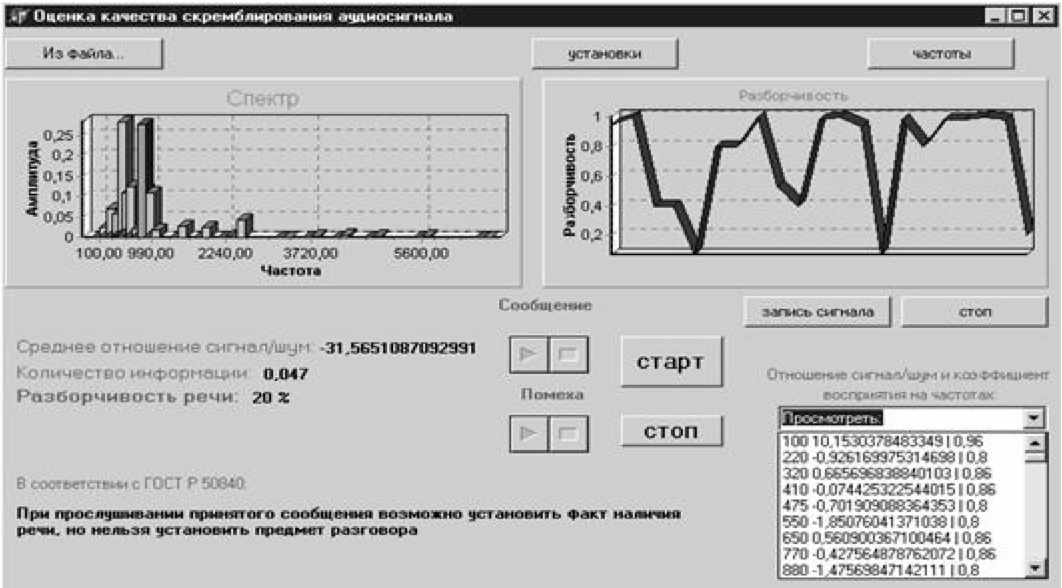
ety of different not interconnected scrambling quality rating methods which practical value leaves to wish the best. Indeterminacy of rating optimality criteria used, frequently forces contributor to make the empirical solutions reducing usually doubtful results. Though attempts of the criteria using, 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:

$$E(t) = F[S(t), \text{Ш}V(t)] \text{ , } \text{Ш}V(t) = \Phi[S(t), E(t)] \quad (1)$$

Where: $E(t)$ is scrambled signal; $\text{Ш}V(t)$ 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.



Среднее отношение сигнал/шум: -31,5651087092991

Количество информации: 0,047

Разборчивость речи: 20 %

В соответствии с ГОСТ Р 50840:

При прослушивании принятого сообщения возможно установить факт наличия речи, но нельзя установить предмет разговора

```
100 10,1530378483349 | 0,96
220 -0,9261699753314698 | 0,8
320 0,6656968388401031 | 0,86
410 -0,074425322544015 | 0,86
475 -0,701909088364353 | 0,8
550 -1,85076041371038 | 0,8
650 0,560900367100464 | 0,86
770 -0,427564878762072 | 0,86
880 -1,47569847142111 | 0,8
```

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%)

It is necessary to underline, that given results should be considered only as dynamic reflection of complex realization variants effectiveness depending on initial keys length and should not be considered as univalent acknowledgement of small value of this length advantages. Generally, initial keys length will be commensurable with initial keys length in the modern ciphers. It is why initial key structure should contain bits assigning virtual sample space discrete form aspect, and also discrete sampling, quantization and scaling parameters.

As a whole, from complex probing follows that its realization in random sequences generator mode is potentially capable to provide indexes that considerable exceed known analogs. Taking into account, that development of a casual (pseudorandom) sequence makes unrolled key forming basis which performances finally determine encryption quality. Obtained lead-out may be generalized on all developed software complex modes.

Given results are obtained at Russian Federation Education Ministry grant (T02-03.1-816) support.

NEW APPROACH TO INFORMATION TECHNOLOGIES QUANTATIVE QUALITY ESTIMATION

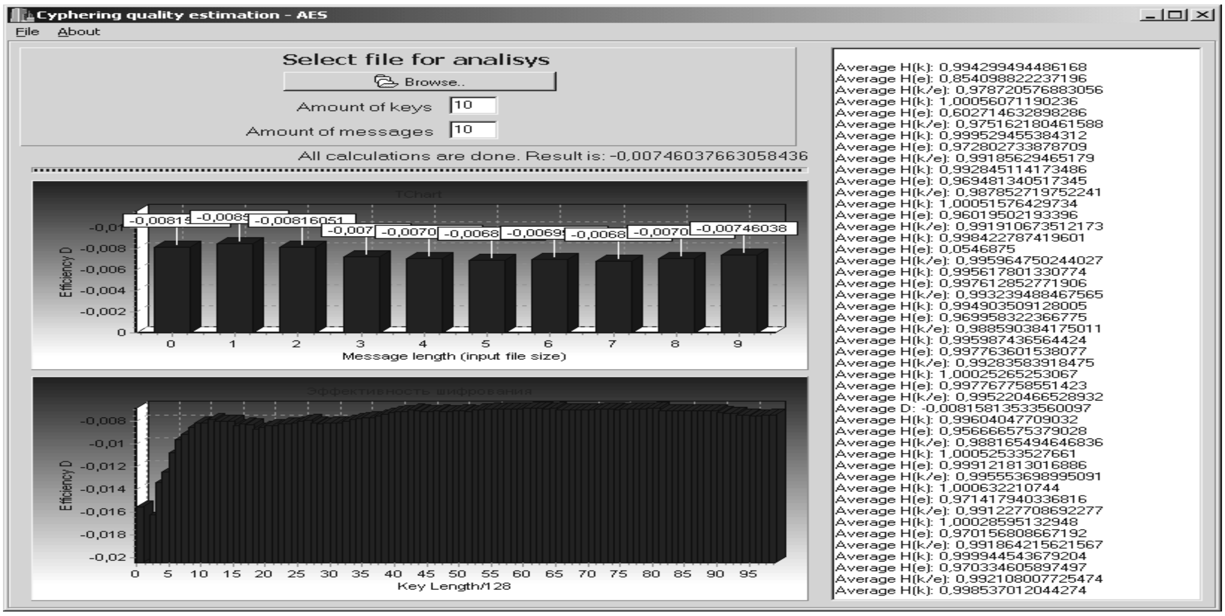
Kotenko V.V., Rumjantsev K.E., Polikarpov S.V., Levendyan I.B.
Taganrog State University of Radioengineering, Taganrog

Progressing growth of information technologies value in the modern world demands perfecting theoretical and practical basis of their protection. It generates problems which solution is rather inconvenient from positions of public approaches to a privacy. The major problem is protection quality estimation. First of all this problem appears in ciphers quality rating vagueness. The reference direction of it was definition of the so-called standard of encryption of XXI century which was carried out within the framework of National Standards institute of Standards and Technologies (NIST) USA conferences series in 1997-2000 The fact is that the best cipher was chosen only by participants of the Third Conference (April 2000) votes. Results of this voting (RIJNDAEL-86, SERPENT 59, TWOFISH-31, RC6-23, MARS-13) determined the best XXI century algorithm RIJNDAEL, obtained during implementation of AES project.

The researches which have been carried out by authors shows that the marked problem may be solved from positions of the approach offering virtual conception of the encryption process. Using of this approach allowed authors to receive analytical expressions for efficiency $D(\Phi,u)$ of encryption Φ and to create software complex, which distinctive features are: 1) possibility of encryption efficiency quantitative estimation, including real-time processing; 2) registration of messages, keys and cryptograms bands statistical performances during encryption; 3) registration of messages radiants information performances influences (first of all redundancies).

Using of the created complex for quality estimation of the ciphers listed above has suggested competency of NIST guidelines. So, efficiency of algorithm RIJNDAEL (fig. 1) for radiants u_A of the English language is $D(\Phi,u_A)=-7.4604*10^{-3}$, That corresponds higher protection quality comparison with algorithm SERPENT, for which $D(\Phi,u_A)=-8.0781*10^{-3}$. The negative values $D(\Phi,u_A)$ mean, that these algorithms do not meet requirements for theoretical undecoding capability which is showed at $D(\Phi,u\ )\geq 0$. In this case higher protection quality of encryption means values $D(\Phi,u\ )$ tented to zero in the negative axis.

Using of the offered approach and the program complex created on its basis opens fundamentally new area of researches in the field of information technologies protection quality estimations. Given results are obtained at Russian Federation Education Ministry grant (T02-03.1-816) support.



Amount of keys 10

Amount of messages 10

```
All calculations are done. Result is: -0,00746037663058436
```

```
Average H(k): 0,994299494486168
Average H(e): 0,854098822237196
Average H(k/e): 0,978720576883056
Average H(k): 1,00056071190236
Average H(e): 0,602714632898286
Average H(k/e): 0,975162180461588
Average H(k): 0,999529455384312
Average H(e): 0,972802733878709
Average H(k/e): 0,99185629465179
Average H(k): 0,992845114173486
Average H(e): 0,969481340517345
Average H(k/e): 0,987852719752241
Average H(k): 1,00051576429734
Average H(e): 0,96019502193396
Average H(k/e): 0,991910673512173
Average H(k): 0,998422787419601
Average H(e): 0,0546875
Average H(k/e): 0,995964750244027
Average H(k): 0,995617801330774
Average H(e): 0,997612852771906
Average H(k/e): 0,993239488467565
Average H(k): 0,994903509128005
Average H(e): 0,969958322366775
Average H(k/e): 0,988590384175011
Average H(k): 0,995987436564424
Average H(e): 0,997763601538077
Average H(k/e): 0,99283583918475
Average H(k): 1,00025265253067
Average H(e): 0,997767758551423
Average H(k/e): 0,995220466528932
Average D: -0,00815813533560097
Average H(k): 0,99604047709032
Average H(e): 0,956666575379028
Average H(k/e): 0,988165494646836
Average H(k): 1,00052533527661
Average H(e): 0,999121813016886
Average H(k/e): 0,995553698995091
Average H(k): 1,000632210744
Average H(e): 0,971417940336816
Average H(k/e): 0,991227708692277
Average H(k): 1,00028595132948
Average H(e): 0,970156808667192
Average H(k/e): 0,991864215621567
Average H(k): 0,999944543679204
Average H(e): 0,970334605897497
Average H(k/e): 0,992108007725474
Average H(k): 0,998537012044274
```