Intelligent complex security management system FEC for the Industry 5.0

N V Korneev¹,²,³
¹Gubkin Russian State University of Oil and Gas, Moscow, Leninsky Prospect, 65, Russian Federation
²Financial University under the Government of the Russian Federation, Moscow, Leningradsky Prospekt, 49, Russian Federation
³Email: niceyper@mail.ru

Abstract. Taking into account the digital transformation, the prospects for the development of intelligent complex security management system FEC are revealed. For the first time a definition of intelligent complex security management system FEC is given, also, its generalized structure is developed, considering the development of the Russian human-machine concept, as a complex information-energy system, on the basis of intellectualization of theoretical principles of human physiology and psychology. Its main elements are defined: a core, subsystems and components and mathematical dependencies implementing management functions are given. The core, subsystems and components are represented by the protected system at the level of security threat management in the form of a block-functional system scheme with elements of artificial intelligence that differ in the detail level. The mutual influence mechanism of separate subsystems and components is defined through simple, hybrid and complex threats. Besides, system threats of FEC were classified and their definitions were given. As an example, we consider the complex threat related to security of critical information FEC infrastructure. What is more, the basic intelligent management principles of complex FEC security are formulated, based on the block-functional system scheme with artificial intelligence elements and operator state security identification in real time. We obtained general equations of the output state variables vector, which is equivalent to the security model of the operator, vectors of output state variables in case of hybrid, complex, and system FEC threats.

1. Introduction
Rapid development of information technologies has led to the digital transformation [1]. Digital transformation can be considered as an integration process of innovative technologies and business processes. In the digital economy it required to change technologies, culture and principles for creating new products and services. Nowadays, The Industry 5.0 can be defined as the best groups, methods and tools for digital transformation. National artificial intelligence development strategy for the period up to 2030 (Decree of the President of the Russian Federation 10.10.2019 № 490) influenced on the Industry 5.0 development.

The artificial intelligence [2] – this is a dynamic system that is able to (without human intervention) create full-featured models displaying complex world phenomena and itself in this world; analyze an
adequacy (correspondence) of different model variants in order to select the most accurate ones; generate variant predictions of expected consequences based on the selected models.

All of the above offer new opportunities for the information processing systems development. The structure of information processing systems changes fundamentally which is now based on distributed information-computing networks, connected to global data networks, convergent, hyper-converged, neuromorphic and quantum computing systems. At the same time, regulatory requirements are toughened, especially, in terms of complex object security: physical, economic, fire, informational, psychological, intellectual property security, technogenic, security against terrorism, ecological safety and power security. For the fuel and energy complex (FEC) – this is first and foremost Energy security doctrine of the Russian Federation (Decree of the President of the Russian Federation 13.05.2019 № 216), new version of the information security Doctrine (Decree of the President of the Russian Federation 05.12.2016 № 646), Federal law July 26, 2017 № 187-FL "On the Security of the Russian Federation Critical Data Infrastructure", Federal law July 21, 2011 № 256-FL "On the safety of fuel and energy complex facilities", Federal law July 27, 2006 № 149-FL "About information, information technology and data security ". In these documents, the priority is given to the fuel and energy complex facilities safety, including through continuous monitoring of object operation threats.

We consider the concept of the object in its broader notion. Modern management theory considers a person, the world around him and certain parts of this complex system as objects for studying the possible effective impact on them. Let us call the part of this world that interests us - an object of management, we will characterize the position of this part in the world by the term - an object state, purposeful change of object state and the way of achieving certain goals in it by the term-management. Thus, the object of management is any phenomenon of the world (or the subject itself) which is considered in terms of creating some purposeful movement. It is natural to call the final state of the object desired, i.e. which we are interested in and which defines the purpose of management as the conversion of an object to the desired state and the act of conversion as a process of management or just management.

In this case FEC as an object can include the oil, gas, coal and peat industries, electricity and heat supply that is fully corresponds to the energy security Doctrine of the Russian Federation. However, if considering complex object security, expand its use for solving national security problems.

Based on the above, it becomes obvious the essence of the complex security – ensuring all security components of the facility: physical, economic, fire, informational, psychological, intellectual property security, technogenic, security from terrorism, environmental security and energy security including new components.

In this case, the concept of complex security is more flexible и self-organizing for digital transformation of an object, and the theory of management does not change the fundamental principles, that give the opportunity for creating an appropriate object management system for the Industry 5.0 including artificial intelligence elements.

The new concept is not about replacing a person – EC (electronic computer), but in their mutual complement. This approach is described in detail in [3] as a new class of "systems with artificial intelligence elements".

Thus, intelligent complex security management system FEC is a class of managing human-machine systems providing all the fuel and energy complex safety components with elements of artificial intelligence or artificial intelligence.

Currently, the implementation of this approach is observed [2, 3] in all areas of life activity. Separate components of the complex security management system are being developed for FEC. For example: physical [4, 5], economic [6, 7], fire [4, 8, 9], informational [10, 11, 12], individual solutions for intellectual property security offer companies «SearchInform» and «InfoWatch», technogenic [13, 14, 15, 16, 17], ecological safety [18, 19, 20], power security [6, 21, 22], psychological, security against terrorism [4, 23] are unavailable.

It is easy to notice that there aren’t any Russian solutions for the most subsystems and components, generally, there is no Russian intelligent complex security management system of FEC.
Thus, the generalized structure of the intelligent control system for complex security of FEC becomes obvious, based on the Russian concept of the human-machine system development.

2. Results and Discussion

The generalized structure of the intelligent control system for complex security of FEC, taking into consideration the Russian concept of the human-machine system development as a complex information-energy system, based on intellectualizing the theoretical principles of human physiology and psychology is shown in Figure 1.

![Figure 1. The general intelligent complex security management system of FEC](image-url)

It is represented by a set of subsystems $S_n$ ensuring all components of FEC security: physical ($S_1$), economic ($S_2$), fire ($S_3$), informational ($S_4$), psychological ($S_5$), intellectual property security ($S_6$), technogenic ($S_7$), security against terrorism ($S_8$), ecological safety ($S_9$), power security ($S_{10}$) including new elements ($S_n$) and their components: $S_{1p}$, $S_{2e}$, $S_{3f}$, $S_{4s}$, $S_{5h}$, $S_{6l}$, $S_{7t}$, $S_{8r}$, $S_{9v}$, $S_{10g}$, $S_{nk}$. Generally, the number of components in each subsystem is different. The core, subsystems and components – this are a representation of the protected system at the level of security threat management in the form of a block-functional scheme of the system with artificial intelligence elements (Figure 2) that differ in the detail level. For subsystems and components the features of the corresponding FEC security elements are taken into account. It should be noted that if considering the schemes of the system core, the operator of an intelligent integrated security management system of
FEC – is the president of Russia, and, the management system is an element of strategic planning in the sphere of ensuring the Russian Federation security.

The scheme (Figure 2) shows the development of the block-functional scheme [3, 24] in the direction of supplementing the usual human-machine system with artificial intelligence elements. They are mainly related to the right side of Figure 2 under the pointer «Intelect ECM». The following computational models and modules are assigned to this system part: environment – «direct» model 1; the object – «direct» model 2; imitators: model 1 the operator of the environment; model 2 the object of the operator; personality model of the operator; personality module of the corrector; the vector observer module.

Model imitators 1 and 2, as well as the personality model of the operator of the corresponding security subsystem have a task to approximately repeat the security models that exist within the operator. Their tasks – explain and predict the behavior of the operator due to these factors. For example, the operator PCS thinks that a compressor is broken or the operator SIEM (Security Informational and Event Management) thinks that there is a cyber attack on the enterprise's SCADA system. The personality model displays his behavior when such a hypothesis appears. The imitators’ task is to repeat the properties of internal models as closely as possible.

The difference between “direct” object model and the environment in the management system from the internal models of the operator and their imitators, i.e., the display of these models formed by the operator is as follows:

- the direct model of the object is the result of its diagnosis and current monitoring in stationary conditions. In details, this model is significantly more accurate than the internal operator model (especially, if the operator is not highly qualified);
- the direct model of the environment can be formed in the management system objectively (software and hardware), including maps of the current object operation area; communication and interrelation schemes of an object, atmospheric and operating conditions; the presence of dynamic and other types of interference when operating. If considering critical information infrastructure (CII) FEC – reports

**Figure 2.** Block-functional system scheme with artificial intelligence elements
on current operation of potential CII objects, industrial safety data sheet of a hazardous industrial object, protection in the structure of potential CII objects;

the object and environment models of the operator are subjective and deformed by his personality model.

Generally, like the operator identification table, these modules have the character of handlers of accumulated information and devices for generating additional diagnostic actions and actions of an executive nature.

Direct display of the object state and environment based on diagnostic information about the object and the most complete environment available for the management system.

At the same time, we cannot assume that this information is identical to the equation given in the work [3, 24], for this reason:

\[ \tilde{X}[k+1] = \Phi( \tilde{X}, U, \tilde{F}, t) \tilde{X}[k] + \tilde{\Gamma}(t) \tilde{U}[k] + \tilde{G}(t) \tilde{F}[k], \]  

(1)

where \( \tilde{X}[k+1], \tilde{X}[k] \) – the most accurate possible vectors evaluations of the object state and environment; \( \Phi( \tilde{X}, U, \tilde{F}, t) \) – state transition function determined by the most accurately known parameters of the object state and environment; \( \tilde{F}[k] \) – vector evaluation of direct environmental impacts; \( \tilde{\Gamma}(t) \tilde{U}[k], \tilde{G}(t) \tilde{F}[k] \) – integral transformations of the most accurately represented controlling and disturbing influences.

Equations for the secondary object and environment display in the management system. The secondary display is the equation of the secondary models displaying the internal operator models in the management system. They can be recorded in a form similar to the given equation [3, 24] using the double dash sign at the top of the symbol to indicate the secondary model functions and variable estimates:

\[ \overline{X}[k+1] = \overline{\Phi}( \overline{X}, U, \overline{F}, t) \overline{X}[k] + \overline{\Gamma}(t) \overline{U}[k] + \overline{G}(t) \overline{F}[k], \]  

(2)

where \( \overline{X}[k+1], \overline{X}[k] \) – vector condition estimates of object state and environment in the secondary models; \( \overline{\Phi}( \overline{X}, U, \overline{F}, t) \) – the function of the secondary transition model, \( \overline{F}[k] \) – perturbation vector estimate in the secondary model; \( \overline{\Gamma}(t) \overline{U}[k], \overline{G}(t) \overline{F}[k] \) – conversion of the secondary model impacts; \( \overline{Y}[k] \) – vector of the secondary models state variables: \( \overline{Y}[k] = \overline{C} \overline{X}[k] + \overline{\nu}[k], \) где \( \overline{\nu}[k] \) – noise measurement vector; \( \overline{C} \) – estimator matrix of measurable variables.

Equations of the secondary personality model of the operator. This model is constructed similarly, taking into account the object functions and environment models that are already known:

\[ \overline{Y}[k+1] = \overline{\nu}(\overline{Y}, t) \overline{Y}[k] + \overline{\psi}(\overline{X}, t) \overline{X}[k+1] + \overline{F}(t) \overline{U}[k] + \overline{\sigma}(t) \overline{F}[k], \]  

(3)

where \( \overline{Y}[k+1], \overline{Y}[k] \) – operator's actions vectors based on its secondary model; \( \overline{\nu}(\overline{Y}, t), \overline{\sigma}(t) \) – transition function of the operator secondary personality model.

According to (3) the operator's actions are based on internal state and object state prediction and environment. Thus, the influence of the object state prediction and environment on the formation of the vector of operator’s management considers separately. Predictive abilities of the operator for FEC are very important and require special testing and development.

Subsystems (Figure 2) may include separate components that are selected from the complex security subsystems based on the above concept of an object and solved security problem; for example, by the sequential decomposition of environment, object and models to the level of an object with elementary security threats.
It should be noted, that the issue of mutual interrelation of individual subsystems and components on each other is quite important and at the same time difficult to solve. In the Figure 1 links that characterize this effect are highlighted in bold. Such interaction is related to the mutual impact of individual subsystems and components on each other. One of the possible ways to account for this impact is related to the concepts of hybrid and complex threat.

Complex threat – a threat consisting of several different elementary threats, connected by means of certain synchronized mechanisms and not necessarily existing in one space.

Hybrid threat – a variation of a complex threat, which necessarily contains elementary threats that affect different areas of the protected system.

It is also worth noting that the existence of hybrid threats is closely related to the term “hybrid war” [25, 26, 27]. These are subtypes of complex threats and characterized by the property of forming and implementing the threat components not in a single space (for example, only in the physical) and in several spaces simultaneously (for example, in physical and information space).

The work [28] examined the practical problems of complex threats (CT) and the peculiarities of their formation and implementation. On that basis, proposed the approaches to ensuring security, which can most effectively be manifested in the presence of tools and methods for identifying the very fact of the presence of CT and determining the list of possible targets of CT. Implementation of these mechanisms can be achieved using big data analytics integrated from various sources, for example at the object level – FEC enterprise.

At the system core level, not only complex FEC threats are considered, but also FEC system threats that can be defined like this.

FEC system threat – this is a complex threat to the oil, gas, coal and peat industries, electricity and heat supply. In a system threat sets of complex threats are already subjects for consideration, selected on the basis of the above object concept and solved subsystem security problem and united, for example in a cluster. As an example of state systems, operating at the level of system threats – State system for detecting, preventing and eliminating the consequences of computer attacks, SIS FEC (State information system of the fuel and energy complex).

Further, as an example we will consider the complex threat connected with ensuring the security of the critical data infrastructure of the FEC. We will consider the FEC enterprise as an object. For the certainty in security tasks, assume that we know the basic threat model of the object (Figure 1) and includes information security threats (subsystems $S_4$), technogenic ($S_7$). The considered problem relates to complex threats, but we will take its variation – a hybrid threat that includes elementary threats: 1 information security threat and 1 technogenic safety threat. In short, assume that the environment in case of information security threat is formed by security events in SIEM (Security Informational and Event Management), technogenic safety – event report in PCS.

In this case, we will have two systems of block-functional structure (Figure 2). Using the example of these systems, we formulate the basic principles of intelligent management of complex FEC security based on the block-functional scheme of the system with artificial intelligence elements. This approach is based on identifying security states of the operator (Figure 2) in real time [3, 24].

1. Selection of the controlling element set used by the operator. For a considering task we assume that both operators have the ability to respond to a security event, using the computer mouse and entering data from the keyboard. It should be noted that in real conditions we can use advanced systems for actions control.

2. Defining the conditions when implementing event or set of events that are synchronized by a specific mechanism, for example time $t$ can be considered as security threat. This problem has a lot of solutions. For example, the most well-known is the use of a rules set as a part of SIEM based on heuristic methods [29]. However, this option refers to an analytical approach of modeling that does not always adequately reflect reality, especially in the context of complex interaction processes in the real world.
The proposed intelligent complex security management system FEC (Figure 1) allows to realize not only analytical, but also informational approach based on modern data mining technologies and big data processing methods [28].

For a considering task we assume that both operators can respond to a security event directly using a computer mouse, but to respond to a security threat you must use the keyboard. This condition allows you to initially isolate a threat from security events in SIEM at the operator action level. This approach is justified because most of the events registered by SIEM are not threats and the operator scroll through them using the computer mouse. At the same time, for a threat such as domain control attack by selecting a software password RDP, the operator will be required to use the keyboard to create more complex password for RDP.

3. Identification of a functionally complete threat measurement system. According to modern concepts such measurement system contains:

1. Sensor of event 1 – \( Y_1 \), frequency of event 1 – \( Y_1 \).
2. Sensor of event 2 – \( Y_2 \), frequency of event 2 – \( Y_2 \).
3. Sensor of event 3 – \( Y_3 \), frequency of event 3 – \( Y_3 \).
4. The sensor of the left key of a computer mouse – \( U_1 = \xi_1 \).
5. The sensor of the right key of computer mouse – \( U_2 = \xi_2 \).
6. Computer mouse scroll sensor – \( U_3 = \xi_3 \).
7. Keyboard activity sensor (buttons Enter) – \( U_4 = \xi_4 \).

In the list below we mentioned three event sensors. In real conditions their number is determined according to the analysis of the exploited vulnerability of the threat, i.e. a factor, based on the protected system properties or protection methods that are used when implementing a specific elementary threat. The dash sign means the sensor indicators as measurable coordinates: \( Y \) – measurable (output) state variables; \( U \) – control actions of the operator.

A significant number of identification variables follows from this set of sensors: for sensors number 4…7 the actions of the operator are also characterized by the direction (sign) of the impact which is essential for this class of systems. It should be noted that for other FEC objects measurable state variables and operator control actions can be similarly allocated.

It allows you to create the following table 1.

| Sensor number | Action direction | Impact direction | Impact |
|---------------|------------------|------------------|--------|
| 4             | keypress         | \( \xi_{11} = \xi_{1+} \) | \( \xi_{121} = d\xi_{11}/dt \) |
| 4             | button release   | \( \xi_{12} = \xi_{1-} \) | \( \xi_{122} = d\xi_{12}/dt \) |
| 5             | keypress         | \( \xi_{21} = \xi_{2+} \) | \( \xi_{221} = d\xi_{21}/dt \) |
| 5             | button release   | \( \xi_{22} = \xi_{2-} \) | \( \xi_{222} = d\xi_{22}/dt \) |
| 6             | up               | \( \xi_{31} = \xi_{3+} \) | \( \xi_{321} = d\xi_{31}/dt \) |
| 6             | down             | \( \xi_{32} = \xi_{3-} \) | \( \xi_{322} = d\xi_{32}/dt \) |
| 7             | keypress         | \( \xi_{41} = \xi_{4+} \) | \( \xi_{421} = d\xi_{41}/dt \) |
| 7             | button release   | \( \xi_{42} = \xi_{4-} \) | \( \xi_{422} = d\xi_{42}/dt \) |

Thus, \( \xi[k] \) – vector of output (measurable in the control system) state variables, which is equivalent to the security model of the operator, can be represented as follows:

\[
\xi[k] = \Lambda(V,U,t)V[k] + V[k],
\]
where $\Lambda(V, U, t)$ — a vector-function, identifying the security state of the operator; $v[k]$ — a noise vector accompanying operator’s action. In case of an analytical approach the vector-function is defined by an extended object space, based on differential equations in Cauchy form [24], information approach – data mining technologies and big data processing methods [29].

It is noteworthy that the output state variables vector for the second system of the block-functional structure will be similar (Figure 2), determining the threat to technotronic security. Then the record of the output state variables vector of the considered example in case of a hybrid threat will be:

$$
\xi[k]_{hyb} = \xi[k] \cap \xi^2[k],
$$

where the upper indexes belong to the considering block-functional structure systems (Figure 2).

Based on (Figure 1) the record of the output state variables vector in case of a complex threat will be:

$$
\xi[k]_{com} = \bigcup_{k_1} \bigcup_{k_2} \xi[k],
$$

in case of a hybrid threat:

$$
\xi[k]_{hyb} = \text{var} \xi[k]_{com}.
$$

The equations (6, 7) are valid if the object and environment are equivalent.

Based on (Figure 1) the record of the output state variables vector in case of a system threat will be:

$$
\xi[k]_{sys} = (\triangleright \triangleleft \xi[k]_{com}),
$$

where operator $\triangleright \triangleleft$ denotes a method for joining vectors of output state variables in the case of a complex threat, for example, clusterization - is a natural join.

3. Conclusion

Among the local models included in the structure (Figure 2) the personality model of the operator has the greatest non-stationarity. Studies of the current identification of this model parameters are a scientific complex security problem, where the tasks are: constructing procedure for identifying the object management style using the fuzzy set theory, identification procedures for an extended object threat model based on modern data mining technologies and big data mining methods, procedures of intelligent complex security management of FEC by replacing the operator with artificial intelligence, for example, in the form of a self-learning neural network or a neurograph [4]. We note that these tasks determine the need to consider dynamic evaluations which change according to conditions, and, above all - the state of the operator.

References

[1] Patel K and McCarthy M P 2000 Digital transformation: the essentials of e-Business leadership (New York: McGraw-Hill) p 144
[2] Korneev N V 2008 Printsyip postroeniya sovremenyykh tekhnicheskikh sistem s elementami iskusstvenogo intellekta [Principles of construction actual technical systems with elements of artificial intellect] Tekhnika mashinostroeniya 2(66) 2–7 (in Russian)
[3] Korneev N V 2008 Intellektual'naya sistema upravleniya transportnym sredstvom s uchetom lichnykh osobennostei voditelya [Intellpect system control transport mashin based on driver's personal characteristics] Tekhnika mashinostroeniya 3(67) 54–56 (in Russian)
[4] Korneev N V 2019 IOP Conf. Ser.: Earth Environ Sci. 224 012021
[5] Mosolov A S and Grafova O V 2010 Proc International Conference on Security of Information and Networks (Rostov-on-Don: ACM Press and Digital Library) pp 134–136
[6] Cao J, Wang Y, Zhu C, Zhang Y, Guo C and Cao Y 2012 Automation of Electric Power Systems 2 77–81
[7] Yu Y X and Luan W P 2009 Zhongguo Dianji Gongcheng Xuebao / Proceedings of the Chinese Society of Electrical Engineering 34 1–8
[8] Danilov A I, Mel’kov S A, Solov’eva N V, et al 2019 Russ. Meteorol. Hydrol. 44 300–304
[9] Thompson P and Marchant E 1995 *Fire Safety Journal* **24**(2) 131–148
[10] Markov A S, Barabanov A and Tsirlov V 2018 Periodic Monitoring and Recovery of Resources in Information Systems *Probabilistic Modeling in System Engineering* ed A Kostogryzov (London: IntechOpen) chapter 10 p 278
[11] Korneev N V 2013 *Algoritmicheskie i programmy metody i sredstva otsenki alternatunnykh proektov zauchity sistemy obrabotki informatii predpriyatiya na osnove mnogokriterial'noho analiza* [Algorithmic both program methods and tools estimation of alternative projects of the guard data reduction system of firm on the basis of the multicriteria analysis] (Togliatti: Volga Region State University of Service Press) p 116 (in Russian)
[12] Korneev N V and Korneeva Yu V 2014 *Audit sistemy menedzhmenta informatsionnoi bezopasnosti* [Audit of system management information security] *Standarty i Kachestvo* **7**(925) 60–64 (in Russian)
[13] Kershenbaum V, Grigoriev L, Kanygin P and Nistratov A 2018 Probabilistic Modeling Processes for Oil and Gas *Probabilistic Modeling in System Engineering* ed A Kostogryzov (London: IntechOpen) chapter 3 p 278
[14] Oliveira L E S and Alvares A J 2016 *Procedia CIRP* **53** 198–205
[15] Wei L, Chuipin K, Qiang N, Jingguo J, Xionghui Z 2020 *Robotics and Computer-Integrated Manufacturing* **61** 101842
[16] Peng L, Tianliang H, Chengrui Z 2011 *Procedia Engineering* **15** 840–847
[17] Korneev N V and Yanitskiy A I 2019 *Russ. Electr. Engin.* **90** 696–701
[18] Gerardo A, Vibeke S May-Britt E, Jukka T and Adrian T *Sustainability* **11**(17) 4611
[19] Smolenskaya N M Smolensky V V, Korneev N V 2018 *IOP Conf. Ser.: Earth Environ. Sci.* **121** 052009
[20] Smolenskaya N M, Korneev N V 2017 *IOP Conf. Ser.: Earth Environ. Sci.* **66** 012016
[21] Koyalev A 2017 *Energy manager* **1** 3–5
[22] Karasev Y, Konev V, Evlanov M and Krykov I 2014 *Automation and IT in energy* **11**(64) 23–33
[23] Young C 2014 *The Science and Technology of Counterterrorism* (Oxford: Butterworth-Heinemann) p 512
[24] Korneev N V, Kustarev Yu S and Morgovsky Yu Y 2008 *Teoriya avtomaticheskogo upravleniya s praktikumom* [Theory automatic control with workshop] (Moscow: Publishing house Academia) p. 224 (in Russian)
[25] Davis Jr J R 2015 *The Three Sword Magazine* **28** 19–25
[26] Hunter E and Pernik P 2015 *The challenges of hybrid warfare* (Tallinn: International Centre for Defence and Security) p 7
[27] Mälksoo M 2018 *European security* **27**(3) 374–392
[28] Korneev N V and Merkulov V D 2019 Intelligent analytics for complex security *Secure Information Technologies* (Moscow: Bauman Moscow State Technical University Press) pp 215–219
[29] Markov A S, Matveev V A, Fadin A A and Tsirlov V L 2016 *Vestn. Mosk. Gos. Tekh. Univ. im. N.E. Baumana Priborostro.* **1** 98–111