6. Melnyk R.S. Administrative Law System of Ukraine: Monograph. Kharkiv: Publishing House of the Kharkiv National University of Internal Affairs, 2010. 389 p.

DOI https://doi.org/10.30525/978-9934-26-045-2-37

FORESIGHT THE COUNTER SABOTAGE CAPABILITIES OF THE CRITICAL INFRUSTRUCTURE PROTECTION UNIT

Sukonko S. M.
Doctor of Philosophy in State Security,
Associate Professor at the Department of Tactical and Special Training
National Academy of the National Guard of Ukraine

Chepel M. O.
Doctor of Philosophy in State Security,
Senior Instructor at the Department of Social Sciences and Humanities
National Academy of the National Guard of Ukraine

Kolianda V. V.
Doctor of Philosophy in State Security,
Associate Professor at the Department of Tactic
National Academy of the National Guard of Ukraine
Kharkiv, Ukraine

One of the main directions of public administration in the field of state security is the assessment of counter sabotage at critical infrastructure, and this confirms the necessity in the foresight the counter sabotage capabilities of the critical infrastructure protection unit.

A significant contribution to the theory of protection of critical infrastructure has been made in the works of domestic and foreign scientists: Kirichenko [1, p. 165], Grynenko [2, p. 23−25], Stepanov [3, p. 97], Leus [4, p. 46−49], Radaev [5, p. 28−32], Zenov [6, p. 23−32], Borovskyi [7, p. 235−243], Wadoud [8, p. 831−839].

Today, there are a number of new threats to the critical infrastructure, such as the detonation of life support facilities outside these facilities, the destruction of vulnerable technology systems by the small-size unmanned

aerial vehicles, and others. However, the existing theoretical basis does not allow forecasting the counter sabotage capabilities of the critical infrastructure protection unit in full, including taking into account the identified threats.

Thus, the assessment of the counter sabotage capabilities of the critical infrastructure protection unit is one of the main approaches of the mechanism of public administration in the field of state security. However, with the emergence of new threats to critical infrastructure, namely the implementation of sabotage outside these facilities using small-size unmanned aerial vehicles, the theory that exists today in this area of research is underdeveloped.

Therefore, in order to predict the capabilities of critical infrastructure protection units, taking into account the identified threats, it is suggested to develop the following models:

1. A model for determining the number of personnel required to conduct search actions to detect a sabotage and reconnaissance group in the area of responsibility of the critical infrastructure protection unit.

2. Model for determining the number of personnel required to combat small-size unmanned aerial vehicles during the protection of critical infrastructure.

3. Model of foresighting of the critical infrastructure protection unit capabilities.

The models will allow using the selected indicators and criteria to predict the counter sabotage capabilities of the critical infrastructure protection unit.

The scientific novelty of these models is to provide estimates for foresighting the counter sabotage capabilities of the critical infrastructure protection unit, while taking into account the peculiarities of service at the specified facility, performance of tasks on detection and neutralization of the sabotage and reconnaissance group at the protection unit area of responsibility, as well as threats that can be made with small unmanned aerial vehicles. Consequently, the use of these models allows making decisions that are more informed on the organization of critical infrastructure protection and determination of the required number of personnel of these objects protection units in the process of implementing measures in the system of public administration in the field of state security.

References:

1. Кириченко І. О., Горєлишев С. А., Побережний А. А. Технологічні основи інформаційно-аналітичного забезпечення службово-

бойової діяльності сил охорони правопорядку : монографія. – Харків : Академія внутрішніх військ МВС України, 2013. – 291 с.

2. Гриненко В. А. Общий поход к описанию параметров модели нарушителя. *Спецтехника и связь*. 2011. № 1. С. 23–25.

3. Степанов Б. П., Годових А. В. Основы проектирования систем физической защиты ядерных объектов : учеб. пос. – Томск : Томский политехнический институт, 2009. – 118 с.

4. Леус А. В. Математическая модель оценки эффективности систем физической защиты. *Т–Comm–Телекоммуникации и транспорт*. 2018. № 6. С. 46–49. URL: https://cyberleninka.ru/article/v/matematicheskaya-model-otsenki-effektivnosti-sistem-fizicheskoy-zaschity (дата звернення 10.12.2020).

5. Радаев Н. В. Приближённые оценки защищенности объектов от террористических действий. *Безопасность. Достоверность. Информация*. 2007. №. 3 (72). С. 28–32.

6. Зенов А. Ю. Комплексный подход к обнаружению, классификации и распознаванию нарушителя на охраняемой территории. *Технические науки. Информатика, вычислительная техника*. 2012. № 2(22). С. 23–32.

7. Боровский А. С. Приближённая оценка защищенности потенциально опасных объектов. *Програмные продукты и системы*. 2013. №. 3. С. 235–243.

8. Wadoud A. A., Adail A. S., Saleh A. A. Physical protection evaluation process for nuclear facility via sabotage scenarios. *Alexandria Engineering Journal*. 2018. No. 57. P. 831–839.