УДК 621.039.58

SIMULATION OF PREVENTIVE AND PROTECTIVE MEASURES AGAINST INSIDER THREAT

P.A. Amoah, M.N.S. Ansah, E.A. Shcheglova

Scientific Supervisor: Professor B.P. Stepanov

Tomsk Polytechnic University, Russia, Tomsk, Lenin Ave., 30, 634050

E-mail: amoah@tpu.ru

МОДЕЛИРОВАНИЕ ПРОФИЛАКТИЧЕСКИХ И ЗАЩИТНЫХ МЕР ОТ ИНСАЙДЕРСКОЙ УГРОЗЫ

П.А. Амоах, М.Н.С. Ансах, Е.А. Щеглова

Научный руководитель: профессор, д.т.н. Б.П. Степанов

Национальный исследовательский Томский политехнический университет,

Россия, г. Томск, пр. Ленина, 30, 634050

E-mail: amoah@tpu.ru

Аннотация. *Проведено исследование эффективных мер по предотвращению саботажа на ядерных объектах и хищения радиационных материалов. В исследовании используются эффективные превентивные и защитные меры, которые были реализованы в институте, чтобы показать надежность гипотетического объекта. Цепи Маркова, которые представляют собой комбинацию вероятностей и матричных операций, моделируют превентивные и защитные меры на гипотетической ядерной установке. Результаты реализуются в процессе оценки реализованных стратегий. Некоторые из процессов оценки включают разработанные алгоритмы предотвращения длительных и / или внезапных краж, саботажа и сговора между внутренними нарушителями. Следовательно, эффективность превентивных и защитных мер против злоумышленников также зависит от эффективности процесса оценки, проводимого экспертами [1, 2].*

Introduction. A study on the advancement of effective measures to prevent the sabotage of nuclear facilities and radiological theft has been conducted. The strategic approach used is Markov chains, which addresses the insider threat as shown in Fig. 1 and proposing comprehensive measures, required to justify the need to enhance and prioritizing preventive measures to control the insider threat. The hypothetical nuclear facility designed for this research has instituted preventive and protective measures to deter, detect, delay and respond to threat. These include vetting and review of individuals, approval for individuals with authorized access and to critical assets or vital areas, detection of a malicious act, and the interruption of the malicious act [3]. The development of sabotage scenarios and based on the characteristics defined in the threat assessment or Design Basis Threat and an assessment of the impact of those scenarios or targets provides protection against stand-off attacks. This aids in also identifying potential vulnerabilities. Protection measures that may protect against or mitigate the consequences of a stand-off attack include increasing the stand-off distance to exceed the range of weapons the adversary might use, obscuring lines of sight to the target from potential stand-off attack areas, increasing detection and deterrence through off-site patrols and surveillance, using barriers to intercept missiles or absorb blast or fragments, modifying layouts of facilities to protect sensitive targets and hardening facilities to resist the attack.

Research method. The method used in this research is the Markov chains. These are a combination of probabilities and matrix operations that model the preventive and protective measures instituted by the hypothetical nuclear facility[4]. Algorithms are generated from the transition diagram analysis of the qualitative representation of the preventive and protective processes that have been instituted. Table 1, Fig. 1 and Fig. 2, give an appreciable representation. The initial state vector is a recommended probability representation of the 90% preventive and 10% protective measures by the regulatory body to be: [0.9 0.1]. The transition matrix is multiplied by the initial state vector to achieve the new state vector approaching the steady state, as obtained from Fig. 2 as: $\begin{matrix} 1 & 0 \\ \frac{2}{3} & \frac{1}{3} \end{matrix}$

Table 1

Representation of interaction preventative and protective processes

Measures	Qualitative Designators	Probability
Vetting of Personnel	High	1
Reduction of Potential Insiders	High	2/3
Authorized Access Approval	Medium	1/3
Occurrence of Malicious Act	Low	0

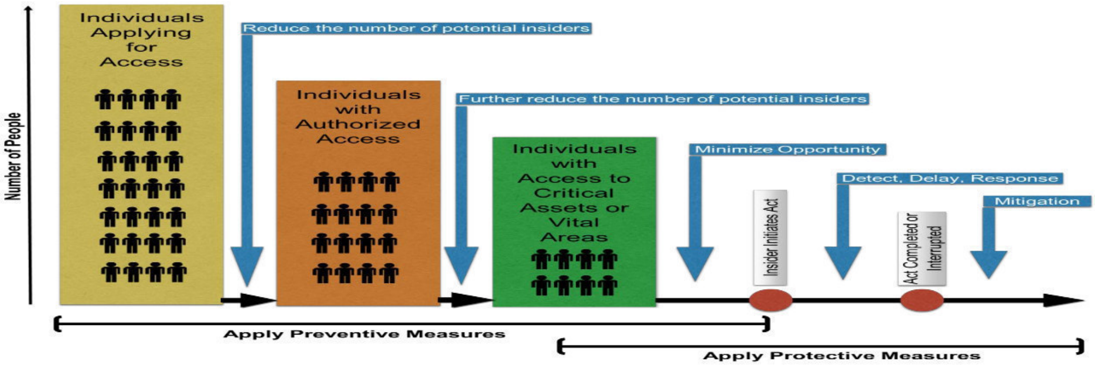
Number of People
Individuals Applying for Access
Reduce the number of potential insiders
Individuals with Authorized Access
Further reduce the number of potential insiders
Individuals with Access to Critical Assets or Vital Areas
Minimize Opportunity
Detect, Delay, Response
Mitigation
Insider Initiates Act
Act Completed or Interrupted
Apply Preventive Measures
Apply Protective Measures

Fig. 1. Steps for preventive and protective measures against potential insiders.[5, 6]

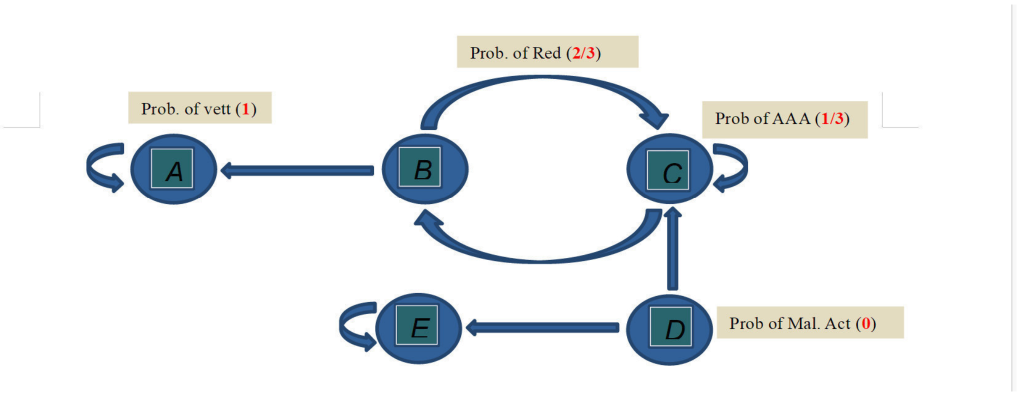

Fig. 2. Transition diagram of the two measures

A - vetting and review of persons/individuals applying for access.

B - approval for individuals with authorized access.

C - approval for individuals with access to critical assets or vital areas.

D - initiation of insider malicious act.

E - malicious act completed or interrupted.

Results. A product of the initial state vector and the transition matrix provides a vector value that eventually after many system updates, tends to plateau or stabilize, assumably due to an enhanced effective nuclear security culture. ie. $\begin{bmatrix} 0.9 \\ 0.1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \frac{2}{3} & \frac{1}{3} \end{bmatrix} = \begin{bmatrix} 0.97 \\ 0.03 \end{bmatrix}$; our new state vector representing the updated measures has 97% preventive measures and 3% protective measures.

Conclusion. The activities of insiders and the threat that they pose to the nuclear industry at nuclear and radiological facilities can not be underestimated. Qualitative and quantitative remedial approaches through research such as this contribute to justification to the need to prioritize the effective resourcing of preventive measures. From the theoretical assessment, it is realized that a 97% effective preventive measure and a 3% protective measure relative to the overall security system interaction processes will contribute to annulling the insider malicious act. A long-run Markov chain will present a steady state which will also contribute to a theoretical representation of the effective nuclear security culture practice at the hypothetical facility. The series of data collected is inputted in a python programme. This provides a platform for flexible alterations during system upgrades or adaptation of practice by similar nuclear facilities. To help sustain and continuously improve upon the implemented system, an introduction of a quantitative concept of maintaining the performance of people, procedures and equipment is required. A requirement of monitoring performance, motivation, and leadership to create organizations that collaborate, innovate and produce consistently superior outcomes. A key aspect of sustainability involves maintenance and testing programmes to enhance the physical protection systems which coordinate harmoniously with other components of the security system.

REFERENCES

1. Objective and Essential Elements of a State's Nuclear Security Regime: Nuclear Security Fundamentals. – Vienna: IAEA Nuclear Security Series, 2013. – №. 20. p. – 32.
2. Physical Protection of Nuclear Material and Nuclear Facilities: Implementing Guide in preparation (NST023). – Vienna: IAEA Publishing Section, 2014. – 136 p.
3. Nuclear Security Culture: Implementing Guide. – Vienna: IAEA Nuclear Security Series, 2008. – № 7. – p. 48.
4. Brandon, C.F. (2012). Finite Mathematics - Introduction to Markov Chains. Retrieved 27 November 2019 from http://www.bcfoltz.com/blog.
5. The Twenty-Seventh International Training Course on the Physical Protection of Nuclear Facilities and Materials, April 29 - May 18 2018, Albuquerque, New Mexico, Preventive and Protective Measures Against Insider Threat, p. 12.
6. Preventive and Protective Measures against Insider Threats, Implementing Guide, IAEA Nuclear Security. – Vienna: IAEA Series Publishing Section. – 2020. – №. 8-G. – p. 12.