>