Технологии 2004

Информационно-телекоммуникационные технологии

INFORMATION AND BANK SYSTEMS CORRESPONDENTS AUTHENTICATION BASED ON VIRTUAL IDENTIFIERS SHAPING

Kotenko V.V., Rumjantsev K.E., Polikarpov S.V., Levendyan I.B.
Taganrog State University of Radioengineering, Taganrog

Fast progressing development of information and computer technologies opens a new qualitative level of possibilities for the further bank system. Unfortunately, these possibilities implementation efficiency today collides with a lot of problems which threatens operation of the bank system. Main of these problems is bank information authentication quality lowering at magnification of computer technologies part during its handling. The argument for this is constant growth of the system correspondents identifier unauthorized access threats that recently appears. The situation is complicated that existing approaches to authentication problem realization are not capable to provide given problem decision..

Carried out authors researches in the field of practical implementation of absolute undeciphering capability conditions show, that the given problem may be solved by using the approach consisting in virtualization of identifiers bands sample spaces. It is supposed, that the bank system uses 2 sorts of identifiers: virtual and working. Virtual identifiers are for correspondents and are formed by them. A feature of the prospective approach is that sample spaces of virtual identifier bands X* is continuous, therefore its infinite entropy (H [X *] = ∞ is ensured for the unauthorized user. Passage from the continuous form of identifiers sample space to the discrete form, mandatory in the bank system, is carried out by using of the authentication program complex developed and patented by authors (fig. 1)

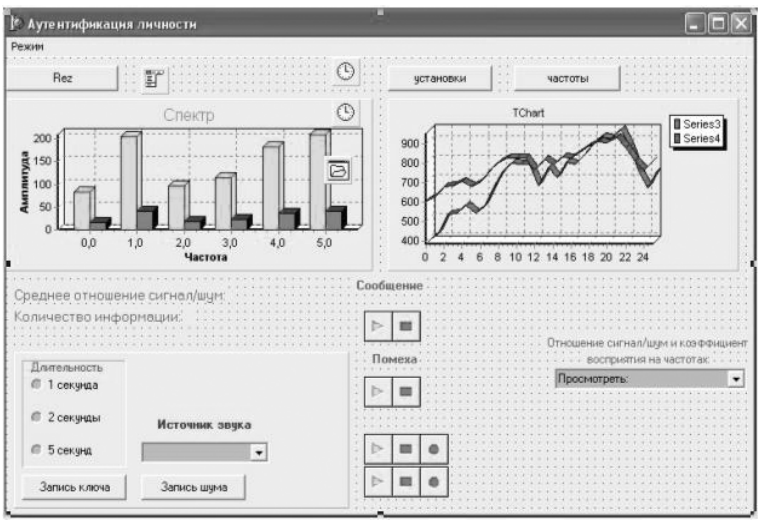


Figure 1.

The basis of the complex operation is definition of an average information content and articulation. Numerical values of these parameters combination may be used as the working identifier. Two complex operations modes are supposed: 1) working identifier creation mode; 2) authentication mode.

Key features of the offered approach are:

1) For the authorized access of the correspondent to the bank system only the virtual identifier which is formed by the correspondent in analogue mode independently is used. It absolutely eliminates possibility of a fake imitation.

2) The working identifier is used only as the measurement standard for matching that removes necessity of its special protection.

3) The correspondent operatively may change the virtual identifier, representing the working identifier appropriate to him in bank.

The offered approach and its implementation opens the newest **area** of the bank system perfecting in a direction of unauthorized access to the bank information security.

Given results are obtained during researches spent by writers at support of Russian federation Education Ministry T02-03.1-816

INFORMATION TECHNOLOGY OF SCRAMBLING METHODS QUALITY RATING ESTIMATION

Kotenko V.V., Rumjantsev K.E., Polikarpov S.V., Levendyan I.B.
Taganrog State University of Radioengineering, Taganrog

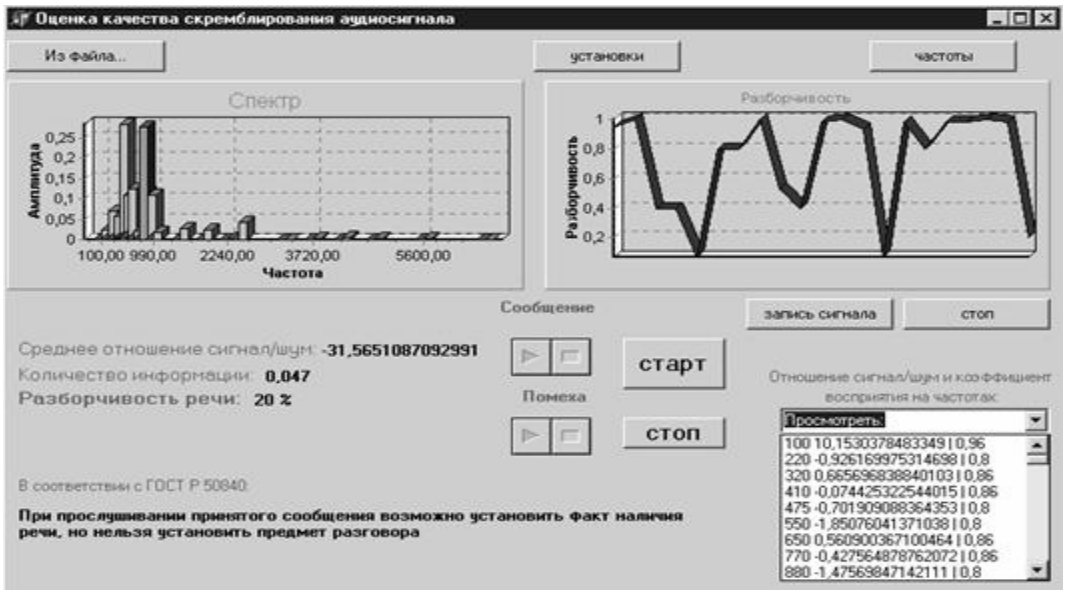
Even common acquaintance with a modern status of researches in the field of audioinformation security methods effectiveness analysis reveals enough dangerous situation consisting in common approach to given class problems solution lack for today. It naturally entails vari-

ety of different not interconnected scrambling quality rating methods which practical value leaves to wish the best. Indeterminacy of rating optimality criteria used, frequently forces contributor to make the empirical solutions reducing usually doubtful results. Though attempts of the criteria using, providing scrambling methods separation (computing resistant and unconditionally resistant) justify themselves in some cases, however as a whole, insert additional indeterminacy. All this promotes forming a situation in which judgment that the level and a degree of speech scrambling systems privacy are rather conventional concepts is dominant. Introduction of virtual scrambling noise concept allows solving this problem. Taking this concept into consideration scrambling process may be submitted as modification of voice call $S(t)$ by virtual noise $V(t)$ process. The projection of this performance to the real area is defined by the expression:

$$E(t) = F[S(t), ШV(t)], ШV(t) = Ф[S(t), E(t)] \quad (1)$$

Where: $E(t)$ is scrambled signal; $ШV(t)$ is projection of virtual noise. Expressions (1) define common mathematical model of scrambling methods effectiveness rating. Researches in the given approach realization field give quite reassuring results. The testimony to this was creation of a hardware-software complex of audioinformation security current quality control.

The complex is intended for audioinformation quality control in real-time mode. Virtual rating algorithms are applied for these purposes for the first time. It allows using traditional performances utilized for purposes of audioinformation quality rating estimation: intelligibility and average information content. On its basis the possibility to recommend users how to organize private talks is provided. Given results are obtained during researches spent by writers at support of Russian federation Education Ministry T02-03.1-816.



VIRTUAL ENCRYPTION COMPUTER TECHNIQUE

Kotenko V.V., Rumjantsev K.E., Polikarpov S.V., Levendyan I.B.
Taganrog State University of Radioengineering, Taganrog

Existing ciphers are not capable to provide theoretical undecodeability. Spent researches showed that one this problem solution ways is encryption process virtualization. Using this approach allowed to receive a lot of ciphers, potentially capable to provide theoretical undeciphering capability. On these ciphers computer realization basis information security software complex was developed. This complex experimental research carried out with statistical tests NIST STS using (tab. 1), has shown its advantage in relation to existing ciphers including cipher Rijndael developed in AES frameworks which was recommended as XXI century encryption standard. So, even at 1 bit key length (primitive variant) encryption quality similar to quality of modern ciphers, operating 128 and more bit key length is ensured. And, even insignificant magnification of key length (up to 4 bit) considerably allows to improve these indexes.

Table 1.

Generator	Amount of tests at which testing have passed more than 99 % of sequences	Amount of tests at which testing have passed more than 96 % of sequences
BBS	134 (70.8%)	189 (100%)
Gryada – 1M	130 (68.8%)	184 (97.4%)
Primitive variant	134 (70.8%)	189 (100%)
Simple variant	150 (79.4%)	189 (100%)