UDC 621.31(045)
DOI:10.18372/1990-5548.87.20907

[1]Vladyslav Pevnev,
[2]Roman Odarchenko

DETERMINING THE EFFECTIVENESS CRITERIA FOR INTELLIGENT DETECTORS IN INTEGRATED VIDEO SURVEILLANCE SYSTEMS

Department of Telecommunication and Radio Electronic Systems,
State University "Kyiv Aviation Institute", Kyiv, Ukraine
E-mails: [1]mrbydapesht@gmail.com ORCID 0009-0006-8252-276X,
[2]roman.odarchenko@npp.kai.edu.ua ORCID 0000-0002-7130-1375.

Abstract**—***The paper considers a comprehensive methodology for evaluating the effectiveness of video surveillance systems based on classical motion detection and neural network object recognition algorithms. A system of technical, financial, and operational performance indicators is outlined, including event miss probability, recognition precision, false alarm rate, response time, infrastructure costs, staffing expenses, and operator workload index. The integral detection quality metric based on the F1-score, defined as the harmonic mean of Precision and Recall, is characterized. A weighted aggregation model is proposed that accounts for the criticality level of the protected facility and enables adaptive balancing between technical and economic factors. The mechanism of incident cost impact on financial efficiency through expected losses from missed events is analyzed. Comparative calculations are presented for facilities with different camera counts (10 and 200) and different criticality levels. It is established that under high-criticality conditions neural network algorithms demonstrate significantly higher overall efficiency compared to traditional motion detectors due to lower miss probability and reduced operator workload.*

Keywords—Video surveillance systems; neural network analytics; motion detection; object detection; F1-score; operational efficiency; incident cost; critical infrastructure security.

I. INTRODUCTION

The development of security systems is increasing and growing every year, just like other areas of IT. This is facilitated not only by technological development, but also by the availability of components that are no longer in short supply or require independent production, which has led to the creation of a large number of companies that, in turn, present new approaches, tools, and prices for "security." Thus, the most widespread and popular analytical tool – the motion detector, invented back in 1996 – is already being replaced by more modern and accurate analytics based on neural networks.

Despite this, a large number of government and commercial facilities still remain in the "past" and use motion detectors as the main component of their systems. Despite changes and improvements to the basic algorithm, it should be noted that this tool was not accurate in its concept from the outset and does not allow for accurate results in the modern world. At the same time, this approach is the most budget-friendly and accessible for businesses of any level or for ensuring the security of private property.

An alternative to motion detectors are trackers, "Neurotrackers," "Object Detection Detectors," and others, which allow you to detect objects with high accuracy, ignore false alarms or noise, quickly notify you of a specific object you are looking for, and classify it, describing its characteristics, color, direction of movement, and even items of clothing. Such a variety of tools can significantly increase the efficiency of the system, but in turn, they require more powerful and expensive equipment, as well as professional specialized software.

The cost of implementing such systems is the most significant factor preventing their widespread implementation. The second, equally important criterion is the lack of clear and accessible performance indicators that clearly demonstrate the technological "leap" and the results of such detectors. Accordingly, in most cases, a system is chosen that already has a known operating principle, free outdated analytics, and does not have the efficiency that is possible today. As a result, we get an outdated system that, according to its efficiency index, does not allow us to solve the tasks effectively, and that is why they require constant improvements, a lot of attention, operational resources, and processing of false requests.

It is also necessary to consider the aspect that determines where such an approach can be ignored or simplified, namely criticality. The importance of the object, its classification, and level of value determine the requirements for the security and video surveillance system. If we take a private house or apartment for comparison, the level of criticality for it is low, but if it is an enterprise, production facility, or warehouse, the level of criticality is medium. and if we consider shopping and entertainment centers, critical infrastructure facilities, energy facilities, logistics and infrastructure facilities such as airports, then the level is high. Therefore, when building security systems that include a video surveillance subsystem, it is necessary to take into account the level of criticality, which allows you to assess the financial and technological feasibility of implementing modern analytical systems.

It should also not be forgotten that security is the most important area of all modern research and inventions, which is the basis of medicine, law, technology, and sociology, which was laid down in the first groups of people and ensured the survival of humans as a species. Ignoring it is unacceptable, as the consequences of losses are always greater than what is invested in building security.

II. Analysis of Existing Analytical Methods

The first analytical method to be considered is the motion detector. Its operating principle is simple and was first applied to analog video surveillance, but at that time, due to the specifics of analog signal processing, it responded to the amplitude of the signal, which was weak in terms of noise immunity, and many factors could affect the constant signal, although even then, in the 1970s, it was a significant technological breakthrough. Later, after Axis created digital IP cameras, this detector began to work more efficiently.

Motion detector technology involves analyzing successive frames of an image generated by a camera and determining the difference in pixels. If a pixel in the second image was changed, it meant movement. For basic filtering of static images and events where a change occurred, this significantly reduced the amount of digital material for analysis. Later, this detector had various settings for sensitivity and object size (number of pixel groups), which helped to make its work more accurate and efficient. The latest iterations of the detector's mathematics include pixel group templates that help to more effectively determine the structure of an object so that noise such as changes in lighting or vegetation movement is recorded less frequently.

As already mentioned, the concept of this detector was not intended to be an accurate detection tool, as it only detects movement, which is not effective enough in current systems. Therefore, this tool is basic and available in all modern systems and is even supported on board video cameras.

Unlike the mathematical approach, where the system expects a predictable change in pixels, this analytics uses machine vision, which does not work with a signal or sequence of pixels between frames, but analyzes a specific frame and identifies an object on it.

The accuracy of the analytics is determined by the number of layers, which is achieved by the volume of material on which the analytics is trained. Each layer consists of neurons that are capable of generating a "weight" or confidence coefficient for the characteristics of an object. After the image has been transferred for analysis, several key stages occur with the image in order for the analytical neural model to provide a result. It is important to note that the neural model does not give a definitive answer, such as "yes" or "no," but rather provides a confidence percentage with which it has calculated the probability that the object is actually in the frame, expressed as a fractional number – 0.93, 0.32, 0.17.

The main stages of image processing and analytical analysis:

1) Image preprocessing

This is a critically important stage that prepares the image for the matrix format standards on which the network was trained. First, the resolution is changed to the required one (for example: 640x640, 320x320, etc.), which is not simply stretched, but using special algorithms, such as "LetterBox," reduces the matrix while maintaining proportions to prevent distortion of objects.

2) Image normalization

The required color scheme of BGR/RGB channels is selected, and color values are converted from 8-bit representation to floating point numbers. This approach allows computing blocks to calculate float32 fractional numbers, which is much simpler and more stable than working with integer numbers. The CPU is not suitable for these tasks, so GPU/NPU computing units are used, which cope well with these tasks due to their different architecture, since the main difference between them is in the number of cores and parallel instruction processing.

3) Creating a tensor

This is the final stage in preparing an image for analysis, where a regular image is converted into a mathematical (algebraic) computational resource. In fact, a tensor is a regular unified container in which data is stored according to the required structure [N, C, H, W] or [C, H, W], which will be understandable for neural network frameworks.

4) Feature Extraction

Detection of objects using mathematical algorithms that first filter data into useful and useless, working by identifying horizontal and vertical lines and color transitions. After identifying blocks with useful information, they are analyzed for understandable object characteristics and then compressed.

5) Inference

The finished tensor with selected objects is transmitted and moves through layers of neurons that analyze it and record the probability. Modern networks allow you to determine the following probabilities:

1) The probability of an object being present in the image.

2) The probability of a class (human, car, dog/cat).

3) The coordinates of the rectangle (object boundaries).

According to official manufacturer data, the result achieved is 53–53% mAP % accuracy on COCO, which is actually a very high indicator, since the research is conducted on random images from the Internet, and their angles, object positions, distortion of proportions, and noise are not standardized as in security systems. Therefore, using official sources and in cooperation with the video surveillance system manufacturer AxxonSoft, a series of studies were conducted in which this indicator reached 95–99% accuracy. The difference in the result lies in the initial image, which will be approximately the same in any location, country, or facility in accordance with the rules and regulations for installing video cameras on the perimeter and inside premises. Thus, standardization is only beneficial, and analytics show extremely accurate results.

III. Determining Criteria for Evaluating Effectiveness

To build effective systems, it is necessary to accurately assess all input data, which will allow calculating the necessary variables, according to which it is possible to mathematically calculate the index of effectiveness of implementing such systems, and it is precisely this approach that can be effective for initial analysis and further implementation. Together with the comparative characteristics obtained during the study, the efficiency coefficient can be used to build a technical and economic justification and assess risks based on figures rather than feelings.

To form such a standardized approach, it is necessary to determine a number of values and variables that are important for decision-making. In my study, I define the following criteria.

Input parameters of the object:

- criticality of the object;
- time mode of operation of the object;
- SLA (Response time requirements);
- number of video cameras at the object;
- zone coverage;
- scene saturation;
- saturation error coefficient.

Technical variables:

- Probability of omission
- Probability of correct recognition
- Probability of false recognition
- Response time

Financial and operational variables:

- Technology and software costs - CAPEX
- Maintenance costs - OPEX
- Employee costs (operators, administrators)
- Operator attention/fatigue index
- Incident cost

Input variables for the importance coefficient:

- Criticality weight of misses
- False alarm weight
- Response time weight

By defining these indicators and dividing them into several separate blocks, it is possible to determine each individual performance indicator, as well as the effectiveness of the system for each block, which ultimately allows us to derive an overall performance index.

IV. Results of the Efficiency Method

We will experimentally determine the effectiveness of analytical detectors and evaluate their effectiveness for two objects with different levels of criticality, which will allow us to understand the need for their implementation, namely at objects with low and high levels of criticality (coefficients 1 and 3, respectively).

For both cases, we will use static parameters of 10 and 200 cameras, simulating a small and medium-sized security facility. There will also be other variable parameters, such as area coverage, scene saturation, operating mode, and response time that are shown in Table I.

TABLE I. INITIAL DATA FOR ANALYSIS

No	Value	VMD 10 Ch	Neural 10 Ch	VMD 200 Ch	Neural 200 Ch
Criticality	K	1	1	1	1
Operating mode	–	24/7 = 1	24/7 = 1	24/7 = 1	24/7 = 1
SLA	SLA	30 s = 0.5	30 s = 0.5	30 s = 0.5	30 s = 0.5
Number of cameras	N	10	10	200	200
Coverage areas	C_{cov}	0,5	0.5	0.8	0.8
Stage saturation	ρ	0.3	0.3	0.4	0.4
K. Saturation errors	α	0.08	0.08	0.14	0.14
Probability of omission	P_{miss}	0.4	0.05	0.4	0.05
Probability of correct recognition	$P_{correct}$	0.20	0.95	0.20	0.95
Probability of false recognition	P_{false}	0.80	0.05	0.80	0.05
Response time	T_{react}	10 s	2 s	45	5 s
CAPEX	$CAPEX_m$	2 666	9 111	47 921	95 967
OPEX	$OPEX_m$	800	2 733	14 376	28 790
Employee expenses	C_{staff}	0	0	120 000	60 000
Attention/fatigue index	F_{fat}	20	3	200	60
Cost of the incident	C_{inc}	0.2	0.2	0.5	0.5
Criticality weight of omission	w_{miss}	0.60	0.60	0.60	0.60
The weight of false alarms in identification	w_{false}	0.25	0.25	0.25	0.25
Weight of reaction time	w_{rt}	0.15	0.15	0.15	0.15

Calculation of technical components

1) Scene saturation penalty

$$\Phi(\rho) = 1 - \alpha$$

$$\Phi(\rho) = 1 - 0.08 \cdot 0.3 = 0.976$$

$$\Phi(\rho) = 1 - 0.14 \cdot 0.4 = 0.944$$

2) Determining the actual volume of recorded events

$$R = 1 - P_{miss}$$

$$R = 1 - 0.40 = 0.60$$

$$R = 1 - 0.05 = 0.95$$

3) Integral quality of F1 detections

$$Q_{det} = \frac{2PR}{P+R}$$

$$Q_{det} = \frac{2 \cdot 0.20 \cdot 0.60}{0.20 + 0.60} = \frac{0.24}{0.80} = 0.30$$

$$Q_{det} = \frac{2 \cdot 0.95 \cdot 0.95}{0.95 + 0.95} = \frac{1.805}{1.90} = 0.95$$

4) Determination of the correct detection rate

$$Q_{false} = 1 - P_{false}$$

$$Q_{false} = 1 - 0.80 = 0.20$$

$$Q_{false} = 1 - 0.05 = 0.95$$

5) Standardization of response time in relation to SLA

$$Q_{rt} = \min\left(1, \frac{SLA}{T_{react}}\right)$$

$$Q_{rt} = \min(1.30/10) = 1$$

$$Q_{rt} = \min(1.30/2) = 1$$
$$Q_{rt} = \min(1.30/45) = 0.667$$
$$Q_{rt} = \min(1.30/5) = 1$$

6) Calculation of combined technical efficiency

$$E_{tech} = C_{cov} \cdot \Phi(\rho) \cdot (w_{miss} Q_{det} + w_{false} Q_{false} + w_{rt} Q_{rt})$$
$$E_{tech} = 0.5 \cdot 0.976(0.60 \cdot 0.30 + 0.25 \cdot 0.20 + 0.15 \cdot 1) = 0.488(0.18 + 0.05 + 0.15) = 0.488 \cdot 0.38 = 0.185$$
$$E_{tech} = 0.5 \cdot 0.976(0.60 \cdot 0.95 + 0.25 \cdot 0.95 + 0.15 \cdot 1) = 0.488(0.57 + 0.2375 + 0.15) = 0.488 \cdot 0.9575 = 0.467$$
$$E_{tech} = 0.8 \cdot 0.944(0.60 \cdot 0.30 + 0.25 \cdot 0.20 + 0.15 \cdot 0.667) = 0.7552(0.18 + 0.05 + 0.100) = 0.7552 \cdot 0.33 = 0.249$$
$$E_{tech} = 0.8 \cdot 0.944(0.60 \cdot 0.95 + 0.25 \cdot 0.95 + 0.15 \cdot 1) = 0.7552(0.57 + 0.2375 + 0.15) = 0.7552 \cdot 0.9575 = 0.723$$

7) Calculation of basic monthly expenses

$$C_{base} = CAPEX_m + OPEX_m + C_{staff}$$
$$C_{base} = 2666 + 800 + 0 = 3466$$
$$C_{base} = 9111 + 2733 + 0 = 11844$$
$$C_{base} = 47921 + 14376 + 120000 = 182297$$
$$C_{base} = 95967 + 28790 + 60000 = 184757$$

8) Expected losses from missed or unrecorded incidents

As the base level of losses – L_0, we set the cost at 100,000 UAH/month as a static value.

$$L_{inc} = L_0 \cdot \left(\frac{N}{10}\right) \cdot C_{inc} \cdot P_{miss}$$
$$L_{inc} = 100000 \cdot \left(\frac{10}{10}\right) \cdot 0.2 \cdot 0.40 = 8000$$
$$L_{inc} = 100000 \cdot 1 \cdot 0.2 \cdot 0.05 = 1000$$
$$L_{inc} = 100000 \cdot \left(\frac{200}{10}\right) \cdot 0.5 \cdot 0.40 = 400000$$
$$L_{inc} = 100000 \cdot 20 \cdot 0.5 \cdot 0.05 = 50000$$

9) Calculation of total monthly expenses

$$C_{total} = C_{base} + L_{inc}$$
$$C_{total} = 3466 + 8000 = 11466$$
$$C_{total} = 11844 + 1000 = 12844$$
$$C_{total} = 182297 + 400000 = 582297$$
$$C_{total} = 184757 + 50000 = 234757$$

10) Cost normalization (conversion to a value between 0 and 1)

$$Q_{cost} = \frac{1}{1 + \frac{C_{total}}{C_{ref}}}$$
$$Q_{cost} = \frac{1}{1 + \frac{11466}{100000}} = 0.897$$
$$Q_{cost} = \frac{1}{1 + \frac{12844}{100000}} = 0.886$$
$$Q_{cost} = \frac{1}{1 + \frac{582297}{100000}} = 0.147$$
$$Q_{cost} = \frac{1}{1 + \frac{234757}{100000}} = 0.299$$

11) Standardization of personnel costs

$$Q_{staff} = \frac{1}{1 + \frac{C_{staff}}{C_{ref\_staff}}}$$
$$Q_{staff} = \frac{1}{1 + \frac{0}{100000}} = 1$$
$$Q_{staff} = \frac{1}{1 + \frac{120000}{100000}} = 0.455$$
$$Q_{staff} = \frac{1}{1 + \frac{60000}{100000}} = 0.625$$
$$Q_{staff} = \frac{1}{1 + \frac{0}{100000}} = 1$$

12) Standardization of fatigue and workload for personnel

$$Q_{fat} = \frac{1}{1 + \frac{F_{fat}}{F_{ref}}}$$
$$Q_{fat} = \frac{1}{1 + \frac{20}{50}} = 0.714$$

$$Q_{fat} = \frac{1}{1+\frac{3}{50}} = 0.943$$

$$Q_{fat} = \frac{1}{1+\frac{200}{50}} = 0.20$$

$$Q_{fat} = \frac{1}{1+\frac{60}{50}} = 0.455$$

13) Overall financial and operational efficiency

To determine this E_{ops}, we need to use empirical criticality values for each parameter of financial costs, human resources, and the fatigue factor $v1, v2, v3$.

We take the following values in order: 0.4, 0.4, and 0.2.

$$E_{ops} = v_1 Q_{cost} + v_2 Q_{staff} + v_3 Q_{fat}$$

$$E_{ops} = 0.40 \cdot 0.897 + 0.40 \cdot 1 + 0.20 \cdot 0.714 = 0.902$$

$$E_{ops} = 0.40 \cdot 0.886 + 0.40 \cdot 1 + 0.20 \cdot 0.943 = 0.943$$

$$E_{ops} = 0.40 \cdot 0.147 + 0.40 \cdot 0.455 + 0.20 \cdot 0.20 = 0.281$$

$$E_{ops} = 0.40 \cdot 0.299 + 0.40 \cdot 0.625 + 0.20 \cdot 0.455 = 0.461$$

14) Calculation of overall efficiency

$$E_{total}(K) = a(K) \cdot E_{tech} + (1 - a(K)) \cdot E_{ops}$$

$$E_{total} = 0.55 \cdot 0.185 + 0.45 \cdot 0.902 = 0.508$$

$$E_{total} = 0.55 \cdot 0.467 + 0.45 \cdot 0.943 = 0.681$$

$$E_{total} = 0.55 \cdot 0.249 + 0.45 \cdot 0.281 = 0.263$$

$$E_{total} = 0.55 \cdot 0.723 + 0.45 \cdot 0.461 = 0.605$$

The second experiment will focus on calculating efficiency for highly critical facilities, where every mistake or missed incident is unacceptable. The basis for this was a checkpoint in a protected area and a shopping and entertainment center.

V. Result

According to our calculations, we have three indicators of implementation effectiveness: technical, economic, and overall are shown in Table II. and Fig. 3. It is better to take the technical aspect of efficiency as a basis, as it is the most accurate and shows how much more efficient the system can be in terms of real figures are shown in Fig. 1, while the financial indicator can only be indicative, since it is sometimes impossible to measure the indicators for the most critical objects in numbers, where the issues of implementation and ownership costs take a back seat are shown in Fig. 2.

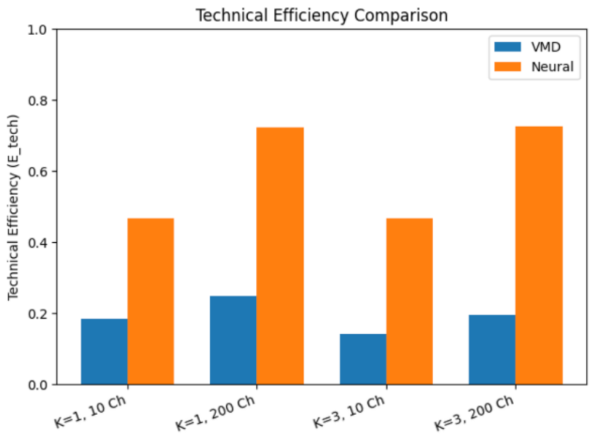

Fig. 1. Technical Efficiency Comparison

TABLE II. COMPARISON OF RESEARCH RESULTS

Script	Technical efficiency	Financial performance	Overall efficiency
K=1 VMD 10	0.185	0.902	0.508
K=1 Neural 10	0.467	0.943	0.681
K=1 VMD 200	0.249	0.179	0.217
K=1 Neural 200	0.723	0.344	0.552
K=3 VMD 10	0.142	0.521	0.142
K=3 Neural 10	0.468	0.624	0.468
K=3 VMD 200	0.195	0.155	0.195
K=3 Neural 200	0.725	0.367	0.725

The efficiency indices of a low-criticality system for a private home show a difference of 2.534 times, which means a significant increase in efficiency, and for a warehouse with a larger volume of cameras and digital material for analysis, this indicator increases by 2.903 times. This indicates a natural trend and proportion, where increasing and scaling the system leads to a decrease in the efficiency of a classic detector and an increase in the efficiency of intelligent analytical tools.

It should be noted that it is only advisable to consider low-criticality objects from a scientific point of view for comparing empirical results, which is why the second calculation used for high criticality demonstrates this pattern even more clearly. For a small system with 10 cameras, the difference in indices is 3.295 times, while in a system with 200 video channels, this ratio is 3.717 are shown in Fig. 1.

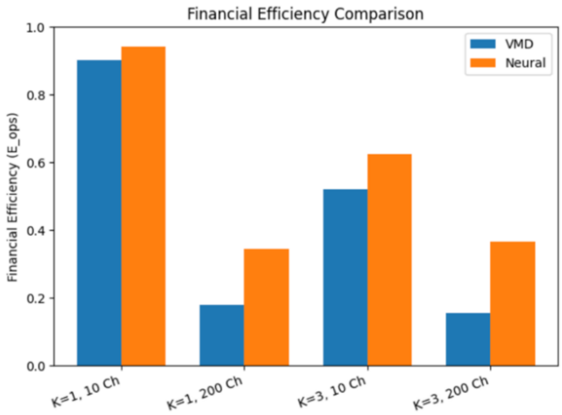

Fig. 2. Financial Efficiency Comparison

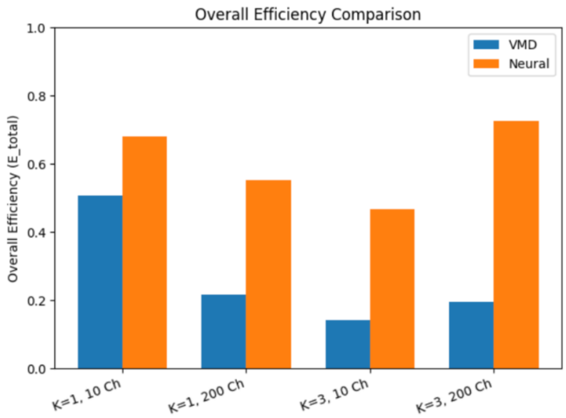

Fig. 3. Overall Efficiency Comparison

VI. Conclusion

Summarizing this study and the efficiency formulas, we observe that only a change in the use of analytical tools can increase the efficiency of the overall system by almost 4 times.

VII. Acknowledgments

The research was conducted using the technical infrastructure and analytical tools of AxxonSoft. The authors express their gratitude to the engineering team for providing experimental data and technical support.

References

[1] P. Viola and M. Jones, “Rapid object detection using a boosted cascade of simple features,” *Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR)*, 2001, pp. I–511–I–518. https://doi.org/10.1109/CVPR.2001.990517.

[2] P. Viola and M. Jones, “Rapid object detection using a boosted cascade of simple features,” *Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR)*, 2001, pp. I–511–I–518. https://doi.org/10.1109/CVPR.2001.990517

[3] K. He, X. Zhang, S. Ren, and J. Sun, “Deep residual learning for image recognition,” *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2016, pp. 770–778. https://doi.org/10.1109/CVPR.2016.90

[4] K. He, X. Zhang, S. Ren, and J. Sun, “Deep residual learning for image recognition,” *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2016, pp. 770–778. https://doi.org/10.1109/CVPR.2016.90

[5] J. Davis and M. Goadrich, “The relationship between Precision-Recall and ROC curves,” *Proceedings of the 23rd International Conference on Machine Learning (ICML)*, 2006, pp. 233–240. https://doi.org/10.1145/1143844.1143874

[6] D. M. W. Powers, “Evaluation: From Precision, Recall and F-measure to ROC, informedness, markedness and correlation,” *Journal of Machine Learning Technologies*, vol. 2, no. 1, pp. 37–63, 2011.

[7] I. Valera and S. A. Velastin, “Intelligent distributed surveillance systems: A review,” *IEE Proceedings – Vision, Image and Signal Processing*, vol. 152, no. 2, pp. 192–204, 2005. https://doi.org/10.1049/ip-vis:20041247

[8] A. Hampapur et al., “Smart video surveillance: Exploring the concept of multiscale spatiotemporal tracking,” *IEEE Signal Processing Magazine*, vol. 22, no. 2, pp. 38–51, 2005. https://doi.org/10.1109/MSP.2005.1407718

[9] W. Bewley, Z. Ge, L. Ott, F. Ramos, and B. Upcroft, “Simple online and realtime tracking,” *2016 IEEE International Conference on Image Processing (ICIP)*, 2016, pp. 3464–3468. https://doi.org/10.1109/ICIP.2016.7533003

[10] R. Szeliski, Computer Vision: Algorithms and Applications, 2nd ed. Cham, Switzerland: Springer, 2022. https://doi.org/10.1007/978-3-030-34372-9

Received: December 29, 2025
Accepted: January 21, 2026
Published: March 03, 2026

Pevnev Vladyslav. ORCID 0009-0006-8252-276X. Postgraduate Student.
State University "Kyiv Aviation Institute", Kyiv, Ukraine.
Education: National Aviation University, Kyiv, Ukraine. (2021)
Research interests: system analysis, intelligent data processing, applied cybernetics, big data analytics, decision-making models in telecommunication systems.
Publications: 2.
E-mail: mrbydapesht@gmail.com

Odarchenko Roman. ORCID 0000-0001-7151-0743. Doctor of Technical Sciences. Professor.
State University "Kyiv Aviation Institute", Kyiv, Ukraine.
Education: National Aviation University, Kyiv, Ukraine. (2010)
Research interests: telecommunications systems and networks, data reliability and consistency, information system design, 5G/6G networks, cybersecurity, unmanned systems communication, intelligent data analysis.
Publications: more than 250 scientific papers.
E-mail: roman.odarchenko@npp.kai.edu.ua

В. І. Певнев, Р. С. Одарченко. Визначення критеріїв ефективності інтелектуальних детекторів в інтегрованих системах відеоспостереження

Розглянуто методологію комплексного оцінювання ефективності систем відеоспостереження з використанням класичних детекторів руху та нейромережевих алгоритмів розпізнавання об'єктів. Окреслено систему показників технічної, фінансової та операційної ефективності, що включає ймовірність пропуску події, точність розпізнавання, частоту хибних тривог, час реакції, витрати на технічну базу та персонал, а також індекс операторського навантаження. Охарактеризовано інтегральний показник якості детекції на основі F1-метрики як гармонійного середнього між Precision та Recall. Запропоновано модель зваженого агрегування критеріїв з урахуванням рівня критичності об'єкта, що дозволяє адаптивно змінювати баланс між технічною та економічною складовими. Розкрито механізм впливу вартості інциденту на фінансову ефективність системи через очікувані втрати від пропущених подій. Подано результати порівняльних розрахунків для об'єктів з різною кількістю відеокамер (10 та 200) та різними рівнями критичності. Встановлено, що при високій критичності об'єкта нейромережеві алгоритми демонструють суттєво вищий рівень загальної ефективності порівняно з традиційними детекторами руху, що обумовлено зниженням ймовірності пропуску подій та зменшенням навантаження на персонал.

Ключові слова: системи відеоспостереження; нейронна мережева аналітика; виявлення руху; виявлення об'єктів; F1-показник; операційна ефективність; вартість інцидентів; безпека критичної інфраструктури.

Певнев Владислав Ігорович. ORCID 0009-0006-8252-276X. Аспірант.
Державний університет «Київський авіаційний інститут», Київ, Україна.
Освіта: Національний авіаційний університет, Київ, Україна. (2021)
Наукові інтереси: системний аналіз, інтелектуальна обробка даних, прикладна кібернетика, аналітика великих даних, моделі прийняття рішень у телекомунікаційних системах.
Публікації: 2.
E-mail: mrbydapesht@gmail.com

Одарченко Роман Сергійович. ORCID 0000-0001-7151-0743. Доктор технічних наук. Професор.
Державний університет «Київський авіаційний інститут», Київ, Україна.
Освіта: Національний авіаційний університет, Київ, Україна. (2010)
Наукові інтереси: телекомунікаційні системи та мережі, надійність та цілісність даних, проектування інформаційних систем, мережі 5G/6G, кібербезпека, зв'язок у безпілотних системах, інтелектуальний аналіз даних.
Публікації: понад 250 наукових праць.
E-mail: roman.odarchenko@npp.kai.edu.ua