Original Contribution

MODEL FOR ADMINISTRATIVE SECURITY MANAGEMENT IN A MUNICIPALITY

Iliana Simeonova, Tsvetelina Metodieva

SECURITY OF INFORMATION AND COMMUNICATION TECHNOLOGIES, FACULTY OF TECHNICAL SCIENCES, KONSTANTIN PRESLAVSKY UNIVERSITY OF SHUMEN, SHUMEN 9712,115, UNIVERSITETSKA STR., E-MAIL: i.simeonova@shu.bg, ts.metodieva@shu.bg

ABSTRACT: *Administrative security is critical to the effective functioning of government organisations. It is an attest component of governance and plays a key role in protecting public institutions. Bulgaria, with its distinctive geopolitical and historical context, represents a unique environment for exploring the conceptuality of administrative security and its functionality. Understanding and assessing administrative security is essential for the development and stability of the country.*

KEY WORDS: *administrative security, information security, threats, measures, municipalities*

1. Introduction

The administrative security model in a municipality is a structured approach to managing and protecting information. The need for a model is demonstrated in this publication through a survey.

The purpose of the survey is to present general information about the level of administrative security in municipalities and the need for a model for administrative security management.

The questionnaire includes 21 questions which respondents answer anonymously. Ten of the questions are generic, focusing on administrative security in the municipality. The other ten questions will be defined as specific, since they address one of the areas of administrative security, in particular: information security, cyber security, organizational security, physical security and the person as a security factor. The last question provides information on the respondent's years of professional experience in the municipality.

The survey was conducted in 2023. The survey included 251 respondents from 12 different types of municipalities: size, population, location, size of administration and municipal council.

This diversity allows the results to be compared and to ensure that the conclusions drawn from the results are valid for all municipalities or represent a particular case for any specific municipality.

2. Exhibition.

2.1.Processing and analysis of survey results.

The surveys are processed in excel, and in a pre-prepared matrix with the questions, the personal answers of each of the respondents are reflected. The surveys are anonymous and during processing only encrypted with a letter symbol for the municipality and a number, as well as a serial number of the interviewee from the respective municipality. Cipher by municipalities is aimed at observing whether certain results are general or specific only to a particular municipality.

Question No. 1: Do you think that administrative security in your municipality needs to be improved?

The question is general and should focus on the content of the survey and the survey itself. The answer is presented as a choice on a scale of 1 to 5, with answer 1 being a resounding NO and answer 5 being a resounding YES. The aim is to eliminate subjective assessment and present quantitative agreement or disagreement as an opinion on the matter.

Table 1. Answers to Question No 1

	1	**2**	**3**	**4**	**5**	**Total**
number of respondents' answers	0	0	10	30	211	**251**
Answers defined in %	-	-	4 %	12 %	84 %	**100 %**

In the lowest scores of the answer, i.e. those who are inclined to answer NO, there are no choices. This shows that the respondents determine that the administrative security in the municipalities in which they work needs to be improved. From tab. 1, it is evident that only 4% of the respondents fall into the average score on the scale, and the remaining 96% choose the highest levels in the scale. This shows a perceived weakness in administrative security and the need for its improvement. The high percentage (84%) of respondents who stated the categorical need to improve administrative security in their municipality is also impressive.

Question No 6: Do you think that if a Security Directorate/Unit is established, it will contribute to the better management of administrative security in your municipality?

The answer is presented as a choice on a scale of 1 to 5, with answer 1 being a resounding NO and answer 5 being a resounding YES.

Table 2. Answers to Question No 6

	1	**2**	**3**	**4**	**5**	**Total**
Number of respondents' responses	8	16	43	95	89	**251**
Replies defined in %	3,2 %	6,4 %	17,1 %	37,8 %	35,5 %	**100 %**

Bringing out a directly responsible structure is often taken into account in favor of the management of the specific area. This creates internal institutional ownership and ensures constant direct monitoring and control. To ensure administrative security in municipalities, it is possible to establish a security unit (in some municipalities there are already established ones). From the answers to the survey, it is noteworthy that many of the respondents (73.3% – those who answered on the scale with "4" and "5") are of the opinion that the creation of a unit directly responsible for the security in the municipality will lead to better management of administrative security. Less than 10% of respondents believe that the presence of a specific unit (structure) in the municipality that is responsible for and monitors security will not lead to its improvement. Municipalities are very different in size and structure and in this sense they cannot be obliged to form a security unit. The answers to the question, however, point to the conclusion that if a model for administrative security management in municipalities is being developed, measures should be included that either encourage the creation of a security unit or provide a working toolkit to replace it.

Question No. 7: Does your municipality have adopted policies, strategies, rules, instructions, etc., related to administrative security management?

Three standardized answers are proposed: "YES", "NO" and "I don't know".

Table 3. Answers to Question No 7

	YES	NOT	I don't know	Total
number of respondents' answers	214	3	34	**251**
Answers defined in %	85,3 %	1,2 %	13,5 %	**100 %**

The question aims to present the level of regulatory preparedness and security in municipalities in terms of administrative security. The internal regulatory provision of municipalities in terms of administrative security may include a package of documents, such as strategies, policies, rules, instructions, procedures, document templates, etc. The presence of such documents shows that the municipality has a good basis for ensuring administrative security. Of the answers to the question – over 85% of the respondents answered positively, which shows that the municipalities in which they work have a good basis for ensuring administrative security. Only 3 of the respondents say that there are no adopted normative documents related to the administrative security of the municipality, but since they fall as respondents in different municipalities, it can be assumed that their answers are due to lack of information.

Question No. 8: Does the process of providing services in your municipality lead to a threat to administrative security?

The answer is presented as a choice on a scale of 1 to 5, with answer 1 being a resounding "NO" and answer 5 being a resounding "YES". The main function of each municipality is to provide services to its citizens and businesses. The provision of different services implies the inclusion of different contractors as employees of the administration, with different powers and with different qualifications. The provision of each individual service or type of service can be considered as a process that to a certain extent threatens administrative security. The purpose of the question is to make a quick assessment based on the experience of employees about the level of vulnerability of administrative security in the provision of administrative services.

Table 4. Answers to Question No 8

	1	2	3	4	5	Total
number of respondents' answers	5	34	41	108	63	**251**
Answers defined in %	2 %	13,6 %	16,3 %	43 %	25,1 %	**100 %**

In the answers to the question, a five-point scale is proposed in order to be able to more objectively choose the level of security or threat in the provision of administrative services. A total of 171 employees or 68.1% (those answered with "4" and "5" from the scale) of the respondents determined that there were significant weaknesses or threats to administrative security in the provision of administrative services. Of these, 63 persons or 1/4 (25%) determine that administrative services categorically hide security threats. 41 of the respondents place the provision of services to citizens and businesses at the average level, i.e. that they may threaten administrative security. It is indicative that only 5 (only 2% of all those included in the survey) of the employees do not see security threats arising from the administration of services in municipalities.

The high percentage of persons identifying the administrative activity of providing services as highly vulnerable to security indicates the need to develop and implement an appropriate toolkit, such as the administrative security management model.

Question No. 9: When briefing employees, does familiarization with the rules and norms related to administrative security be included?

Two standardized answers are proposed: "YES" and "NO". The briefing of employees in each field, including in the public sector, aims to familiarize them with the potential threats in the organization and possible prevention actions.

Table 5. Answers to Question No 9

	YES	NOT	Total
number of respondents' answers	8	243	**251**
Answers defined in %	3,2 %	96,8 %	**100 %**

The answers are very indicative – only 8 (3.2%) of the respondents say that during the briefing the employees are familiarized with the rules and norms related to administrative security. Given that these 8 respondents are representatives of different municipalities, their answers cannot be accepted as an event for a particular municipality. It can be reported as alarming that 96.8% of the respondents say that during the briefing at the workplace they do not get acquainted with the introduced policies and new ones in the field of administrative security.

The data from the question point to the need to develop a model for managing administrative security, and staff training can be included as a tool for carrying out some measures to limit potential security threats.

Question No. 11: In your opinion, the vulnerabilities in information security are:

Five standardized answers are proposed: "Communication links", "Control of implementation", "Management decisions", "Methods of assignment and disposal" and "Means of exchange and storage of information". Respondents were explained that they could choose more than one of the proposed answers. All 251 respondents answered the question, choosing a total of 750 answers.

The purpose of this question is to provide more specific information about the vulnerability of information security. The answer "Management decisions" was identified with the least vulnerability. The answer was chosen by 39% of respondents. Less than half of the respondents indicated "Control of implementation" (48.2% - 121 respondents) and "Methods of assignment and disposal" (48.6% or 122 respondents).

Table 6. Answers to Question No 11

	Communication links	Performance control	Management decisions	Methods of assignment and disposal	Means of exchange and storage of information	Total
number of respondents' answers	180	121	98	122	229	**750**
Answers defined in %	24 % (71,7 %)*	16,1 % (48,2 %)*	13,1 % (39 %)*	16,3 % (48,6 %)*	30,5 % (91,2 %)*	**100 %**

* *The first percentage is defined as a ratio to the total number of responses, and the second percentage is defined as a ratio to the number of respondents.*

Very high vulnerability is defined as "Communication links". They were identified as vulnerable by 180 people or 71.7% of the surveyed employees. As the most vulnerable place for information security in municipalities, respondents have identified "Means of exchange and storage of information". The answer was chosen by 229 respondents out of a total of 251, which shows 91.2% identify this part as vulnerable. The identified weaknesses for information security define it as one of the most vulnerable areas in general in the administrative security of municipalities. In the development of the model for administrative security management in municipalities, these vulnerabilities are used to identify security threats.

Question No. 12: Do you think there is a need to improve cybersecurity in your municipality?

Three standardized answers are proposed: "YES", "NO" and "I can't decide".

The question focuses on cybersecurity as an area of administrative security. The aim is to assess the reliability of the applied methods and tools for ensuring cybersecurity through the experience of the employees themselves.

Table 7. Answers to Question No 12

	YES	NOT	I can't judge	Total
number of respondents' answers	151	45	55	**251**
Answers defined in %	60,2 %	17,9 %	21,9 %	**100%**

A very high share of the surveyed employees (151 respondents, 60.2% of the respondents) believe that there is a need to improve cybersecurity in the municipality in which they work. Employees usually respond based on their personal experience and confidence. Respondents associate cybersecurity with their personal access and rights in the performance of their job duties. Employees are looking for a high level of security so that their activities are not compromised.

Question No. 13: What do you think are the main threats to cybersecurity?

Five standardized answers are proposed: "Unauthorized access", "Misuse of personal data", "Misuse of information", "Disruption of the work process" and "Loss of information". Respondents were explained that they could choose more than one of the proposed answers. The purpose of this question is to provide more specific information about cybersecurity vulnerabilities.

Table 8. Answers to Question No 13

	Unauthorized access	Misuse of personal data	Misuse of information	Disruption of the work process	Loss of information	Total
number of respondents' answers	164	96	99	137	152	**648**
Answers defined in %	25,3 % (65,3 %)*	14,8 % (38,2 %)*	15,3 % (39,4 %)*	21,1 % (54,6 %)*	23,5 % (60,6 %)*	**100 %**

* The first percentage is defined as a ratio to the total number of responses, and the second percentage is defined as a ratio to the number of respondents.

With the least vulnerability, two answers were identified: "Misuse of personal data" and "Misuse of information". 'Misuse of personal data' was chosen as a possible answer by 96 respondents or 38.2%. "Misuse of information" as a threat to cybersecurity was indicated by 99 employees or 39.4% of the respondents. "Disruption of the work process" is indicated as high vulnerability (54.6% - 137 respondents).

Two of the cybersecurity threats have been identified with the highest vulnerability: "Loss of information" and "Unauthorized access". "Loss of information" was identified as a danger by 152 persons (60.6%) and "Unauthorized access" – by 164 employees or 65.3% of the total respondents in the survey.

Overall, the results of the question present a high degree of uncertainty regarding cybersecurity. The presented weaknesses for cybersecurity define it as one of the highly vulnerable areas in general in the administrative security of municipalities. Cybersecurity creates a special sense of insecurity because it is associated with the personal access of employees and the performance of their personal duties. In the development of the model for administrative security management in municipalities, these vulnerabilities are included as threats to cybersecurity.

Question No. 18: Do you think that there is a need for additional training in terms of security for employees in the municipality?

The answer is presented as a choice on a scale of 1 to 5, with answer 1 being a resounding NO and answer 5 being a resounding YES. The constantly changing conditions affecting administrative security are a major prerequisite for the change in the methods and tools for its provision, and on the other hand, the introduction of new technical means and software also raises the issue of additional training of employees. Training in public institutions is often directed only to the management levels, neglected for employees with executive functions.

Table 9. Answers to Question No 18

	1	2	3	4	5	Total
number of respondents' answers	4	16	33	117	81	**251**
Answers defined in %	1,6 %	6,4 %	13,1 %	46,6 %	32,3 %	**100 %**

Indicative are the answers that only 4 people (1.6% of the respondents) answered that they do not need additional security training, and 16 others (6.4%) indicated that they have little need for such training. The extremely high share of persons who, on the contrary, answer that there is a need for training in terms of administrative security, is also indicative. These are the respondents who chose answers "4" and "5" from the scale – 78.9% or a total of 191 of the respondents. The implementation of additional measures,

policies, software, etc. Without additional familiarization and training of employees, there would not be the expected efficiency.

Question No 20: In your opinion, is there a need to implement a model for administrative security management in the municipality in which you work?

Three standardized answers are proposed: "YES", "NO" and "I can't decide". This question to the respondents determines the need for the implementation of a model for administrative security management in municipalities.

Table 10. Answers to Question No 20

	ДА	НЕ	Не мога да преценя	Total
number of respondents' answers	215	3	33	**251**
Answers defined in %	85,7 %	1,2 %	13,1 %	**100%**

A strong disagreement was reported in the answers of only three respondents or 1.2% of the total respondents. The share of persons who abstain from an opinion by choosing the answer "I cannot decide" (13.1%) can also be reported as low. The approval for the implementation of an administrative security management model in municipalities is shared by 215 of the municipal employees, which represents 85.7% of the participants in the survey. In this case, the direct question also provides a direct answer, which encourages the development of a model for managing administrative security in municipalities.

2.2.Description of the model.

The model for managing administrative security in municipalities is a matrix of different areas of security, as parts of administrative security. Potential security threats are brought to each of the areas. A set of response or preventive measures is proposed for each of the threats in the individual districts. Prioritization in the application of measures is carried out according to the weight of significance and danger assigned to the threat.

The effectiveness of the model is enhanced by the inclusion of interaction levels, i.e. the hierarchical level at which the threat is derived or which is responsible for the implementation of the measure.

 The purpose of the model is to assist Bulgarian municipalities in ensuring administrative security. The model has been developed for municipalities and can be applied in any municipality in Bulgaria, and the results allow for comparability. The model is developed as an open system that can be supplemented and changed according to the characteristics and

risks to administrative security in each municipality. The model can be quickly adapted in the event of a change in the regulatory framework or for use by other public sector institutions. The model can be applied as an element in the analysis of the overall risk assessment in municipalities. The convenience of the model is that there is no specific time commitment. It can be prepared once to determine the threats to administrative security at a given time. With the implementation of measures and the suspension of specific threats, it can be constantly updated, thus prioritizing the potential threats at the moment.

An annual review of the state of administrative security through the model provides an objective assessment to assist management in making management decisions.

2.3. **Stages in the development of the model**

The creation of the model goes through several main stages: grouping the main critical areas in the management of administrative security in municipalities, distinguishing the levels of interaction, analyzing the potential weaknesses and threats in each area and level, deriving activities/guidelines for prevention/response to threats and initiatives for improvement.

Stage 1: Grouping the main critical areas in the management of administrative security in municipalities is a fundamental step in building the author's model.

This multiplicity of potential threats to administrative security requires them to be grouped into several key areas. For the purposes of the model, five key areas for the management of administrative security in municipalities have been formed:

- *Information security* – this is the broadest category. It includes information sources and channels, correspondence, communication links, documentation, access to information, etc.

- *Cybersecurity* – this area includes all activities related to the use of software, digital content and networks and systems for the purposes of the model.

- *Physical security* – for the purposes of the model, this area includes the material and material security of the administrative process. Here under observation are the building stock, premises for carrying out activities, archive rooms, various technical means and equipment, etc.

- *Organizational security* – in this area of administrative security, for the purposes of the model, the established organization as a

structure, the established hierarchical levels, the distribution of functions and responsibilities, the formed communication links, the mechanisms for monitoring and control, etc.

- ***The "human factor"*** – this area of administrative security is considered by the person as a performer. For the purposes of the model, here we consider the person – the employee engaged in the provision of services. In this context, the performance of the activities of each employee may pose threats to administrative security – making mistakes, negligence, failure to meet deadlines, using inappropriate information or sources, exceeding authority, misuse of information and personal data, violation of ethical standards, etc.

Stage 2: Differentiate the levels of interaction. The functions and activities of municipalities as institutions presuppose uniformity in terms of structure and organizational structure.

For the purposes of the current model of administrative security management, the differentiation of interaction levels is based on the hierarchical levels formed in the municipalities. On this basis, the model distinguishes three levels: senior management, administrative management and executive level

Stage 3: Analyzing potential weaknesses and threats in each area and level.

At this stage, all potential threats to administrative security are identified. Threats are systematized in the model matrix, ranked according to the level and area of security where they can occur. The aim is to address any expected weaknesses in terms of administrative security. The rich set of included security threats allows each municipality to specify them according to its level of administrative security. The potential weaknesses or threats identified include the ability to determine weight. The weight in the model is a free field that each municipality determines according to its analysis of the level of security for each threat. In this way, the assessment of administrative security gives objective results and prioritizes the measures for the prevention of individual threats.

Stage 4: Implementation of threat response measures and improvement initiatives.

A set of different actions (measures) for prevention is derived from the weaknesses and threats already identified in the previous stage. In the implementation of the model, the implementation of measures can be applied

in two aspects. On the one hand, measures that relate to threats with a higher priority (weight) may be applied with priority, on the other hand, measures that are included as a response to more than one threat may be applied with priority. It is best to apply the measures at the same time, where possible. In cases where the implementation of one measure is conditional on the implementation of another measure, their priority should be respected.

Stage 5: Construction of the Model – a matrix of interaction between the areas of administrative security and hierarchical levels.

Table 11. Model for management of administrative security in municipalities.

		HIERARCHICAL LEVEL								
		Senior Management (GK)			Administrative management (AR)			Executive Level (IN)		
		Threats	weight	Measures	Threats	weight	Measures	Threats	weight	Measures
ADMINISTRATIVE CERTAINTY	Information Security									
	Cyber Security									
	Physical security									
	Organizational Security									
	"The Human Factor"									

3. Application and monitoring of the model.

The administrative security management model can be applied as an element in the analysis of the overall risk assessment in municipalities. The model can be easily adapted for application in other public institutions and even in the private sector. Adaptation of the model is also possible in case of changes in the regulatory framework, the environment of application or under the influence of external factors. The convenience of the model is that it is built as an open structure, which allows it to be constantly supplemented and changed.

Monitoring on the model can be applied permanently. There is no set time slot for monitoring. Periodic monitoring will ensure a constant objective assessment of the state of administrative security. The security areas identified separately provide the opportunity to be monitored independently. The division of hierarchical levels also allows them to be monitored independently and provoke specific actions or decisions for the specific level.

It is good to monitor the model and the implementation of its measures at least once a year in order to assess the evolution of potential threats and the progress of the implementation of the measures, eliminating individual threats or limiting the possibility of their actual manifestation.

Conclusion:

1.The survey shows a good culture and level of awareness in the field of administrative security of employees. From the survey, the respondents confirm the need to create a model for administrative security management in municipalities, which will help in ensuring their administrative security.

2.The Administrative Security Management Model has been developed for a wide range of users as an open system that can be supplemented and changed according to the characteristics and risks of administrative security in the municipality. The model can be applied in any municipality in Bulgaria, and the results allow for comparability.

References:

[1]   Metodieva, Ts. Problems of the economic development of Bulgaria, SocioBrains, бр. 89, January, 2022. pp. 148-150, ISSN: 2367-5721. http://sociobrains.com.

[2]   Metodieva, Ts., Parashkevanova, G., Mahmud, A. "Threats on the Internet. Phishing and Financial Mule", International Scientific Conference "Cybersecurity in the Information Society", Vasil Levski National Military University, Faculty of Artillery, Air Defense and CIS, Shumen, 20-21 April 2017, ISBN 978-954-9681-82-6, pp. 157-160

[3]   Dimanova, D., Risk Management, Episkop Konstantin Preslavski Publishing House, Shumen, 2016, ISBN: 978-619-201-095-9..

[4]   Slatinski, N. (2010). The five levels of security. Sofia.

[5]   Law on Administration, promulgated with State Gazette. Pc. 130 of 05.11.1998, last amended and/or supplemented by SG No. 33 of 12.04.2024

[6]   Law on Internal Audit in the Public Sector, promulgated with State Gazette. Pc. 27/31.03.2006, last amended and/or supplemented by SG No. 100 of 20.12.2019......