атаковано Державне підприємство "Адміністрація морських портів України". Перед тим шкідливе програмне забезпечення виявлено в інформаційних системах Одеської філії Державного підприємства "Дельта Лоцман".

Також у 2016 році було виявлено спроби проникнення до комп'ютерних мереж українських банків із застосуванням спеціалізованих програм, які потенційно мають ознаки шкідливого програмного коду. Ретельне вивчення обставин та технологічних даних про зазначені атаки дозволило зробити припущення, що вони спрямовані на отримання несанкціонованого доступу до операторських місць системи SWIFT, які знаходяться у банківських установах України.

У червні 2017 року зафіксовано факти несанкціонованого втручання в роботу інформаційно-телекомунікаційних систем органів державної влади та управління, компаній енергетичного комплексу, державних та приватних фінансових установ, операторів зв'язку та провайдерів телекомунікаційних послуг, що викликали значний резонанс у суспільстві. Вказана атака стала відома у світі під умовною назвою "Petya.A".

Розповсюдження ШПЗ здійснювалось через оновлення системи електронного документообігу (SupplyChainAttack – атака через довірене джерело).

Зловмисники викрали аутентифікаційні дані адміністратора та з використанням його прав змінили конфігураційний файл оновлень прикладного програмного забезпечення.

Основними цілями зловмисників були великі державні та приватні компанії, порушення штатного функціонування інформаційних інфраструктур яких може дестабілізувати ситуацію в країні.

У січні та квітні 2018 року російськими спеціальними службами організовано кібернетично-інформаційну операцію з несанкціонованого втручання в роботу офіційного сайту Державного підприємства "Антонов" та поширення недостовірної інформації з метою дискредитації державного підприємства на міжнародній арені.

Також у 2018 році виявлено та попереджено акцію кібернетичної розвідки ФСБ РФ, яка реалізована хакерським угрупуванням "TURLA" та спрямована на отримання несанкціонованого доступу до інформаційних систем Міністерства закордонних справ України.

Sergiy Kuchma
Компанія «Автор»
Київ, Україна

RADIO COMMUNICATION AND IP NETWORKS PROTECTION

Radio communication with improved anti-jamming ability and udition protection

This is intended to provide high stealth, noise immunity and protection against eavesdropping.

Features:

- Digital methods of voice and data transmission.
- Stealth and noise immunity improvement: FHSS, DSSS – wideband signals for direct spread spectrum.
- Crypto protection of guaranteed sustainability.
- SDR implementation of radio station.
- Mass and dimensional characteristics of radio station units do not exceed the analogues parameters of the P-863 radios
- Use of the existing cable and antenna-feeder system installed at the aircraft will ensure the replacement of radio stations without making changes to the construction of the aircraft.

Main regimes work and characteristics for radio station:

- Amplitude modulation/Frequency modulation - to ensure compatibility with other types of aviation radio stations.
- FHSS, DSSS - to provide increased secrecy in use.
- Digital voice transfer with speeds 2000 bit/s and 4800 bit/s.
- Data transmission with speeds up to 32 kbps.
- Emergency radio receiver.
- Strong crypto protection for analog and digital modes operation.

Audition protection of analog VHF/UHF radio

The system of protection intended to protect radio aviation channels against eavesdropping. The system consists of device for protecting negotiation - flight operator, pilot and software for generating and managing of key information and provides cryptographic protection of information transmitted by analogue radio channels of the ultra-short waves and short waves range.

Features:

- Voice bitrate – 4800/2000 bps.
- Encryption according to national encryption standard GOST 28147: 2009, key length - 256 bits. International encryption standards may be implemented.
- Delay – less then 0.5 sec.

IP networks protection

AVTOR's IP encryption complex is a totality set of tools, which is necessary and sufficient for construction of a Virtual Private Network (VPN) through any IPv4-networks. The information is transmitted over IPv4-networks in tunnel mode when the original IP-packets are encrypted and

encapsulated in entirely new packets, which are transmitted between nodes (IP-encryptors) of the protected network.

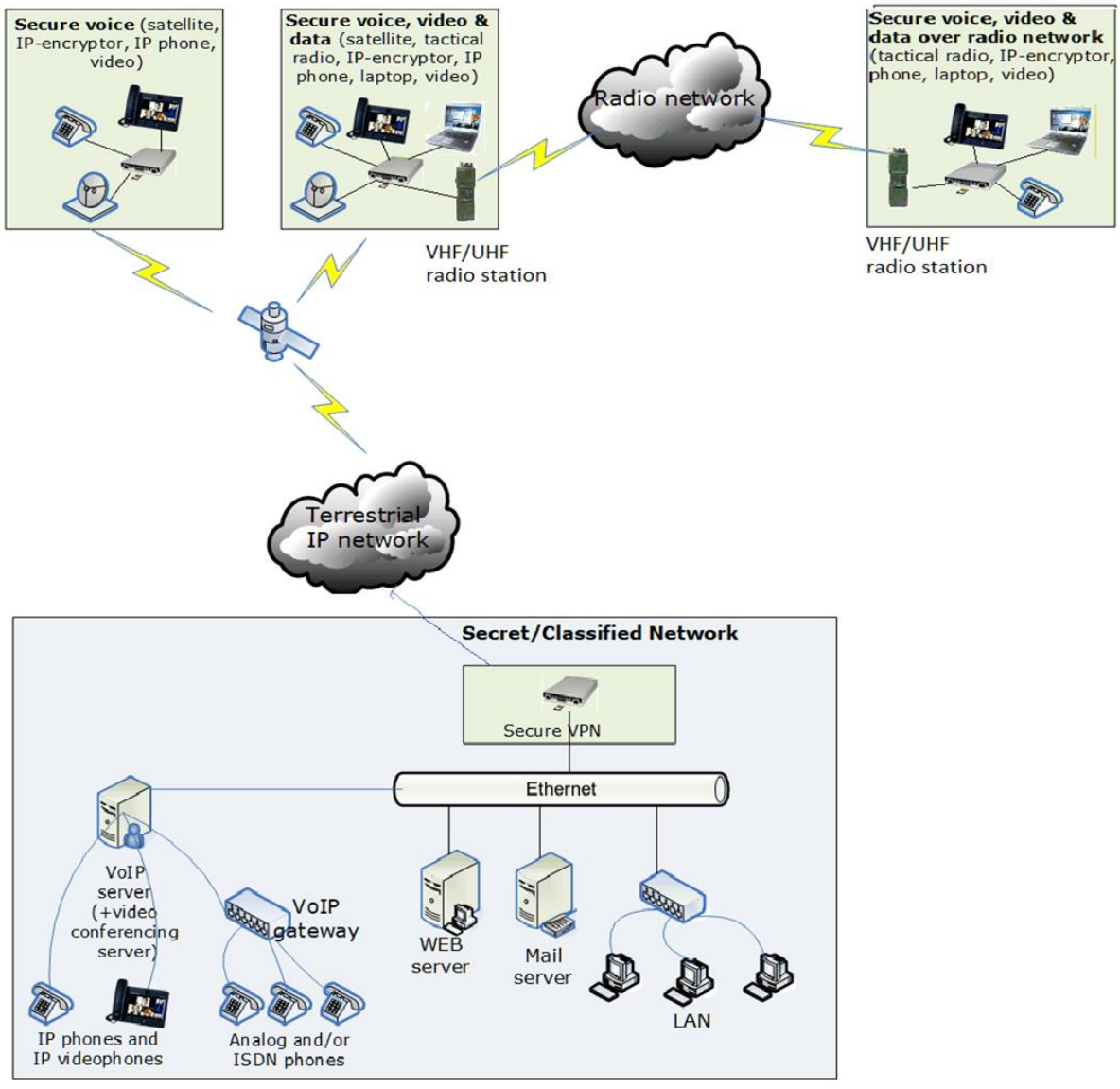
IP-encryptors in IP networks provide:

- data confidentiality and integrity;
- data source authorization;
- protection from traffic analysis;
- hiding of the protected network topology.

IP-encryptors key features:

- Software defined Hardware encryption (256-bit key)
- Security Smart card Crypto Ignition Key & key storage
- Easy insertable/removable Crypto Ignition Key (sim card form factor)
- Local (via USB) and secure remote (via Black network) management and monitoring
- Local and remote key zeroing
- Fanless, low power consumption devices

Protected IP network architecture



Smart card technologies

The main smart cards advantage is the presence of a highly intelligent chip that provides a wide range of uses. Smart cards can analyze information, perform mathematical calculations and make logical conclusions. In addition, the memory of smart cards exceeds the volume and speed of all its competitors.

Smart cards have a much higher level of reliability and security than all other carriers do. The production of smart cards has reached a level where the intelligence card provides the highest level of protection against unauthorized use. Due to the unique code fixed in each card, duplication of its data is impossible.

The multi-step process of card personalization makes it the most reliable for storing sensitive information All user data is encrypted and protected by encrypted passwords.

Attempting to break a smart card leads to the fact that her work stops temporarily or permanently. There is also the possibility to close access to the modification of certain data stored on the card.

Advantages:

- Encryption processing is implemented inside of smart chip;
- Encryption keys never appears outside of smart chip;
- Hardware protection against PIN code attack and tampered access;
- Own operating system;
- We use smart cards that based on NXP and Infineon chips. Certificates: Common Criteria CC EAL5+, CC EAL6+.