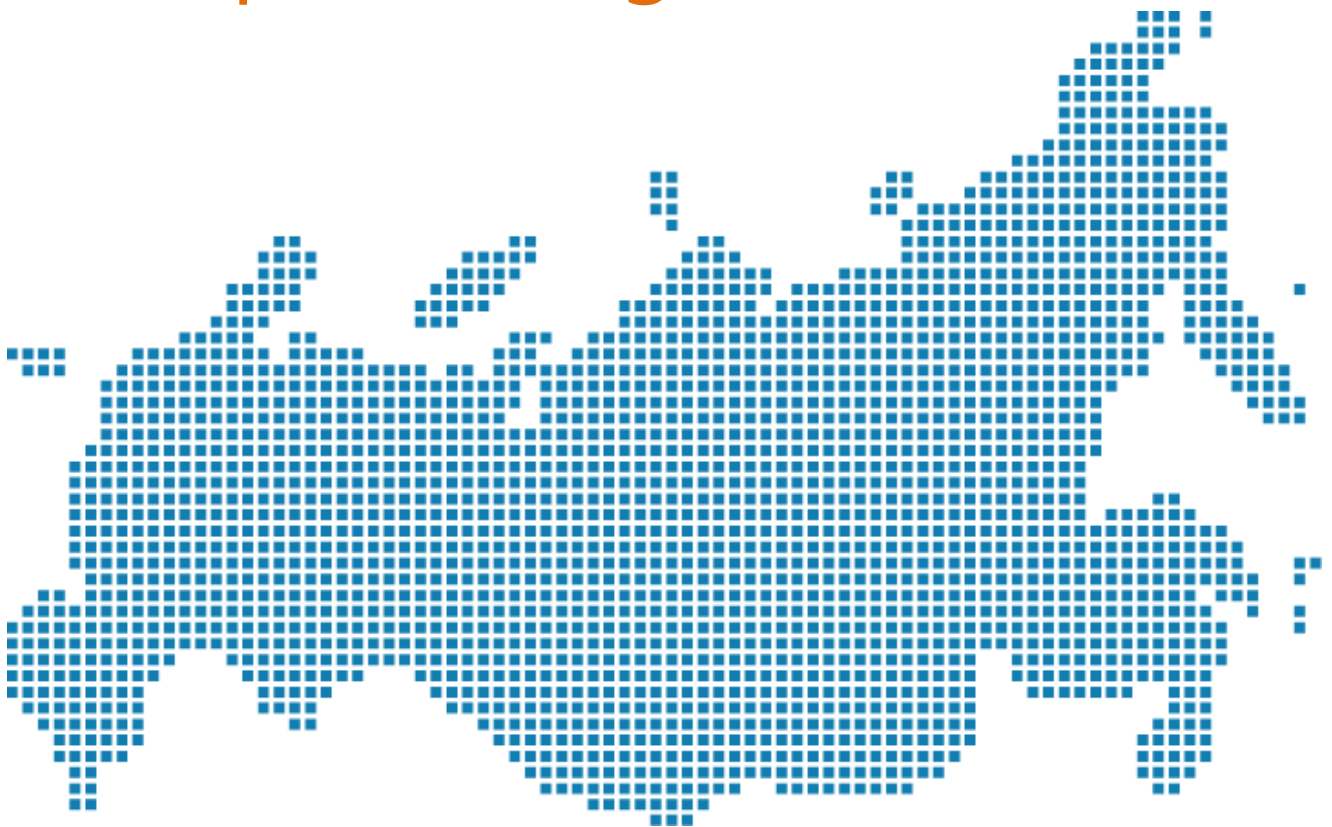


# Presentation of Research

## Information Security Market 2009: Beginning of the Compliance Age



## Contents

|                                                                             |           |
|-----------------------------------------------------------------------------|-----------|
| <b>Contents.....</b>                                                        | <b>2</b>  |
| <b>List of figures and tables .....</b>                                     | <b>3</b>  |
| <b>Research Overview.....</b>                                               | <b>4</b>  |
| <b>Basic Conclusions .....</b>                                              | <b>5</b>  |
| <b>Basic Characteristics of Information Security Market .....</b>           | <b>7</b>  |
| Information Security Market Volume .....                                    | 7         |
| Structure of Information Security Services Consumption .....                | 15        |
| Key Players of Information Security Market .....                            | 20        |
| <b>Security Threats in 2009 – 2010.....</b>                                 | <b>27</b> |
| Software Exposures .....                                                    | 27        |
| Distribution Vectors .....                                                  | 30        |
| Intruders' Goals.....                                                       | 31        |
| Conclusions .....                                                           | 34        |
| <b>Development of the Information Security Market Management .....</b>      | <b>36</b> |
| № 152-FZ “On Persona Data” – Works Commencement .....                       | 36        |
| Standard of the Bank of Russia .....                                        | 41        |
| Development of Information Security Management Systems Implementation ..... | 44        |
| <b>Development of Particular Segments of Technical Protection Aids.....</b> | <b>48</b> |
| Peculiarities of Certified Aids Use for Personal Data Protection .....      | 48        |
| Antivirus Market .....                                                      | 51        |
| Decisions on Ensuring Control over IS Requirements Compliance.....          | 55        |
| DLP systems .....                                                           | 60        |
| <b>Investigation of Information Security Incidents.....</b>                 | <b>65</b> |
| <b>Preview. Research Following the Results of 2010.....</b>                 | <b>69</b> |

## List of figures and tables

|                                                                                                                   |    |
|-------------------------------------------------------------------------------------------------------------------|----|
| Figure 1. Volume of “Open” Information Security Market, \$mln.....                                                | 13 |
| Figure 2. Growth Ratio of “Open” Information Security Market, %.....                                              | 14 |
| Figure 3. Basic Segments of Information Security Services Consumption, \$mln .....                                | 16 |
| Figure 4. Information Security Consumers, % .....                                                                 | 17 |
| Figure 5. Shares of Market Players, %.....                                                                        | 21 |
| Figure 6. Diagram of the Initiated Personal Data Protection Projects Number Increase.....                         | 39 |
| Figure 7. Growth of Russian Organizations’ Expenses on Information Security Personal Data Protection, \$mln ..... | 40 |
| Figure 8. Market Growth of Antivirus, \$mln .....                                                                 | 52 |
| Figure 9. Growth Ratio of Antivirus Market, %.....                                                                | 52 |
| Figure 10. General Expenditures Level for Organizations’ IS of Various Maturities.....                            | 57 |
| Figure 11. Information streams controlled by means of DLP system.....                                             | 60 |
| Table 1. Basic Segments of Information Security Services Consumption, %.....                                      | 17 |
| Table 2. List (alphabetic) of Russian companies promoting services in Information Security sphere .....           | 22 |
| Table 3. List (alphabetic) of major Russian vendors .....                                                         | 23 |
| Table 4. Cost of Databases.....                                                                                   | 32 |
| Table 5. Certified ISMS as of the beginning of 2010.....                                                          | 45 |
| Table 6. Three Leaders on the Antivirus Market .....                                                              | 51 |

## Research Overview

LETA IT-company presents the fourth expert report on information security market: "Information Security Market 2009: Beginning of the Compliance Age". The first report was issued at the beginning of 2007, the second – in the middle of 2008 and the third – in the middle of 2009, with the many estimates becoming recognized facts on the IT market.

This research is dedicated to the Russian Information Security market. The research provides information on its volume, structure and key players. For the purposes of this research, the IS market means the market of all services including services providing information security of networks, equipment and systems of state and commercial organizations.

It is emphasized that it was not the aim of the authors to cover all the Russian IS market segments in detail. Thus, a certain number of market segments were left aside, in particular, network security, web-security and etc. LETA IT-company had to limit the choice of segments due to constrained resources and information with respect to certain segments.

A special attention in this research is drawn to the problems of the personal data protection, being the most important issue of the IS market in 2009.

Information for the given research was obtained by interrogation of the market participants by the expert interview method, and analysis of publications in mass media and other public domains. The authors used public information of the leading research companies— IDC, Gartner, PwC, Ernst&Young and etc.

All the numerical data represent the expert opinion of journalists, market participants and analysts of LETA IT-company. The research refers to the estimates of the top authenticity sources, leading business and specialized mass media, representatives of major companies and etc.

Tendencies and forecasts on the IS market are compiled on the basis of tendencies and forecasts of the RF economy development in general, development of the IT market, Russian and world IS market, estimates and calculations of LETA IT-company's analysts.

The peculiarity of this research is that it states the names of the articles authors, which makes it possible for the readers to get in touch with them, should any questions, proposals or remarks arise.

| Author                  | Company         | Topic                                               |
|-------------------------|-----------------|-----------------------------------------------------|
| Valentin Krokhin        | LETA Group      | Science editor                                      |
| Alexander Sanin         | LETA IT-company | Personal data protection                            |
| Evgeniy Tsarev          | LETA IT-company | Standard of the Bank of Russia                      |
| Nikolay Zenin           | LETA IT-company | DLP, compliance                                     |
| Dmitry Artemenkov       | LETA IT-company | Personal data protection                            |
| Ilya Sachkov            | Group-IB        | Investigation of the information security incidents |
| Maria Akatieva          | LETA IT-company | ISO/IEC 27001:2005                                  |
| Vyacheslav Zheleznyakov | LETA IT-company | ISO/IEC 27001:2006                                  |

## Basic Conclusions

1. The year of 2009 witnessed the emergence of a new modern Information Security market in Russia which is associated with successful commencement of the first all-Russia large-scale compliance project – realization of the requirements set forth in the Federal Act "On Personal Data".
2. The volume of the "open" market in 2009 reached \$561 mln. In general the market growth within the next two years will remain on the level of 8 – 12%. As compared with 2008, the growth made less than 2% (as per the updated data, the market volume in 2008 reached \$552 mln.).
3. In the first half-year the IS market, as against the IT market, fell "barely" by 15% in comparison with 2008, and the second half-year was marked by growth. The following factors influence the market growth in terms of crisis: regulators' requirements, increased level of threats and new threats emergence. As a result, the market stagnated in a positive range.
4. Since the crisis outset, many companies stuck to individual implementation of IS systems as a basic consumption model of information security products and services. But everything changed after the adoption of the Act "On Personal Data".
5. 2009 proved the tendency presupposing the gradual change of consumer structure alongside with the market development. Accordingly, the market will demonstrate: increase of governmental bodies' share, decrease of major businesses' share, growth of the SMB and household consumers segment.
6. The business within the companies-integrators segment is successfully developing. However the segment of Russian producers of Information Security services is in crisis conditions. Being oriented at a constricted market share, but not at the average consumer, the native developers created products of constrained functionality which are difficult to be implemented in a large-scale. Contraction to narrow niches may completely "beat" such producers, as niche activity is not characterized by large money flows without which it is impossible to develop product.
7. The most evident recent growth is demonstrated by two major areas of malicious activity – expressed extortion of small money amounts and

establishment of accounts databases (both with and without authentication information) for subsequent sale.

8. The attack target is practically always set at execution of malicious code introduced into the processed object, and, as a consequence, obtaining the account privileges on which behalf the attacked software is run.

9. It can be definitely ascertained that the demand for services on bringing PDIS (Personal Data Information Systems) in compliance with the regulators' requirements in 2010 will increase. The expenses will amount to \$110 mln.

10. The prompt approval by the regulators of the new version of the Standard of the Bank of Russia and recognition of its requirements as sufficient to fulfill the requirements of 152-FZ and the regulators' requirements will result in the banking community acquiring adequate and branch-adapted documents allowing to perform works on personal data protection under the STO BR IBBS. According to our estimates, from 2011 to 2013, banks will spend more than \$60 mln. on the standard requirements implementation. What is more, the successful launch of this standard will definitely enhance the tendency to develop other branch standards.

11. The introduction of the IS policies management automation systems will become a significant area of the IS market development beginning with 2010.

12. The last year demonstrated that ISMS, as an integral complex of processes, appeared to be less in demand than its separate elements.

13. The antivirus protection market volume in Russia in 2009 reached \$195 mln.

14. The DLP market volume in Russia in 2009 reached \$33 mln.

# Basic Characteristics of Information Security Market

## Information Security Market Volume

The year of 2009 is referenced as a most important period in terms of information security (IS) market development as a whole. It is possible to ascertain that it was exactly in 2009 when the new contemporaneous IS market was established.

However at the beginning of 2009 nothing evidenced to the fact that the year would become crucial. The world financial crisis coming into its active phase in 2008 stamped tremendously on the information technologies (IT) application.

In terms of crisis, companies of all sectors and scales, and not only in Russia but in the world as a whole, attempted to reduce the expenditures not directly influencing core business processes. The reduction of IT expenditures became one of the opportunities to reduce general expenditures. Russia demonstrated a significant drop. Thus, according to the Ministry of Communications, the IT market fell by 13.8%; according the IDC data – the fall reached 43% (which seems to be a more adequate estimate). Thus, the drop in certain segments in the first half-year reached 70% (concerning, first of all, hardware supplies).

The information security market could not but downfall following the IT market. However there was no considerable reduction, the market dropped a little, and the second half-year was marked by the growth.

The explanation for the comparatively moderate reduction observed in the first half-year is that security budgets were the last to be reduced. Information security market once more proved that security in its various manifestations remains a basic need, even if it concerns information technologies. And amidst instability, security is the last to be sacrificed by an organization, and taking into account the fact that information assets became the most important concern of any organization, expenditures on information assets protection remain an important item of organizations' and private users' budgets.

However, despite all the positive factors, the market nevertheless sloped. This was influenced by the following factors:

1. *General reduction of expenditures aimed to cut the organizations' budgets on servicing technologies, including IT and IS.*
2. *Updating slowdown.* Companies practically did not spend money on development and updating of the systems being already in use.
3. *Works rescheduling from integrators to internal services.* Integrators' and internal consultant services were in demand only in situations when the in-house IT and IS service failed to solve the set tasks (lack of competence or the sphere being regulated by regulatory acts).

At the same time the forecast did not prove true with respect to the following factors:

1. *Piracy intensification.* Still for some years the IS market made a considerable advance, and correlation of pirate and license software remained practically the same.
2. *Transition to "free" and open source products.* Certain experts forecasted that in context of tight resources the corporate sector might start massive transition to "free" and open source products. But this was not the case. And if a portion of household users turned to "free" and open source products, the corporate sector decided that risks associated with such transition were not justified.

As a result, in the first half-year the IS market, as against the IT market, fell "barely" by 15% in comparison with 2008. And such a fall took place basically for account of SMB sector companies occupying the lower part.

The following factors made it possible to retain the IS market from fall:

1. *Increased level of threats, including appearance of the new ones.* In context of crisis, criminal risks are growing, which means the increase of expenditures on overcoming of such risks. Herewith, risks as such may change, new threats may appear, and previous long forgotten threats become topical. For example, there was an increase of threat from the part of in-house personnel.

The personnel loyalty falls caused by headcount and actual income reduction that is why it is possible to expect both facts of sabotage and security leakage.

Similarly, contracting markets demonstrated competition increase which provoked stiffening of competitive struggle. And attacks on various corporate electronic resources were among those manifestations of such struggle.

2. *Requirements of partners.* The tendency did not reduce its influence, but vice versa, it strengthened in context of threats number increase. Since business relations were not terminated, in spite of the crisis, a problem of mutual trust became urgent.

In context of crisis, when mutual trust between the economic activity participants is severely disrupted, the trust factor on the level of delivery and storage of confidential information grows inversely. For certain companies, information security became a far more precious than money.

3. *Increase of IS significance.* Information security for all major and a great many of medium-size companies which experienced the period of massive IT introduction, transformed from an applied discipline into the issue of business level. The IT system was then used to store and process really prime data essential for business existence and survival. As a result, for many companies the issue of information storage and maintaining the integrity of IT systems and IT infrastructure transformed from secondary tasks into the highly significant purpose, and costs reduction became impossible.
4. *Regulators' requirement.* In the first half-year many companies did not profoundly understand what to do with the regulators' requirement and thus did not take active measures. Basically, it was the period of competence upgrading. The similar wait-and-see attitude was also typical for quasi-mandatory documents.

But in the middle of the last year it was understood that fulfillment of the requirements set forth in the Act "On Personal Data" would be mandatory and therefore rather expensive. Besides, in order to fulfill the requirements of all the subordinate legislation acts, the companies – personal data operators – will have to invite not only specialists in the IT and IS sphere, but also lawyers and specialists on business processes re-engineering. Consequently, the problem which seemed to concern only information security specialists reached the level of business.

It was the transition of the IS problems to the business level that became a crucial point for the market. In Russia within the period of 2000-2009 information security specialists were constantly striving to prove not only the significance of their work, but also the significance of IS for business as a whole. And they seemed to have all tools as these were the years when information technologies became those of the business foundations. Therewith, IT specialists

could take advantage of international experience which included standards, best practices and methods of risk assessment. So, IT specialists could share terms common to business. This was the matter of discussion of the previous LETA researches.

With some minor exceptions in certain major and medium-size companies information security failed to take its own place within the corporate management system as it was perceived as one more supportive system similar to the Administrative Supply Department. Many companies lacked an assigned IS manager, and the functions of information protections were delegated to the IT department. The IS policy was something exotic. However, in the second half of the 2000-2009 the situation started to gradually recover, though, at a very slow rate.

Works commenced in 2009 in the sphere of PD protection made it possible not only to elevate the IS to the business level, but drew the business concern to the activity practically realizable due to informational security. Consequently, the IS significance increased for companies in general, which provoked the increase of expenditures, as in context of increased attention towards the IS specialists possessing the relevant knowledge it became easier to motivate the expenditures on implementation and use both of IS services and various standards and management systems. The outcomes of this process were that decisions in the IS sphere became strategic which means that goals of their implementation planning were transformed from short-term into medium-term which also stimulated the expenditures increase.

The second major consequence of the business interest growth towards the IS was the boom of the branch standards development, first of all in the sphere of personal data protection (in particular, standards developed in spheres of communication, medicine, education and bank sector, private pension funds). And further on it is expected that standards in the sphere of personal data protection will be transformed into information security standards.

With standards available, it is easier to justify the IS expenditures, primarily, on organizational measures. It means that IS gradually ceases being just a technical problem as it was very often considered. Correspondingly, introduction of organizational measures presupposes IS market expenditures and considerable growth of consulting services share. Finally, Russian market will reach the state

of the developed countries where expenditures on organizational measures and consulting within IS projects amount to 45-50%. It is worth mentioning that the process of relevant organizational measures implementation under Russian conditions will not be quick (unless new standards appear in the near future), tradition is still very strong, but the process is inevitable. Thus, for example, according to our estimates in 2009 80% of the companies using more than 300 PCs employed information security managers.

It should be noted that mass appearance of IS managers led to the increase of interest to education in the given sphere. After all, it is not the IS specialists who are appointed to this position due to the de facto lack of the latter. Owing to increase in the number of qualified and trained specialists in the IS sphere, the market will start to expand, as well as the companies' IS expenditures, due to the capability of such specialists to apply the best practices. According to our estimates, the IS in a great deal of companies and organizations was either underfunded or works within IS were funded under other projects (the so-called latent market). In the pre-crisis period the IS expenditures of the companies, employing organized and trained personnel, were higher as against those lacking it (due to implementation of internal standards and policies implemented by the trained personnel).

Changes introduced by the FSTEC (for details see the corresponding chapters) will not provoke the growth impairment of the PDIS security market. Alternately, they will support it as the new requirements are more reasonable and executable. This means that the increasing number of companies, for which the risk of previous requirements non-fulfillment exceeded overall expenditures on bringing the PDIS in compliance with the regulators' requirements, will launch projects on securing their systems according to the new requirements.

Therefore, it is possible to ascertain that the first large-scale compliance project in Russia has been successfully launched, and the compliance age has commenced in Russia though being several years late.

Besides the abovementioned reasons for market growth in the midterm, it is necessary to mention the following:

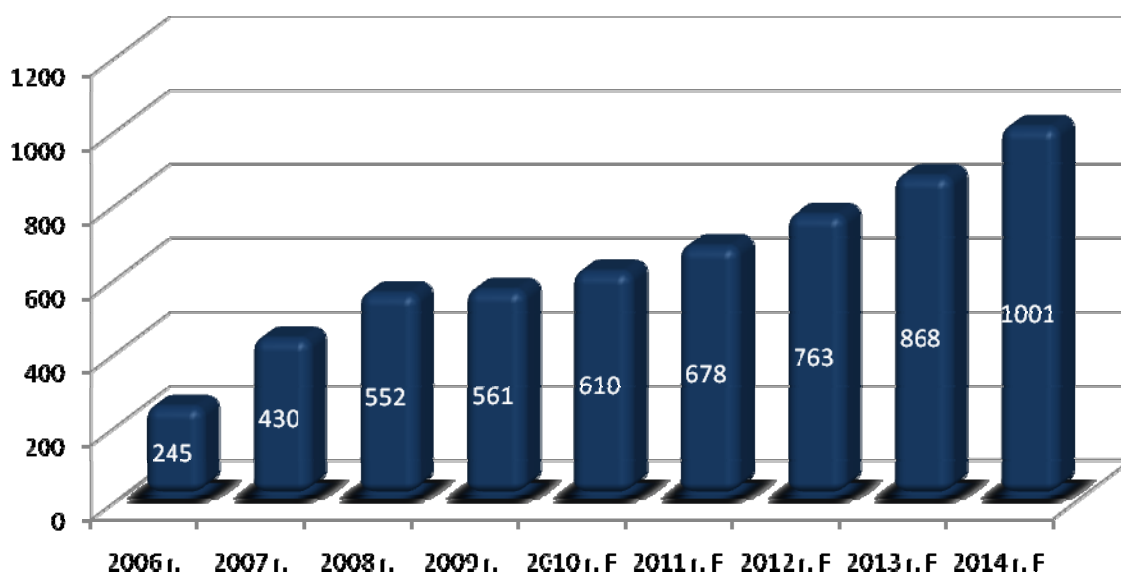
1. *Economic rehabilitation.* The growth in IS services consumption both in household segment and business and state structures.

2. *Revision of the Act "On Electronic Digital Signature"*. In the middle of this year it is planned to adopt a new act governing legal status of electronic digital signature. The previous act turned out to be inefficient. The revisions of the act under consideration at the moment appear to be more logical and applicatory. This means a fast growth of the EDS use which will lead to expansion of the relevant IS systems implementation. It should be specially emphasized that according to the draft act it is possible to implement both Russian and foreign systems.
3. *Introduction of PCI DSS requirements. Term – until 2011*. This autumn is the maturity period for VISA users to bring their systems into compliance with the requirements of the PCI DSS standard. But as of the beginning of 2010, the VISA members of Russia do not meanwhile make any considerable effort to bring their systems into compliance with PCI DSS. According to our estimates, the boom of PCI DSS will outburst in 2010 with punitive measures enforced.
4. *Partners' requirements*. Adopted in Russia after several years of delay, the world tendency presupposes that a partner, having secured confidential data (e.g. personal data) and while transferring it, should be sure that the security of the very data within another organization will be at least as reliable as within the its own premises. The tendency finds its reflection basically in the series of standards ISO – 27 00X. For the last couple of years the interest to certifications according to this standard has considerably increased. And the certification itself, apart from organizational requirements introduction, entails the introduction of new IS services in companies.
5. *IS availability enhancement*. Technologies became more comprehensive and more available first of all for small and medium-size companies; their introduction and use became simpler.
6. *Technologies development, new solutions appearance*. Primarily, the following technologies, capable of becoming drivers of the Russian market growth, should be mentioned:
  - Virtual media protection;
  - Incident management systems;
  - Systems facilitating the compliance with the requirements and regulators;
  - CAM protection.

7. *Aggressive advertising campaign of producers.* It's not a secret that IS services producers spent considerable money on advertising, including the excessive "fear appeal" of the clients.
8. *New threats emergence.* Indeed, recent years witnessed the emergence of new threats which companies are forced to face. Most commonly it means the increase of IS expenditures.
9. *Sophistication of the IS-solved tasks.* The growth and sophistication of IS systems is accompanied by the growth of IS expenditures.

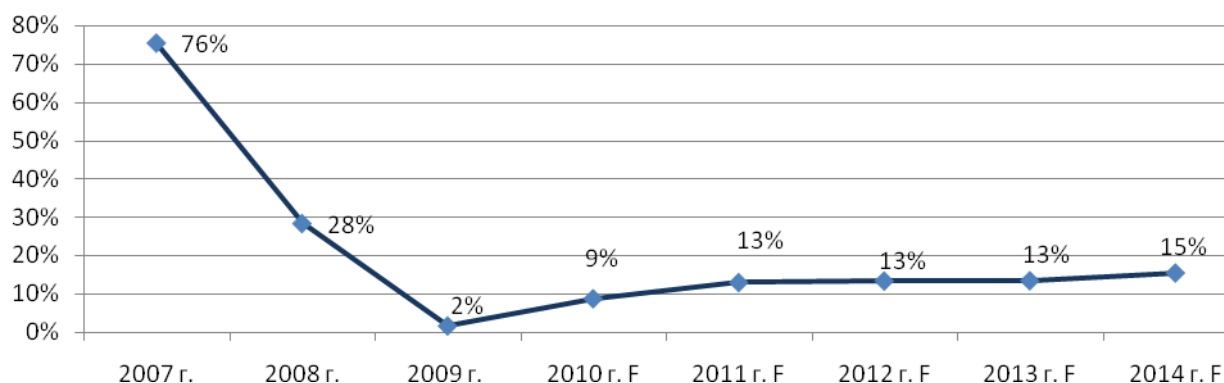
Relying on this vast list, it is possible to draw the conclusion that it was not one or event two factors that influenced the IS market growth, but a whole bunch thereof.

**Figure 1. Volume of "Open" Information Security Market, \$mln**



Source: LETA IT-company

**Figure 2. Growth Ratio of "Open" Information Security Market, %**



Source: LETA IT-company

As a whole, the market is not able to repeat its heavy growth as, disregarding all the factors promoting market growth, it is the economic situation that defines the tendency. According to all estimates, during the next five years the economic advance, if any, will be minimal. But the remaining factors will contribute to its growth by 10-15%.

Thanks to the researches carried out by LETA IT-company it was discovered that the Russian IT market lacks transparency, its structure does not satisfy the world tendencies. Although, there is another fact: all the remaining segments of the IT market fit well into the world tendencies.

In the context of the previous researches, the existence of "latent" IS expenditures market was revealed. It includes "pirate" expenditures and other unclassifiable expenditures. Inclusive of the "latent" market, the IS expenditures in 2009 reached a little more than \$1.1 bln.

## Structure of Information Security Services Consumption

Since the crisis outset many companies stuck to individual implementation of IS systems as a basic model of consumption of information security products and services, which was stipulated by the expenditure reduction. The transition appeared to be rather harsh which testified to the fact that this was not the one-year tendency. The necessity to fulfill the requirements of the Act "On Personal Data" revealed the problem of extremely little knowledge of the IS personnel in the majority of companies in Russia. Indeed, a in-house personnel of companies was able to implement projects on basic security requirements but they lacked qualification for a complex project with consulting component. As a result basic IS expenditures in 2009 were associated with resolution of problem of personal data protection which entailed a heavy growth of demand on professional services of external consultants. And since the introduction of various mandatory standards in the given sphere will constantly increase, the share of consultants will increase as well.

If only several years ago IT and IS departments (or outsourcing companies) of major corporations and companies of the top SMB segment preferred to implement IS solutions individually, the sophistication of technologies, new requirements introduction, commencement of new standards application entailed the lack of specialists in such departments to cover the whole spectrum of decisions. Consequently, the implementation was delegated to specialized companies and the in-house structures were vested with maintenance. That is why it was the major companies that started to resort to the IS companies' services.

Medium-size business preferred independent implementation often without retrieving the IS as independent projects. Taking into consideration the fact that SMB sector companies dominate in the economy of Russia, the consulting share remained minor as these companies very seldom invited consultants.

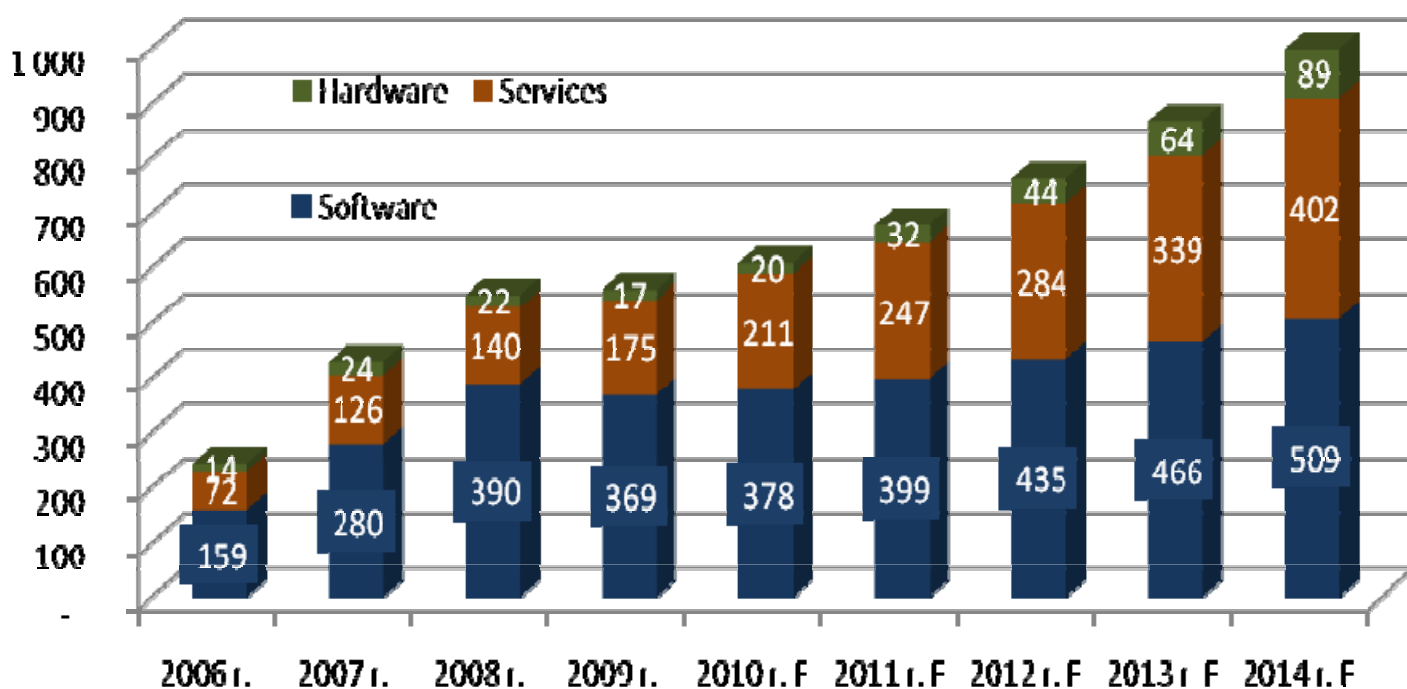
But everything changed after the adoption of the Act "On Personal Data". In theory, major companies could individually perform works on bringing in-house PDIS into compliance with the regulators' requirements but, as proved by experience, often they resorted to the services of professional consultants. And

the medium-size business companies for the most part could not have the required competence. That is why many of them confine themselves to PDIS investigation by own resources and introduced the necessary software with minimal organizational measures taken. However, a great deal of companies still invited external consultants. Basically, it was minor projects but they were quite many throughout Russia.

Small companies generally ignored the regulators' requirements as the requirements contained in the first version of documents were practically unenforceable. But nevertheless they procured software.

As a result the domination of products sale tendency in 2009 was broken, which means it is impossible to speak of the market conservatism.

**Figure 3. Basic Segments of Information Security Services Consumption, \$mln**



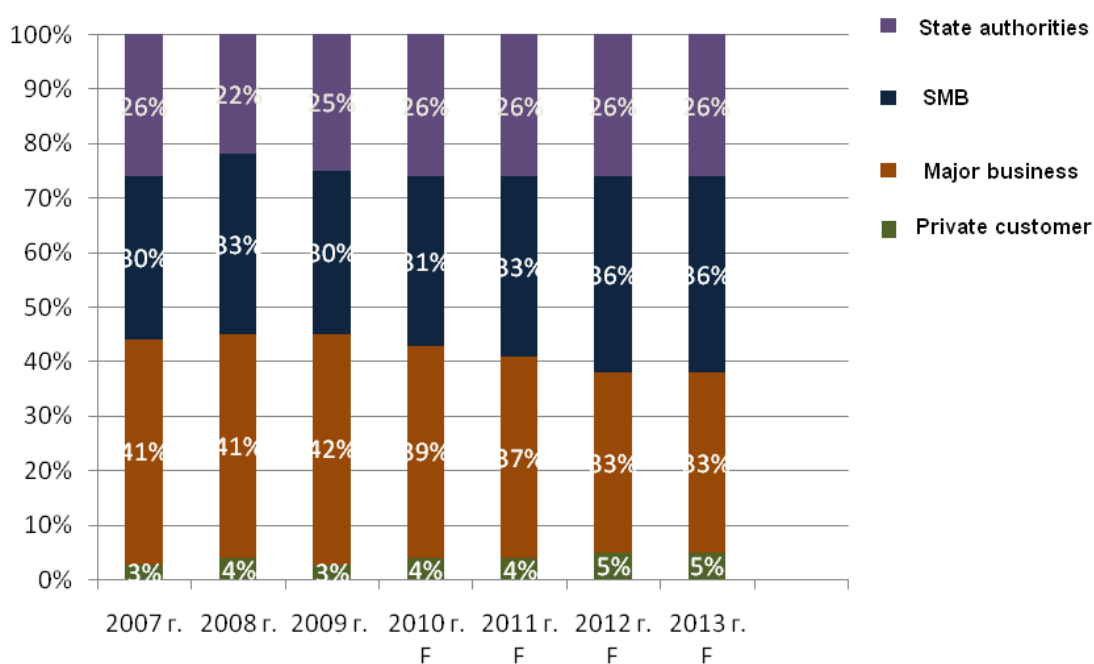
Source: LETA IT-company

**Table 1. Basic Segments of Information Security Services Consumption, %**

|        | Hardware share (%) | Services share (%) |
|--------|--------------------|--------------------|
| 2006   | 65                 | 29                 |
| 2007   | 65                 | 29                 |
| 2008   | 71                 | 25                 |
| 2009   | 66                 | 31                 |
| 2010 F | 62                 | 35                 |
| 2011 F | 59                 | 36                 |
| 2012 F | 57                 | 37                 |
| 2013 F | 54                 | 39                 |
| 2014 F | 51                 | 40                 |

Source: LETA IT-company

**Figure 4. Information Security Consumers, %**



Источник: LETA IT-company

The year 2009 proved the tendency presupposing that the consumers' structure gradually changes alongside with the market development. Correspondingly, the market will feature:

- State authorities share increase;
- Decrease of major business share;
- Increase of SMB segment;
- Increase of private consumers segment.

State authorities share increase.

The year 2008 seemed to be the commencement of gradual general decrease of state authorities' expenditures on automation. In the 90s and beginning of 2000s it was the state authorities that were the basic IT consumers, but the market development and gradual repletion of state authorities with modern IT, the money allocated for IT procurement (including security) will be reduced, which will lead to a steady decrease of their share. However the increase of state authorities share is still possible.

In 2009 the new project on IT implementation in state authorities was put into practice and the expenditures of the latter went upwards again, primarily concerning G2C (Government-to-Citizen) systems and relevant web-applications. With the IT expenditures growing, there will be an increase in the IS expenditures as well.

Besides, the state authorities will be forced to spend considerable money on bringing their PDIS into compliance with the regulators' requirements.

Decrease of major business share.

Major business has generally passed the stage of gross automation and, accordingly, there will not be huge expenses. It is necessary also to consider the fact that many Information Security systems in major companies were initially built with due consideration of regulators' requirements and various standards. It is the major companies being very prone to inspection risks that are the first to implement regulators' requirements.

The segment demonstrates the highest demand on services associated with IT audit and protection of the previously insecure areas, implementation of

centralized management systems, CAM protection systems. That is the core expenditures in the IS sphere will fall on IS systems maintenance. And the company shifting to a more advanced management level will face expenditures on introduction of policies, regulations, works aimed at standards compliance and regulatory acts, implementation of IS services of advanced complexity levels. In prospect this will be one of the most considerable items of IS expenditures.

#### Increase of SMB segment/

The SMB companies have to decide two problems: compliance with the regulators' requirements and introduction of efficient security systems which are to protect crucial IT systems. And considering that the SMB sector companies will spend considerable funds on IT introduction during the next five years, they will need relevant IS solutions.

The expenditures increase will be conditioned by the fact that the SMB sector companies did not invest into protection of their PDIS under the first version of the regulators' requirements. The second version is more realizable which will mean that it will be easier for the companies to execute new requirements rather than to bear the non-fulfillment risks.

What is more, alongside with the economy growth, the IT systems will become more complicated and able to solve new tasks, which means the proportional growth of their protection expenditures.

#### Increase of private consumers segment.

Private consumers beginning to "pure" their software; the volume of original product procurement will gradually grow. Besides, the given segment growth is facilitated by OEM programs when a private buyer obtains installed security services together with computer hardware.

In general, it is the security services market which is the less "pirate". This fact is associated with high rate of new threats appearance. Data protection is one of the paramount objectives for corporate and private consumers, and "pirate" products are not able to withstand the evolving threats. This is precisely why the security services market was the first to come out of the shadow.

## Key Players of Information Security Market

The fact that in context of crisis the IS market not only sustained but even demonstrated the emergence of new segments (primarily, works associated with regulators' requirements fulfillment), testifies that the market has become even more attractive for the most of the players.

A great deal of new specialized IS companies has appeared on the market with the majority of "major" and "medium-size" system integrators opening IS departments. There was no practically a single major IT company in Russia by the end of 2009 which would not claim having the IS services within its activity.

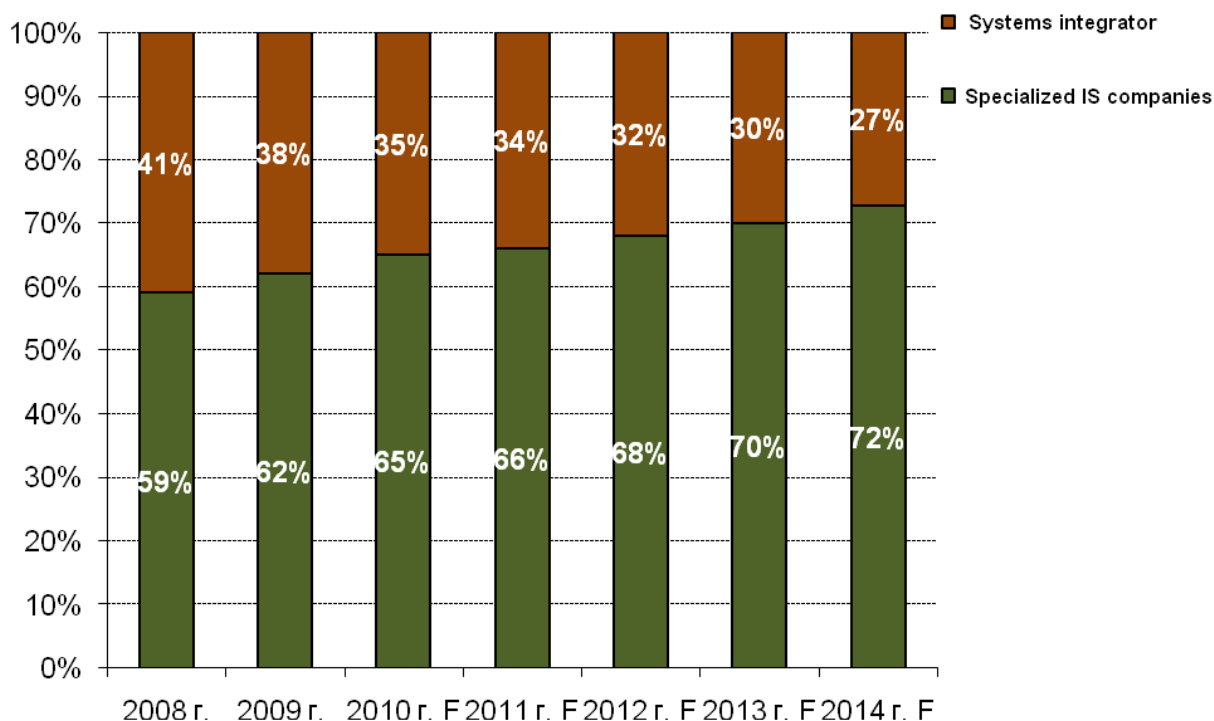
Unfortunately, such sudden increase in the IS departments did not induce qualification enhancement among integrators. With some minor exceptions, the quantity failed to turn into quality, and at the beginning of 2010 many of those who claimed having IS services started to reject their claims. It happened because the client companies are for the most part conservative and prefer ordering such critical services from the companies having a particular image on the IS market. That is why there was no fundamental redistribution of forces among the leaders, which means that competition on this prospective market is likely to strengthen.

Herewith, the peculiarity of this market is that it is impossible to differentiate which companies are technological leaders and which are thought leaders. Practically all IT companies introduce protection services. There are no companies within the market which would be able to set the pace to the whole market, but they are likely to appear.

With respect to its formal matter, the IS market is attractive in terms of investment, though there are no merger or takeover transactions (with some minor exceptions). To a large extent it can be explained by the conservatism of the companies and their owners.

Also it is important to note that "purely" IT companies have actually abandoned the IS market. None of the major consulting companies has launched the IS services though many claimed that. It was the obligation to get a license for information security services (and primarily personal data security) from the FSTEC of Russia and the lack of available specialists that was the reason for the consulting companies not to launch the services.

**Figure 5. Shares of Market Players, %**



Source: LETA IT-company

Specialized IS integrators still enjoy a very important advantage, that is a more sophisticated level of competence which enables them to implement complex technical and consulting projects. Likewise, an important competitive advantage is the experience in complex IS projects implementation, abiding by and use of all necessary regulatory acts, standards and licenses.

One more factor influencing the market development is the fact that major IT companies faced particular obstacles within the SMB segment. Major system integrators initially worked with corporate sector and state authorities but recent changes on the IS market with SMB companies gradually taking leading roles prove that today's "alligators" are difficult to adapt to the new situation.

In their turn, specialized companies are perfectly aware of the technological IS basis but have little knowledge in "economic" approach.

Consequently, only those companies offering their clients both “economic”<sup>1</sup> approach and sound technologic basis may work to the full extent at the market.

**Table 2. List (alphabetic) of Russian companies promoting services in Information Security sphere**

| Name of the integrator company |
|--------------------------------|
| ICL-KPO                        |
| LETA IT-company                |
| ReignVox                       |
| AMT-GROUP                      |
| Informzaschita Company Group   |
| Jet Infosystems                |
| Croc                           |
| “Eshelon” R&D company          |
| Orbita                         |
| RNT                            |
| SDB Contour                    |
| Elvis-Plus                     |

Source: LETA IT-company

Increased competition on the IS market induces the leading companies promoting IS services to develop competence necessary for the market, develop modern type services. A critically important factor of the market success is the personnel policy and considerable financial resources. Herewith, the leadership factor is more likely to be achieved owing to the ability to solve the clients’ business tasks but not to the technical properties of solutions.

<sup>1</sup> See “Main Tendencies in the ILDP on the Russian Market” research for more information.

Changes, and first of all, the “economic” approach introduction on the given market will provoke the situation when many IT companies being oriented only at technologic solutions will not be able to timely and completely meet the demands of clients who have by this time realized the necessity of new approaches to business conduction.

This may result in reduction of the number of companies able to render services in demand, and in emergence of new companies oriented exactly at the “process” approach and rendering type services. Moreover, in the result of market changes an increase in consulting companies share as well as in companies rendering type services is expected.

For the last few years a number of “major” and “medium-size” integrators have offered their type services, “box services”, to the market. This approach was recognized among IS specialists as it is based on standards and policies already approbated on the world market. As long as the IS market tends to IS creation on the basis of standards and policies, the type services which particularly allow for accurate forecast of the results of prospective implementation and use are gaining vast acceptance.

However if within the integrator companies segment business demonstrates successful development, the Russian IS producers segment is faced with a crisis which commenced long before the economic crisis.

Russian producers of IS services may be conventionally split in two unequal groups. The first group includes a small portion of companies attempting to establish business using the best world practices. This means that the IS services development is performed within the frames of standards which include modern product: management, optimal testing and subsequent technical support. What is more, these companies organize their activity according to the classic pattern “vendor – partner (distributor, re-seller, and integrator) – client”. The companies of this group orient their products at the mass market. The following companies fall within this group:

**Table 3. List (alphabetic) of major Russian vendors**

| Name of the vendor company |
|----------------------------|
| Dr.Web                     |

---

InfoWatch

---

Positive Technologies

---

SecurIT

---

Infotechs

---

Kod Bezopasnosty

---

KriptoPro

---

Kaspersky Lab

---

C-Terra CSP

---

*Source: LETA IT-company*

The second group includes numerous developers of Information Security services oriented at fulfillment of the state regulators requirements. Such companies possess decent technologies but they are “dragging” Russian development downwards, to nowhere.

Developments of the second group’s companies could not gain a sufficient market share for a great while. Producers lacked the necessary promotion resources (financial and organizational). It should be mentioned, as well, that frequently the functionality of domestic solutions was worse than that of foreign analogues.

Domestic solutions shared a common advantage, they were certified both with the FSTEC of Russia and the FSS of Russia. It was not considered essential as with some exception companies could freely apply foreign uncertified products, and, in case of urgency, particular lots of foreign network security products were subject to certification.

Consequently, the market was split: foreign services or products of the first group’s companies were used to actually secure the market; and products of the second group’s companies – to fulfill the regulators’ requirements.

As a result, being oriented at a narrow market strip but not at the mass user, domestic developers created products of limited functionality, difficult to be implemented in a large-scale. Such products are characterized by deficient description and lack of decent technical support.

But the situation could have changed with the introduction of the first version of the FSTEC of Russia documentation on personal data protection. According to the stated requirements, companies had to use mainly certified products of Russian production. As a result, products of the second group's companies reached the mass market, but since they were not adapted to it the majority of them were not demanded.

The software producers hoped that, motivated by the necessity to fulfill the FSTEC of Russia requirements, consumers will be forced to buy their products. And indeed, there was a heavy increase of interest towards them. Herewith, the producers did not take any effort to enhance the quality of their products (basically, consumers were unsatisfied with non-compatibility of such products with other systems) or support level. Many adopted the principle "take what is given; all the same there is nothing else".

Such policy resulted in mass rejection of such products by the market. This was the reason for the most personal data operators to claim introduction of changes into the documentation of the FSTEC of Russia, which would allow them to use other developments. Simultaneously, Russian producers experienced one more shock. Western vendors learnt to license their production. A good example was set by ESET and Stonesoft companies. As a result, many companies lost their advantage and devolved to the narrowest niche – security of systems under state secret or any other systems requiring complex certification.

Devolving to narrow niches may practically "kill" such producers as work in the niche does not presuppose considerable money flows essential for the product development.

Another problem for a great deal of Russian producers of Information Security products is that they launch mono-products or structure their policy around their lead product. This scheme was popular with western producers a decade ago but presently they follow absolutely different policy. Leading vendors strive to suggest a maximally possible extended choice, including buying external developers. Basically, Russian companies are in a different cycle, which in short and mid term perspective may prevent them from competing with foreign producers.

As far as government orders are concerned, they can be quite substantial. The tender held by the Ministry of Internal Affairs in 2009 (RUB 210.35 mln.) may be set as example. But such events are rather sporadic and could not be taken as basis for the long term strategy development.

As the case stands, a merger could be the solution for many Russian vendors. There are several companies in Russia which could become centers of producers' consolidation. To begin with, it would be "GK Informzaschita", "Kaspersky laboratory", "Infortechs" and "KriptPro". Some companies are known for attempts to become a core for consolidation of independent producers, but there have not been considerable breakthroughs still. If in years to come Russian vendors fail to find internal resources to establish major companies, including by M&A, the Russian market will be taken over by western companies.

## Security Threats in 2009 – 2010

### Software Exposures

After a certain “stagnancy” in the area of detection of “critical” level exposures, characteristic of 2008, the second half-year of 2009 and beginning of 2010 were notorious for a whole bunch of a problems typical practically for all developers occupying a considerable share in the area of customer software.

For the most part the revealed critical exposures refer to the attacks of “buffer overflow”, “integer overflow” and “insecure transformation of indicators”. The aim is practically always execution of the malicious code embedded into the processed object, and, as a result, obtaining account privileges on behalf of which the attacked software is run.

In 2009 lists of critical exposures included:

- a range of Adobe company’s software intended both for PDF-documents imaging and multimedia content reproducing (at the very least, twice for the last year major computer security research centers issued recommendations to completely prohibit processing unreliable PDF-documents until upgrade removing the exposure, which is an extremely grave factor both for the format gaining such major distribution and for its developer);
- office package of Microsoft company which several times (including once for all of the Microsoft Office line from 2000 to 2007) over the last year suffered from exposures, permitting to execute the malicious code included into non-reliable DOC, XLS and PPT documents due to errors on the stage of its analysis;
- integrated applications of Microsoft Windows operating system (system procedures of graphic format imaging, execution of .NET-code, analysis of URL-links, elements of video files decoding); herewith it is a matter of concern that new generation of operating systems by Microsoft company (Vista/2008) introduces new (not previously involved, for instance, in Windows XP) exposures in such seemingly thoroughly worked out procedures as provision of access to general files and printers in the local network or TCP/IP protocol stack.

- Java Virtual Machine (JRE) and therein integrated Java Web Start (JWS) technology intended for downloading of fully functional Java-applications from the network and their launching on a computer outside browser process; herewith, one of the JWS exposures is paradigmatic: nucleus developers foresaw the possibility (and more likely – for the purposes of testing and debugging) to replace (by start-up parameters) the library executing virtual machine functions specifying full path to the alternative library, and programmers responsible for JWS implementation as such for operating systems of Windows and Linux families failed to attend the data parameters filtering during start-up; as a result, intruders gained the possibility to force the JWS nucleus to download and execute with high privileges in the system any library, including those potentially incorporating a malicious code;
- Apple QuickTime video decoding components which, as a result of integers processing error, permit to execute buffer overflow with the subsequent execution of malicious code imbedded into the processed file.

For the last year the situation with web-browsers exposures has not changed practically at all, disregarding the fact that security of utilization is positioned as the most priority trend in advertising campaigns of almost every representative of the given class software. Exposures lists still include the most popular browsers and still, according to the authors, the most active policy aimed at the revealed exposures removal is pursued by Mozilla Firefox developers.

This year Microsoft Company, to its honour, offered an open support to the movement (initially spontaneously established by the developers) on informing the users' community on the drawbacks of the off-market Internet Explorer 6 browser. At the present time the majority of exposures revealed within browsers of this company falls within the share of still officially supported 6<sup>th</sup> version (throughout the estimates, its share makes from 15% to 20% of the total volume of worldwide used browsers). However, last year the latest 8<sup>th</sup> version was also exposure "noted", permitting execution of random code on a PC, having visited a malicious web-site.

A particular attention should be drawn to the exposure of automatic search service and wireless network adjustment within the OS Microsoft Windows

Vista/2008. This exposure is realizable if the intruder has a possibility to install a false access point within the radio-availability range of WiFi-network of the system being attacked and formation of malformed utility packages with its software. The attack result, which is not influenced by user's activity (and can be executed in the absence of the latter), manifest itself in buffer overflow and execution of malicious code on the attacked system. In practice attack may be performed from outside of the physical perimeter of the company security.

The previously registered growth tendency of the researchers' interest to errors and exposures of security facilities themselves remained in the last year as well. Methods of inactivation or partial denial of servicing (DoS) were published as regards program products of several firewall producers and virtual private networks (including, one of the leaders of the given market - Cisco Systems Company). Instantaneously several known antivirus program products and spam-filters appeared to be exposed at the stage of analyzed files processing (spam-filters – particularly at the stage of letter headings processing).

## Distribution Vectors

Vectors of malicious code distribution remained practically unchanged:

- malicious code distribution on "own" web-sites with potential victims somehow allured to make visits;
- hacking of popular (usually thematic) web-sites and forums for the purpose of supplementing their home pages with unfeatured harmful inserts.
- distribution both of code and links thereto by mail, ICQ and especially by blogs and social networks which are meanwhile steadily taking leading positions as per users activity;
- fraudulence with dead windows of antivirus activity, false requirements of the installed software activation or accounts on game servers, blog servers and social networks;
- remote use exposure;
- autoplay on removable media.

Despite the fact that the majority of exposures revealed last year were officially removed by the producers before the publication of technical details of exposure on open access, the scale of virus epidemics, using already closed exposures, and even exposures of 2 or 3 years old astonish with their extent. Thus, hither to as of spring 2010 the share of Conficker (Kido) virus using exposure removed by the Microsoft Company in October 2008 is within the limits of 6-9% out of all invasions registered by the antivirus companies.

## Intruders' Goals

The most evident growth is recently demonstrated by two major trends of malicious activity – expressed extortion of small amounts of money and establishment of accounts data bases (both with and without authentication information) for subsequent sale.

### *Extortion and fraud*

Viruses executing various desktop interlocks demanding acquisition of the release code by SMS became so common that presently any user working in the Internet is aware of them either judging by their own experience or by the talks of acquaintances. Practically universally in order to “strengthen the effect” the locked screen is accompanied by messages and photographs as though evidencing the fact of the victim visiting sites of frivolous and sometimes of explicit criminal content. This stimulates a PC user, especially in office environment, to try to “resolve the situation” by means of paying a small money amount rather than involve computer specialists and attention of management.

Certainly, such additional physiologic impact plays into the intruder’s hands, but apart from that, and which is much more dangerous for organizations, – it stimulates to conceal the incident of the information security breach by an employee. Moreover, in the long-term perspective the successful pay back option creates one more threat for the organization’s information security. First of all, it engrains the personnel with the false confidence that certain security incidents do not mandatory require consideration from the Information Security specialists, and, secondly, nudges to the attempts to resolve any contingency situation on the working computer in private capacity, without notification of management and IT or security services.

Approximately the same path, though differing in incentives, is followed by viruses and Trojan Horse software making phishing attacks on popular sites according to the following pattern. During a regular attempt to enter a web-site actively used by user, for example, any social network or free on-line game, browser displays an interface precisely reproducing the target with the message that the visits to the server became chargeable and in order to activate the account it is required to send an SMS of a moderate cost at the specified short number.

### *Databases of network users*

The black market of the databases of network users has confidently taken its position in the unauthorized access area. The approximate cost of such information for the time being, to the extent covering domestic users, is presented in the table:

**Table 4. Cost of Databases**

| Information Type                                               | Approximate cost | Units of measurement |
|----------------------------------------------------------------|------------------|----------------------|
| <b>Account data (with authentication information)</b>          |                  |                      |
| Yandex-Money, WebMoney (depending on account balances)         | RUB 500 – 3000   | for 1 pc             |
| Skype (depending on account balances)                          | RUB 100 – 300    | for 1 pc             |
| Bank (plastic) cards (with codes for Internet purchases)       | RUB 100 – 200    | for 1 pc             |
| Bank (plastic) cards                                           | RUB 50 – 100     | for 1 pc             |
| Scanned copies of citizens' passports                          | RUB 20 – 60      | for 1 pc             |
| "Voices" of the social network VKontakte                       | RUB 3            | for 1 pc             |
| VKontakte accounts                                             | RUB 700 – 1000   | for 1000 pcs         |
| Mail boxes of the mail.ru server                               | RUB 150 – 250    | for 1000 pcs         |
| <b>Lists without account data (for mailing, spam and etc.)</b> |                  |                      |
| Cell numbers                                                   | RUB 20 – 50      | for 1000 pcs         |
| Postal addresses (depending on the subject relevance)          | RUB 5 – 20       | for 1000 pcs         |
| ICQ numbers                                                    | RUB 5 – 10       | for 1000 pcs         |

Source: LETA IT-company

### *Other goals*

Trojan Horse software oriented at bank details theft (Client-Bank, Internet-Bank and similar systems) is demonstrating the increasing activity and variety of goals. At the beginning of this year one of the leading developers of domestic bank systems warned users on the discovery of a virus code within the network which was capable of targeted theft of the keys used to perform exchange with the bank unless their protection involves the use of hardware means (tokens). Moreover, even with tokens the threat of remote desktop management (and the similar functionality is becoming a norm for the existing Trojan Horse software) may be manually implemented by the intruder with the intent of money assets transfer.

The share of intentional and unintentional impacts on organizations' IT assets from the employees is still rather high. Discontented with the forthcoming dismissals, redundancy and sometimes with simple working relations, the employees:

- Copy internal documents and databases for a "rainy day";
- Destroy or damage information assets components;
- Develop and introduce back enters for remote management of computers after dismissal;
- In certain cases install script-bookmarks triggering destruction or distortion of data in a particular period of time.

The risk of similar actions is particularly high from the IT specialists, thoroughly knowing the organization infrastructure and its vulnerable areas.

## Conclusions

The analysis of the publically available portion of the exploited exposures leads to unpromising conclusion that software development technology, both in corporate and user segments for commercial and open-source products, presently failed to reach the required level of quality and code security. Practically none of the program products may be secured against exposures becoming real threats in certain circumstances.

In such a situation only a multilevel complex of both proactive and reactive measures may help organizations to lower risks, arising due to business processes automation, to the acceptable level.

Amidst the proactive measures conferring the best figures of the "expenses/results" correlation with due consideration of modern specific nature of attacks on the information systems, it is possible to differentiate:

- Forced, urgent and controlled policy of software upgrading (including microcode within hardware);
- aggressive filtration and screening of incoming and outgoing information flows, and primarily – WWW traffic and e-mail;
- minimization policy for certain users' rights both within the workstation and within corporate information system for the purpose of potential losses reductions in case of Information Security threats realization.
- Amidst the reactive measure it possible to mention:
- policy of reliable and complete logging and monitoring of activity of users and systems, meaningful for business processes;
- thorough qualified incidents analysis in the filed of Information Security for the purpose not only to eliminate the incident and threat consequences, causing the possibility of their realization; but to find conceptual drawbacks on the stages of design, implementation and support of projects and provision of their information security.

Generally, the implacably increasing qualification (more often due to increased focus) of the developers of malicious codes and fraudulent schemes, on the one part, and readiness of the criminal market to use the results of their developments, on the other part, form a high threat level in the area of IT

security. This fact, in its turn, obviously require from organizations to take security measures in the Information Security area in order to secure the integrity and continuity of their business.

# Development of the Information Security Market Management

## № 152-FZ “On Persona Data” – Works Commencement

Actual works on personal data protection were segregated from the Information Security consulting works range into a separate trend comparatively a short time ago. Quite for an extensive period after the enforcement of No. 152-FZ “On Personal Data” the given trend has not been considered to be a prospective one. Information Security experts opinions differed and the majority viewed works on personal data security primarily as one of the all sorts of compliance services types such as bringing into compliance with the Standard 27001, PCI DSS, STO BR IBBS and etc. However the practice proved that the number of the initiated projects on personal data protection exceeded the number of projects, concerning all other compliance service taken as a whole!

The beginning of 2009 was characterized by a slight information crisis in the area of personal data protection. It stood to reason that something was to be done, but methods fell far beyond public comprehension. Primarily it was associated with the fact, that the regulatory documents of the FSTEC of Russia on personal data protection, the so-called “Tetratouch”, were classified as DSP (for administrative use). For another thing, it was bruited about that these documents were not ad infinitum approved by the FSTEC of Russia and the DSP label would be removed after official approval. There were even examples set that at different times personal data operators received different versions of the “Tetratouch” against official requests to the FSTEC. All that facilitated such an event as “deferred demand” when personal data operators did not hurry to by all means launch the “right now” projects having decided to wait for the final and clear requirements form the part of regulators.

Nevertheless the tendency remained unchanged – the demand on personal data protection started to gather pace. What was it associated with? First of all with the fact that No. 152-FZ “On Personal Data”, contrary to all other compliance in the Information Security area, was binding for any legal body working on the territory of the Russian Federation. Naturally, none of the personal data

operators wanted to be sanctioned by Roskomnadzor, FSTEC of Russia and FSS of Russia and it was the very risk that provoked the increase in demand for similar services.

By the end of second – beginning of the third quarter of 2009 the demand was so high that many IT and Information Security integrators decided to expand the regular office staff of their specialists on personal data protection. Never before had an Information Security specialist having working experience in personal data protection enjoyed such freedom of choice on the labour market. Everyone needed the ample quantity of specialists. To some extent the given tendency somewhat corrected the compensatory cover funds of such specialists having brought wages to the pre-crisis level. Concurrently, the problems of personal data protection started to receive wide coverage during events associated with information security. Eventually, market started to treat this direction pretty much as the primary Information Security concern for the next year or year and a half.

Associations, representing interests of various activity branches, were not on the slab-heap of the process. For good reasons, the representatives of banking branch were the first. It was exactly the time when the Association of Russian Banks began assuming its right place suggesting amendments into the STO BR IBBS standard in the part, related to personal data protection. In this connection the given initiative was met by the banking branch representatives as the most acceptable and convenient. The essence of the initiative conferred legal confirmation of the provisions wherein the bank branch organizations, introducing the new version of the STO BR IBBS standard, would automatically cover the requirements on personal data protection. In practice this would mean that the transformation of recommendatory STO BR IBBS standard into mandatory. Moreover, the bank community representatives were not at all pleased with the prospect of two more bank regulators emergence (Roskomnadzor and FSTEC of Russia). By the way, this initiative is presently approaching its logical completion (there is only an interdepartmental order confirming the initiative to be coordinated and signed).

The critically significant fact within the planned development of demand for services on personal data protection was the ability of the companies, offering such services, to model the proper pricing in such a manner which stabilized the market by the middle of the second – beginning of the third quarter of 2009.

Offers to “do nobody knows what for big money” ceased to appear. I.e., prices for consulting services on personal data protection became adequate and reasonable.

The previously mentioned “deferred demand” for personal data protection services started to be implemented to the full extent at the beginning of the fourth quarter of 2009. That was the period when almost all specialized integrators experienced lack of proper resources for implementation of such a number of projects. It was bruited about long queues formed by personal data operators willing to launch a project with particular integrators. In this connection a great many of non-core companies, providers of personal data protection services, have appeared, which mildly reduced the tension as related to demand but also affected the quality of the services rendering. Nevertheless, it was exactly the fourth quarter of 2009 which became peaking in terms of demand. It was then when the majority of contracts on personal data protection were concluded.

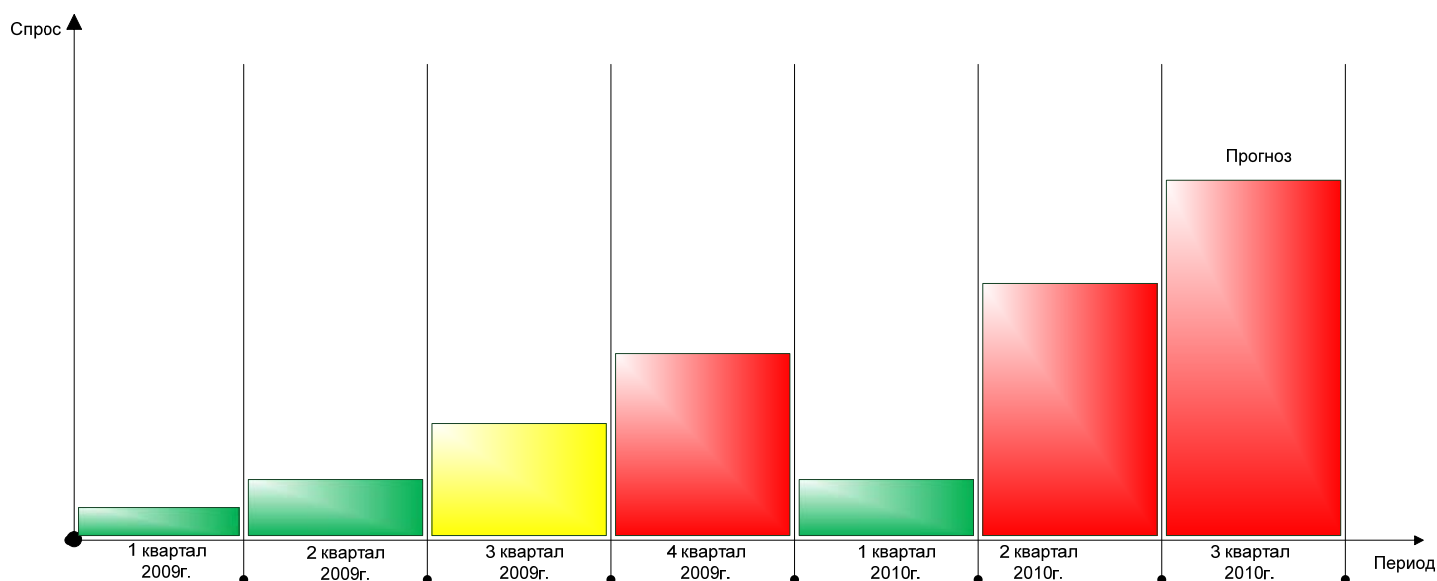
It is impossible not to mention one of the landmarks of the beginning of the fourth quarter of 2009 – parliamentary hearings on the topic “Actual Issues of Development and Application of Legislation on Protection of Citizens’ Rights while Processing Personal Data” which were held in the State Duma on September 20, 2009. The basic goal of this event was to analyze if the existing situation in the area of personal data protection. Therewith, positions of the personal data operators’ representatives, facing problems while fulfilling legislative requirements in the area of personal data protection, were announced. It was during this event when the offers to adjourn the 01.01.2010 term (according to No. 152-FZ “On Persona Data”, companies had to bring their personal data information systems into compliance with the legislative requirements by this term) were first announced. In this connection the given term was proposed to be adjourned for a year or even for three. And it happened. At the end of the fourth quarter of 2009 the above-mentioned term was adjourned for one year and then the deadline is 01.01.2011. Many personal data operators will feel relieved as there is no more need to hurry.

The beginning of 2010 was much more tranquil. Long January holidays coupled with deadline adjourning for the period of one year caused the downswing of demand for personal data protection services. But not for long. This time news came from the regulators’ part – from the FSTEC of Russia. At the beginning of

2010 it was the very agency to officially remove the DSP label from the regulatory documents. And a little later there came the order No. 58 of the FSTEC of Russia and decision of the FSTEC of Russia. The essence of these events resolves itself into the mitigation of requirements set forth to the operators as related to personal data protection. The FSTEC of Russia abolished two of its documents from the "Tetratouch", having replaced them with the order No. 58. Probably, in the first instance it was consequential to the pressure from the part of personal data operators. And, as a parenthetical note, many prevailing requirements were actually superfluous and financially unreasonable. Anyway, these events influenced the increase in the demand for personal data protection services to the level of the fourth quarter of 2009.

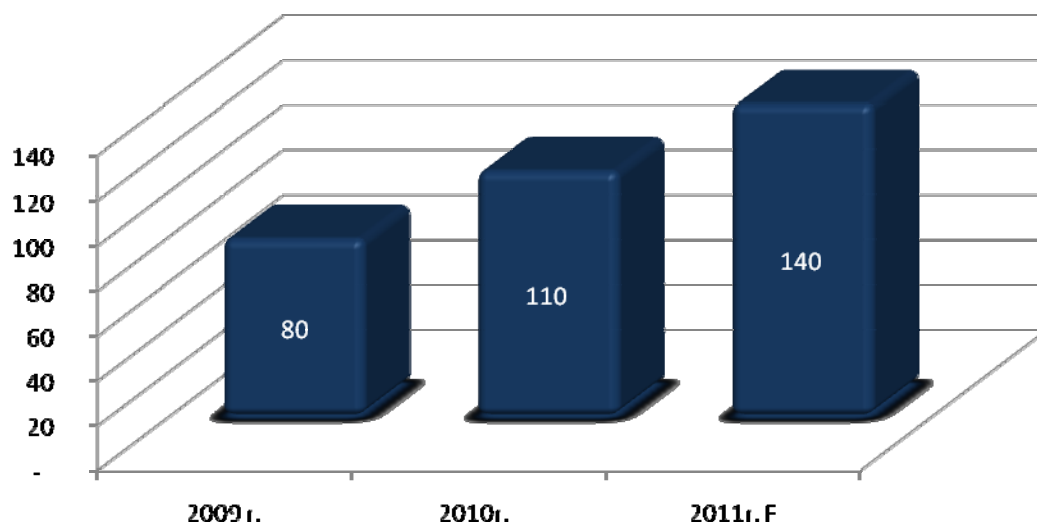
The second quarter of 2010, judging by demand, has completely overlapped the fourth quarter of 2009, and even partially exceeded the results thereof. On the one part, it was determined by the mitigations of requirements, and on the other – many operators who failed to launch projects in 2009 nudged their activity in the stated period. Thus, the increase in demand for personal data protection services in 2010, which is observed on the market, is the continuation of the tendency initiated in 2009. But there is one considerable difference: the number of the projects initiated in 2010 promises to be by far as high. If we picture the demand indicator graphically, we will get the following diagram:

**Figure 6. Diagram of the Initiated Personal Data Protection Projects Number Increase**



Source: LETA IT-company

**Figure 7. Growth of Russian Organizations' Expenses on Information Security  
Personal Data Protection, \$mln**



Source: LETA IT-company

At the present time, various opinions, concerning the development of demand for personal data protection services in 2011, are expressed. But these are plain speculations, and it is only possible to positively state that demand for such services in 2010 will grow.

## Standard of the Bank of Russia

A powerful impetus was given to the branch standard of the Bank of Russia on information security. Basically, it was associated with emergence of requirements on personal data protection within the revised draft of STO BR IBBS. Works on search of solutions on credit organizations compliance with the requirements of 152-FZ were started in spring of 2009. There was not an obvious solution. Within the frames of several working groups of the Association of Russian Banks, the work on preparation of amendments to 152-FZ and adaptation of STO BR IBBS was commenced.

In less then a year of active work the existing documents were completed with simultaneous development of brand new documentation. Draft documents of new version of the standard are available at the web-site of the Association of Russian banks: <http://www.arb.ru/forums/conf152FZ/2/docs.php>.

New documents were introduced into the BR IBBS complex:

- Branch private model of security threats of personal data during their processing in personal data information systems of organizations within the bank system of the Russian Federation;
- Requirements on personal data security provision in personal data systems of organizations within the bank system of the Russian Federation.

And methodical documents:

- Recommendations on legislative requirements execution during processing of personal data in organizations within bank system of the Russian Federation.

In their essence the documents explain debatable provisions of the federal legislation, governmental regulations and regulators' requirements, and provide methodical recommendations on adequate PDIS establishment.

All documents are complaint with the order No. 58 of the FSTEC and ISO standard on personal data protection which was developed basing on ISO/IEC 27002-2005.

It is noteworthy that the suggested methodic recommendations include provisions which significantly simplify the process of bringing personal data information systems (PDIS) in compliance with the regulators' requirements. For example, the provision stating that not all automated systems, processing personal data, may be considered PDIS, but only those which intent presupposes personal data processing. In compliance with this provision, for example, Automated Bank Systems shall not be considered PDIS conferring all the resulting positive consequences for personal data operators.

Currently (spring 2010) a new version of the standard is not coordinated with the regulators in the area of personal data protection (Roskomnadzor, FSTEC, FSS). Should the new version of the standard be coordinated and the requirements thereof be recognized sufficient in terms of 152-FZ requirements and regulators' requirements fulfillment, the bank community will receive adequate and branch-adapted documents allowing to perform works on personal data protection within the scope of STO BR IBBS.

Upon the coordination completion, a procedure of incorporation of self-regulating organizations (SRO) will be initiated. This structure is qualified to discharge functions of civil regulator organization with tasks including regulation of rights protection of personal data subjects within the scope of organization joining its membership. The admittance card to this organization will be the introduction of the whole of the mandatory STO BR IBBS documentation system. The thing is that all standards in the Russian Federation are of recommendatory character and may become mandatory only if introduced by internal orders of mandatory execution.

In this particular case recognition of the mandatory execution of STO BR IBBS enables a crediting organization to considerably cut the problems associated with PDIS establishment and simultaneously launch the process of bringing into compliance with the recognized branch standard.

We anticipate that the fact of adoption of this new version of STO BR IBBS by the personal data regulators will considerably increase the number of credit organizations, initiating works on information security provision in compliance with the given standard. As a result, the standard of the Bank of Russia will become de facto mandatory and its mass implementation will commence which is supposed to cause the increase in consulting services on the Information

Security market as well as the Information Security expenditures. According to our estimates, from 2011 to 2013, banks will spend more than \$60 mln. on the standard's requirements implementation. Besides, the successful start of this standard will undoubtedly strengthen the tendency of other branch standards development.

## **Development of Information Security Management Systems Implementation**

In 2009 the condition of the Information Security management systems market in compliance with the requirements of ISO 27001:2005 changed considerably. If earlier systems implementation in a greater degree pursued the goal of marketing benefits for the company, the last year crisis introduced its correctives: the markets shifted to implementation and realization of systems being only of "vital importance" for business.

After more than 5 years following the moment of the first implementation of ISMS in compliance with ISO 27001:2005 in Russia, last year demonstrated a substantial growth of the general level of Information Security management principles comprehension, which found its reflection in numerous requests for complex IS systems establishments. Practically every tender request for complex IS provisioning included requirements for IS management systems implementation alongside with technical subsystems, and in compliance with ISO 27001:2005.

The year of 2009 has evidently defined the limits and approaches towards implementation of management systems by reference to actual demand of IS provisioning and compliance certificates acquisition. In 2009 the certificate was issued and prolonged to the market companies for the business of which it was really crucial to have the international certificate ISO 27001:2005. Concurrently with that the Russian market arena of certified companies lost those participants for the business of which maintaining of certification became unprofitable from the point of view of certification expenditures. The crisis, acting as natural selection, preserved the most essential company qualities from the point of view of market survival; those irrelevant for survival were eliminated.

Last year demonstrated that ISMS, being an integral complex of processes, turned out to be less in demand than its separate elements. The fully specified system introduction became unprofitable from the economic point of view which led to fragmentary implementation of distinct management elements: risk management systems, incident managements systems, awareness enhancement systems, efficiency management of the implemented IS solutions.

The Act 152-FZ introduced its changes as well. The last quarter of 2009 – the first quarter of 2010 was marked by rather complicated requests for ISMS realizations not only in compliance with the international standard but with simultaneous consideration of the requirements No. 152-FZ.

**Table 5. Certified ISMS as of the beginning of 2010**

| Company                        | Auditor                      | Standard           |
|--------------------------------|------------------------------|--------------------|
| 1 Bank24.ru, Ekaterinburg      | Bureau Veritas Certification | ISO/IEC 27001:2005 |
| 2 CMA Small Systems AB         | BSI                          | BS 7799-2:2002     |
| 3 CROC Incorporated, Moscow    | BSI                          | ISO/IEC 27001:2005 |
| 4 Lukoil-Inform, LLC           | BSI                          | ISO/IEC 27001:2005 |
| 5 Luxsoft, Moscow              | LRQA                         | ISO/IEC 27001:2005 |
| 6 Multiregional TransitTelecom | BSI                          | ISO/IEC 27001:2005 |
| 7 Rosno, SC                    | BSI                          | ISO/IEC 27001:2005 |
| 8 TransTeleCom                 | SGS                          | ISO/IEC 27001:2005 |
| 9 LANIT, CSC                   | BSI                          | ISO/IEC 27001:2005 |
| 10 Rutenia, JSC                | BSI                          | ISO/IEC 27001:2005 |
| 11 M-City                      | BSI                          | ISO/IEC 27001:2005 |
| 12 CBI                         | BSI                          | ISO/IEC 27001:2005 |
| 13 CB, Renaissance Capital     | BSI                          | ISO/IEC 27001:2005 |
| 14 BTA Bank                    | BSI                          | ISO/IEC 27001:2005 |
| 15 IBS DataFort                | LRQA                         | ISO/IEC 27001:2005 |
| 16 HandyBank                   | VNIIS                        | ISO/IEC 27001:2005 |

*Source: International Register of ISMS Certificates*

The majority of companies in the Russian Federation and Commonwealth of Independent States retain their loyalty towards the BSI MS brand.

Being a leader of Russian certification market, BSI MS dictates new modern trends for 2010. Right now we observe emergence of new bunch of trends on the following topics:

- Information security risks management in compliance with the recommendation of the international standard ISO/IEC 27005;
- Provision of IT and communications continuity in compliance with the recommendations of British standard BS 25777, particularly within the scope of financial organizations from the point of view of 242-P implementation;
- Organization risks management. Standard BS 31100;
- Products certification in compliance with EU Directives and etc.

For the time being the market awakening is observed, both in terms of preparation for certification and actual information security organization in compliance with ISO 27001:2005. Presently more and more companies come to conclusion that it is better to implement the ISMS from "below", first having established a base of processes of IS provision (assets management, management of exposures, changes, incidents), and following these processes establishment within the company – to proceed with the fully-featured IS risk analysis implementation.

In 2010 this approach is likely to gather pace as many companies having implemented risks analysis without concurrent IS process have realized by their own bitter experience that risks analysis lacking actual information on threats, exposures, incidents and all changes in business environment has no practical importance neither for IS nor for the company business in general.

In 2010 a still greater demand is likely to be observed with respect to the management processes automation and organization of fully-featured integration of the already available IS services for the purpose of acquisition of practical mechanisms of IS management. In particular, this is evidenced by the market outcome and gradual distribution of new program technologies on IS management and solutions on their mutual integration. Presently the similar solutions are offered by the major vendors on the IS market. The first step of creation of process-thematic model of IS management presupposes compiling

and analysis of configuration management database (CMDB – configuration management database) containing description of such company resources as software, technical aids, employees and procedures.

The increasing demand for system integration and selection of the appropriate approach with respect to ISMS implementation provoked the recent issuance of the new standard ISO / IEC 27003:2010 "Information Technology. Information Security Management System Implementation Guidance". Application of this standard in 2010 will disallow a number of questions on ISMS implementation. ISO/IEC 27003:2010 covers the ISMS process from the production beginning until implementation, the way of development and planning of ISMS project.

However, direct use of models and standards of ISO/IEC 27001 and ISO/IEC 17799:2005 for the purpose of ISMS establishment is rather complicated. They are too much concretized, and usually every organization has its own set system of processes, roles, administrative regulatory orders of information security, which are to be integrated into the IS management system. Herewith, the priorities, the so-called "directive weights" which are applied in audit standards, are not defined. Otherwise, they are to the contrary very much general. For example, standards contain either a set of control directives or a general approach to management systems, that is, stipulate the issue to be done but not the methods.

The year of 2010 will be as well oriented at integration of principles of ISO 27001:2005 and recommendations of, in particular ITIL (Information Technology Infrastructure Library, the library of the best world practices concerning IT service work organization) being widespread among Russian companies. This necessity is also motivated by the fact that there is a great number of companies on the Russian market, where information security departments are included into IT departments.

# Development of Particular Segments of Technical Protection Aids

## Peculiarities of Certified Aids Use for Personal Data Protection

Sufficient time elapsed from the date of the Federal Act No. 152-FZ "On Personal Data" and the so-called "Tetratouch" issuance so that operators, processing personal data, and system integrators could to the fullest extent analyze the given documents and develop necessary methodology on personal data protection organization.

The majority of provisions of No. 152-FZ stipulate execution of namely technical requirements on personal data protection. It is noteworthy that a number of operators have already established a personal data protection system in compliance with the stated requirements. System integrators, in their turn, have defined a certain "basket" of basic technical aids of information protection, which cover the necessary requirements of the regulatory authorities for personal data protection.

The existing provisions were rough enough, and at the beginning of 2010 certain changes concerning personal data protection projects took place:

February 05, 2010, the order No. 58 of the FSTEC of Russia "On Approval of Regulation of Methods and Means of Information Protection within Personal Data Information Systems";

March 05, 2010, publication of the decision of the FSTEC of Russia according to which the two methodical documents of the FSTEC of Russia, included in the old version of the "Tetratouch", were abolished: "Recommendations on Personal Data Security Provision during their Processing within Personal Data Information Systems" and "Basic Measures on Establishment and Technical Support of Personal Data Security while Processed within Personal data Information Systems".

Any volunteer having decided to study the order No. 58 and Supplement thereto will immediately read the following: "This Regulation does not touch

upon issues of personal data security provision as referred according to the established procedure to the data classified as state secret, and issues of application of cryptographical methods and means of information protection.”

And there is nothing to be surprised at – cryptography has always been, is and will be the patrimony of the FSS of Russia. That is why, while choosing aids involving cryptography (for example, when establishing a communication link providing the transferred information protection), operators or system integrators will have to use the regulatory documents of the FSS of Russia.

Concerning application of certified aids of information protection and according to the new Regulation, the use of Information Protection Aids (IPA) subjected to compliance assessment with respect to the absence of the non-declared options (NDO) is mandatory only for Class K1 personal data information systems (PDIS). For PDSI of other classes the use of IPA, subjected to the stated compliance certification type, is not mandatory and is left to the operator’s discretion.

Everything is more or less clear with Class K1. As for the PDIS of Class K2 or K3, according to the order No. 58, the protection aids shall pass established compliance assessment procedure. According to the Federal Law “On Technical Management”, three types of assessment exist:

- mandatory certification;
- voluntary certification;
- declaration of compliance.

According to the Regulation and order No. 85, operator, processing personal data of Classes K2 and K3, may use any IPA certified by the FSTEC of Russia on TC, which considerably extends the IPA choice options. Nevertheless, in the context of choosing the IPA, it is essential to consider the requirements described in Annex 1 to the Regulation on methods and means of information protection within personal data information systems.

In short, this idea may be expressed as follows: should any protection aid be claimed for personal data protection within the systems of Classes K2 and K3, it should have the certificate attesting the fact that the stated aid is capable of execution of the very necessary functions being claimed.

This actually facilitates the choice and extends the technical aids list which may be used while establishing personal data protection systems.

## Antivirus Market

Antivirus market is traditionally the largest segment within the information security market. Russian and international vendors strive to take leadership of exactly this segment.

But unfortunately there are no reliable data on antivirus tool sales. The situation persisted in 2009 too. Intense competition between vendors leads to companies using their own sales statistics as a method of controlling, that is why it is impossible to trust implicitly the published data on sales volumes.

To a large extent it is explained by the Russian market peculiarity, particularly by the existence of major domestic vendors. While western companies cooperate with research organizations and, as public companies, disclose their data, domestic companies for a long time have tried not to disclose their sales statistics to the full extent, that is why many controversies can be easily traced in the published data.

However, the situation is gradually beginning to change. At the beginning of 2010 the key players of the Russian market presented reports that more adequately reflect the actual figures and correlate with other resources, such as distributors' data and polls carried out by various sociologic companies, methodology used by LETA company in the previous research.

Having compared various resources it becomes possible to determine that the AVT market volume in Russia in 2009 reached \$195 mln., and in 2008 – \$175 mln.

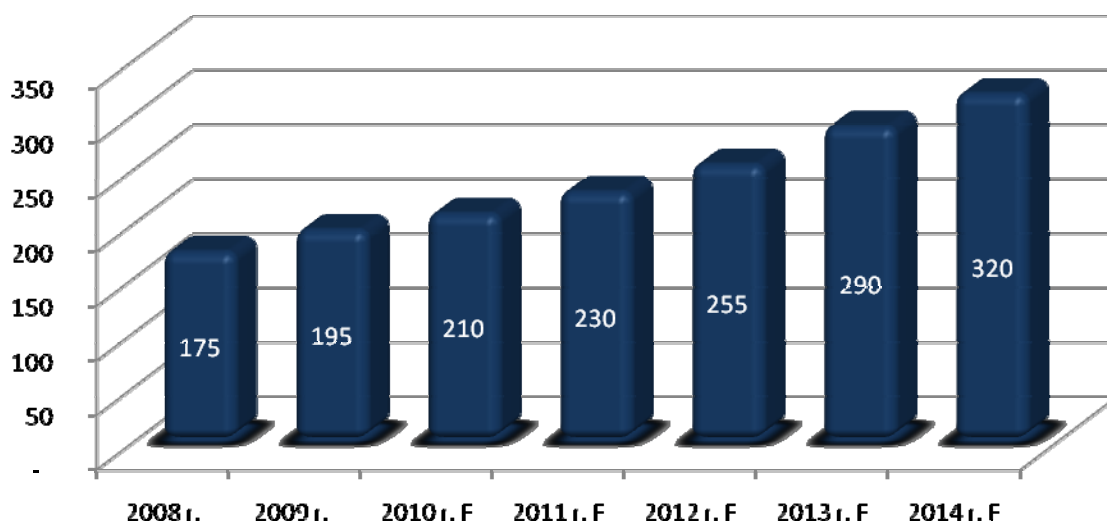
Notwithstanding various estimates, it possible to distinguish three leaders with respect to the sold licenses.

**Table 6. Three Leaders on the Antivirus Market**

|                      |
|----------------------|
| Kaspersky Laboratory |
| ESET                 |
| Symantec             |

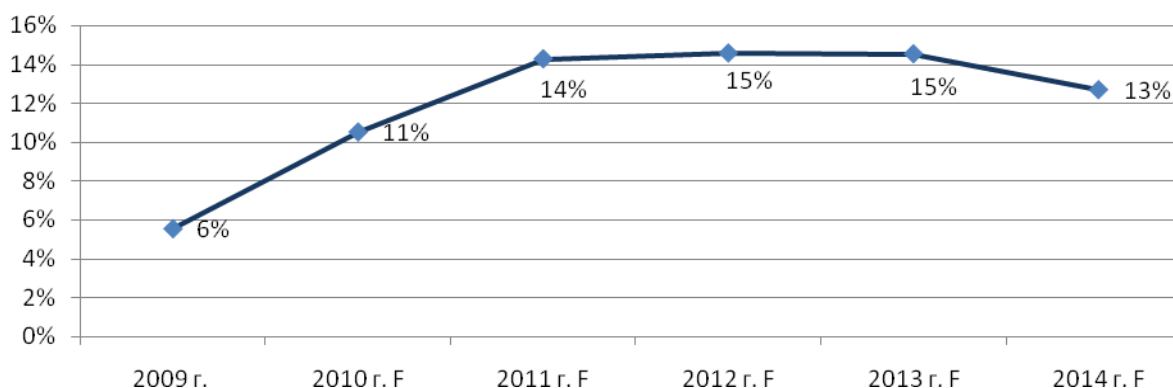
Source: LETA IT-company

**Figure 8. Market Growth of Antivirus, \$mln**



Source: LETA IT-company

**Figure 9. Growth Ratio of Antivirus Market, %**



Source: LETA IT-company

According to LETA IT-company's estimates, 2009 was not marked by any considerable redistribution of vendors' shares. The leadership is held by Kaspersky Laboratory, market share of this company has not changed for the past year. ESET comes in definite second and increases its share basically due to the follow up players.

In the forthcoming years there is a likelihood of struggle for leadership within this market.

In terms of crisis the Antivirus Market was supported by several factors:

1. Retail. However paradoxical it may seem, but it was the retail that suffered least from the crisis. Private users continued buying and prolonging antivirus programs. PCs' security apprehension prevailed over the habit to install "pirate" software versions. That is why it is possible to confidently ascertain that in future the SOHO and home users market is likely to continue progressive advance.

The year of 2010 may be named a year of struggle for retail. Leader will be defined exactly in terms of retail. Leading vendors' retail share exceeded 50%. This segment's winners will define the future outlook of Russian AVT market. For the time being the shares of Kaspersky Laboratory and ESET amount to 80-85%, somehow noticeable retail sales belong to Symantec and DrWeb. In the future a fairly good growth potential within the stated segment is attributable to Symantec.

Companies armed themselves with all existing tools and are now using them for promotion of their products which practically became FMCG. A wide range of promotion methods is being used, beginning with direct advertising on the radio and out-door advertisements and ending with attempts to establish "special" relations with retail. Thus, it is possible to ascertain that AVT is the first in Russia in terms of software that managed to gain status of a really staple product.

2. Regulators' requirements. Antivirus form the integral part of the PDIS protection system. However application of the antivirus in certain PDIS requires their certification as per high classes. And at the end of 2009 a "certification pace" was launched. ESET was the first western vendor to obtain the FSTEC of Russia certificate of Class K1.

Kaspersky Laboratory, DrWeb and VirusBockAda declared that their certificates may be attributed to the stated class and may be as well used to secure data within PDIS up to the Class 1 inclusive. The remaining vendors announced their de factor abandoning of this market. But the new documents issued by the FSTEC of Russia allow using simple certification as per TC for low leveled PDIS. At the beginning of 2010 Symantec and TrendMicro filed their documents for certification as per TC. If they obtain the necessary certificates it will become possible to speak of the end of the "war of certificates" and appearance of two

vendor groups: vendors with "high" certificates and vendors with "low" certificates.

Considering the fact that the FSTEC of Russia is preparing distinct documentation on antivirus protection (which means the certification significance will grow), all the vendors working in Russia may be expected to obtain these of those certificates. And the availability of such certificates will define the vendor's position on state and corporate market.

The major business segment is marked both by western companies: Symantec, TrendMicro, McAfee, ESET, and Russian company Kaspersky Laboratory.

Aside from Symantec, in 2009 none of the major companies launched a large-scale promotion campaigns and established in Russia a proper Product Support Services which is overwhelmingly important for Russia.

However, following the change of management in TrendMicro, a harsh breakthrough of this vendor may be expected to Russian market. Hypothetically, the new director of McAfee in Russia, appointed in June 2010, will also strengthen the standing of this company.

Eventually, the leadership in the major business segment is retained by the market leaders as a whole: Kaspersky Laboratory, ESET, Symantec. And this breakaway is continuously increasing. And if other companies do not implement in the nearest future serious and capital-intensive promotion programs, it will be possible to ascertain that the three leaders will increase the gap with the competitors and the present market structure will remain stable for as least 5-7 years.

## Decisions on Ensuring Control over IS Requirements Compliance

For the past few years an implicit problem has been created on the Russian IS market related to its skyrocketing development. In particular, the IS decisions applied in practice have been implemented as an immediate reaction to the emerging local IS threats. Thus antiviruses were developed in response to first viruses, then – firewall means due to the necessity to counteract against external threats. Not so long ago new problems of insider threats have become prominent, – as a result organizations started to implement DLP systems. Reactive approach to the development of IS system undoubtedly simplifies the process of justification of the respective projects and shows practical results in the selected segments. However, in organizations that have implemented a great number of private IS decisions, the subdivisions responsible for corporate safety policy and risk management have actually lost control over fulfilling the complex of IS requirements. IS market has become overmuch technological and loosely connected to the activity carried out by business units.

Another approach of proactive development of the information safety system is implemented only by a few organizations. This approach is based on a complete image of the organization's IS status and preliminary (proactive) introduction of safety ensuring measures. Compulsory methods of such approach are:

- Availability of acting IS policy of the organization. Corporate Policy is developed in compliance with regulatory and legislative IS requirements.
- Availability of the processes of control over compliance of IS status with IS corporate policy requirements.
- Analysis of the results of examinations carried out on a regular basis with assessment and prioritizing.
- Implementation of compensatory measures on the basis of risk-oriented assessment.

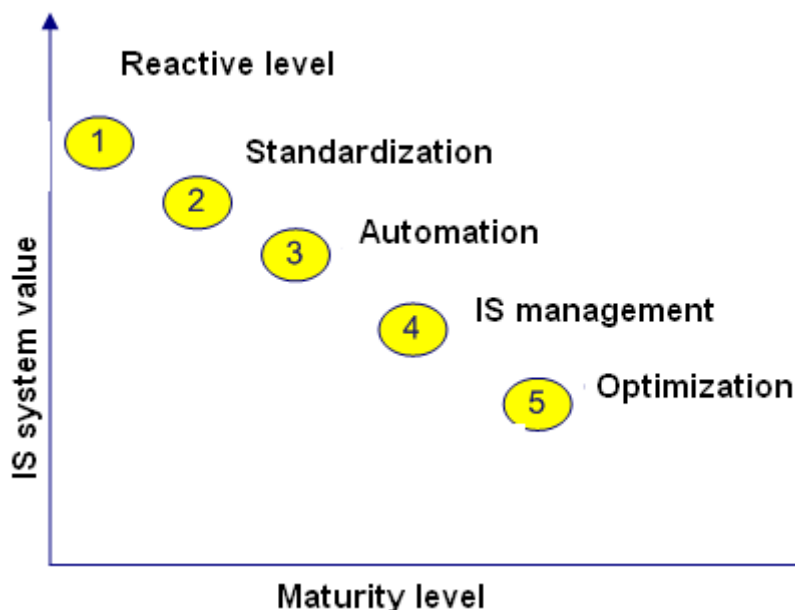
Proactive approach presupposes analyses of not only the existing but also of the potential threats in future, as well as timely planning and introduction of compensatory measures. Notwithstanding the seeming complexity of the

organizational elaboration of the IS issues, adherence of the organization to such approach provides decrease of capital and operational expenditures due to the following factors:

- Reduction in expenditures for implementing the measures on ensuring compliance with external IS requirements.
- Less faults regarding the results of IS audits. According to the existing practice in the projects on preparation and evaluation according to the IS requirements each organization experiences a number of failed attempts. Expenses on correction of incompliances greatly exceed the total project cost.
- Continuity of business processes. In case of lowering the total level of risks, failures of information systems, supporting business activities, are much less frequent.
- Decrease of risk of financially significant leakage of information.

In 2010 there will be a mass movement of organizations towards enhancing the level of IS system maturity, stipulated first of all by economic indicators.

**Figure 10. General Expenditures Level for Organizations' IS of Various Maturities**



Source: LETA IT-company

Nowadays, the majority of organizations is between 2 and 3 levels of maturity: IS means and infrastructural decisions, standardized for the enterprise in general, are implemented, but the processes of examination of compliance with corporate requirements are not automated at all enterprises. Safety scanners that are currently applied (for example, MaxPatrol, Qualys) automate not only the process of finding vulnerable aspects but also perform the necessary examination of settings of servers, databases, active network equipment.

Only a few organizations have reached the following 4<sup>th</sup> level of maturity. In such companies security strategies, same for the whole company, have been developed and implemented. Management of strategies (their creation, distribution, control over execution and implementing of corrective measures) is usually executed within the framework of specialized technical decisions.

The 5<sup>th</sup> level of maturity presupposes the arrangement of IS management processes in such manner that implemented technical decision not only examines the security status but also automatically launches the processes of correction of detected vulnerable spots (including, installation of IS systems

updates, creation of request in ServiceDesk to correct the server settings, deleting inactive records from the user catalogue).

In 2010 the Russian IS market is taking active steps on transition from the 2<sup>nd</sup> and 3<sup>rd</sup> to the 4<sup>th</sup> level of maturity, approaching to the decision of a high-level task in the area of risk management. For this task a complex solution is being elaborated, which is considered as a part of internal corporate security system and as an element of connection of the information protection system in the network of interconnected enterprises. At this stage development and implementation of various interconnected IS standards plays the key role. Compliance with these standards will become the major long-term tendency of the corporate IS market. Thus, "Compliance Age" is beginning.

Organizations use various instruments in order to solve the tasks on IS management:

- Creation of security strategies (DS Kondor, Positive Technologies MaxPatrol, netIQ, Symantec, OpenPages, Acher, Numara, Paisley, Compliance Spectrum, Microsoft SharePoint),
- Inventory check of the stored information resources (Symantec, Websense, McAfee, RSA Security),
- Technical examinations performing (Qualus, MaxPatrol, netIQ, Symantec, tripware, RSA Security, McAfee, Configuresoft, DS Grif),
- Filling in the indicators of IS status in the form of questionnaires and drawing up reports in accordance with the standards (Symantec, Modulo, Agilience, McAfee, Relational Security, Archer, Omanda),
- Correction of the detected incompliances (Symantec ServiceDesk, HP Software, LANDesk, FrontRange, Remedy).

Not all decisions are widespread in Russia, not all solutions are integrated. As it is easier and more convenient to perform development of strategies, inventory check of the assets under protection, performing of technical examinations, filling in questionnaires and correction of incompliances (the whole list of operations that is particularly urgent for the companies of the 5<sup>th</sup> level of maturity) on a single platform, integrated decisions of one or several

manufactures enabling to perform the whole scope of the above mentioned actions are expected. As of the mid of 2010 such a decision, being implemented in Russia, is Control Compliance Suite of the only company – Symantec.

Regarding interaction of several factors:

- New IS requirements that must be met by several types of organizations (in particular, introduction of the requirements stipulated by the Act 152-FZ "On Personal Data", requirements to the organizations – issuers of vouchers PCI DSS, the standard of the Bank of Russia STO BR IBBS);
- Post-crisis economic conditions when organizations became more focused on the efficiency and long-term return on investments;

Starting from 2010 implementation of the system of automation of IS strategies management will become one of the main tendencies in the market development.

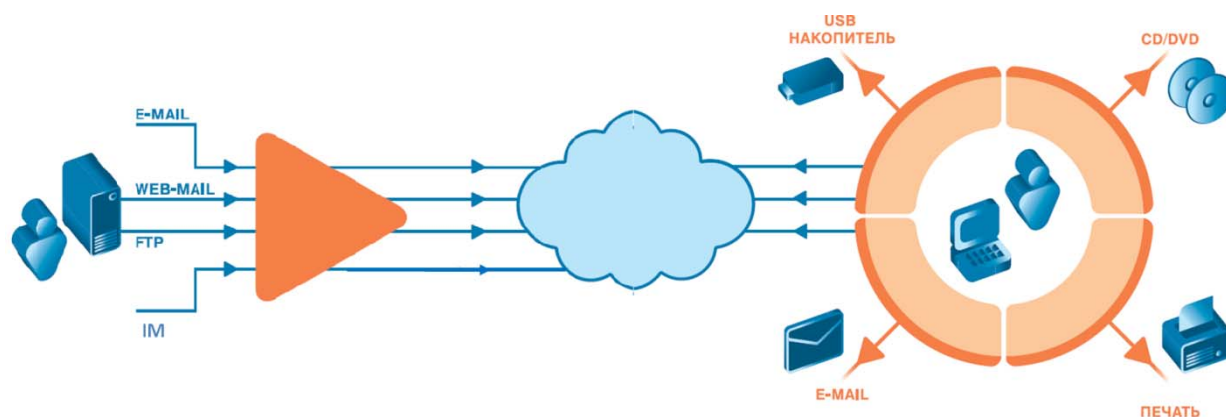
## DLP systems

DLP (Data Loss Prevention) is the fastest growing segment of the market. Even under the conditions of crisis it continued to grow by 5%. The main reason of such growth lies in the fact that in the course of development of IT-market itself into IT-systems of enterprises, a large amount of confidential data have been transferred that need to be protected from leakages within the company.

During 2009 solutions of DLP class have become widely spread and the market participants clearly understood the concept of DLP-systems. According to a common market view the major designation of DLP is to provide protection from accidental or purposeful disclosing of confidential information by the employees having access to the information due to their office duties. At the same time any DLP-system may be adjusted to counteracting against the insiders with malicious intents.

DLP solution combines control over transferring information at the level of communication with external network (fig. F1), and at the level of users terminal equipment (fig. D1). Besides, another important function of the classical DLP solution is the possibility to scan the stored files and databases to detect the location of confidential information.

**Figure 11. Information streams controlled by means of DLP system**



Source: LETA IT-company

Each developer of DLP solution presents its own architecture of decomposition, but in general the main system modules are as follows:

- interceptors/controllers on various information transmission channels;

- agent programs set in the terminal equipment;
- central controlling server.

Interceptors analyze information streams that may extend outside the company, detect confidential data, classify information and transfer it to the controlling server for processing of a potential incident. Interceptors may be used for copying outgoing traffic as well as for installing in the interruption of the traffic. In the latter case the potential leakage may be prevented by means of DLP system.

Controllers for detecting the stored data launch the procedures of detecting confidential information in the network resources. The methods of launching the process of detection vary to a great extent: from scanning from controller server to starting some special program agents on the existing servers or working stations.

Controllers for operations on working stations distribute the security strategies to the terminal equipment, analyze the result of activity and transfer the data of a potential incident on the controlling server.

Agent programs on terminal working place detect confidential data in the processing and monitor the compliance with such rules as saving to a removable information medium, sending, printing out, and copying via clipboard.

The controlling server compares the data sent by interceptors and controllers and provides an interface of incidents processing and reporting.

Thus, the aim of DLP solutions is a centralized control over the total incidents of violation of security strategies in relation to confidential information.

The apparent tendency of development of technological platform of DLP system is manifested in the fact that the developers have started to integrate actively their DLP solutions with other subsystems such as:

- Documents rights management (Enterprise Digital Rights Management). Prime examples – integration of RSA DLP Suite and Microsoft AD RMS, integration of Symantec DLP with a number of solutions including Microsoft RMS, Liquid Machines, Oracle IRM. DLP finds stored copies of

confidential documents and transfer to the EDRM system an instruction on security provision.

- Cryptographic protection of files and containers. Standard examples – McAfee Endpoint Encryption and McAfee Host DLP, Symantec Endpoint Encryption and Symantec DLP, Verdasys.
- Subsystems for gathering and analyzing security events and incidents management. Example – Symantec DLP and Symantec SIM, RSA DLP Suite and RSA eNvision.
- Security compliance control systems. Example – Symantec DLP and Symantec Control Compliance Suite (version 10).
- Systems for control of access to the ports of working stations and devices.

As it is clear from the examples, a number of DLP solutions are integrated with the solutions of other developers.

Another tendency of DLP market development is that the customers started to pay significant attention to the consulting component of the process of creation of the system meant for counteracting against leakage of information. The peculiarity of DLP solutions lies in the fact that the system needs to be incorporated with the logic that will be the basis of classification of confidential/open information. Integrated DLP mechanisms allow automating to the maximum extent and making the process of system education easier due to the methods applied. A couple of years ago there were only two main methods of description of classification conditions:

- 1) labeling the secret documents (a text label was necessary or changing the properties of each text by hand);
- 2) selection of words and expressions (sometimes a linguist was needed to make up the glossary of typical business terms for the organizations that should become the basis of the system activation) as well as routine expressions.

Nowadays DLP solutions combine a wide range of composite methods:

- 3) digital prints of documents and their parts (hundreds of thousands of documents are entered into the system by means of one command);
- 4) digital prints of databases (extracts from the clients databases and other structured information that need to be protected from disclosing are entered into the system);
- 5) statistical methods (increase in sensitivity of the system in the event of repetition of violation).

Modern systems of DLP class include a set of established rules for responding to detection of, for example, credit cards data, Russian passports data, and standard forms of financial accounting. But the most significant element of DLP systems have become the method of digital prints based on the samples of confidential data currently in circulation.

Attempting to consider the issue of DLP implementation on a large scale, it would have been necessary to classify and inventory check confidential information that is currently in circulation. Another extremity – to be limited to the original set of selected confidential documents (in the course of time this setting becomes irrelevant if the selected items are not updated). Many customers prefer to adhere to the medium level of development of the base of confidential documents as a working option:

- First of all, when DLP system is being implemented, 1-3 most crucial business processes are allocated within the scope of which 2-4 most crucial categories of information resources are determined (for example, personal data, strategic developments);
- Then the processes of conversion of the selected groups are described and written in the implemented system;
- Appropriate regulatory base is being developed for ensuring the processes of updating of DLP system educational base;
- Additionally a set of standard branch templates and rules for reacting in case of detecting other groups of confidential documents are made.

The above described consulting preparation to the launch of DLP system increases the scope of work within the project but it also provides a significant and long-term financial return on the project of DLP system implementation.

Thus, the two described tendencies (integration of DLP with other types of solutions and expansion of the consulting component), the projects of developing the systems of counteraction against insider threats will be complex and will encompass the most crucial threats for business.

The major players of DLP market for 2009 were more than a dozen of international companies, solutions accepted on the Russian market and implemented by the native organizations shall be especially mentioned among them:

- Symantec Data Loss Prevention;
- Websense Data Security Suite;
- McAfee Host Data Loss Prevention.

Besides, Russian organizations widely use DLP system of the Russian developer InfoWatch Traffic Monitor.

As of the end of 2009, Russian company InfoWatchin was the leader on the Russian market in money terms with its own products.

But since 2009 the situation has drastically changed. The products of Symantec, Websense and McAfee companies have become leaders among new implementations. Their total share was equal to 70% of all new projects.

These solutions present particular interest for SMB sector. This exactly sector will become the growth driver but at the moment there are no competitive products on the market except for McAfee Host Data Loss Prevention.

Expenses incurred by the Russian organizations for DLP solutions in 2009 were equal to \$53 mln. In future the market growth will be kept at the level of 15% per year.

## Investigation of Information Security Incidents

It happens that despite sound security policy supported by modern technical solutions, information leakage, hacker attacks and such other incidents may occur. The question "How to protect?" is not that much topical for today. Many works are devoted to this topic, numerous theories developed. It is the question "What to do should an incident occur?" which is a real headache. Computer criminality, crimes within information field, incidents in the area of information security – these are the topics discussed in this article.

The term "Computer criminality" first appeared in the USA at the beginning of the 60s. It was the time of the first crimes involving information technologies. Basic features of computer crimes were formulated in 1974 at the Conference of American Bar Association in Dallas in 1979. Three trends of computer crime were distinguished:

- use or attempt to use computer, computer system or network for the purpose of money, property or services acquisition;
- deliberate unauthorized operation intended to change, damage, destroy or steal a computer, computer system or network, or software, programs or data contained therein;
- deliberate unauthorized communication blackout between computers, computer systems or networks.

Within the passed years certain terms were changed: "information crimes", "crime accomplished with the use of information technologies", "cyber crime". But the essence remained intact, and every passing year exponentially increased the number of such incidents. Over the last decade the number of incidents has increased 23 times, but the statistics reveals only registered occurrences. And it is a common practice for the majority of companies not to announce violations. For the moment being three trends of computer crimes are distinguished:

- crimes against information security;
- crimes presupposing electronic information being a tool or means of another crime commission;

- crimes committed using computers and other electronics.

Western countries' governments were quick to realize that computer crimes constitute a real threat to the national and economic security. That is why beginning with the 70s specialized computer criminality control departments were established in western countries within the law-enforcement agencies, educational establishments began lecturing on methods of information crimes investigation within the frames of criminalistics courses, research works are conducted.

By virtue of state support taking forms of gross investments into the investigation in the area of computer criminalistics and legislation support in such states as Germany and the USA, cyber terrorism control departments have been and will conduct efficient works.

Legal side of the issue deserves a separate mention. As we are speaking about crime, breach and incident, then the punishment is supposed to be constitutionally defined. That is why coincidentally with the establishment of departments on state legislative level the works on establishing of a juridical base were performed. And the legislative power activities were so much coordinated that the relevant laws were considerably quick to appear and at the first onset were put into practice.

It should be noted that abroad they observe an intense development of commercial services for information incidents investigation. Let us point out the famous FoundStone ([www.foundstone.com](http://www.foundstone.com)) which for the moment being acts as McAfee subdivision. FoundStone is a specimen for organizations and specialists worldwide.

According to expert opinion, Russia is 5 years behind the West with respect to computer criminalistics. Presently, the analysis of norms of the existing criminal, criminal-procedural and administrative legislation of Russia unveils underdevelopment, inaccuracy and inconsistency of the regulatory system. The very tendencies are traced within scientific, methodical and academic works on criminal law, criminalistics, forensic enquiry, investigative activities and information science.

But nevertheless it impossible but mention the considerable advances in the given area. The financing of the internal affairs bodies of the Russian Federation

on computer crimes control is being increased. A particular attention is drawn to the employees' advanced training and criminalistics procedures refinement. "K" departments, specializing in computer crimes, were created within the internal affairs bodies.

The Internet provides statistics on cases solved by the internal affairs bodies: it appears that only 10% of the solved crimes stand for "hi-tech" crimes committed by highly skilled hackers. At the same time there are dozens of phishing sites in the Internet, DDOS attacks are continuous and etc.

We'd like to draw attention to one more problem of the Russian state authorities – high probability of the incident information appearing in mass media which is badly undesirable for commercial organizations. As the information, claiming the company's being attacked by hackers, or leakage of confidential information, constitutes a tremendous blow for the company's goodwill. That is why companies prefer to suppress information on the occurred incidents encouraging with the violators the sense of impunity. Moreover, particular companies still go on using counterfeit software and consequently they are not able to appeal to state special services unless completely switched to license software.

And what is supposed to be done should investigation be of emergence or it is inadmissible to flaunt the incident occurred within the company? Then help may arrive from the organizations specializing in computer crimes investigation on a commercial basis.

In the West such companies have for long occupied their segment on the security market, but in Russia the situation is quite different. It is much more profitable to implement security systems and receive guaranteed money rather than be engaged into the activity which may appear to be fruitless. And the activity requires great effort from the scientific and research point of view. In fact the personnel of the similar organization must be composed of professionals whose knowledge and skills match those of the villains committing computer crimes. Investigation may be dead-locked and it is not quite clear how to estimate the works expenses. And the main thing is that when the investigation of the crime essence is concerned, the matter will not be the villain's image mediated upon while risk assessment, but the contact with c

particular criminal/ violator/ attacker or any group thereof. And this requires special training.

The basic trends of the given market in Russia and in the world are:

- Incident response
- Incidents discovery (eDiscovery)
- Digital Forensic
- Incidents monitoring
- Legal support of incidents

For the moment being only one player is defined within the market of Russia who is implementing in complex all the trends of the given market – the Group-IB.

## Preview. Research Following the Results of 2010

The research to be published in the middle of 2011 will be devoted to the development of the information security market and distinct segments thereof. The research will analyze old and new factors influencing the IS market. Amidst the new factors the following are worth mentioning:

- Act "On Electronic Digital Signature"
- PCI DSS

Besides, the new research performed by the specialists of LETA and other companies will analyze and provide description of the following IS market segments:

- Virtual Media Protection
- APSC Protection
- Network Security

Specialists of LETA IT-company are open to all suggestions with respect to the new research. If you or your company enjoy recognized authority on the IS market, possess knowledge on factors and segments influencing information security development, LETA will be delighted to invite you to participate in the research following the results of 2010.