Contribution ID: **314** Type: **Poster**

System Evaluation Methods in practice for insider mitigation

In ensuring nuclear security, addressing the issues of countering the insider threat is one of the most difficult.
The main elements of the physical protection system are the technical means: CCTV, access control, locks, radiation monitors, etc., for which you can develop management scenarios, service and support procedures, modernization and improvement programs.
In turn, counteraction to the insider threat includes analysis of the behavioral manifestations of each individual person, his emotional and mental state, motivation, up to his relationships in the family, with friends and colleagues.
This significantly complicates the process of developing countermeasures to the insider threat, as compared, for example, to countering the terrorist threat.
In this case, the classical measures of physical protection, such as perimeter fencing, checkpoints, perimeter lighting, etc., lose their effectiveness and are not able to counteract the insider threat.
The approaches to evaluating the effectiveness of measures taken to counter the insider also change. Determining the time to overcome physical barriers becomes irrelevant and meaningless.
In this case, it requires the development of a completely different approach combining the functions of classical physical protection, digital technologies and cyber security, safety security and the assessment of the behavioral characteristics of workers.
The national operator of Kazakhstan for the extraction and processing of natural uranium, NAC Kazatomprom JSC, in its practice of ensuring nuclear security and countering the insider threat, attempted to combine these functions.
In terms of providing classical physical protection, access control systems, full-coverage video surveillance and alarm systems have been introduced.
In terms of integrating digital technology and safety security, systems such as SC - visualization of key production processes (>500), ERP - financial planning and accounting, MES - Production Management, APS - operational planning, LIMS - laboratory information system, EAM - service, spare parts, APCS - automated process control system. These systems are integrated into a unified data management system and are presented in the Situation Center of the headquarters of NAC Kazatomprom JSC. The data management system allows real-time monitoring of changes in the equipment's normal operation mode and blocking the introduction of these changes in case of critical deviations, which significantly complicates the implementation of the task of the insider during sabotage.
In terms of evaluating the behavioral functions and reliability of the staff, digital technologies are also actively used. As part of the Government's implementation of the Digital Kazakhstan strategy, various information about the employee on tax arrears, administrative fines, travel bans, registered business, being in the register of wanted persons, etc. is available on a single portal providing state services.
With the help of special IT-aggregators, the Security Service of NAC Kazatomprom JSC carries out inspections of workers, including through open accounts in social networks. Conducting these activities allows you to generate primary information about the employee before interviewing him in the course of the assessment of reliability.
All of these measures allow an assessment of the measures taken to counter the insider threat, identify vulnerabilities and work out ways to improve the overall security system of the enterprise.

State

Kazakhstan

Gender

Male

Primary author: Mr NIKHANOV, Eldar (NAC Kazatomprom JSC)

Co-author: Mr ALZHANOV, Bekzhan (NAC Kazatomprom JSC)

Presenter: Mr NIKHANOV, Eldar (NAC Kazatomprom JSC)

Track Classification: PP: Insider threats