Current Issues in Education as Pertaining to the Realm of E-Commerce Legal Protection

Konev S.I., Kulagin A.S., Morozov N.V.
Department of General Jurisprudence
And Legal Framework for Safety Provisions
National Research Nuclear University MEPhI
(Moscow Engineering Physics Institute)
Moscow, Russia
{SIKonev, ASKulagin, NVMorozov}@mephi.ru

Levakin I.V.
Department of Legal Framework
for Management Practice
MGIMO (U)
of the Russian Ministry of Foreign Affairs
levakin@ya.ru

ABSTRACT

The authors analyze some major problems of developing competent human resources, first of all legal experts, in the electronic commerce (e-commerce) legal protection sphere. To date, the educative process has been evolving mainly around technically- or economically-oriented academic programmes; however, in actual practice there is a strong demand for an integrative approach to education that implies the acquisition of comprehensive knowledge including legal knowledge among others. Starting out from such courses already having been taught by NRNU MEPhI for years as "Technical aspects of information security", "Legal regulation of e-document flow and making use of digital signatures" as well as several others, the authors suggest that such kind of a comprehensive approach be applied to the specialist training in the sphere of e-commerce legal protection.

Keywords: e-commerce, digiatlsignature, e-document flow, protection of personal data, education, specialist training.

I. INTRODUCTION

One of the key tasks within the modern educational system is the manpower training with due account for both current and anticipated demands arising from the labor market. A vivid example of setting up a problem in such a manner is an educative process applicable to the e-commerce legal protection area. The overall performance of any electronic commerce system undoubtedly relies on a multifaceted integrative approach to that system's security enforcement. Obviously, legal protection alone is incapable of physically confronting, say, computer program hacks or any other adverse technical effects. But the law, taken as a whole, does possess all means and mechanisms that are necessary for enabling preventive legal arrangements, settlement and legalization of advance developments in the sphere of e-commerce legal protection, and enforcement of legal remedies in the event of any infringements, to name a few.

When working on this article, the authors based themselves on e-commerce market surveys and the corresponding skill requirements, as well as on their own expertise in teaching students. The general concept is expounded in Section 1. The authors' own experience in training professionals with the activity profile under consideration is reviewed in Section 3. Conclusions are presented in Section 4.

II. RELATED WORKS

Advanced telecommunication technologies designed for commercial purposes require some kind of protection, in particular, by means of legal arrangements. Electronic commerce and electronic banking have become an integral part of the contemporary economic system (Fig. 1) [1].

Top 10 E-commerce countries in turnover (EUR billion)					
1	China	405 €	6	France	57 €
2	USA	363 €	7	Canada	21 €
3	UK	127 €	8	Russia	18 €
4	Japan	102 €	9	S. Korea	17 €
5	Germany	71 €	10	Australia	16 €

Fig. 1. Top 10 E-commerce countries in turnover.

A fair number of informative international publications deal with the research of e-commerce legal protection problems based on the above-mentioned integrative approach. They include such articles as *Accountable mobile E-commerce scheme via identity-based plaintext-checkable encryption* [2], *The effects of E-commerce on the demand for commercial real estate* [3], *E-commerce trends and impacts across Europe* [4] et al. At the same time, little attention has been paid so far to this subject in Russian scientific literature. It is noteworthy that exactly the integrative approach, i.e. the one comprising legal, technical, information analysis and other aspects, is missing there.

Russia is in the top-ten list of advanced countries worldwide in terms of e-commerce volumes, but by no means is it playing a leading part among them – "just" EUR18 billion per annum. Even so, statistics data show a tangible progress achieved in

recent years, and one may forecast with certainty that this phenomenon will continue demonstrating rapid growth in Russia (Fig. 2) [5].

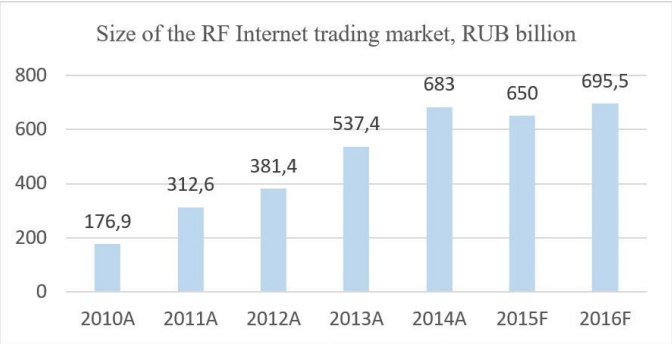


Fig. 2. Size of the RF Internet trading market, RUB billion.

The purpose of this article is to analyze the skill formation problems existing in the field of e-commerce legal protection, first of all, regarding the professional training of legal experts. To achieve this, the authors took as a basis their personal experience as well as the following educational courses developed by the NRNU MEPhI Department of General Jurisprudence and Legal Framework for Safety Provisions: "Information network security architecture", "Information law", "Legal framework for information security", "Technical aspects of information security", and "Legal regulation of e-document flow and making use of digital signatures".

The authors adhere to a definition, pursuant to which e-commerce is a set of relationships arising in connection with doing business on the information and telecommunications network Internet.

In Russia the specialist training efforts in the sphere under consideration are governed by the "Information Society Development Strategy for the Russian Federation" approved by Decree of the President of Russia of 07.02.2008 No.Pr-212. To date, the educative process has been evolving mainly around technically- or economically-oriented academic programs. At the same time, there is demand for an integrative approach to education, which implies the acquisition of comprehensive knowledge including legal knowledge among others. It is essential to build up competences that are necessary for a modern type of a trained professional. In particular, such professional has to:

- know the fundamental principles of the national and international legislation in the information sphere; specifics of parties to a legal relationship within this sphere; norms of responsibility for any wrongdoings with respect to the information and/or information technology circulation;

- know content search and analysis technologies being widely used on the Internet;

- have a good command of the legal groundwork methodology for information security;

- possess necessary knowledge and skills related to e-document system management;

- be able to conduct researches of product assortment, marketability, and the consumer online audience;

- be able to knowledgeably interpret provisions of the law of torts with respect to information, information markets and e-commerce issues.

Teaching the e-commerce legal protection course is essentially performed following just general approaches, while the special-purpose legal regulation issue usually steps in just on a case-by-case basis. Moreover, the legal framework supporting e-commerce is still in the process of taking shape. The main enabling factors here are the development of information technologies along with any precedents emerging in this sphere. Problems in teaching the e-commerce legal protection topic are normally solved taking into account experience accumulated by leading Russian higher education institutions during the development and delivery by them of general and ad hoc courses.

Some of those institutions are:

- NRU HSE (National Research University "Higher School of Economics"). Within its curriculum there is a course "Management in the sphere of electronic business and Internet projects" aimed at training professionals who are supposed to have the skill and knowledge sufficient for implementing their own Internet projects or on-line representations of businesses;

- RANEPA (The Russian Presidential Academy of National Economy and Public Administration). One of the programs in its curriculum is "Electronic business" with an empiric course teaching trainees how to integrate the capabilities of web-based technologies into marketing and strategy of legal entities;

- Instituto Internacional de Marketing (with branches in Spain and several other countries in Europe and Latin America). Its approach allows building up a system of knowledge on technical features of e-commerce and on strategies and platforms needed for the successful e-commerce implementation at small businesses.

Each of these institutions develops competences according to applicable regulatory requirements, corporate inquiries, etc.

III. ANALYSIS OF OWN EXPERIENCE IN TRAINING PROFESSIONALS

Education in the field of e-commerce protection calls for due consideration of certain challenges that are briefly overviewed in this section.

In a modern society, a concept of "document" has undergone some changes. Actually, the very term "electronic document" is virtually a fiction, at least because of the fact that an electronic document, as distinct from a paper medium (aka "hard copy"), cannot be perceived by us directly. When we print it out or display on a computer monitor, we are dealing with its analog representation rather than with the entity dubbed "electronic document" itself. Besides, electronic documents are separable from their media.

It is noteworthy that demand for the use of electronic documents grows from day to day. This process naturally

shows up in the legal environment. The Russian Federation, like many other countries, has to develop and clarify the dedicated legislation oriented towards the use of electronic documents in the public management as well as e-commerce and banking domains. Therefore, during the establishment of the appropriate education system all these particularities should be taken into consideration [6].

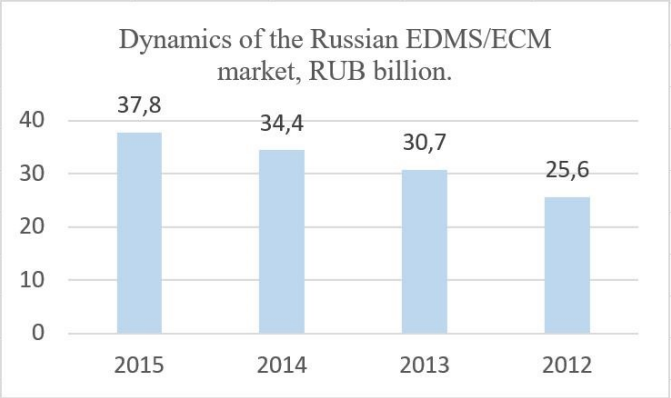


Fig. 3. Dynamics of the Russian EDMS/ECM (Electronic Document Management System / Enterprise Content Management) market, RUB billion.

When it comes to training a legal expert capable of independently implementing and operating electronic document management systems, it is necessary to lay emphasis on the principle of identity, i.e., maximum consistency with common document management techniques. Otherwise, these two systems will be permanently in conflict with each other thus producing a negative impact on their functioning. In the process of education one has also to take care of such issues as the identification of an electronic message author(s), checking and maintaining the message fidelity, assignment of persons responsible for signing electronic documents and obtaining required approvals, establishment of procedures for generating and storing digital signature keys.

Training legal experts must rest upon up-to-date laws in the sphere of e-commerce protection. For example, the law on digital signatures in the Russian Federation (Federal Law of 06.04.2011 No. 63-FZ) has been in effect since 2011.

Legally enforceable procedural enactments treat electronic documents and traditional hard-copy documents as being of equal legal validity. To ensure it, a digital signature technique is employed nowadays. In fact, it means an encryption item, or a ciphered code (a sequence of symbols), attached to an electronic document and allowing to ascertain the fidelity of this document's text, and, where appropriate, also identify a person who created the signature (the signer).

It should be taken into account that the lawmaker has chosen to minimize the equivalence requirements, which undoubtedly will produce some beneficial facilitating effects in practice.

The Russian legislation distinguishes the following kinds of digital signatures: simple and strengthened, while the latter can be subdivided into qualified and unqualified types. A message with a simple or unqualified digital signature can be actually considered as an analogue of a common traditional document, provided the counterparties have preliminary agreed so. A strengthened qualified digital signature needs to be confirmed with a certificate issued by a duly accredited certifying center; in any case, it is equated with a paper document indorsed by one's own hand.

Training professionals in the field of e-commerce legal protection includes not only legal aspects of digital signature, but also its cryptographic foundation. The corresponding range of problems is exhaustively covered in a discipline "Legal regulation of e-document flow and making use of digital signatures". It is important to realize that in a technical sense the digital signature mechanism is based on an irreversible ("hard-to-revert") mathematical function: while the direct computation is a sufficiently trivial task, the reversal operation, on the contrary, is practically impossible.

One of such functions is (1):

$$F(x)=ax \pmod p \quad (1)$$

Several digital signature generation algorithms are built upon it: DSA, ElGamal cryptosystem, Diffie-Hellman Key Exchange algorithm, and some others.

The students have to master fundamentals of the mechanism of generating and validating digital signatures offered by ElGamal (this algorithm is cheaper as soon as it is not patented and does not require any licensing fees, unlike the Diffie-Hellman method) (Fig. 4).

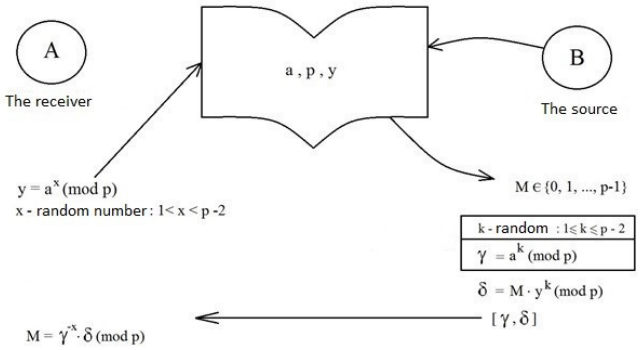


Fig. 4. Diffie-Hellman scheme.

At the first stage of the ElGamal algorithm two encrypting keys (public and private) are generated. This stage consists of the following actions:

- Generate a random n-bit long prime number p.
- Choose a random integer number (generator, or primitive root): a modulo p.
- Choose a random integer x from interval (1,p), coprime with p-1.
- Compute (2):

$$y = ax \pmod p \quad (2)$$

- The public key is (a, p, y); the private key is x.

The second stage includes encryption.

A message M is encrypted as follows:

- Choose a random secret number k, coprime with p − 1.
- Compute (3):

$$\gamma = ak \pmod p,$$

$$\delta = M * yk \pmod p, \quad (3)$$

where M is the original message. A pair of numbers (γ, δ) is a resulting ciphered text.

From a legal viewpoint, the students are actually dealing with a presumption: we assume that the private key of the signature is sufficiently cryptosecure (i.e., not computable analytically), which guarantees us the secured exchange of legally valuable electronic documents.

While developing the curriculum, one has to make provision of the fact that the national legislation does not specify in sufficient detail the electronic data interchange (EDI) issue in terms of the optimum relationship between the norms of administrative, civil and other branches of law. Thus, some criteria have to be developed to ensure compliance with a mandatory written form supporting the use of electronic documents.

Yet another open issue relative to the organization of a teaching process in the field of e-commerce legal protection is the Internet-related jurisdiction legislation. In Russia the competence of courts as regards the litigation proceeding with respect to disputes under civil law is determined by the civil procedural legislation (Civil Procedural Code of the Russian Federation), arbitration procedural legislation (Arbitration Procedural Code of the Russian Federation), and administrative procedural legislation (Code of Administrative Court Procedure of the Russian Federation). In order fora court to be considered competent, it is necessary to observe the applicable jurisdiction rules.

One should realize in the context of teaching disciplines within the e-commerce legal protection realm that the probability of having a foreign person as defendant is very high due to the transboundary nature of the Internet itself and transactions effected therein. The national law admits a wide range of discretion of contractual parties through their choice of a competent court: they are free to choose a judicial body either in Russia or abroad. Moreover, contracts normally concluded in the e-commerce sphere often contain prorogation agreements in favor of a foreign court. Norms of international law, in particular, the EC Regulation on the law applicable to contractual obligations (the Rome I Regulation of June 17, 2008 No. 593/2008) [7], contain a set of peremptory consumer protection rules. A consumer is automatically deemed to be a weaker party and thus subject to protection against the aggressive obtrusion by an entrepreneur of contractual terms and conditions meant for the benefit of that entrepreneur. These issues are comprehensively investigated and taught within the "Information law" course.

A whole bunch of problems to be addressed within the curriculum deals with maintaining confidentiality of online personal data. Any on-line shop or other type of consumer-centric web resource is inevitably engaged, one way or another, in handling information that can be used to identify a specific person. It can be the user's login and password, email address, photo, bank account or credit card numbers, as well as other private data specified by that user during her online registration or placing an order.

By means of employing modern information processing techniques, we can get a reasonably precise picture of each user's interests and preferences in reliance just on her search queries and kind of information that is stipulated as "publicly available" by the law "On information, information technologies and information security".

On the one hand, it helps develop necessary skills and teach efficient methods of selling goods or services and bringing in new clients. On the other hand, none of personal data subjects is going to be happy due to the awareness of the fact that somebody is collecting her financial solvency and soundness data, if only with benevolent intentions.

It is evident that such an approach to employing e-commerce capabilities in many cases will result in affecting an individual's privacy. Besides, the very structure of personal data is not yet clearly specified: there are no distinct criteria that could be applied in order to classify with certainty various pieces of information as personal data. The same data can be often assigned to the information category assuming data with restricted access. All that leads to the expansion in the number of complaints on the part of physical persons. Statistics collected by Roscomnadzor (Federal Supervision Agency for Information Technologies and Communications) gives a self-explanatory visual representation of the situation (Fig. 5) [8]:

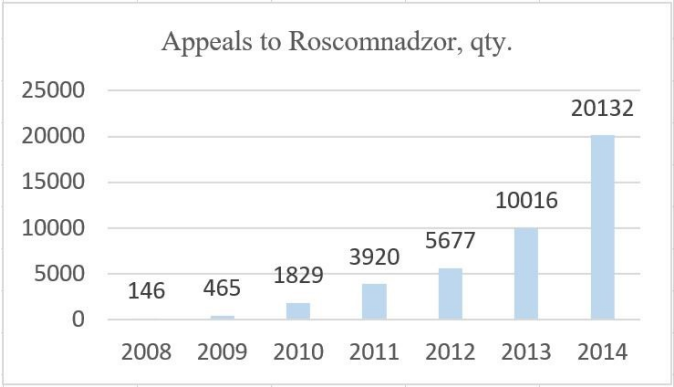


Fig. 5. Appeals to Roscomnadzor.

No wonder people tend to minimize their private data that are going to appear online, which apparently does no good to the popularity of electronic transactions. This range of problems is thoroughly investigated by future professionals within the confines of such classroom disciplines as "Information network security architecture" and "Technical aspects of information security".

NRNU MEPhI, being at the top among higher education establishments of Russia, for a long time has been providing the comprehensive training of its students in this sphere. A number of disciplines having been implemented by the Department of General Jurisprudence and Legal Framework for Safety Provisions since 2002 let the graduates be perfectly

competitive in the labor market. The list of those disciplines includes:

- Information network security architecture;
- Information law;
- Legal framework for information security;
- Technical aspects of information security;
- Legal regulation of e-document flow and making use of digital signatures.

The students acquire integrated knowledge pertaining to the legal regulation of information-driven relationships, including the following domain-specific topics:

- protection of data with restricted access;
- safety of business entities;
- information circulation across the Internet and related security matters;
- legal aspects of operating automated information systems;
- legal aspects of document flow organization and management.

Throughout the whole period of implementing the above-mentioned disciplines, they were studied by more than 300 students. On completing the studies, all the graduates were able to put their knowledge into practice at private businesses as well as in the system of state agencies exerting regulatory treatment and control over the e-commerce sphere.

The content of some disciplines has undergone substantial changes since the time these disciplines were first introduced. It mainly occurred due to the changing legislation. Furthermore, other new challenges came in lately. Thus, for instance, at present a work is being performed on establishing interaction between international payment systems and the national payment system of Russia. Some doctrinal approaches to this legal problem are under development.

The practical experience in implementing some courses at issue has shown that their separate learning, i.e., not in connection with the general educational system, does not allow us to perform the skill formation as effectively as we would like to. The carrying-out of academic programmes with the assistance of qualified specialists in the fields of jurisprudence, management, system analysis, computer networks and others will facilitate a solution to the problem of shaping target competencies of future e-commerce experts. Only a task-oriented interdisciplinary approach to studying all disciplines within a holistic curriculum is actually called for in the contemporary world.

IV. CONCLUSION

It is fair to say that education in the sphere of e-commerce legal protection is global in nature and assumes the acquisition of comprehensive knowledge including legal methods, technical legal means and, most notably, technological tools. Therefore, it is quite within reason to suggest that particular attention should be paid to the e-commerce protection issues within a special course on e-commerce fundamentals for students enrolled in Bachelor's degree and specialist programmes.

It is essential to implement courses on legal regulation of e-commerce not just for students of law, but also for professionals in the field of information security and management.

One of the most important focus areas, as far as the further educational activity in the sphere of e-commerce legal support is concerned, should be the development of corresponding Master's degree programmes. The theoretical elaboration and practical implementation of the "Legal framework for e-commerce" Master's degree programme based on available experience will make it possible to perform more efficiently the training of personnel for both private and government sectors. It is proposed to use a task-oriented interdisciplinary approach upon studying all disciplines of the programme, which is predetermined by the discipline specifics. This also implies the students' recourse to certain corresponding matters within other disciplines, such as:

- Hardware and software information security facilities;
- Administration and programming of secured networks;
- Integrated information security system for enterprises;
- Organizational protection of information;
- Legal protection of information;
- Computer virology.

The availability of specialty courses on legal regulation of e-commerce within the Bachelor's degree, specialist and ad hoc Master's degree programmes in linkage with the Jurisprudence academic curriculum will contribute to meeting the growing demand for professionally trained labor force in the sphere under consideration.

REFERENCES

[1] European B2C E-commerce Report 2015. URL: http://www.ecommerce-europe.eu/website/documents/-b2c-ecommerce-europe-report-2015-light99gsuy-q7887q-sdq9qdhqd9qdjaknlaknx (access date: 29.03.16)

[2] Danlei Zhang, Pengyu Zhu, Yanmei Ye. The effects of E-commerce on the demand for commercial real estate. Cities, Volume 51, January 2016, Pages 106-120

[3] Martin Falk, Eva Hagsten. E-commerce trends and impacts across Europe. International Journal of Production Economics, Volume 170, Part A, December 2015, Pages 357-369

[4] Jinguang Han, Ye Yang, Xinyi Huang, Tsz Hon Yuen, Jiguo Li, Jie Cao. Accountable mobile E-commerce scheme via identity-based plaintext-checkable encryption. Information Sciences, Volume 345, 1 June 2016, Pages 143-155

[5] J'son&PartnersConsulting. Besplatnye obzory rynkov. URL: http://www.json.ru/poleznye_materialy/free_market_watches/ (access date: 29.03.16) (In Russian)

[6] Gosudarstvo. Biznes. IT. Rynok SJeD v RF. URL: http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A1%D0%AD%D0%94_%28%D1%80%D1%8B%D0%BD%D0%BE%D0%BA_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8%29 (access date: 29.03.16) (In Russian)

[7] Biznes i vlast'. Reglament № 593/2008 Evropejskogo parlamenta i Soveta Evropejskogo Sojuza "O prave, podlezhashhem primeneniju k dogovornym objazatel'stvam ("Rim I"). URL: https://www.lawmix.ru/abrolaw/2988 (access date: 29.03.16) (In Russian)

[8] Otchety o dejatel'nosti Upolnomochennogo organa po zashhite prav subjektov personal'nyh dannyh. URL: http://rkn.gov.ru/personal-data/reports/ (access date: 29.03.16) (In Russian)