book strong measures are needed. This includes governmental propaganda of reading especially among children and youth. Some of the steps that are being realized in Ukraine are:

– the annual Lesya Ukrainka contest of professional reciters;

– book trailers broadcast, which is the announcements of books using short video clips representing book's content through its bright and significant scenes. Such kinds of videos are created by publishers or the readers themselves to encourage others to read the book.

– book fairs. Ukraine is a frequent guest of international book fairs, it also holds book fairs on its territory.

– book popularization through media and advertisement. However, it must be noted that the number of advertising campaigns to support books and reading is extremely small.

– marketing techniques used by book sellers. It is also an effective way to stimulate readers' interest by sales, special and advantageous offers for regular readers.

In conclusion, it is worth mentioning that modern book publishing is going to face global-scale problems, which are the need to keep a steady reader demand for books, to resist the decreasing of book publishing volume, predicting the reader's request, stimulating the audience, motivating it to buy books. At the same time it is important to understand the modern reader personality. He is mobile, goal-oriented, searching, used to getting information almost immediately. He cannot be blamed for the lack of literacy and education, active stand in life, which largely results from reading books. He shows his interest in all new products. The appearance of e-readers is explained by their curiosity. That is why it is important for the publisher to predict audience demands, meet its needs. After all, it does not matter in what form the book exists: the man does not give up reading, he is just changing the information sources.

Scientific supervisor: Tereminko L.H.,
Senior Lecturer

UDC 004.056 (043.2)

Lugovets D.V.
National Aviation University, Kyiv

FRAUD TECHNOLOGIES OF CYBERCRIMINALS

As digital technology advances and more people rely on the Internet to store sensitive information, cybercrimes are becoming more and more of a threat to people across the world. Raising awareness about how information is protected and the tactics cybercriminals use is important in today's world.

Any cybercrime is generally defined as an offence committed against individuals or groups of individuals with a criminal motive to intentionally harm

the reputation of the victim or cause physical or mental harm, or loss, using modern telecommunication networks such as Internet (networks including but not limited to chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS). Computer fraud is considered to be any dishonest misrepresentation of a fact intended to let another person do or refrain from doing something which causes loss due to altering in an unauthorized way; destroying or suppressing output or deleting stored data. Other fraud forms, such as bank fraud, carding, identity theft, extortion, and theft of classified information may be facilitated using computer systems and target consumers and businesses.

Today much of personal information can be easily obtained online, especially on various social networks, where we can learn a person's profile, location and relocation with reference to time, income level, a focus of interests, etc., which is often used by employers, banks, marketing specialists, and, of course, fraudsters. This makes public Wi-Fi-networks particularly vulnerable to data interception and the first widespread way of personal data hacking. False hoc networks created by the fraudsters do not require data encryption and can easily allow important information to fall into wrong hands. The possible solution to this problem is to create the virtual private area network (VPN) to make the use of public Wi-Fi-networks much safer.

The second popular way of stealing confidential information is by cracking telephone conversation or Bluetooth/SMS/MMS transmission to get access to bank account. An effective problem prevention here is to avoid transmitting sensitive data via mobile phone services.

The third way is related to theft of biometric data, such as voice, face recognition, fingerprints and iris in order to steal someone's identity for financial theft, espionage or other crime. In present-day discussions about identity theft, reliability of biometrics receives a lot of attention because of possibilities for its covert use. Iris-based systems are considered to be far more accurate compared to face recognition ones and hand scans, which cannot provide a high level of security any more. The use of multi-modal systems that combine and verify biometric characteristics before access is granted, is a good solution to the problem of identity theft.

Another way to obtain confidential information is through a variety of fraudulent services and programs such as Trojans: programs blockers, banking "Trojans", fake online stores and services, which allow the intruder to gain easy access to the computer system. A difficult password and a special virtual card for internet payments can serve as a protection against this kind of hacking.

A special way to steal personal information can be theft of a sim-card being made to bypass two-factor authentification used in many online services from instant messaging to online banking. To prevent such a theft users are recommended not to publish their sim-card numbers anywhere on the Internet and use a separate sim-card for online services. Re-registration of the sim-card to someone else's name can also be a way of fraud and result in financial losses.

Since many people today have various gadgets, it is possible to identify individual devices which are most often exposed to hacking. These vulnerable to security devices are smartphones, PCs, navigators, webcams and video nurses, cloud storage services, network printers, and game consoles. Special antivirus protection, regular software update, and complete rejection of the unlicensed digital products can secure electronic gadgets.

Passport data, payment details, pin codes of credit cards, and passwords to different services have been defined as the most hunted information for fraudsters. The most effective way to protect personal data is by creating a password-protected data archive or crypto container; cloud data encryption as well as full disk encryption.

It can be concluded, that anybody who uses the Internet for any reason can easily become a victim, which is why it is very important to raise people's awareness of possible protection while online.

Scientific supervisor: Shulga T.V.,
Senior Lecturer

UDC 005/96:378 (043.2)

Lutsenko M.S.
National Aviation University, Kyiv

LOGISTICS IN UKRAINE: WIDESPREAD PROBLEMS IN PERSONNEL TRAINING

Nowadays logistics becomes rather popular in business market service. But, unfortunately our country loses workers with a great potential and skills.

Logistics business develops rapidly, it dictates its demands in the labour market, but, unfortunately it doesn't receive a due response. Qualified specialists are the basis of the successful performance of all economical sectors. Nowadays representatives of the logistics business notice a professional staff shortage in logistics and supply chain management. Logistics market is losing high qualified professionals because of the economical instability in Ukraine.

According to statistics there are 25% of personnel that have an educational certificate in the field of logistics, 65% has economical education, not connected with shipments, 7% has humanitarian education and finally 3 % doesn't have high education at all. Logisticians have to get knowledge about functional supply area, manufacturing and distribution and be ready to extract all the problems and misunderstandings in logistics.

The origin of logistics professional problems hides in education. Basics of logistics are only taught an universities when the theory must be supported by