IT security unit "Cert.lv» found that the plug has been China's servers from eight public institutions networks. Currently «Cert.lv» already found a number of infected phones and trying to find out whether and what information has traveled to the east.

US since last week's Chinese phones are no longer in vogue. IT security company specialists found that 50 dollars worth of phone every 72 hours on servers in China secretly transmit phone messages, contacts and call lists. On this private data leakage owner is not aware of and can also disable.

Hosts spy company BLU product sold in one hundred and twenty thousand customers. It is programmed Chinese company «Shanghai Adups Technology». This same company programmed devices used by 700 million people, including Electric Vehicle and Latvian commercially available «Huawei» phones.

Company trying to justify oneself that spyware feature is only for marketing purposes. For mobile phone manufacturer to explore users habits. American authorities at the moment it is unclear whether behind this event does not lie in the Chinese government's efforts spying..

After the events in America on data flow to China drew Latvian IT security incident prevention institution "Cert". Experts found that the suspicious servers in China flow information from the Latvian state officials phones.

**VARIS TEIVANS  
«Cert.lv»Deputy Leader**

*Atpresent, a checkandinfactonlytoday, wecanseethatthereareseveralhundredcasesofloginfromtheLatvianauthorities to theseChineseservers. Atthemoment it istooearly to judgewhethertheyarethesamephones, becausetheirprevalenceLatvianbeenobserved. Perhapsthisisdue to thefactthattheLatvianofficialshavepurchasedtheequipmentandbrought to Latvia, oris it related to otherapplicationsforwhichwedonotknowanything.*

Atpresent, expertshavedeterminedthatcontactwithChinawithouttheownertried to forecastexactlyphones. Severalhavebeenfoundandarecurrentlyinvestigating "Cert". Theorganizationdoesnotrevealwherethenationalauthoritiesthepossibledataleakoccurred. Also, donot post thepurposesforwhichtheinformationwascollected.

**VARIS TEIVANS  
«Cert.lv»Deputy Leader**

*In all epopee it is involved in a number of companies that deal with both the advertising market and the improvements in the quality, the same physical equipment vendor, distributor and manufacturer of the software. Whole range and one of them also maintain these servers. What he further with these data do, that is the question.*

The telephone is not the only device that can spy on us. "Cert" in a public institution has established video surveillance cameras, which the manufacturer has programmed the flexibility to access from the side.

An unnamed government department installed hundreds of cameras, each a few hundred euros. They are manufactured by a Chinese company Milesight. The company is serious, it is represented in the US market. Also, the camera itself is from the expensive end.

**VARIS TEIVANS  
«Cert.lv»Deputy Leader**

*We found her in this case, together with the researchers some chance.*

«Cert.LV» holdsregular IT securityexpertsmeasure «CyberChess». Atthe Internet technologyexpertstry to cracktheorganizersselectedequipment.

**KIRILS SOLOVJOVS  
ITsecurityexpert**

*Wefiguredthat it wouldbeinteresting to securitycameras. It is a themethatisveryup to date. Peoplearedeployedintheirhomes, businesses.*

*Mytaskwas to makesothat it wouldbeinteresting to protectthecameraandontheotherhandthebreak. Hopingthatprofessional-levelcameraseverythingisfinewithsecurity, I thinkneedsomethingpretend, trainingpurposesandmake a hole.*

*However, it provedthat it hadalreadybeentakencareofbythesamemanufacturer. Thechamberfound a numberofvulnerabilities, whichcouldbeusedknowledgeablemalefactors.*

The chamber was at least five different vulnerabilities - five different ways to access the user's data. At least two of the following ways allowed to obtain complete control over the camera. During the year security holes in a patch, but it has not been easy to force producers to do it. Solovyov also has examined other areas, all of them have been found in greater or less flawed.

China is produced the lion's share of the world's electronic devices and their components. It is among the leaders in the software industry. The scandal with the spy phones are not the only thing that creates suspicion about China's ambitious efforts to collect data using consumer electronics. In October, the Pentagon reported that Chinese manufacturers Lenovo computers have spyware software.

Former National Security Council Secretary and the Constitution Protection Bureau deputy GundarsZalkalnsconcedes that the Chinese government could relate to spy devices.

**GUNDARS ZALKALNS  
Former National Security Council Secretary**

*FrommyexperienceinAsia to publicandprivateparticularlyindustrialstructuresismuch, muchcloserrelationshipthaninWesterncountries, I donotknow - maybe it fromancienttimeshasbeenitstraditionalrendering.*

Experts are convinced that Latvia is not a Chinese spy purpose. Rather, it is considered that the device arrived here without a special intention. Perhaps it is for other, larger economies.

**JANIS GARISONS  
Defence Ministry State Secretary**

*I rather would not want to speculate on whether the Chinese government knows or does not know. This is about what to talk in general about the attitude of the IT security and cyber security. As well, you can find other places produced devices that have security risks. But I do not deny that such devices are used not only peaceful but also espionage. US and NATO it is already defined as a new domain battle. Of course, we have to look at it alongside land, sea and air space, cyber domain is a new battleground.*

Garison is convinced that public sector IT security is not the worst situation. The biggest problem is private, who are trying to save, such as antivirus programs or buying the least expensive phones and tablets, without assessing their safety. This can endanger not only their own, but also their business partners, including the state.

Asshownthanpersonalobservations - defectiveChinesesurveillancecamerasareinstalledintheLatvianStateMuseumof Art. Museumwasopenedlastyear. Thirty-onemillionworthofreconstructioncontractingwastheRigaCityCouncilPropertyDepartment.