Comprehensiveness of Response to Internal Cyber-Threat and Selection of Methods to Identify the Insider

Sergey Igorevich Zhurin

National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoye Highway 31, 115409, Moscow, Russian Federation
Email: sizh@mail.ru

Abstract. A range of international regulatory documents state the importance of counteracting insiders, especially cyber-insiders, in critical facilities and simultaneously providing complex protection, which includes technical, administrative and information protection. In that case the insider, who is familiar with the protection or information system, will be able to find vulnerabilities and weak points in the protection of the information system or control system. One of the most important aspects of the preventive measures against insiders is personnel checks using different techniques, including interviews, social network analysis, and local area network analysis. In the case of having limited financial resources, it is necessary to choose a technique from a checklist rationally.

Keywords: *cyber-insider; cyber-insider threat; insider; insider identification; methods for personnel check; evaluation of personnel.*

1 Introduction

Nowadays security of critical facilities against outside attacks (by an intruder or hacker) can be guaranteed by a highly efficient information protection system (IPS). The hacker attack is detected and then neutralized by firewalls. The possibility of outsider actions proving successful can be lowered considerably through the use of multilevel protection: access control systems, firewalls, honey-pots. It is difficult for an outsider to gain information about the elements and vulnerabilities of the IPS necessary for the successful preparation of an intrusion, due to specific administrative and information protection measures implemented in accordance with the current regulatory documents [1].

Thus, an employee of the object can become the primary source of information for an outsider. The former can also make an attempt to lessen the efficiency of the IPS. It is also not impossible that two or three employees might conspire to use their official powers to pursue such an agenda [2]. Also, the simplest approach for protection against hackers is disconnection from the Internet, but the protection from cyber-insiders is not so simple.

Received October 2nd, 2014, 1st Revision November 26th, 2014, 2nd Revision January 7th, 2015, 3rd Revision March 6th, 2015, Accepted for publication March, 17th, 2015.
 ISSN: 2337-5787, DOI: 10.5614/itbj.ict.res.appl.2015.8.3.5

Lately, insider criminality has become more and more relevant. This is proved by a range of international regulatory documents [3]-[6]. Relevance of protection against insiders (cyber-insiders) is reflected in several Russian and foreign documents [7]-[10], largely devoted to nuclear facilities as the most dangerous objects.

Insiders involved in the theft of nuclear or other high-value and dangerous materials from critical facilities becomes more likely nowadays due to low wages, crisis-related firings, lowering the level of terrorism alertness and activity [11]. It is necessary to analyze the cyber part in this malicious act, because there are a many information systems that control the process of dangerous materials movement and detection. Also, protecting information against copying, destroying or modification is necessary in modern-world conditions, where employees change their jobs very often, sometimes more than once per year.

This article is devoted to the complex counteraction against insiders, including cyber-insiders, and the main aspect of that counteraction – the identification of insiders (cyber-insiders) by various psycho-physiologic methods (and special cyber-methods) and making a rational choice among them.

2 Cyber-Insider Threat Definition

Let's first define what a cyber-insider threat is. A cyber-insider threat is a malicious threat to an organization that comes from people within the organization itself, able to cause harm to the organization by exercising their official powers using information control or information technologies. The harm can be evaluated materially (for instance, according to the price of an object stolen by using access to the accounting system and modifying the database according to the quantity of the stolen object as well as the history of transactions), in the form of lost profits (such as theft of information considered state or commercial secrets and its transfer to competitors), politically (such as loss of confidence, for example in the case of the theft of a customer database), in the form of victims and people affected (in the case of the sabotage of a reactor when an insider has the information needed to control the reactor control system).

Cyber-insider threats are especially dangerous because a cyber-insider, unlike an outside intruder, enjoys the following: knowledge and official powers; opportunity to obtain information from other employees; knowledge of weak points in information systems and points of entry; opportunity to choose the most convenient moment for malicious action (preventive work, temporary

delegation of greater powers, etc.); greater opportunity to form a conspiracy with other employees who enjoy the powers he lacks.

During the working process it is difficult to detect previously trustworthy and now potentially dangerous employees. A highly educated specialist who leaves the company for a competitor and brings along the knowledge he has obtained, digital copies of exploratory studies and personal contacts to the other company or other specialists also poses an indirect insider threat.

Factors that 'protect' a company from insiders or cyber-insiders (including the disloyal – who can resign – [2]) can be divided into the following categories:

1. The trustworthiness taught from childhood by parents, school, university and other elements in their environment.
2. Satisfaction with the job (wages, prospects) and unwillingness to lose it.
3. Resources (material and psychological, including health) and their adequate management, minimizing the risk of additional, illegal income streams being pursued.
4. Understanding that it is impossible to commit the crime due to the levels of security.
5. Evidence left after the crime has been committed, such as log entries (also digital) or video registration. The existence of such evidence results in an understanding that in the case of an inquiry, the criminal will be detected.
6. Difficulty in obtaining profits, even in the case of successful action.
7. Fear of punishment for the committed crime.

The most typical form of theft is theft of information or program code when changing jobs. This can also be the reason why a person changes jobs.

It is also worth noting that the following factors are necessary to provoke illegal actions [2],[12]:

1. urgent need (mainly financial);
2. psychological readiness (or a state of stress due to the urgent need);
3. the possibility of committing an undetected crime (lack of evidence, punishment) and of selling the goods;
4. lack of awareness of the health consequences (when stealing nuclear or other health hazardous material).

Lack of any of the numerated factors may make a crime impossible. However, as it is difficult to detect insiders before a crime is committed, it is necessary to protect from them, starting from appropriate preventive measures and ending with physical barriers, and technical and information detecting means, so that employees do not consider the possibility of committing an unlawful act.

3 Special Cyber Threat Comprehensive Protection

There is a special feature of cyber threats: actions related to cyber threats are not always detectable; traces can be removed. There are the typical hazardous actions: malfunctions in network-based connections of security system devices; data falsification in accounting systems; deactivation of detection alarms; generation of false alarms, and others.

The model of the cyber-insider should include: powers (limited (operator) or 'full' (administrator, developer)), tools (hackers programs, mobile phones, tools for connection to PC), knowledge (attack point, protection system, audit system), experience (social engineering, program application, code writing).

The full list of options for protecting a cyber environment (from cyber-insiders) consists of:

1. Personnel (human reliability checks, work with personnel, separation of authorities, monitoring professional development);
2. Computers and equipment (protection of hardware, limited access to rooms, video surveillance of access, communication-line protection from unauthorized connections);
3. Networks (firewalls, antivirus protection, encryption, DLP-systems);
4. Software environment (access control, documenting and accounting, encryption, integrity checking, audit logging);
5. Automated systems on the whole (development of secure automated systems, certified software, exclusion of access to the OS);
6. Information (protection from data leaks, disclosure, dissemination);
7. Developers and vendors (reliable vendors, software and hardware tests);
8. External environment (security strategy, insurance, risk management).

4 Insider Threat Counteraction Focusing On Personnel

Counteraction to insider threats at the level of the company as a whole must be secured at the three following levels:

4.1 Employment

Pre-employment checking prevents the employment of a penetration agent or a person facing problems (potentially capable of unlawful acts), such as: financial problems, deviances, various dependencies (gambling, drug addiction, etc.), anti-social background (for example ex-convicts, religious radicals).

This involves a comprehensive inspection of the applicant using: analysis of questionnaire data, conducting verification activities, psychological tests,

database analysis, social network analysis, obtaining information from previous jobs, interviews, etc. and integrated analysis of all the information.

4.2 During work

It is essential to create conditions in which committing a crime is impossible for the employees from the following angles:

1. informational (system of organizational and technical measures to protect information);
2. physical (physical protection system);
3. psychological (human resource management must work with staff to build a strong culture of awareness and motivation to work);
4. organizational (the system of power separation, control, punishment);
5. legal (the system of legal protection – the presence of a system of sanctions and punishment for unlawful acts);
6. technological (system of protection against accidents).

Also a system should be established for monitoring employee information, forecasting crime and their disclosure, supporting employees who have problems on the job and need psychological correction.

It is important to establish internal and external audits on the implementation of the rules within the company and finding weaknesses and eliminating them.

4.3 Dismissal

In the process of a dismissal the following actions should be undertaken: analyze knowledge (possibly stolen data known to the employee, the scope of further work), correction of security protection for objects based on analysis of the dismissed employee (for administrators of databases especially), monitoring the employee being dismissed or having already been dismissed, signing of a nondisclosure agreement.

5 Counteraction Component During Work

5.1 Physical Protection System (PPS)

PPS [1] makes the insider incapable of actions through: making it impossible to obtain visual information beyond the boundaries of the employees' admission area; barriers that prevent physical intrusion into unauthorized areas; refusing access attempts to unauthorized areas; detection and detention of intruders; security object location control.

Physical protection is based on a complex of technical means and guard forces.

5.2 Information Protection System (IPS)

An IPS makes cyber-insiders' actions impossible due to: the impossibility of obtaining information about security systems and protected documents or their location; the existence of information barriers that prevent information penetration in unauthorized areas; information detection, blocking and information location control.

The main IPS elements include [2],[13],[14]: hardware and software access control systems, means of information encryption, antivirus protection, means of firewall shielding, means of access control, security administrators' workbenches, video surveillance tools, protection against power failures, mail servers and workstation activity filters.

5.3 Administrative and Psychological Protection

Administrative and psychological measures are sufficiently intertwined, since both are aimed at preventing the desire to commit illegal acts. [2],[15]

The personnel management system, in terms of preventing insider threats, must be aimed at motivating employees and is designed to form: interest in and desire to work (career growth, interesting and/or profitable work); job satisfaction (in terms of benefits: career growth, professional development, salary, benefits, prospects, good team, short distance from home, etc.); awareness of the unavoidability of punishment.

5.4 Legal Protection

Legal protection forms the employees' awareness of possible punishments for committing certain unlawful actions. The legal protection system intersects with the administrative system in terms of penalties for disloyal behavior. During recruitment an employee signs a contract in which he learns about and agrees with (signs) the applicable restrictions and penalties for their violation.

For offences that violate the employer and employee relationship under the Labor Code, an employee is punished within the company: reproof, bonus reduction, reprimand, dismissal. When crimes under the Criminal Code are committed, the court appoints punishment. Ways of punishment enumerated in the Criminal Code have a stronger deterrent effect on the consciousness of potential insiders compared to the threat of dismissal or public censure.

5.5 Process Control System

The process control system of a complex technical assembly (reactor, refinery, etc.) provides stability of the undergoing process (chemical, nuclear, technical, etc.) within given deviations and projected (planned) accidents. Also, in these systems when one or more critical elements of the system breakdown, management errors, emergency protection systems or hardware correction systems (e.g. valves that reduce excess pressure) are triggered. The intruder can reprogram the system of decision-making, triggering some devices. To prevent this, periodic monitoring is required.

5.6 Protection Comprehensiveness

The protection systems are not separate components, they are closely intertwined. Figure 1 shows the intersections of the protection systems. They can be separated from each other: the enterprise can fail to state loyalty requirements, different departments can be responsible for information and physical protection, and often they are formed independently.

The largest 'holes' in the protection often arise at the joints of the systems. For example, the administrative system does not account clearly for untrustworthiness, physical protection can be switched off by some technological actions, or the administrative (information) system does not consider that a former employee who stole secrets is not legally accountable. Therefore, at the stage of the creation (design) of the protection systems, the interrelation of the systems on documentary, physical, informational and psychological levels must be taken into account.

5.7 The Employee Information Monitoring System

After recruiting an employee, the quality of his work, professional suitability and behavior must be evaluated. Though it is constantly checked informally in the work process, subordinates, employees or executives do not always pay due attention to illicit actions, especially if the employee is trying to hide them.

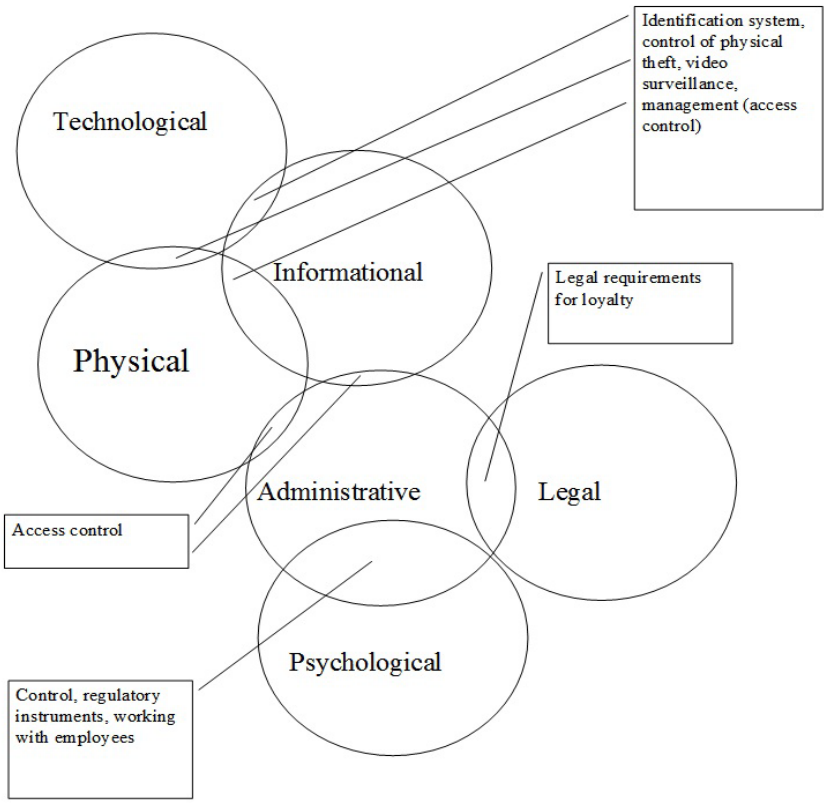

Figure 1 Protection systems' intersection in facility.

To provide assessment of employees in the company, a special system for monitoring their condition can be implemented, consisting of [2],[16]:

1. information sources;
2. collection, processing and analysis of information from sources;
3. decision-making system and system of preventive work with employees who may become insiders or commit wrongful acts.

The two main reasons for wrongful actions are the existence of motives for them and the opportunity to commit them. When opportunity may be prevented by creating a powerful barrier with 5 levels of protection (information, physical, legal, technological, administrative), identification of the possible motives requires invasion of the employees' privacy and significant investments.

6 Choosing Methods for Personnel Check

However, even despite complex counteractions, insiders may still appear. Therefore, it is advisable to use means for their detection or personnel checks.

Currently, there are more than 20 methods of personnel checks. Moreover, there are several ways each method can be organized: 10-20 ways of implementing them, depending on the diagnosed signs of the person being tested.

What to do in a situation where it is necessary to check the staff? Acceptable options are: apply to a known, reliable company for professionals to advise; act as acquaintances would have done; apply to familiar psychologists.

Each of these options is acceptable for organizations with different levels of appropriation for personnel checks. For large organizations the first option is best suited; for average sized organizations, the second, and for small organizations, the third. However, in any case, an economic analysis, i.e. a comparison of the efficiency of the available methods should be conducted.

Except for large corporations, an economic analysis is conducted for comparing two, or at most three parameters (expenses, reliability, and duration), without applying mathematical methods. With more parameters the choice problem is not obvious, nor is there one method of choice. There are several and each is advisable to apply in different cases.

To answer the question which methods are better and which are less adequate, in order to choose the optimal procedure for the task at hand, it is necessary to learn how to compare the different methods. Each method is characterized by several parameters; each technique has its advantages and disadvantages, so the problem of comparing them with each other and selecting the best is a multi-objective optimization problem (in other terms, a multi-objective decision-making problem). This problem arises in cases where it is necessary to select the best of several options when the 'quality' of each option is measured not by one but by several parameters [17].

Let us describe a mathematical model of the problem.

X – is a set of options (types of methods);

Y – is a set of outcomes (i.e. the results of selecting a particular method);

$fi, : Y \to R, i = 1, ..., m$ – is a set of quality indicators (criteria);

$\varphi: X \to Y$ – is a function relating a set of alternatives to the set of outcomes.

Here R is a set of real numbers.

It is assumed that each decision $x \in X$ corresponds to a unique element $y \in Y$, where $y=\varphi(x)$. The 'quality' of each outcome y, and thus the relevant method x, is evaluated by several (m) numbers according to functions fi. Using the relation

$$Ji(x)=fi(\varphi(x)),\ i=1..m$$

we are able to directly assess the quality of option x and work with its vector display:

$$J: x \to R^m,\ J=(J_1,..J_m),\ J(x)=F \subset R^m$$

Thus, mathematically the multi-objective optimization problem has to optimize simultaneously all m criteria, i.e. optimize functionals $Ji(x)$ on the set of feasible solutions X⊂Rn:

$$Ji(x) \to max,\quad i=1..m,\ X \subset Rn,\ x \in X. \qquad (1)$$

The set X is called the set of feasible solutions and further denoted as D. Let us consider traditional 'engineering' methods of multi-criteria optimization that reduce Problem (1) to some of its single-criterion versions.

6.1 The Main Criterion Method

In this method one of the functionals *fi*, for example *f1*, that from the researcher's point of view most completely reflects the quality of the $x \in X$ is selected as objective function. Other requirements to the results, described by functionals *f2, .., fm*, are taken into consideration by introducing the necessary additional restrictions. Thus, instead of Problem (1) another single-criterion problem is solved. The latter takes the form

$$f1(x) \to max;\quad fi(x) \geq ti,\ i=1..m,\ x \in D1 \qquad (2)$$

Formally, a simpler problem of finding the maximum of a functional f1 on the new feasible set $D1 \subset D$ is received. Restrictions in the form of $fi(x) \geq ti$ are added, showing that we agree not to seek the maximum values for functional f2, .., fm, keeping their requirement bounded below acceptable levels. It is important to understand that the transition from Problem (1) to Problem (2) is not a transition from one equivalent problem to another. There is a significant change in the original formulation of the problem, which in each situation requires a separate study. It should be noted that intuitive application of this method usually encounters difficulties associated with the possible presence of several 'main' criteria conflicting with each other. Besides, the algorithm for choosing the lower boundaries ti is not always clear. An unreasonable choice can lead to an empty set *D1*.

6.2 Linear Convolution Method

This is the most widespread method for 'scalarisation' (convolution) of Problem (1), which allows for replacement of the vectorial optimality criterion *f=(f1..fm)* with a scalar criterion *J: D→R*. It is based on linear integration of all individual objective functionals fi:

$$J(x)=\Sigma\alpha_i f_i(x)\rightarrow max\ x\in D;\ \alpha i>0,\ \Sigma\alpha i=1. \quad (3)$$

Weighting factors αi can thus be considered as indicators of relative importance for individual criterial functionals. The more importance we attach to the criterion *fj*, the greater the contribution to the sum (3) it must give, and therefore the higher the chosen value of αi should be. In the case of significantly different criteria it is usually quite difficult to specify the final set of factors αi on the basis of informal considerations or, usually, the results of an expert analysis.

6.3 Maximin Convolution Method

Usually used in the form of:

$$J(x)=min\ fi(x)\rightarrow max;\ x\in D.$$

Here, in contrast to the method of linear convolution, the target functional *J(x)* is affected only by one individual optimality criterion, which at a given point x corresponds to the smallest value of the corresponding function *fi(x)*. And if in case (3), generally speaking, there may be 'bad' values of some fi due to sufficiently 'good' values of the remaining objective functionals, in the case of the maximin criterion calculations are performed 'for the worst case' and according to the value of *J(x)* a guaranteed lower boundary for all functionals *fi(x)* can be determined. This fact is considered as an advantage of the maximin criterion method in comparison with linear convolution.

If necessary, the standardizing of individual objective functionals, i.e. scale coercion of individual objective functionals *fi(x)*, a 'weighted' form of the maximin criterion is used:

$$J(x)=min\ \alpha ifi(x)\rightarrow max;\ x\in D.$$

where the weight factors αi comply to the requirements of (3). By choosing different values for (3) αi, the optimization process can be affected in a certain way using a priori information available.

How to choose the right set of methods to solve the problem? First, the requirements for the survey (a required set of examined qualities, cost constraints, the required accuracy of the test, etc.) must be defined.

At the first step let us choose the significant attributes of test methods for personnel check: cost per person; reliability of the result; secrecy/open format (secrecy characterizes the 'invisibility' of the methods used in relation to the test object); legal application; checking time per person; time before achieving result per person (see Table 1).

Techniques can be used separately or together. When used together, the reliability of the data increases.

At the second step let us grade the importance of the parameters depending on the nature of the problem to be solved (see Table 1): hiring; promotion to an important position (PP); internal investigation (II); long analysis of the causes of the information leakage (LAIL); routine (random) check (RC).

Table 1 Gradation of parameters for personnel checks.

Method parameter	Hiring	PP	II	LAIL	RC
cost per person	2	2	3	4	2
reliability of the result	3	1	1	1	3
secrecy/open format	5	3	4	2	5
legal application	1	4	5	5	1
checking time per person	4	5	2	3	4
time before achieving result per person	4	5	2	3	4

Where 1 is the highest range and 5 is the lowest.

The pair-wise comparison and the Saati and Cogger method were used for evaluation (8 personnel checks were conducted).

At the third step let us estimate the personnel check methods using a five-grade scale (Table 2).

Currently the following personnel check methods are in use:

1. analysis of disloyal information activity (UIA) in information systems (including information security systems) in our facility;
2. analysis of disloyal information activity in the Internet, social networks;
3. interviewing using polygraph (IUP);
4. psychological testing (PT);
5. expert survey of security officers and heads of departments;
6. situational check;
7. questioning;
8. handwriting analysis (HA);
9. interview, polystructural interview;
10. observation;

11. using special equipment (SE) for covert surveillance;
12. collecting information from information databases (IDB);
13. analysis of medical data (AMD);
14. alcohol and drug control.

Psychological testing (PT) is aimed at revelation of mostly negative psychological personality traits (rare mental disorders) unacceptable or undesirable in the workplace.

Expert survey of security officers and heads of departments is used to gauge any common knowledge about the person concerned and is also used to learn about his possible loyal and disloyal actions.

A situational check is used to test a person by creating a testing situation for him, such as occasionally giving more money for a business trip than stated in the register, or having others suggest that he sell information about the object.

A polystructural interview is an interview with a psychologist/psychiatrist based on a structured tree of questions.

Observation is used to obtain data on the person concerned through ongoing monitoring.

Using special equipment (SE) for covert surveillance obtains data by means of information retrieval. Questioning obtains data on the person concerned based on an analysis of questionnaires filled out by him, and a written biography.

Collecting information from information databases (IDB) allows us to learn of any criminal record held by the person concerned, his military service situation and other data in existing federal databases.

Handwriting analysis is the identification of individual psychological variability in the handwriting. The procedure is designed to identify manuscripts (e.g. signatures) and mental states or personality traits of the author.

Collecting information from the place of residence (IPR) is obtaining information about the person concerned from people residing in the same house or building with him, not related directly to his work.

Analysis of medical data (AMD) means obtaining information about the person concerned based on medical records or medical examination to identify data indicating him to be unsuitable for his employment or that could provoke potential disloyalty.

Methods can be used separately or together. When used together, the reliability of the data increases.

Table 2 Evaluation of the parameters of the personnel check methods.

Type	Cost	Relia-bility	Sec-recy	Legal applicat ion	Check-ing time	Time before result	E1	E2	E3	E4
UIA	1	3	4	2	2	2	4	3	3	2
Expert survey	1	3	4	2	3	3	4	3	3	2
Situational check	2	5	3	3	3	5	4	-	4	3
Questioning	1	3	1	5	5	4	-	-	-	-
IUP	3	5	1	4	4	4	5	5	4	5
HA	1	4	2	5	5	4	4	-	-	2
PT	1	4	2	5	4	4	3	-	-	-
Interview	1	4	2	5	4	4	3	3	-	1
Observation	5	5	5	2	1	5	2	4	3	3
Using SE	4	5	5	1	2	5	3	4	5	5
IDB	2	5	5	3	3	5	-	-	-	-
AMD	2	3	4	3	3	3	3	-	-	-

E1 is efficiency for hiring, E2 for promotion, E3 for an internal investigation, and E4 for an analysis of the information leakage. Efficiency of the method is an integral index derived from the weight of the applied method (Table 1) and its significance (Table 2) based on a linear convolution method for expert data [18],[19].

Deciphering of expert values is shown in Table 3.

Table 3 Expert values.

Value	Cost, $ dollars	Reliability, efficiency, secrecy	Legal application	Checking time, hours	Time before achieving result, hours
1	10	Low	Officially forbidden	More than 3 days	-
2	100	Bad	Not allowed	Less than 3 days	-
3	500	Acceptable	Not always allowed	Less than 10	Less than 5
4	3000	Good	Allowed under a contract	Less than 1	Less than 2
5	От 3000	High	Officially allowed	Less than 0,2	Less than 0,2

7 Methods Classification by Examined Features

Methods can be classified by the examined (revealed) features of the subject analyzed:

1. professional suitability (psychological, mental, physical skills and experience in his field of work);
2. satisfaction (degree of conformity of the services offered (salary, benefits, prospects) to the requirements/needs of the candidate);
3. loyalty (fulfillment of the requirements of the object);
4. internal threat;
5. criminal background;
6. criminal inclinations (forecast for possibility of criminal acts);
7. confirmation of the authenticity of the person and his documents;
8. individual unacceptable features (alcohol addiction, drug addiction, previous mental diseases).

Let us make a table of five-grade scores for suitability of each method for detection of each particular feature (see Table 4).

Table 4 Evaluation of test procedures by type of detected features.

	Professional suitability psych/ment/ phys			**Satis-faction**	**Loyal-ty**	**Threat**	**Criminal inclina-tions**	**Criminal back-ground**	**Confir-mation**	**Indivi-dual features**
UIA	2	2	3	4	4	4	4	4	1	3
Expert survey	3	3	4	5	4	3	3	3	1	-
Situational check	2	4	5	5	5	3	5	3	2	-
Questioning	2	3	3	4	3	0	2	3	2	2
IUP	2	2	5	3	5	5	5	5	5	5
HA	5	-	4	-	3	1	4	-		-
PT	5	5	4	-	4	1	4	2		-
Interview	4	5	4	5	5	2	4	3	2	3
Observation	3	3	-	3	1	2	3	-		3
SE	-	-	3	-	-	4	-	-	-	3
IDB	2	2	-	2	-	2	-	4	2	-
AMD	3	-	-	-	-	1	-	-	1	--

Where: 1 – extremely low efficiency; 2 – low efficiency, may be obtained as additional to the main features detected, prone to error; 3 – average efficiency, is used to detect the given feature, adjusted for the veracity of the data reported by the person in question; 4 – good efficiency, slight chance of hiding data, high accuracy; 5 – high reliability, extremely low probability of hiding detecting feature.

8 Choice of a Rational Set of Methods

Finally, how to choose a rational (optimal) set of methods?

1. Select the solvable task (hiring, investigation, etc.);
2. Select personnel features to be detected;
3. Select all the methods that detect the selected features on the main criterion (Table 1), not below a predetermined value;
4. Determine the required total accuracy;
5. Evaluate the potential costs overall;
6. Make a choice.

Below we consider a numeric example to apply this rational set of methods.

Example

Suppose we want to promote one of three employees to replace a head of department retiring in three months. It is necessary to appoint one of them, therefore it is necessary to rank the features of the employees:

1. loyalty (even a competent employee may cause harm by disloyal actions);
2. professional suitability;
3. criminal inclinations.

Assessment of satisfaction makes no sense, since the employee will be transferred to new conditions. We will carry out the main criterion method.

Reliability will be used as the main criterion according to Table 2. The next criterion is value. It is desirable to carry out the survey secretly – this is the third criterion. Time and legal status do not play a significant role, because only three months are available there only legal methods are listed in the table.

Let us now make a table of the methods with efficiency higher than three (or equal to three) for the sum of the three criteria, ordered by reliability and applicability in this situation (see Table 5).

Table 5 Method choice example.

Method	**Professional suitability**			**Loyalty**	**Criminal inclina-tions**	**Reliabi lity**	**Cost**
	psych	ment	psys				
Situational check	2	4	5	5	3	5	0
IUP	2	2	3	5	5	5	150
PT	5	5	4	4	3	4	100
Interview	4	5	4	4	3	4	0
Expert survey	3	3	3	3	3	3	0

As can be seen from the table, it is advisable to identify mental abilities by interview and additionally conduct a survey (it is undesirable to often arrange

checks). Experience can be verified by a situational check and survey; loyalty and criminal inclinations are tested by a check; and a survey is conducted to confirm. It is always advisable to use at least two methods based on different principles.

For psychological qualities the last three methods are acceptable. However, what is the best way: free interviews and surveys or paid psychological testing?

The method of successive concessions can be used for making a selection using two existing criteria: Are we willing to reduce the reliability (the main criterion) with a decrease in the second criterion? In other words, are we ready to pay $100 for psychological checking with reliability 5, or can we reduce the reliability to 4 and implement an interview, as well as confirm the survey of other employees? In this case, if an employee consistently showed himself capable in stressful situations, we can limit the reliability of the two methods with 3 and 4, which together will be more than 4 but less than 5. If it is unknown how the employee performs in stressful situations (while he is promoted to a higher position, where stress-resistance is necessary), it is desirable to spend $100 on psychological analysis.

As shown, by the use of the proposed method, not only can the economic costs be reduced, but also the choice of methods can be made most effectively [18,19].

Let us include criminal inclinations into our analysis. If we append it into our analysis we can fill out the next Table (6).

Table 6 Numeric analysis (analyze medium of max values and then analyze minimum of each point).

Set	Common cost, $	Loyalty	Criminal inclination	Professional suitability	RESULT: Cost/ Medium reliability
Expert	0	3	3	3	**0/3,67***
survey		4	3	4	
Interview		**4 – max**	**3 - max**	**4 - max**	***(4+3+4)/3= 3,67**
Expert	100	3	3	3	**100/4**
survey		4	3	4	
Interview		4	3	5	
PT		**4 – max**	**3 – max**	5 **– max**	
Expert	250	3	3	3	**250/5**
survey		4	3	4	
Interview		4	3	5	
PT		5	5	4	
IUP		**5 - max**	**5 - max**	**5 - max**	

In the table we can see the numeric results: in the first two lines the medium reliability is not bad, but severe criminal inclinations are detected, so we should choose line three for $250, because this is the best way to decrease the internal threat.

9 Conclusion

In the course of the work, a complete group of systems to counteract insider threats was made; 'weak points' that arise at the intersection of the systems were defined. Their protection should be thought of very carefully. Comprehensive programs to counteract insider threats are implemented at critical facilities.

The article also lists all the modern methods of personnel checks, defining their parameters; their comparative analysis is provided, as well as methods of selecting the set of rational methods for testing personnel with limited funding.

This methodology is currently being implemented in the 'Testing personnel' program (which is used in critical facilities) designed to assess employees of critical facilities and is scheduled for testing in late 2014 within the pilot program 'Improving the reliability of personnel at critical facilities'. During implementation of the program modules, all methods are implemented and the data from the second part of the article are loaded. The results of the testing program will be presented in a following article.

References

[1] Shemigon N.N. & Petrakov A.V., *Protection of Objects: Machinery and Technology*, Energoatomizdat, Moscow, 2005.

[2] Zhurin S.I., *Framework for Counteracting Insider Threats*, Textbook: MEPhI, Moscow, 2013.

[3] *Insider Threat Attributes and Mitigation Strategies*, SoftWare Engineering Institute, https://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_57590.pdf (5 March 2015).

[4] *Common Sense Guide to Mitigating Insider Threats*. SoftWare Engineering Institute 4th Edition, 2012, http://resources.sei.cmu.edu/asset_files/TechnicalReport/2012_005_001_34033.pdf (5 March 2015).

[5] *The 'Big Picture' of Insider IT Sabotage Across U.S.* Critical Infrastructures. 2008, https://resources.sei.cmu.edu/asset_files/TechnicalReport/2008_005_001_14981.pdf (5 March 2015).

[6] IAEA, *Preventive and Protective Measures against Insider Threats*. IAEA Nuclear Security, Series 8, 2008.

[7] INFCIRS, *Convention on the Physical Protection of Nuclear Material*, INFCIRS/274/rev. 1, 1987.
[8] RF Government, *Rules of Physical Protection of Nuclear Materials, Nuclear Plants and Storage of Nuclear Materials*, RF Government Decree number 456, Approved 19.07.2007.
[9] INFCIRS, *Physical Protection of Nuclear Material (NM) and nuclear facilities (NF)* - INFCIRS/225/rev. 5, 2011.
[10] *Memorandum: Army Directive* 2013-18 (Army Insider Threat Program), http://www.fas.org/irp/doddir/army/insider.pdf (5 March 2015).
[11] *The Russian Federal Law 'On Combating Terrorism,* from 25.07.98. № 130-FZ.
[12] Kudryavtsev, B.N., *Genesis of crime*. 'Infra-M', Moscow, 1998.
[13] Duran F. Conrad S., Conrad G. Duggan D., Held. E., *Building a System for Insider Security*, IEEE Security and Privacy, **7**(6), pp. 30-38, 2009.
[14] Kanaskar, N., Bian, J., Seker, R., Nijim, M., Yilmazer, N., *Dynamical System Approach to Insider Threat Detection*, IEEE International Systems Conference (SysCon), pp. 232-238, 2011.
[15] Kharskiy K.V. *Loyalty and Trustworthiness of Staff*. PITER, Sankt-Peterburg. 2003.
[16] Zhurin S.I., *Automated System for Preventing Crimes as Part of The Security of An Important Public Facility (Thesis for The Degree of Candidate of Technical Sciences)*, MEPhI, Moscow, 2000.
[17] Shapiro D.I., *Multicriteria Models for Forming and Choosing Systems*, M. Energoatomizdat, Moscow, 1983.
[18] Kini, R.L. & Rayfa, H., *Decision-Making at Many Criteria: Preferences and Replacements*, Radio and Communications, Moscow, 1981.
[19] Litvak, B.G., *Expert Information: Obtaining Methods and Analysis*, Radio and Communications, Moscow, 1982.