algorithmic mathematics and mathematical modeling

Computer tools in education, 2022
№ 2: 32–40
http://cte.eltech.ru
doi:10.32603/2071-2340-2022-2-32-40

PLANNING AND QUALITY EVALUATION OF PHYSICAL PROTECTION SYSTEMS USING SIMULATION MODELING

Sharkov I. K.[1,2], Postgraduate, ✉ shark2.1@mail.ru, orcid.org/0000-0001-7290-7013
Krylov V. M.[3], PhD, Associate Professor, victor@cctv.ru, orcid.org/0000-0002-4678-423X
Kolesov Y. B.[2], PhD, ybk@mail.ru, orcid.org/0000-0002-6307-6710

[1]Peter the Great Saint Petersburg Polytechnic University,
29, Polytehnicheskaya str., Saint Petersburg, 195251, Russia
[2]Complex systems, LLC, Skolkovo Innovation Centre,
42, Bolshoy Boulevard, bld. 1, off. #32, 143026, Moscow, Russia
[3]PENTACON LLC, 25 D, Krasnogo Kursanta str., 197198, Saint Petersburg, Russia

Abstract

This article reviews quality evaluation problems of Physical Protection Systems (PPS) at its design stage. «AKIM» simulation modeling software is proposed to reach the quality evaluation of PPS. «AKIM» software complex uses drawing of a planned PPS for an automated creation of an agent-based model that can simulate intruder attacks and security's responses, assess the quality of a defense system and reach security system technical requirements.

Keywords: *Physical protection system, simulation modeling, agent-based model, graphic engineering, quality evaluation, terms of reference, AKIM.*

Citation: I. K. Sharkov, V. M. Krylov, and Y. B. Kolesov, "Planning and Quality Evaluation of Physical Protection Systems Using Simulation Modeling," *Computer tools in education*, no. 2, pp. 32–40, 2022; doi:10.32603/2071-2340-2022-2-32-40

1. QUALITY EVALUATION OF A PPS AT A PLANNING STAGE

At the moment there is no available data about the tools for computer simulation and PPS quality evaluation that use an object oriented method and allow for the agent-based model that imitates intruder attacks and lets users assess the system's security level to be built from the secured facility's drawing. A graphical language describing the designed object and a security system's simulation model accelerate the designing process, allow for the study of model's properties and, as a result, lead to an increase in the quality of terms of reference for a PPS implementation.

Existing solutions for a PPS modeling are based on intruder attack graphs and conceptual ideas about a system [1]. Used models allow to plan the control points (CP) placement on the way to the critical elements (CE) and to determine a probability level of detection PDet. and neutralization PNeut. of intruders to provide the required security level. The results of this modeling become the requirements for the structure of a future PPS.

For an adequate evaluation of the planned PPS the clear and detailed drawing of its structure is required. For example, a two- or three-dimensional digital drawing (made with AutoCAD,

NanoCAD, Revit, etc.). There are implementations [2] that allow, based on projects' BIM (Building Information Modeling), to form the graphs of intruders' movements through a secured area. The limitations of such solutions are a quite high difficulty threshold for a conceptual design and also a requirement to graph the paths based on the building plans that exclude the description of a security on its surrounding area. Such method can only be used for already existing facilities that have digital drawings.

If a PPS drawing is used as a base for formation of its mathematical model, then simulation software can be used. That software allows making the digital twin of an object in the form of a scheme using prefabricated components (standard elements) of engineering and technical security assets and guard forces. Aside from PPS elements there must be components for implementing the external factors (weather, false alarms) and an intruder model that take the place and the purpose of an invasion into account. A model must include: the models of an engineering (EMoP) and a technical means of protection (TMoP), a security forces (SF) model. The modeling purpose is the evaluation of PPS effectiveness with at least two quantitative security ratings:

- Intruder detection possibility (PDet.);
- Intruder neutralization possibility (PNeut.) by security forces.

There are various methods of the computer modeling in PPS evaluation tasks [2–4], however almost all of them describe a PPS structure using a path graph. The more detailed is the system's description, the more difficult a PPS model is and the harder it is to describe it with a graph. Increasing the size of a graph (or using a superimposed grid) leads to an exponential increase of the modeling data [2, 3, 5, 6]. Due to this, it's rational to use a simulation modeling method for the quality evaluation tasks. Thanks to the high computational power of personal computers and an ability for parallelized simulation experiments, it's possible to conduct enough experiments to get a quality assessment with the necessary degree of accuracy using small enough confidence intervals (around $\varepsilon = 0.01$ or even lower).

2. MATHEMATICAL MODEL IMPLEMENTATION IN ANYDYNAMICS

There are many different tools fitting for the tasks of a PPS simulation model development: MATLAB, AnyDynamics, Dymola, MapleSim, AnyLogic, Scilab, Maxima [7]. For the creation of PPS model a high performance environment for the development of the multicomponent models of complex dynamic systems AnyDynamics that can create embeddable in applications models (dll) was used. Agent-based model was picked. This method allowed to describe the agents' interaction on a language understandable by PPS developers and evaluating experts. Some of these conceptual models are known [8], and can be used for developing these agent-based models.

Presentation of classes of all entities of such model is shown in Figure 1.

Creation of an intrusion scenario is provided by the developed algorithms for the formation of event-driven paths with the use of behavior maps, and it is implemented with the help of «Polaris» [9] pathfinding algorithm. These algorithms provide an automated attack scenario forming a process that requires only starting and finishing conditions. Because of that there is no need in path graphs, laid through the drawing of PPS digital twin.

The modeling of interaction between an intruder and PPS elements allows for the collection of necessary data about a process and results of each experiment. Based on data from numerous statistical experiments the quantitative quality evaluations of the modeled system can be collected.

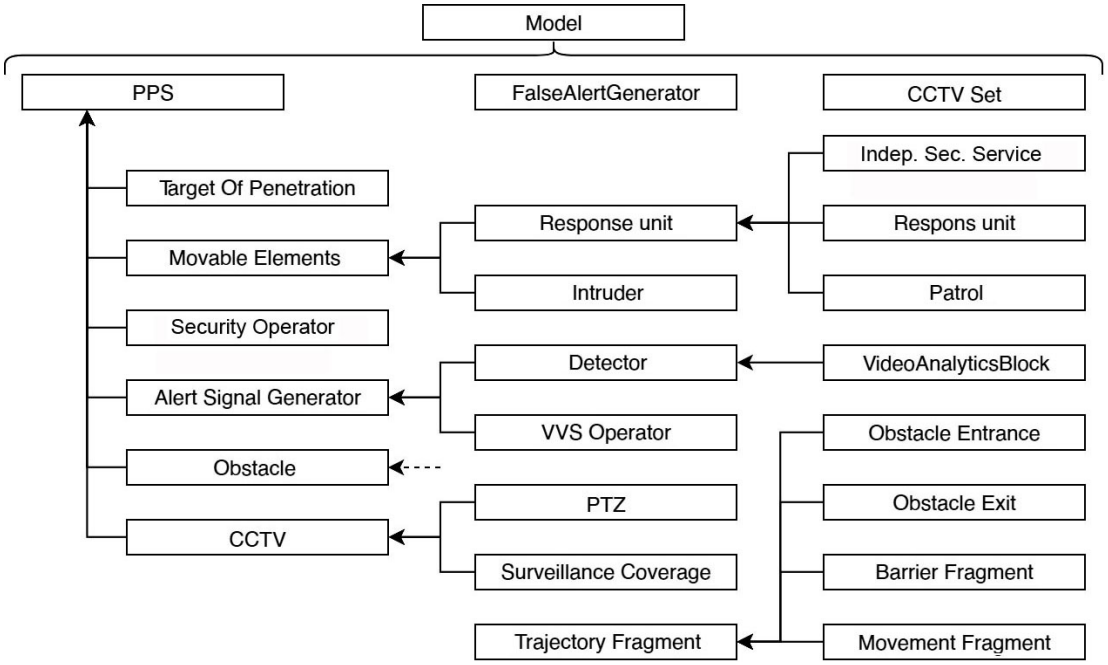

Figure 1. Scheme of classes and their heritage of a developed model

3. FRAMEWORK OF THE GRAPHIC ENGINEERING AND THE SIMULATION MODELING OF PPS

Since a structure of a planned PPS is described by a drawing, every element must have a unique component with its own raw data associated with it. The raw data is working parameters (detection possibility, movements delay intervals, etc.), graphic information: device placement location coordinates, obstacle dimensions, the detection zone geometric form, etc. Thus, a PPS digital twin's structure can be formed using a special graphic constructor.

For a complete PPS description a graphic editor models must have these functions:

1. PPS: Creation of the drawing for a surrounding area using a description of its infrastructure and topology, which affects intruder's possible paths.
2. PPS: Creation of EMoP elements with necessary qualities of its spatial geometric form and an intruder deterrence ability.
3. PPS: Creation of TMoP elements with the necessary qualities for determining a spatial geometric form of detection zones, the method of its functioning and the probability of a reaction to any given type of intruder action.
4. PPS: Creation of a SF structure on a site such as a guard posts placement, number of guards there (response unit), patrols and their paths, operators and their functional purpose as well as parameters responsible for the behavior of each unit, response tactics, movement or decision making, described in designed mathematical model.
5. External factors: assigning the parametric characteristics of weather conditions, the dynamics of their change and the parameters of a false alarms model.
6. Intruder: setting up an intruder model as a parametric set describing its behavior and characteristics.
7. Intrusion path: setting up a method for the path generation (in this case our own heuristic pathfinding algorithm Polaris), as well as designation of intruder's entry places and types of their preferred targets.

8. Outcome: assignment of intrusion targets (secured zones on a PPS territory) and the characteristics of their interactions with an intruder.

«AKIM» software complex was developed by LLC PENTACON for the realization of such designing method and the modeling of PPS. «AKIM» includes models and algorithms developed in AnyDynamics, pathfinder «Polaris», a graphic editor for PPS twins and a module for an assembly and the statistical test results analysis for forming the security quality rates and program reports alongside them.

«AKIM» software complex allows for the PPS models development and the creation of condition for the intruder's breach simulation experiments using its own graphic language. This language is a drawing instrument with a construction element which helps to build PPS from prefabricated model-blocks.

The program interface and its graphic editor are shown in Figure 2 collage:

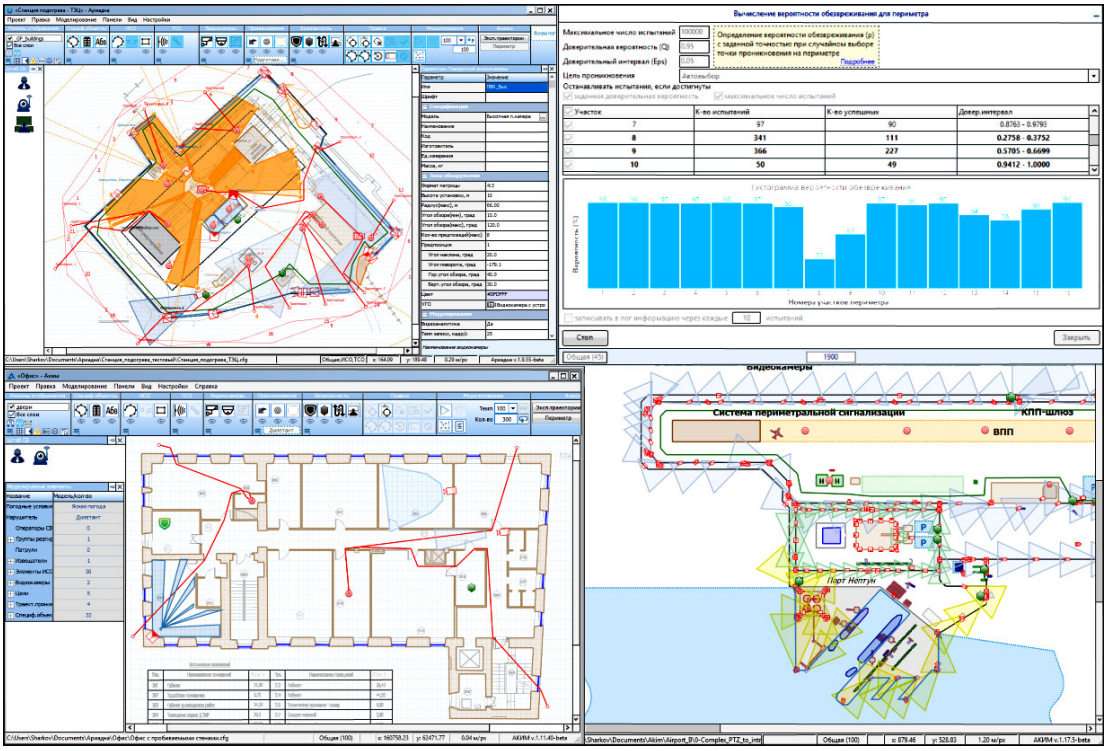

Figure 2. Graphic presentation of the PPS models of different secured sites in «AKIM» plan editor

For a PPS digital twins' graphic editor next modeling elements that can be used in a constructor were implemented:

- «**Building**» (impassable obstacle) — a structure that limits the intruder's movement, blocks vision and passage through it. Building walls and similar obstacles can be described with it.
- «**Specific zone**» — a section of a special zone that affects human's movement speed and sight distance. Such as a body of water or a shrubbery.
- «**Fence**» — a prime EMoP element designed for the site's protection along the guarded zones perimeter.
- «**Obstacle**» — an additional EMoP element describing a protective obstacle that takes up a large area (ditches, barbed wire stretched over an area, etc.).
- «**Barrier**» — additional EMoP element describing a wide variety of elements: from a barricade tape to a glass in a window frame.

- «**Detector**» — TMoP element designed for the detection of intruder's actions. It can be represented with the different types and geometries of detection zones (Figure 3).
- «**Fixed**» and «**PTZ**» video cameras — TMoP elements, allowing for the remote monitoring of a site by the operators and the video analysts.
- «**Response unit**» — a moving unit of the security forces (a guard) who can move through the site according to operator's commands or while pursuing an intruder.
- «**Patrol**» — a specific case of «response unit». A guard who patrols site's territory according to their set path and schedule.
- «**Independent security service**» — a specific case of «response unit». A guard arriving to the secured location from outside of it in a predetermined time after an alarm.
- «**Security operator**» — a security team member who monitors for alert signals and is responsible for the decision making.
- «**VSS operator**» — a security team member who monitors a video surveillance system (VVS).
- «**Secured area**» — a secured territory on a facility area. It can have different access levels for different guards.
- «**Intrusion perimeter**» — a perimeter surrounding the secured location, separated into sectors and describing points of intrusion.
- «**Intrusion target**» — point or a zone on a secured site that will be the goal for an intruder.

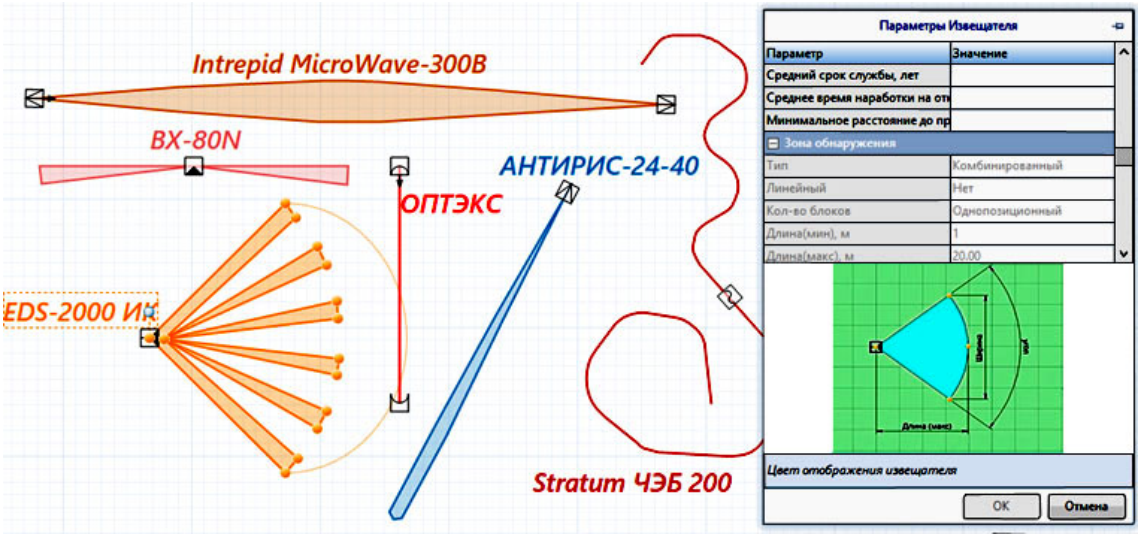

Figure 3. Defectors examples in «AKIM» with an open properties window for one of them

Also in «AKIM» editor the next modeling conditions are determined:

- A parametric model of an intruder and their equipment;
- A model of weather conditions;
- A model of false alarms and triggering.

Simulation modeling software is developed in two versions:

- Software shell, written in Delphi («AKIM»);
- Software shell, written in C# («AKIM+»).

Both shells share similar functions, but they differ in the PPS model graphic design approach.

4. AN EXAMPLE OF AN INTRUSION EXPERIMENTS

Computational tests using a created PPS simulation model (a digital twin of a secured area) imitate the process of a possible secured site intrusion scenario. Modeling starts from setting up an intrusion target: obligatory creation of the point (zone) on a site that an intruder will seek. During this test these will be modeled:

- Intruder's path, their bypass of an EMoP, interference with a TMoP, criminal action near the target;
- TMoP actions;
- Security operators' actions;
- Patrol and response unit movements, acting in routine and alarm modes.

One simulation experiment allows us to get the data about what happened in the process as well as the results. For getting the quality evaluation of a modeled PPS, as it was already mentioned, we need to conduct many experiments. All the test data then added up in a statistics. An example of an experiment series on PPS can be seen on the Figure 4, where the green lines show that the test ended up with an intruder's interception and the red ones — where an intruder managed to get to the target:

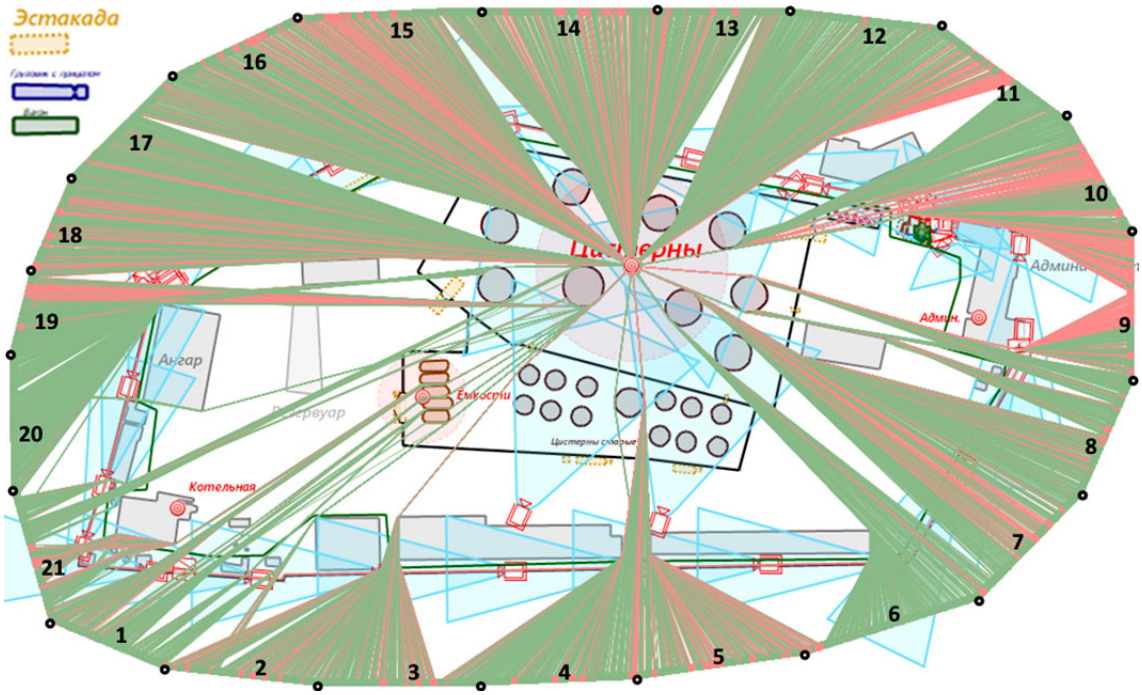

Figure 4. A diagram of intrusion pathways by the site's perimeter sectors

5. THE RESULTS OF PPS MODELING

The results of simulation modeling and a PPS quality evaluation in «AKIM» are presented like this:

- Intruder **detection probability** (P_{Det}) — general detection capability rating for the system as a whole.

- Intruder **neutralization probability** (P_{Net}) by the security forces — general neutralization capability for a PPS as a whole.
- Intruder **containment time** (T_{Cont}) on EMoP — minimum, average and maximum time an intruder needs to get to the target across all tests.
- Intruder **neutralization time** (T_{Neut}) from their detection — minimum, average and maximum time of security forces counteractions in case of successful intruder interception across all tests.
- **Containment efficiency** on EMoP — ratio between the intruder's time to get to the target through EMoP present on location to the time the same path takes without any delays. It allows users to determine the intruder containment effectiveness on obstacles. The higher this number is the more effective the containment — there are no absolute limit. Values close to one mean that the EMoP fails to do its work.
- **The bar graph of neutralization probability by the PPS perimeter sectors** — a rating of PPS perimeter, separated into many intrusion sectors. It allows users to determine the weakest sector of site's security, instead of an average rating for the whole system.
- **Response frequency of TMoP elements** — the response amount characteristic of any given modeled TMoP across all tests. Allows users to determine the workload of each device. This rating can show elements that are not active in tests which can be related to faulty installation or overabundance of a PPSs structure.

The model's information about the results of its study is recorded in automatically generated reports along with each rating and partial result. The results in reports are presented in written, tabular forms and also as a graphic info: diagrams, bar graphs, radar probability diagrams.

The experiments calculation speed depends on the PPS model complexity and a power of a calculating computer. Big security sites (a few dozen square kilometers) with an expansive EMoP with a big number of TMoP (hundreds of elements) and dozens of guards can be modeled at an approximate rate of 330 tests per minute on AMD Ryzen 5 3600 processor. Such speed is possible due to the ability to parallelize tests across all processor cores. There are other optimization method for parallelized calculations.

6. CONCLUSION

The simulation modeling and the PPS quality evaluation method described in this paper provides a possibility for an analysis of already existing system (or project) as well as those that are still on their conceptual design stage. This solves the problem with the transfer of stated requirements and qualitative characteristics into a practical PPS implementation. Rating accuracy can be determined by the method of confidence intervals. The speed of calculation experiments made without referencing an already known complex pathfinding graph is higher than that of alternative algorithms, using a pathfinding on a grid. This allows for a large number of simulation experiments in a short amount of time.

References

1. A. D. Tarasov, *Metod i algoritmy proektirovaniya sistem fizicheskoy zashchity ob"ectov informatizatsii na osnove obrabotki nechetkoy informatsii* [Method and design algorithms of the physical protection systems of an object of informatization based on processing of a fuzzy information], [Doktor. diss], Ufa State Aviation Technical University, Ufa, Russia, 2017.

2. D. Ĉakija, Ž. Ban, M. Golub, and D. Ĉakija, "Optimizing physical protection system using domain experienced exploration method," *Automatika*, vol. 61, no. 2, pp. 207–218; doi: 10.1080/00051144.2019.1698192
3. G. F Shanaev, *Sistemy zashchity perimetra* [Perimeter protection systems], Moscow: Security Focus, 2011.
4. Z. Bowen, Y. Ming, Y. Hidekazu, and L. Hongxing, "Evaluation of Physical Protection Systems Using an Integrated Platform for Analysis and Design," in *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 47, no. 11, pp. 2945–2955, 2017; doi: 10.1109/TSMC.2016.2531995
5. B. P. Stepanov and A. V. Godovykh, *Osnovy proektirovaniya sistem fizicheskoy zashchity yadernykh ob'ektov: uchebnoe posobie* [The basics of physical protection systems design for nuclear objects: a tutorial], Tomsk, Russia: Tomsk polytechnic university publ., 2009.
6. S.-S. Jang, S.-W. Kwan, H.-S. Yoo, J.-S. Kim, and W.-K. Yoon, "Development of a vulnerability assessment code for a physical protection system: Systematic analysis of physical protection Effectiveness (SAPE)," *Nuclear Engineering and Technology*, vol. 41, no. 5, pp. 747–752, 2009; doi: 10.5516/NET.2009.41.5.747
7. I. N. Petrov and A. V. Leus, *Primenenie metodov imitatsionnogo modelirovaniya dlya otsenki vozmozhnosti osushchestvleniya aktov nezakonnogo vmeshatel'stva v deyatel'nost' grazhdanskoy aviatsii* [Application of simulation modeling methods for the evaluation of possibility of committing the illegal acts of interference in civil aviation activities], Moscow: LLC INSOFT, 2012.
8. V. Ustun, L. Yilmaz, and J. S. Smith, "A conceptual model for agent-based simulation of physical security systems," in *Proc. of the 44th annual southeast regional conference on — ACM-SE 44*, 2006; doi: 10.1145/1185448.1185530
9. I. K. Sharkov and E. A. Zheludkov, "Primenimost evristicheskogo algoritma dlya zadach poiska traektoriy dvizheniya cherez sistemu fizicheskoy zashchity" [Applicability of a heuristic algorithm for the tasks of pathfinding through a physical protection system], in *Proc. of 4th Conference on Software Engineering and Information Management (SEIM-2019), St. Petersburg*, St. Petersburg, Russia: SPbPU, 2019, pp. 34–40.

Received 28-05-2022, the final version — 16-06-2022.

Ilya Sharkov, Postgraduate Student at HSCPSC Institute of Computer Science and Technology SPbPU, Complex systems, LLC, Lead Developer, ✉ **shark2.1@mail.ru**

Victor Krylov, PhD, Associate Professor, PENTACON, LLC, CEO, victor@cctv.ru

Yuri Kolesov, PhD, Complex systems, LLC, modeling enigeer, ybk@mail.ru

Компьютерные инструменты в образовании, 2022
№ 2: 32–40
УДК: 004.942
http://cte.eltech.ru
doi:10.32603/2071-2340-2022-2-32-40

Планирование и оценка качества систем физической защиты с помощью имитационного моделирования

Шарков И. К.[1,2], аспирант, ✉ shark2.1@mail.ru, orcid.org/0000-0001-7290-7013
Крылов В. М.[3], кандидат технических наук, доцент, victor@cctv.ru, orcid.org/0000-0002-4678-423X
Колесов Ю. Б.[2], доктор технических наук, ybk@mail.ru, orcid.org/0000-0002-6307-6710

[1]Санкт-Петербургский Политехнический Университет Петра Великого, Политехническая ул., д. 29, Санкт-Петербург, 195251, Россия
[2]ООО «Комплексные системы», территория Инновационного центра «Сколково», Большой Бульвар, д. 42, стр. 1, оф. № 32, 143026, Москва, Россия
[3]ООО «ПЕНТАКОН», ул. Красного Курсанта, д. 25 Д, 197198, Санкт-Петербург, Россия

Аннотация

В данной статье рассматриваются проблемы оценки качества систем физической защиты (СФЗ) на этапе ее проектирования. Оценивать качество предлагается с помощью имитационного моделирования в программном комплексе «АКИМ». Программный комплекс «АКИМ» использует чертеж планируемой СФЗ для автоматического построения агентной модели, позволяющей моделировать атаки, действия охраны, оценивать защищенность объекта, и добиваться требований, предъявляемых к системе защиты.

Ключевые слова: *система физической защиты, имитационное моделирование, агентное моделирование, графическое проектирование, оценка качества, техническое задание, АКИМ.*

Цитирование: Шарков И. К., Крылов В. М., Колесов Ю. Б. Планирование и оценка качества систем физической защиты с помощью имитационного моделирования // Компьютерные инструменты в образовании. 2022. № 2. С. 32–40. doi: 10.32603/2071-2340-2022-2-32-40

Поступила в редакцию 28.05.2022, окончательный вариант — 16.06.2022.

Шарков Илья Кириллович, аспирант ВШ КФСУ института компьютерных наук и технологий СПбПУ, ведущий разработчик ООО «Комплексные системы», ✉ shark2.1@mail.ru

Крылов Виктор Михайлович, кандидат технических наук, доцент, генеральный директор ООО «ПЕНТАКОН», victor@cctv.ru

Колесов Юрий Борисович, доктор технических наук, инженер-моделист ООО «Комплексные системы», ybk@mail.ru