**25 years of Ancort Company**

1. **Foundation of Ancort company**
2. **First customers**
3. **«Fake advice note» case of the Central Bank.**
4. **Chechen wars**
5. **Colombian project**
6. **Certification and entry to foreign markets**
7. **Work with Samsung company**
8. **The first cryptosmartphone in the world**
9. **Diamond cryptosmartphone**
10. **Era of mobile phones**
11. **Stealthphone information security system**
12. **Largest exhibitions of Ancort Company**

**1.**Ancort Company has been founded 25 years ago in October, 1990.

Angstrem plant the greatest manufacture of microchip in USSR became a co-founder of a small state R&D enterprise Ancort.

In 1992 Ancort was the first in Russia to certify a portable encryption device MK-85C with the Federal Agency for Government Communications and obtained a permission to export it.

In 1996 Ancort Company was privatized.
**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**2.** From the moment of the company’s foundation the main customers were:

- USSR President Gorbachev, who used a purpose-built information system supporting his foreign visits and MK-85C;

- Council of Ministers of the USSR, which used an information system processing incoming and outgoing mail;

- Ministry of Defence of the USSR, USSR Ministry of Foreign Affairs, USSR Committee for State Security, who were supplied with encryption devices;

- USSR Foreign Ministry that was supplied with the encryption system for use in case of emergency situations in the Embassy;

- Russian President Boris Yeltsin, who used a purpose-built electronic medical card and MK-85C

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**3.** During 1992 powerful criminal groups acting on the national level stole huge amounts of money from the Central Bank (“Fake advice note” case). Several hundreds of billion dollars were stolen in cash. Around 10 thousand people and a huge number of enterprises, banks and companies took part in the criminal scheme.

Ancort had developed a unique cryptographic security system based on a hardware encryption device designed to secure information on telegraphed and mailed advice notes of the Central Bank. In 3 months the Russian Central Bank received 8 thousand hardware encryption devices. In this period 6 thousand Central Bank employees were trained to use the encryption devices and 2 thousand payment processing centres in Russia were equipped with those devices.

The criminals wanted to capture Angstrem plant that manufactured our devices and only our counter measures prevented the assault. When I told a couple of years later about the possible reasons of those thefts to Mr. Kozlov, the Deputy Chairman of the Russian Central Bank, he started an investigation and half a year later he was shot. After that the Central Bank wrote me an official letter telling me not to speak publicly about those thefts.

The situation in those times in Russia was so critical that the Chairman of the Central Bank trusted no one – neither the security services, nor his employees, that is why we made encryption keys for the Central Bank’s encryption devices in our office under control of the Central Banks’ security services.

Federal Agency for Government Communications and Information was against equipping the Central Bank and tried to press criminal charges against me for non-sanctioned equipment of the Central Bank with cryptographic devices. It is clear that the state servicemen wanted to be on the safe side.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**4.** Ancort Company always cooperated closely with the Russian law enforcement agencies, including the Defence Ministry and the Ministry of Internal Affairs during the Chechen conflict. Those structures were supplied with a big number of encryption devices, and 3000 encryption devices were given to the Ministry of Internal Affairs on pro bono basis, which saved many lives of our soldiers.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**5.** From 1993 to 1998 Ancort executed a big project in Colombia on launching a Russian geostationary satellite, providing telecommunication services for a number of Latin American countries. Ancort had to provide guaranteed security of data going through the satellite for state and commercial structures of those countries. Ancort was leading this project. Unfortunately the project was not completed as the transponder of the satellite was not unfolded and in the end it was bought by the Americans.

6. From 1997 to 2003 Ancort equipment own cryptographic systems more than Russian 500 banks.

**7.** Scientific achievements of Ancort were highly appreciated abroad. Royal Technological Institute of Sweden granting conclusions on Nobel prizes held a deep 2-year-long study of the cryptoalgorithm and acknowledged Ancort’s algorithms non-decryptable even with the use of supercomputers. The algorithm was also tested by the South African government and they have also come to the conclusion that Ancort’s cryptoalgorithm can not be decrypted.

Such technological advances gave a strong push to implementing encryption devices of the company abroad. We have equipped 64 countries with various encryption devices including those developed together with South Africa: cryptophones, cryptofaxes, cryptomodems. Joint work with the South African organizations allowed us to equip a big number of African government organizations with encryption devices. Information security systems based on our devices were created for the leaders of the countries like Oman, Saudi Arabia, UAE, Bahrain etc.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**8.** Ancort has successfully completed a joint project with Samsung on creating secure cryptomail for Russian and foreign customers.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**9.** Ancort has also developed the first cryptosmartphone in the world that encrypted voice, SMS and email. The device was developed in Singapore and assembled in Malaysia. This work was unique because the cryptosmartphone worked on Windows CE operating system that could operate only one microprocessor, while we had 2 microprocessors (second being a cryptochip). We have made significant work to modernize Windows CE OS on the level of source codes. Microsoft’s management expressed their surprise of us being able to do such a complicated task.

Cryptosmartphone was certified by Russian  Federal Security Service (FSS) to protect confidential information in accordance with the KS-1 standard. Each device sold included a significant reimbursement to Atlas. Having invested millions of dollars to develop a cryptosmartphone, the company experienced losses in Russia. Megafon that promised to advertise the project even on TV, took back its promise. In this regard, main sales of the cryptosmartphone were held abroad. There were approximately 8 thousand cryptosmartphones with our foreign cryptoalgorithm that were widely sold for the price of 4-6 thousand Euros per unit with the cost of 300 Dollars. It was used by many VIP’s including Nicolas Sarkozy, the French President

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**10.** To advertise the device among the VIP’s the most famous Austrian designer Peter Alissan had developed a cryptosmartphone encrusted with blue diamonds that cos 1 million 300 thousand Dollars. It was featured in almost all luxury magazines of the world and there are approximately 40 million mentions in the Internet about it.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**11.** Era of mobile phones starts today. As of right now, approximately 6 billion cell phones have been manufactured in the world. According to the Gartner research company, only 5% of all investments in information security are spent on cell phone security. Their data shows that by 2017 those figures will rise to 38%. 95% of information security means are software solutions. Google’s president said that the era of software security solutions is over as the criminals can pick up to 56 billion passwords per second with the use of computers one could buy in any store.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**12.** Recently Ancort shifted its focus to Stealthphone information security system, designed to secure mobile phones and computers. This system was being developed by Ancort for more than 5,5 years with involvement of more than 200 people working in the company. We have implemented two separate projects:

- Cryptographic security of information transferred by mobile phones, mainly for individuals (similar to Silent Circle). This solution is based on open key distribution;

- Stealthphone information security solution for state organizations and military structures, based on the use of a symmetric encryption algorithm and a hardware encryption device.

Exchange of encrypted date can be done via own IP network as well as via existing widespread communication channels with the use of a unique Voice Over GSM technology: GSM/CDMA, IP-telephony applications (Skype, Viber), satellite channels (Inmarsat, Turaya, Global Star) and analogue landlines.Voice Over GSM includes two technologies: providing guaranteed security and a scrambler. According to our evaluation we have reached a very high security level estimated at 1064 for scrambled information security.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**13.** Recently we have participated in 5 largest exhibitions in Brazil, Arabic countries, in Indiа and Germany; those exhibitions have shown that there’s no similar device in the world. That is why we have received numerous offers for our devices.