Abstract—One of the adverse and undesirable impacts of ICT-rich environment is negative deviant behavior of an individual. The urgency of the problem is determined by: the lack of theoretical and methodological elaboration of the foundations in the teaching staff training; the necessity of improving professional and academic qualifications in the field; the increasing needs of science and education in teacher-researchers, who have sustained competence in information security sphere, universal qualities that meet the humanistic ideals of the Information Society development; the lack of attention to psychological and educational problems of information security in the spectrum of scientific research of psychological and pedagogical schools. The article deals with the solution to the problem of information security in the sphere of science, education and high technologies through special training of pedagogical staff that is competent not only in software and technical fields but also in the field of humanitarian aspects of information security.

Keywords: competence approach, information security.

I. INTRODUCTION

The necessity of competence forming in the sphere of individual information security is the reflection of scientific technical development, changes of human being sendsand his activity in nature, society and culture in the conditions of information society and globalization [3].

In this regard it is important for our research to consider the international experience of studying the requirements to competence formation in the sphere of individual information security.

About 70% of problems concerning ICT competence formation, from positions of ensuring competence formation in the sphere of information security, are considered in the document: “Structure of ICT competence of teachers. Recommendations of UNESCO” [1].

So, according the Recommendations [1], a teacher must be able to solve problems of secure use of the Internet and to train pupils to solve the problems.

II. DESCRIPTORS OF COMPETENCE

The document gives examples of methods of training: “To discuss such questions as cyber bullying, suitability and applicability of information for e-mail sending, internet grabbing, forums, problems of privacy and piracy, viruses, fraud, spam, pop-up windows, cookies, intellectual property rights, indecent content, digital citizenship, e-mail etiquette, netiquette, legislation requirements, protection of personal data and passwords problems.

It is suggested that participants should develop the corresponding approaches for studying the mentioned questions and procedures for increasing security on the Internet".
In the UNESCO project "Digital Future. The Catalog of Media-and Information Literacy Skills" [2] requirements to key skills of a competent use of different forms of information are submitted within comprehensive and system approach to the concept of media and information literacy.

According to the content of the given document [2] we can state that the notion which the foreign colleagues called "literacy" may be treated as the notion «competence» which defines requirements to individual activity in the conditions of information society within 8 thematic areas and corresponding problem fields (questions) among which the following three thematic fields define requirements to competences in the sphere of information security:

1. Ethics and values in information and media environment:
   - Communication and media as a subject of the ethical analysis.
   - Ethical problems in the contents of mass information and communication.
   - Ethical problems in communication via mass media.
   - Rules of law in mass media and communication.
2. The law in information and media environment:
   - Types, sources and legal procedures in the context of mass media.
   - Mass media and human rights of a citizen and a child.
   - Exclusive rights and intellectual monopolies.
   - The law on telecommunication.
   - The Law on mass media and public media.
   - Rights of the disabled.
   - Data protection.
3. Security in information and media environment:
   - Protection of personal information and reputation.
   - Anonymity.
   - Secure communication in business.
   - Supervision of the Web.
   - Mass media addictiveness and hygiene when using media.

Descriptors are presented by levels of formal education and lifelong learning.

Table. 1 shows the requirements at the level of "higher education" and the appendix contains requirements on the level of "lifelong learning".

<table>
<thead>
<tr>
<th>Question</th>
<th>Descriptors of the “higher education” level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security in the information and media environment</td>
<td></td>
</tr>
<tr>
<td>- Protection of personal information and reputation.</td>
<td>Students know methods and means of privacy protection. They read and understand the terms and conditions on the web pages, and make a conscious decision to accept these terms or refuse them</td>
</tr>
<tr>
<td>- Anonymity.</td>
<td>Students take considered anonymous decisions in a variety of communicative situations, for example, they sometimes intentionally deactivate the location services in their browser.</td>
</tr>
<tr>
<td>- Secure communication in business.</td>
<td>Students use intelligently means of increasing security of communication. Students are familiar with such means of encryption as PGP / GPG, OTR, and know how to use them.</td>
</tr>
<tr>
<td>- Supervision of the Web.</td>
<td>Students use tools that make supervision difficult. Students consciously select tools for specific purposes, taking into account the possibility that the situation of the communication or content items can be observed by the third party.</td>
</tr>
<tr>
<td>- Mass media addictiveness and hygiene when using media.</td>
<td>Students know how to respond to a negative style of communication, for example, may call the professional help. Students understand the connection between their actions in the media and other aspects of their life; they are able to manage this interrelation.</td>
</tr>
<tr>
<td>Rules of law in the information and media environment</td>
<td></td>
</tr>
<tr>
<td>- Mass media and human rights of a citizen and a child.</td>
<td>Students know how to use the media to defend their rights and the rights of the others publicly.</td>
</tr>
<tr>
<td>- Data protection</td>
<td>Students understand company privacy policy which services they use. They know how to apply the principles of data protection in respect of their publications and services. They know how to send an inquiry to the data protection service for intervention or explanation of the rules. They know how to check their data collected by different service providers or agencies. They know how to register a database and to check whether a particular database is registered.</td>
</tr>
</tbody>
</table>

Thus, in the conditions of the global information society development, the level of importance and urgency of the information security problem increases [4-7].

The problem of improving the system of personnel training in the field of information security is among priorities. Together with the training of information security specialists, an important role is played by the competence formation in the field of information security at the graduates of various profiles, including teachers.

In 201, the draft of the professional teacher standard was discussed and elaborated. It was based on social demands and requirements to graduates' competences of "Pedagogical Education" direction of training. As a part of professional pedagogical ICT competence the following components are defined:

- The use of techniques and following the rules of start, pause, continue and complete the work with ICT
tools, troubleshooting, maintenance of consumables, ergonomics, safety precautions and other issues included into the study of ICT in primary schools;
- following the ethical and legal norms of the use of ICT (including inadmissibility of unauthorized use and imposition of information).

The mentioned draft of the professional standard reflects social requirements and requirements of the professional environment for competences of information security sphere.

These competences as part of professional competence are wider than the corresponding Federal State Educational Standards of Higher Education.

The Federal State Educational Standards formulates General Cultural (GC) competence - 12 more as an element of ideological culture, "the ability to understand the nature and significance of information in the development of modern information society, the ability to be aware of the dangers and threats that arise in the process, the ability to observe the basic requirements of information security, including protection of state secrets" [1].

### III. METHODS FOR ESTABLISHING THE REQUIREMENTS FOR EDUCATIONAL OUTCOMES

The considered requirements allowed forming the "core" of the competence in the sphere of information security which must be based on the conventional system representation of the phenomenon "information security" irrespectively of the students' direction-training. It offers a selection of the following information security levels: standard and legal, organizational, procedural, software and hardware (Figure 1, Table 2), as well as the structure of the competence in the information security sphere of the future teacher.

![Fig. 1. Structure of competence of sphere of information security for graduates of the Pedagogical education direction](image)

According to the conducted research, the marked-out competences cover levels of information security in different share components.

According to the expert assessment, in the considered educational programs of "Pedagogical education" preparation in different profiles, the disciplines which should provide the competence forming are not always corresponded to requirements of educational process regarding to cumulative result formation – the competence in information security sphere.

Tab. 3 illustrates this fact on the example of students’ competences of information security sphere. The students are trained for "Pedagogical Education" on the Informatics profile.

<table>
<thead>
<tr>
<th>TABLE 2. FEATURES OF INFORMATION SECURITY LEVELS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security Level</td>
</tr>
<tr>
<td>-----------------------------</td>
</tr>
<tr>
<td>Standard and legal</td>
</tr>
<tr>
<td>Organizational</td>
</tr>
<tr>
<td>Procedural</td>
</tr>
<tr>
<td>Software and hardware</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TABLE 3. INFORMATION SECURITY LEVELS IN THE STRUCTURE OF COMPETENCE OF INFORMATION SECURITY SPHERE OF &quot;PEDAGOGICAL EDUCATION&quot; DIRECTION OF PREPARATION, THE INFORMATICS AND MATHEMATICS PROFILE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Competence of Information Security Sphere</td>
</tr>
<tr>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>General Cultural Special (GCS) competence-1</td>
</tr>
<tr>
<td>Organizational (15%)</td>
</tr>
<tr>
<td>Procedural (35%)</td>
</tr>
<tr>
<td>Software and hardware</td>
</tr>
</tbody>
</table>

305
Thus, as the table shows, according to the expert’s assessment the greatest attention must be paid to the procedural level of information security. At the same time the providing disciplines don't cover all problem areas while forming the competences.

Taking into account the table data, there was a decision on thematic updating and correcting the content of information security topics in separate disciplines and including some special courses.

IV. DEVELOPMENT OF A SPECIAL COURSE

In this regard a special course of "Information Security in System of Open Education" for "Pedagogical education" training was by E.V. Chernova, G. N. Chusavitina in NMSTU. The special course consists of three modules:

1. Undesirable content (topics: "Undesirable Content", "Access Restrictions to Undesirable Content").


3. Information security of an individual in the ICT-rich environment (topics: "Information and Psychological Security", "Information Culture", "Information Security Enforcement in Educational Institution").

The stated modules and their topics content compensate the revealed defects in competence formation of information security sphere of future teachers.

Technological features of design and implementation of the considered course are:
- the use of module technology when developing the structure allows to make updating by allotting the variable and invariant parts of modules in time;
- The application of the modern educational technologies which are based on interactive methods and forms of training (problem lectures, business game, etc.);
- The focus of the special course on the future professional activity was provided by the application of contextual training technology.

V. RESULT AND DISCUSSION

The practice and the analysis of works by P. S. LomasΧ, T. A. Mal'ykh, E. V. Chernova (Zerkina), G. N. Chusavitina, etc. [8-20, etc.] on elaboration of methodical systems which provide competence formation of information security sphere of future teachers who are trained in the Pedagogical education direction shows that they can be practiced both within one discipline, such as "Methods and means of information protection", and within separate topics of disciplines, such as: "Law Studies", "Information technologies in Education", "Informatics", etc.

In both cases at a design stage it is necessary to provide consistency and coordination of future teachers’ training in the sphere of information security and their general information and law preparation.

Integration and interrelation with allied subjects of the general information and law preparation, elimination of redundancy and duplication of contents.
and so forth can be carried out by detailed study of the
competence passport.

References