

## Comprehensiveness of countermeasures against potential cyber and physical insiders at nuclear facilities

The countermeasures against potential physical insiders and especially cyber insiders is critically important at nuclear facilities (NF); this concern reflected in IAEA Nuclear Security Series documents: NSS-8 (NST-041), NSS-10 (NST-058), NST-47.

Insiders activities confirmed by accidents presented in internet. For example, oil dumping from turbine at Belgium NPP Doel-4 performed by insider (2015) or Stuxnet malicious software injection into uranium enrichment centrifugal system in Natanz, Iran (2009) that shows the necessity of security provision against insiders.

Insider have authorities, knowledge and access (including access to classified information) to nuclear materials and nuclear facility (NF) equipment and NF systems software: NPP Automatic Process Control Systems, Physical Protection Systems (PPS), nuclear materials accounting and control systems. It causes a necessity of special protective and preventive measures complex creation for risk reduction of insider appearance.

It is necessary to apply a complex approach for protection against potential insider (PI):

- in employment: trustworthiness testing multistage process.
- in the process of work: excluding of physical, legal, cyber and psychological ability to conduct a crime by staff prophylactic management, PI identification, detection of personnel close to discharging.
- during discharging/reduction procedure: discharging/reduced personnel authority decrease and information backup provision.

Special multistage trustworthiness assessment procedure shall be conducted for PI employment avoidance. This procedure includes interview, psychological testing, lie detector testing, social networks analysis, records on convictions analysis, tendency to drugs or alcohol addiction.

Also there is a necessity of rules failure analysis both physical (attempting to access into restricted area, attempting to carry out forbidden tools) and digital (attempting to passwords brute force, installing malware) including different types of security systems testing. Personnel behavior testing shall be performed inside and beyond of NF: expensive shopping, criminal contacts, hacking activities.

Besides trustworthiness testing it is necessary to perform general security procedures against insiders: staff access limitation (physical access into facility areas and informational access into information systems), identification of forbidden tools carrying out that could be used as insider's tools (digital: laptops, mobile phones, 3-G modems; physical: cold arms, bench tools) etc.

Great attention should be payed to preventive measures against cyber-insider due to modern malware development; existing security software not always can protect against modern malware, especially against "zero-day" threat.

It should be mentioned that cyber-insider may be high-level qualified (in comparison with physical insider), for example, for security systems information acquisition or malicious software implementation.

In comparison of PPS and information security system effectiveness assessment methods it can be found that a time-line analysis method modeling of adversary penetration have implemented since 1980's (in addition to deterministic approach). A modeling assessment method for effectiveness assessment in IT-area been applying since 2010's (MITRE and CTF models). In 2015 a cyber-physical penetration of adversary been considering in common mathematical approach in PARCAT software. Integration cyber and physical adversary in common approach also considered in SSPA "Eleron".

All above mentioned measures including a large range of others, for example, psychological work with staff, multi-layers physical and informational protection and complex information security provision in NF automated systems provides sufficient protection level against physical and cyber insiders at Russian NF.

It is noteworthy that deterministic approach on security systems conditions assessment can't assess level of protection fully correctly due to fast change of technologies (physical and especially digital) because of up-graded requirements of regulatory documents (and documents itself) been developed only in 2-4 years after new threats identification.

Approach related to PI behavior modeling (in addition to deterministic approach in NSS-8) will be developed by SSPA "Eleron" under IAEA research project J02010 "Improvements in Preventive and Protective Measures against Insider Threats at Nuclear Facilities" (2019-2022) that could improve quality of PI identification in Rus-

sian and other IAEA member states NF.

**Gender**

Male

**State**

Russian Federation

**Author:** Mr ZHURIN, Sergey (FSUE ELERON - Rosatom)

**Presenter:** Mr ZHURIN, Sergey (FSUE ELERON - Rosatom)

**Track Classification:** CC: Information and computer security considerations for nuclear security