UDC 004.05 **doi: 10.20998/2522-9052.2019.4.14**

O. Milov[1], M. Kostyak[2], S. Milevskyi[1], H. N. Rzaev[3]

[1] S. Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
[2] National University "Lviv Polytechnic", Lviv, Ukraine
[3] Azerbaijan State University of Oil and Industry, Baku, Azerbaijan

INFORMATION SECURITY INVESTMENT MODEL: RESOURCE REPRESENTATION AND ORGANIZATIONAL TRAINING

Abstract. Information technology (IT) protection is a key economic concern for organizations. While research in the field of investment in IT security is growing rapidly, they lack the theoretical basis for combining economic and technological phenomena and research directions. The proposed theoretical model is based on the use of the theory of organizational behavior and resource representation. The combined application of these theories allows, within the framework of one model, to present the organizational effects of training that arise when developing the protection of organizational resources using countermeasures of IT security. Identified approaches to the study of investments in information security, which boil down to the following: microeconomic approaches based on game theory, financial analysis based on return on investment (ROI), net present value (NPV) and internal rate of return (IRR), and management approaches based on decision theory, risk management and organization theory. The combination of various theories and approaches leads to the formation of a multi-theoretical model, which allows you to combine the methods of these research areas within the framework of a comprehensive model based on the resource representation and the theory of organizational learning. The difficulties of developing a theoretical model for investment in information security are indicated, namely: the diversity of the nature of countermeasures, covering strategic and operational issues, taking into account legal, technical and organizational aspects; the intended purpose of investments in information security (risk reduction, not profit); the complementarity of the prospects for the operational and strategic periods. Various points of view on investment problems are presented, namely, resource representation and representation in the framework of the theory of organizational learning. The proposed approach allowed us to build an integrated model of investment in information security. Answers to questions arising from the analysis of the integrated model of investment in information security can not only determine future research, but also have managerial consequences that will help firms make informed investment decisions in the field of information security.

Keywords: information security; investment; resource representation; organizational theory of learning; integral investment model.

Introduction

The protection of information technology (IT) today will remain a key task for organizations that need to protect their IT systems, data, intellectual property and business processes from attacks, misuse or technical failures [1-5]. IT threats can lead, for example, to disruption of production and service processes, as well as data theft, which in turn leads to economic damage, including loss of productivity and income, loss of reputation [6]. Many security incidents are related to cybercrime, which can be considered as a growing industry [7]. Industries respond to emerging information security threats with high investments in IT security. The IT security landscape is permeated not only with technological, but also with financial problems. Given budgetary constraints, the key economic issue for organizations is the question of which of their assets (processes, systems, etc.) needs which level of protection, which security countermeasures (for example, firewalls, intrusion detection systems, security training or security policies) provide this protection and how much you need to spend on such countermeasures [8, 9].

A wide range of approaches from various disciplines, including microeconomics [10, 11], finance [12], risk management [13] and organization theory [14], has been proposed to analyze the economic problems of IT security. An analysis of these approaches allows us to formulate three research questions:

1. Why and how can one use a multi-theoretical perspective based on a “resource view” and a “theory of organizational learning” to structure and guide research in the field of investment in information security?
2. To what extent has literature contributed to key issues of investment in information security?
3. What gaps in research into investment in information security have yet to be addressed?

The approach based on generally accepted “views based on resources” and “theory of organizational learning” is based on the desire to provide both static and dynamic (temporary) protection of organization resources at the company level. Adopting only one theory inevitably leads to ignoring a static or dynamic perspective. Using a multi-theoretical approach allows us to propose a new theoretical model of investment in information security.

Literature review on investment in information security. The effectiveness and cost-effectiveness of investments in information security has long been an important research topic [15]. Currently, there are three interdisciplinary areas of research related to investments in information security: (1) microeconomic approaches based on game theory (for example, [10, 16]); (2) financial analysis based on return on investment (ROI), net present value (NPV) and internal rate of return (IRR) (for example, [12, 17, 18]); and (3) management approaches based on decision theory (for example, [19]), risk management (for example, [13, 17]) and organization theory (for example, [14, 20]). The combination of various theories and approaches leads to the formation of a multi-theoretical model, which allows to use the methods of these areas of research into a

comprehensive model based on the resource representation and the theory of organizational learning.

The development of a theoretical model for investment in information security is a difficult task because:

(1) the nature of countermeasures is diverse, encompassing strategic and operational issues, taking into account legal, technical and organizational aspects;

(2) investments in information security are not intended to generate profit, but to reduce risk, that is, they are successful if "nothing happened" and, therefore, potential results (benefits or losses) are often intangible [15]. Examples of intangible results are the benefits of regulatory compliance and public trust. Investing in information security processes or products does not provide direct returns, but can have a positive impact on an organization's effectiveness if it reduces potential risks [22];

(3) The complementarity of ex-ante and ex-post perspectives should be taken into account. First, approaches that use the ex-ante perspective are aimed at providing decision support by assessing the costs and benefits of possible investments [22]. Secondly, approaches that use the ex-post perspective reflect investments made in the past and evaluate whether the budget allocation of the company was effective and efficient [22].

The first two of these problems can be solved based on a resource-based view, because (a) a variety of assets, such as systems, data or processes that need to be protected, can be modeled as resources and (b) both tangible and intangible resources, such as firewalls and security knowledge, can be explicitly considered [21]. The theory of organizational learning is particularly suitable for solving the third problem, since it takes into account the ability of the company to study and integrate time and dynamic feedback cycles.

In general, both the resource-based view and the theory of organizational learning, which are recognized theories in the IS literature [15, 23], provide an appropriate theoretical basis for researching investments in information security.

Multi-theoretical view on investment in information security

The literature on investments in information security can be evaluated from two points of view: from the point of view of the resource representation and the theory of organizational learning. These two points of view complement each other:

(1) A resource-based view is inherently static and focuses on the possession of resources and capabilities [24-25]. This means that it does not take into account the dynamics and time effects. In contrast, organizational learning theory takes into account effects such as learning progress achieved as a result of past mistakes of the organization over time, which ensures that the organization converts "information into valuable knowledge, which, in turn, increases its ability to long-term adaptation" [26]. Thus, it allows the organization to respond to dynamically changing environments.

(2) The resource-based view, as proposed in [27], enters into force and covers the main factors (see Fig. 1) that must be taken into account when making investment decisions [21], for example, the macroeconomic, competitive and target environment of the company. The advantage of a resource-based presentation is that it theorizes the various components of the firm, its environment and relationships with each other, and unlike the organizational theory of learning, does not focus on the organization and its components in detail.

Point of view "resource analysis"

The origins of resource-based representations, one of the most influential theories in the history of control theory [28], can be traced back to [29-32]. The key proposal is that the company should acquire and control valuable, rare, unique and irreplaceable resources and opportunities to achieve a sustainable competitive advantage [25, 33-35].

According to [33], the firm's resources include "all assets, opportunities, organizational processes, attributes of the firm, information, knowledge, etc., controlled by the firm, which allow the firm to develop and implement strategies that improve its efficiency and effectiveness.

According to [21], investments in information security are a subtype of (general) investments in IT, and therefore a resource-based view is suitable for generating investments in information security for three reasons:

(1) Non-security IT resources or assets (IT systems, data, processes, etc.) that need to be protected, and IT security resources that provide protection, can be modeled as resources, covering both tangible resources, such as firewalls, and intangible resources, including knowledge of security [21].

(2) A resource-based view was used in the IS literature to structure investments in information security. For example, [36] uses a resource-based view to evaluate hypotheses regarding organization size, security breaches, and discusses the relationship of resource-based views to security investments. The central elements of a resource-based approach can also be found in [37].

(3) The resource-based presentation has already served as the theoretical basis for literature reviews in the field of IS, such as the "Model of Business Value in the Field of Information Technology" [37]. We will focus on a resource-based presentation that has been adapted to the investment context of information security [21], as shown in Fig. 1 and described in table 1.

In Fig. 1, the relationship between constructs means "can improve." Impacts M_1, C_1 and C_2 describe external factors that affect the investment decisions of the information security of the organization. Country characteristics, such as level of development or government regulations, affect the firm's investment decisions in the field of information security, which is reflected as a result of the impact of M_1. Competitiveness, regulation, technological changes and other industry-specific factors (C_1) and trading partners such as buyers and suppliers (C_2) influence the firm's decision to invest in information security.

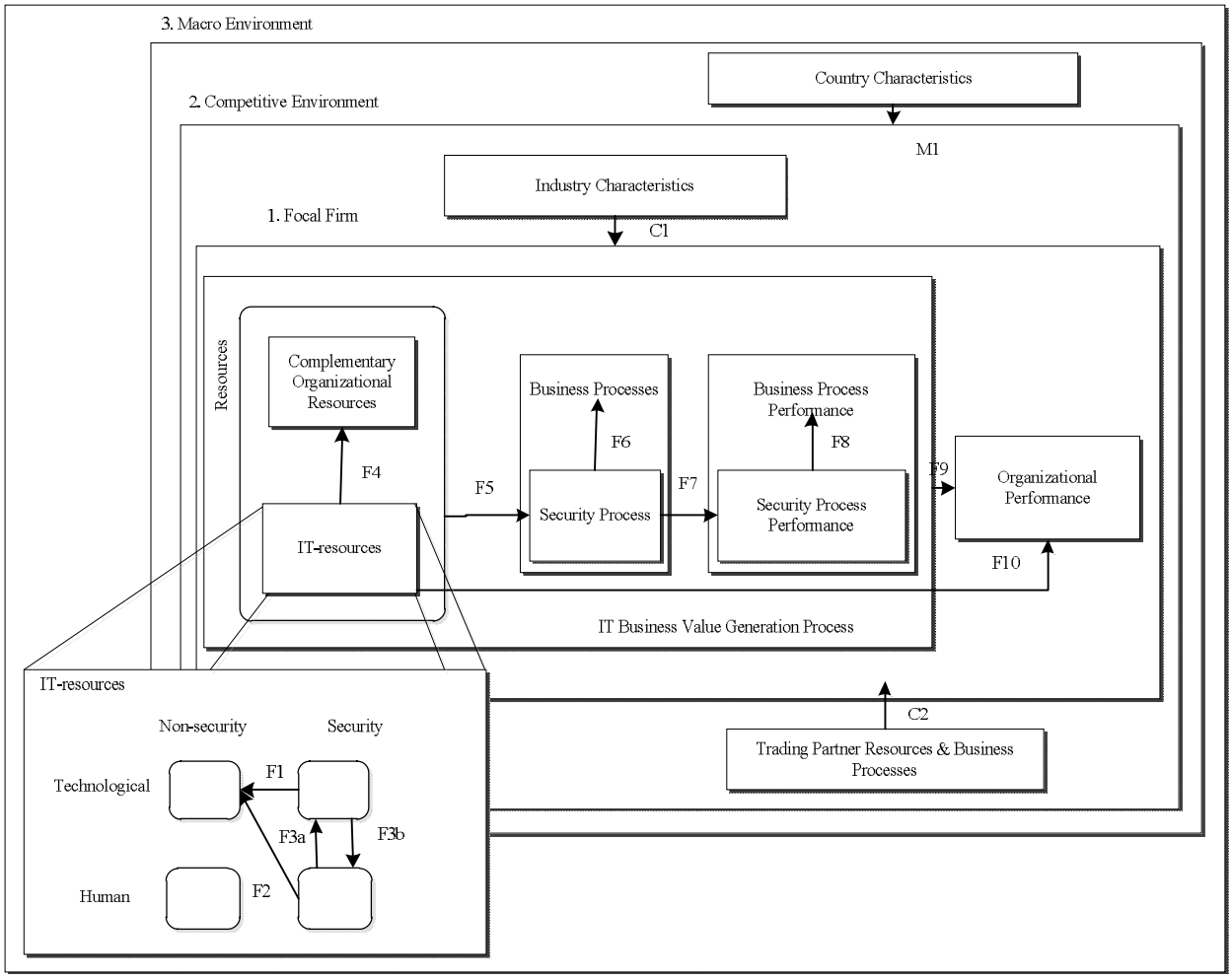

Fig. 1. Resource-oriented presentation of investments in information security

Table 1 – **Definitions and examples of model designs**

Design	Definition and examples
1. Target company	
Resources: - IT resources: - technological - human - security Additional organizational resources	Hardware and software, for example, common technologies and technological solutions for the entire enterprise, procurement, sales, etc. [27] Technical and managerial IT skills, such as training, experience, knowledge, judgment, intelligence and relationships [33] Resources protecting other resources, such as a firewall, intrusion detection system, antivirus software, biometric scanning authentication. Organizational and physical resources that complement IT, such as policies, rules, organizational structure and culture [27], as well as workers, offices and equipment
Processes: - business process - security process	A specific streamlining of work activities and clearly defined inputs and outputs [46], for example, order collection, PC assembly, distribution [27] Processes that help ensure the confidentiality, integrity and accessibility of a firm [47]
Performance: Business process performance Security process performance Organization performance	The operational efficiency of certain business processes [27], for example, customer satisfaction [48], turnover [49], gross margin and quality [45] Operational efficiency of security processes. For example, no registration (FTE), false match rate (FMR) in a biometric authentication system (OECD 2004). The overall effectiveness of the company, including productivity, efficiency, profitability, market value, competitive advantage, etc. [27]
2. Competitive environment	
Industry characteristics Partner Resources and Business Processes	Factors that influence the use of IT in the main company to create value for the business, for example, competitiveness, regulation, technological changes [27] IT and non-IT resources and business processes of trading partners such as buyers and suppliers [27]
3. Macro environment	
Country characteristics	Macro factors forming IT applications and creating value for IT businesses, for example, level of development, basic infrastructure and culture [27]

Impacts from F_1 to F_{10} reflect the impact of investments in various IT security resources within a specialized firm. F1 refers to the impact of IT security technology resources on non-security technology resources, such as investments in a firewall to protect non-security IT resources, such as data (eg, [11, 38, 39]). Since a significant number of security incidents are caused by humans and not by technical failures or by intruders [40], F_2 considers the impact of IT security human resources on non-security technological IT resources. For example, security workshops and trainings focus on data protection. The impact of F_{3a} is related to the impact of IT security human resources on IT security technology resources (for example, seminars on the use of intrusion detection systems affect IDS) with F_{3b}, on the contrary (for example, systems that control file transfer, warn employees and therefore train them awareness).

The influence of F_4 is associated with the influence of IT resources on additional organizational resources, such as the creation of a company, access to which can be protected by authentication systems [41]. Investing in IT security resources and additional organizational resources can improve business processes or launch new ones (F_5 impact). The influence of F_6 refers to the fact that information security processes are designed to protect business processes and their main resources [42, 43]. Security processes are subtypes of business processes because "a security process is doomed to fail if it does not protect the business process" [44]. Security y process efficiency is measured using safety process performance (influence F_7). The performance of the security process affects the performance of the business process, which is the result of the relationship of the business process to the security process and is conceptualized as an F_8 impact. The process of creating value for the IT business, including resources, processes, business performance and security, directly affects the organization's productivity (F_9 impact). Impact F_{10} refers to the "direct relationship between IT and the overall performance of a firm, bypassing the impact of IT on business processes" [45].

Point of View "Theory of Organizational Learning"

In the context of growing globalization and accelerating the dynamics of the competitive environment, organizations need to constantly improve their products and processes in order to create and maintain competitive advantages [50]. The current interest in organizational learning among scientists and practitioners reflects this new competitive field [51].

According to [52], training is defined as "detection and correction of errors, and error as any feature of knowledge or knowledge that makes the action ineffective", and "detection and correction of error produces training, and the absence of one or both prevents learning". In addition, complex and poorly structured problems tend to be more ambiguous and are associated with a higher error rate, which makes it difficult to implement effective plans and actions [52]. Because investments in information security are complex issues, they will benefit from the perspective of Organizational Learning Theory, in particular because it describes how the effectiveness of solutions can be improved over time, taking into account past experience in feedback loops. In addition, the theory of organizational learning provides a dynamic view that can be used to continuously analyze the impact of investments on the level of security [15, 53-54]. Conceptually, the influences that influence decisions about investments in information security can be modeled as control variables, investments in IT security resources can be modeled as action strategies that lead to consequences such as increased security.

We use the Theory of Organizational Learning proposed [55] in the context of investments in information security (see Fig. 2 and Table 2). Organizational learning is defined as a change in the organization's knowledge because a firm gains experience over time (see [56, 57]). The model of Organizational learning includes three interrelated constructs: control variables, action strategies, and consequences. According to the original model [55], relationships are defined as "influencing" (arrows in Fig. 2).

Control variables (construction C_1) are the goals that the company seeks. As organizations bring their actions in line with their goals [55], regulatory variables influence investment decisions in the field of information security (impact I_1). For example, one of the goals may be compliance with state and industry regulations, such as the state law on the protection of information in information and telecommunication systems [58].

Action strategies (construct C_2) are "sequences of movements" [55] designed to achieve specific goals as measured by regulatory variables. In our case, action strategies are investments in IT security resources, such as implementing a firewall or intrusion detection system.

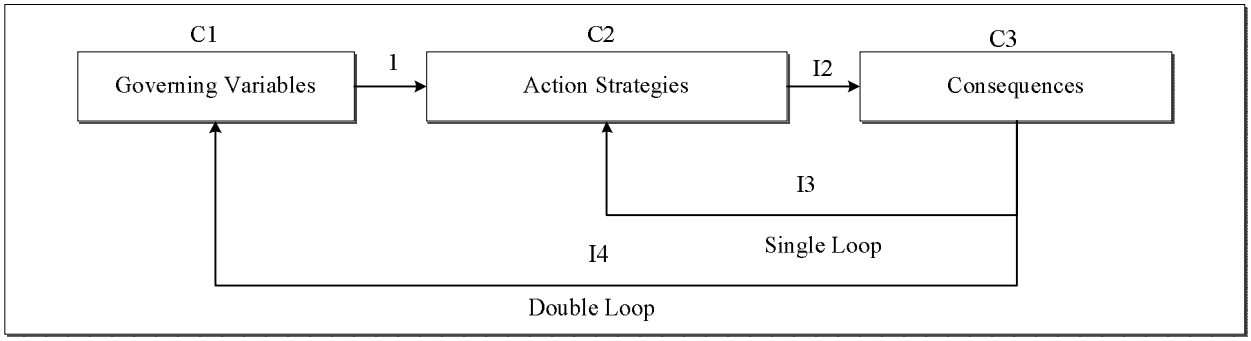

Fig. 2. The relationship of the elements of the organizational learning theory

Table 2 – **Model of constructions and impacts in the theory of organizational learning (see Fig. 2)**

N	Construct / influence	Definition	Example
C_1	Control variables	The goals that the company seeks to achieve [55]	State and industry regulations, the preference of the company for risks
C_2	Action strategies	Sequences used by actors in specific situations to maintain regulatory variables at a satisfactory level [55]	Investments in workshops, firewalls, encryption or access control methods
I_2	Impact of action strategies on consequences	Actions have implications for organizational effectiveness [55]	Investments in safety seminars lead to fewer unintended safety incidents caused by employees [59]
C_3	Consequences	Consequences of strategies, perceived or unintended, productive or counterproductive [55]	Reduce security incidents on the internal network or increase service availability
I_3	Single-loop training	When new action strategies are used within the same control variables. There is a change in action, but not in control variables [55]	If investing in workshops will reduce unintended safety incidents, the firm will learn lessons from efficiency and consider future investments in such trainings
	Double-loop training cycle	Ask questions and change control variables according to the consequences [65]	The organization adapts its investment strategy to changing environmental factors, such as investing in an advanced encryption system, to counter the increasing attacks of hackers

Strategies for action affect the consequences (impact I_2). An example is investment in security workshops, which are expected to reduce the number of security incidents caused by employees [60].

The implications (construct C_3) include all the results associated with investments in information security, whether they are intentional or unintentional, productive or counterproductive [55]. The consequences may correspond to regulatory variables if the firm has chosen an appropriate action strategy. Exemplary consequences are a decrease in the number of security incidents or an increase in the availability of services.

Impacts 3 (I_3) and 4 (I_4) are additional training opportunities that reflect how well the firm is trying to evaluate its investment decisions in the field of information security.

"Impact I_3" refers to one-cycle training, which includes adjustments consistent with the "existing set of rules and norms" [61], that is, it is not associated with changes in control variables [62]. For example, single-loop training occurs if the consequence of an action strategy is to reduce the number of security incidents, and the firm evaluates a positive result to make sure that the action strategy selected is the best without changing control variables.

The influence of I_4 refers to the learning process, which takes place in a double circuit and includes modifications of "fundamental rules and norms that underlie actions and behavior" [61, 63]. In the case of the investment scenario of information security, such training occurs if the consequences of investment decisions do not meet the objectives and prompt the company to overestimate the regulatory variables and invest differently. While single-loop learning is a common model of action, dual-loop learning provides "feedback and more effective decision making" [52]. Nevertheless, "the overwhelming number of training processes implemented in the organization is one cycle, since it is designed to identify and correct errors so that the work is completed and the action remains within the framework of the stated recommendations" [64].

Please note that constructions C_1 to C_3 with exposures I_1 and I_2 imply a time sequence, while exposures I_3 and I_4 describe two possibilities of a firm's assessment and training processes aimed at correcting their potential mistakes and making more effective and efficient decisions in the future.

Integrated Information Security Investment Model

We integrate the resource-based view, as shown in Fig. 1, and the theory of organizational learning, as shown in Fig. 2, into a multi-theoretical model (see Fig. 3), which retains the advantages of both initial theories: the integrated model takes into account the re-evaluation of investments in information security by dynamically including feedback from a single and double training cycle to adjust the corresponding action strategies. In addition, the integrated model creates company-specific components, such as business processes and security resources, which makes it compatible with an established set of research on resource-based presentation.

We combine the initial theories as follows: country features, industry characteristics and resources of trading partners, as well as business processes affect firms when making investment decisions in the field of information security; therefore, these factors are classified as regulatory variables. Control variables have an impact (impact 1 in Fig. 3) on investment decisions in IT security resources that are consistent with action strategies. For example, state regulations of a specific country require certain investments to undergo a safety audit [67]. Investments in technological or human information security resources are associated with action strategies. This means, in particular, that investments in training, education, or raising security awareness are part of action strategies as they relate to IT security human resources.

Investments in IT security resources have an impact on the consequences reflected in Impact 2. Implications include the impact of investments on non-security resources, security processes, security process performance, and overall organization performance. Impacts from 3 to 6 within the consequences are taken from a resource-based view. Please note that the "Business process" design in the "Consequences" refers to the business processes of the target company, while

the "Resources and business processes of the trading partner" design in "Control variables" refers to the business process of trading partners, which affect investment decisions in IT security of the main company and, therefore, are part of the Control Variables.

Single- and double-loop training cycles (effects 7 and 8) are taken from the theory of organizational learning; they represent feedback loops on the consequences for control variables and action strategies.

Definitions and examples of impacts presented in Fig. 3 are presented in table 3. The synthesis of knowledge about investments in information security was based on a new theoretical model of investments in information security (see Fig. 3). This model is based on the integral application of resource-based presentation and organizational learning theory.

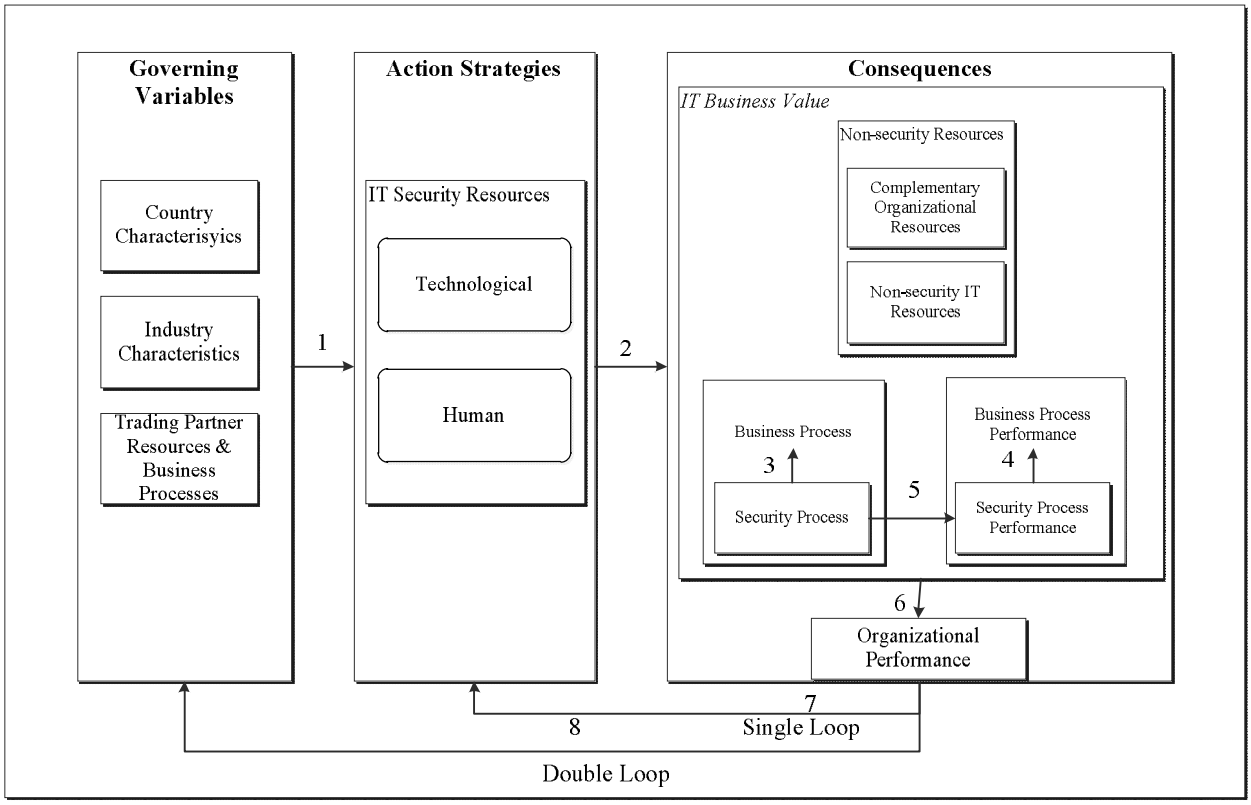

Fig. 3. Integrated model of investment in information security

Table 3 – **Impacts in the integrated model of investment in information security (see Fig. 3)**

No.	Influence	Definition	Example
1	The influence of control variables on action strategies	Country characteristics, industry characteristics, trading partner resources and business processes affect the investment decisions of the company in the field of information security [21, 27].	SOX requires companies to invest in additional IT security resources to undergo a security audit [67].
2	Impact of action strategies on consequences	Investing in IT security resources (technological or human) impacts non-security IT resources, additional organizational resources, processes and productivity [21, 27].	Investments in an IT security technology resource, such as biometric authentication systems, affect non-security IT resources, such as data and equipment, as they prevent unauthorized access to company premises.
3	The impact of security processes on business processes	Business processes are constantly threatened and must work continuously to ensure the success of the company [21, 42, 43].	Biometric authentication is a security process that directly affects the business process, because if the authentication system fails, work processes are violated [21].
4	Impact of the security process on the performance of the security process	The effectiveness of the security process is expressed by the performance of the security process.	The number of true / false or positive / negative authentication attempts measures the effectiveness of the authentication system.
5	Impact of security process performance on business process performance	Security process performance affects business process performance.	The low number of false rejections of the authentication system provides a continuous workflow.
6	The impact of IT business value on organizational performance	All resources, processes and productivity directly affect the overall performance of the company [27].	The effectiveness and productivity of an organization increases when the organization's workflow is rarely interrupted and quickly restored.
7	Single-loop training: the impact of consequences on action strategies	When new action strategies are used to serve the same control variables. There is a change in action, but not in control variables [55]. (watch the tab. 2)	If investing in workshops will reduce unintended safety incidents, the firm will learn lessons from efficiency and consider future investments in such trainings (watch the tab. 2).
8	Double loop Learning: Impact on Control Variables	Ask questions and modify control variables according to the consequences [66]. (see table 2)	The organization adapts its investment strategy to changing environmental factors, such as investments in an advanced encryption system, to withstand the increasing attacks of hackers (watch the table 2).

The answer to the questions posed by the study and the elimination of the gaps associated with this has not only academic significance, but also managerial consequences.

Conclusion

A model of investment in information security is presented, based on two well-established IS theories: a representation based on resources and the theory of organizational learning.

Answers to questions arising from the analysis of the integrated model of investment in information security can not only guide future research, but also have managerial consequences that will help firms make investment decisions in the field of information security.

REFERENCES

1. Anderson, R. (2001), "Why Information Security is Hard - An Economic Perspective", *Annual Computer Security Applications Conference (ACSAC 2001),* pp. 358-365.
2. Frost & Sullivan. 2013. "The 2013 (ISC)2 Global Information Security Workforce Study", available at https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/2013-ISC2-Global-Information-Security-Workforce-Study.pdf.
3. Gartner (2011), "Magic Quadrant for Security Information and Event Management,", *Gartner RAS Core Research.*
4. Gartner (2012), "IT Key Metrics Data 2012: IT Enterprise Summary Report,", *Gartner RAS Core Research.*
5. Whitman, M. E. (2003), "Enemy at the Gate: Threats to Information Security," *Communications of the ACM*, pp. 91-95.
6. Bandyopadhyay, T., Mookeijee, V. S., and Rao, R. C. (2009), "Why IT Managers Don't Go for Cyber-Insurance Products," *Communications of the ACM* (52:11), pp. 68-73.
7. McAfee (2014), "Net Losses: Estimating the Global Cost of Cybercrime,", June (available at http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf).
8. Anderson, R., and Schneier, B. (2005), "Guest Editors' Introduction: Economics of Information Security," *IEEE Security & Privacy* (3:1), pp. 12-13.
9. Gordon, L. A., and Loeb, M. P. (2006), "Economic Aspects of Information Security: An Emerging Field of Research," *Information Systems Frontiers* (8:5), pp. 335-337.
10. Grossklags, J., Christin, N., and Chuang, J. (2008a), "Secure or Insure?: A Game-theoretic Analysis of Information Security Games," *Proceedings of the 17th International Conference on World Wide Web,* pp. 209-218.
11. Grossklags, J., Christin, N., and Chuang, J. (2008b), "Security and Insurance Management in Networks with Heterogeneous Agents," *Proceedings of the 9th ACM Conference on Electronic Commerce,* pp. 160-169.
12. Buck, K., Das, P., and Hanf, D. (2008), "Applying ROI Analysis to Support SOA Information Security Investment Decisions," *IEEE Conference on Technologies for Homeland Security,* pp. 359-366.
13. Hoo, K. J. S. (2000), *How much is enough? A Risk Management Approach to Computer Security,* Stanford University.
14. Cohen, F. (2006), IT Security Governance Guidebook with Security Program Metrics on CD-ROM, *CRC Press.*
15. Kwon, J., and Johnson, M. E. (2014), "Proactive Versus Reactive Security Investments in the Healthcare Sector," *MIS Quarterly* (38:2), pp. 451-471.
16. Sim, W., Kong, X., He, D., and You, X. (2008), "Information Security Problem Research Based on Game Theory," in *International Symposium on Electronic Commerce and Security,* pp. 554-557.
17. Bojanc, R., and Jerman-Blazic, B. (2008a), "Towards a Standard Approach for Quantifying an ICT Security Investment," *Computer Standards & Interfaces* (30:4), pp. 216-222.
18. Bojanc, R., and Jerman-Blazic, B. (2008b), "An Economic Modelling Approach to Information Security Risk Management," *International Journal of Information Management* (28:5), pp. 413-422.
19. Huang, C. D., and Goo, J. (2009), "Investment Decision on Information System Security: A Scenario Approach," in *AMCIS 2009 Proceedings.*
20. Hagen, J. M., Albrechtsen, E., and Hovden, J. (2008), "Implementation and Effectiveness of Organizational Information Security Measures," *Information Management & Computer Security* (16:4), pp. 377- 397.
21. Weishaupl, E., Yasasin, E., and Schiyen, G. (2015), "IT Security Investments through the Lens of the Resource-based View: A new theoretical Model and Literature Review," *ECIS 2015 Completed Research Papers.*
22. Bohme, R., and Nowey, T. (2008), "Economic Security Metrics," *Dependability Metrics,* pp. 176-187.
23. Wade, M., and Hulland, J. (2004), "Review: The Resource-Based View and Information Systems Research: Review, Extension, and Suggestions for Future Research," *MIS Quarterly* (28:1), pp. 107-142.
24. Elsenhardt, K. M., and Martin, J. A. (2000), "Dynamic Capabilities: What are they?," *Strategic Management Journal* (21:1), pp. 1105-1121.
25. Kraaijenbrink, J., Spender, J.-C., and Groen, A. J. (2010), "The Resource-Based View: A Review and Assessment of its Critiques," *Journal of Management* (36:1), pp. 349-372.
26. Schwandt, D., and Marquardt, M. J. (1999), *Organizational learning,* CRC Press.
27. Melville, N., Kraemer, K., and Gurbaxani, V. (2004), "Review: Information Technology and Organizational Performance: An Integrative Model of IT Business Value," *MIS Quarterly* (28:2), pp. 283-322.
28. Kraaijenbrink, J., Spender, J.-C., and Groen, A. J. (2010), "The Resource-Based View: A Review and Assessment of its Critiques," *Journal of Management* (36:1), pp. 349-372.
29. Chandler, A. D. (1977), *The Visible Hand,* Cambridge, MA: Belknap Press.
30. Penrose, E. T. (1959), *The Theory of the Growth of the Firm,* New York: John Wiley & Sons.
31. Stigler, G. J. (1961), "The Economics of Information," *The Journal of Political Economy* (69:3), pp. 213-225.
32. Wernerfelt, B. (1984), "A Resource-Based View of the Firm," *Strategic Management Journal* (5:2), pp. 171- 180.
33. Barney, J. (1991), "Firm Resources and Sustained Competitive Advantage," *Journal of Management* (17:1), pp. 99-120.
34. Barney, J. B. (1994), "Bringing Managers Back in: A Resource-Based Analysis of the Role of Managers in Creating and Sustaining Competitive Advantages for Firms," *Does Management Matter,* pp. 1-36.
35. Barney, J. B. (1997), *Gaining and Sustaining Competitive Advantage,* Addison-Wesley Reading, MA.
36. Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004), "The Effect of Internet Security Breach Announcements on Market

Value: Capital Market Reactions for Breached Firms and Internet Security Developers," *International Journal of Electronic Commerce* (9:1), pp. 70-104.
37. Demirhan, D. (2005), "Factors Affecting Investment in IT: A Critical Review," *Journal of Information Technology Theory and Application (JITTA)* (6:4), pp. 1-13.
38. Jiang, L., Anantharam, V., and Walrand, J. (2008), "Efficiency of Selfish Investments in Network Security," in *Proceedings of the 3rd International Workshop on Economics of Networked Systems,* pp. 31- 36.
39. Torrellas, G. A. S., and Vargas, L. A. V. (2003), "Modelling a Flexible Network Security Systems Using Multi- agents Systems: Security Assessment Considerations," in *Proceedings of the 1st International Symposium on Information and Communication Technologies,* pp. 365-371.
40. Beautement, A., Sasse, M. A., and Wonham, M. (2008), "The Compliance Budget: Managing Security Behaviour in Organisations," in *Proceedings of the 2008 Workshop on New Security Paradigms,* pp. 47-58.
41. Liu, S., and Silverman, M. (2001), "A Practical Guide to Biometric Security Technology," *IT Professional* (3:1), pp.27-32.
42. Neubauer, T., and Heurix, J. (2008), "Defining Secure Business Processes with Respect to Multiple Objectives," in *3rd International Conference on Availability, Reliability and Security (ARES 2008),*pp. 187-194.
43. Wang, X., Zhang, Y., and Shi, H. (2008), "Access Control for Human Tasks in Service Oriented Architecture," in *International Conference on e-Business Engineering (ICEBE),* pp. 455-460.
44. Wattel, B. (2002), "Business Process Security", *Integrity, Internal Control and Security in Information Systems*, pp. 177-186.
45. Dehning, B., and Richardson, V. J. (2002), "Returns on Investments in Information Technology: A Research Synthesis," *Journal of Information Systems* (16:1), pp. 7-30.
46. Davenport, T. (1993), *Process Innovation: Reengineering Work Through Information Technology,* Boston: Harvard Business School Press.
47. Khansa, L., and Liginlal, D. (2009), "Valuing the Flexibility of Investing in Security Process Innovations," *European Journal of Operational Research* (192:1), pp. 216-235.
48. Devaraj, S., and Kohli, R. (2000), "Information Technology Payoff in the Health-care Industry: A Longitudinal Study," *Journal of Management Information Systems* (16:4), pp. 41-67.
49. Barua, A., Kriebel, C. H., and Mukhopadhyay, T. (1995), "Information Technologies and Business Value: An Analytic and Empirical Investigation," *Information Systems Research* (6:1), pp. 3-23.
50. Smith, K. A., Vasudevan, S. P., and Tanniru, M. R. (1996), "Organizational Learning and Resource-Based Theory: An Integrative Model," *Journal of Organizational Change Management* (9:6), pp. 41-53.
51. Hamdan, B. J. (2013), "Evaluating the Performance of Information Security: A Balanced Scorecard Approach," in *SAIS 2013 Proceedings*.
52. Argyris, C. (1976), "Single-Loop and Double-Loop Models in Research on Decision Making," *Administrative Science Quarterly,* pp. 363-375.
53. Culnan, M. J., and Williams, C. C. (2009), "How Ethics Can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches," *MIS Quarterly,* pp. 673-687.
54. Culnan, M. J., Foxman, E. R., and Ray, A. W. (2008), "Why IT Executives should help Employees Secure their Home Computers," *MIS Quarterly Executive* (7:1), pp. 49-56.
55. Argyris, C., Putnam, R., and Smith, D. M. (1985), "Action Science: Concepts, Methods, and Skills for Research and Intervention,",Jossey-Bass San Francisco, CA.
56. Argote, L. (2011), "Organizational Learning Research: Past, Present and Future," *Management Learning* (42:4), PP. 439-446.
57. Fiol, C. M., and Lyles, M. A. (1985), "Organizational Learning," *Academy of Management Review* (10:4), pp. 803-813.
58. Law on Information Protection in Information and Telecommunication Systems. Verkhovna Rada of Ukraine, №80/94-BP, 05.07.1994.
59. Daneva, M. (2006), "Applying Real Options Thinking to Information Security in Networked Organizations", *Centre for Telematics and Information Technology*, University of Twente.
60. Stephanou, A. (2009), *The Impact of Information Security Awareness Training on Information Security Behaviour.*
61. Romme, G., and Dillen, R. (1997), "Mapping the Landscape of Organizational Learning," *European Management Journal* (15:1), pp. 68-78.
62. Argyris, C. (1983), "Action Science and Intervention," *The Journal of Applied Behavioral Science* (19:2), pp. 115-135.
63. Argyris, C., and Schon, D. A. (1978), *Organizational Learning: A Theory of Action Perspective,* Addison-Wesley Reading, MA, pp. 345-348.
64. Argyris, C. (1977), "Organizational Learning and Management Information Systems," *Accounting, Organizations and Society* (2:2), pp. 113-123.
65. Derrick Huang, C., Hu, Q., and Behara, R. S. (2008), "An Economic Analysis of the Optimal Information Security Investment in the Case of a Risk-averse Firm," *International Journal of Production Economics* (114:2), pp. 793-804.
66. Shen, D., and Jones, B. L. (2005), "A New Implication for China's Rural Education Reform: Organizational Learning Theory," *Journal of International Agricultural and Extension Education* (12:1), pp. 27- 36.
67. Ghose, A., and Rajan, U. (2006), "The Economic Impact of Regulatory Information Disclosure on Information Security Investments, Competition, and Social Welfare.," *Workshop on the Economics of Information Security 2006 (WEIS).*

Received (Надійшла) 21.09.2019
Accepted for publication (Прийнята до друку) 30.10.2019

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Мілов Олександр Володимирович – кандидат технічних наук, доцент, доцент кафедри кібербезпеки та інформаційних технологій, Харківський національний економічний університет ім. Семена Кузнеця, Харків, Україна;
Oleksandr Milov – PhD in Technical Sciences, Associated Professor, Associated Professor of Cybersecurity and Information Technologies Department, S. Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine;
e-mail: oleksandr.milov@ukr.net; ORCID ID: http://orcid.org/0000-0001-6767-7524

Костяк Марина Юріївна – асистент кафедри інформаційної безпеки, Національний університет "Львівська Політехніка", Львів, Україна;
Maryna Kostyak – assistant, Department of Information Security, National University "Lviv Polytechnic", Lviv, Ukraine;
e-mail: kostyak@gmail.com; ORCID ID: http://orcid.org/0000-0002-6667-7693

Мілевський Станіслав Валерійович – кандидат економічних наук, доцент, доцент кафедри кібербезпеки та інформаційних технологій, Харківський національний економічний університет ім. Семена Кузнеця, Харків, Україна;
Stanislav Milevskyi – PhD in Economics, Associated Professor, Associated Professor of Cybersecurity and Information Technologies Department, S. Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine;
e-mail: milevskiysv@gmail.com; ORCID ID: http://orcid.org/0000-0001-5087-7036

Рзаєв Хазаіл Нураддін Огли – кандидат технічних наук, доцент, доцент кафедри комп'ютерних технологій і програмування, Азербайджанський державний університет нафти і промисловості, Баку, Азербайджан;
Hazail Nuraddin Ogly Rzaev – PhD in Technical Sciences, Associated Professor, Associated Professor of Computer Technologies and Programming Department, Azerbaijan State Oil Academy, Baku, Azerbaijan;
e-mail: xazail49@mail.ru; ORCID ID: http://orcid.org/0000-0002-1934-4773

Модель інвестицій в інформаційну безпеку: ресурсне подання та організаційне навчання

О. В. Мілов, М. Ю. Костяк, С. В. Мілевський, Х. Н. Рзаєв

Анотація. Захист інформаційних технологій (IT) є ключовою економічною проблемою для організацій. У той час як дослідження в області інвестицій в IT-безпеку швидко ростуть, у них відсутні теоретичні основи для об'єднання економічних і технологічних явищ і напрямків досліджень. Пропонована теоретична модель заснована на використанні теорії організаційної поведінки і ресурсного уявлення. Спільне застосування цих теорій дозволяє в рамках однієї моделі представити організаційні ефекти навчання, що виникають при розробці захисту організаційних ресурсів за допомогою контрзаходів IT-безпеки. Визначено підходи до вивчення інвестицій в інформаційну безпеку, які зводяться до наступних: мікроекономічні підходи, засновані на теорії ігор, фінансовий аналіз, заснований на прибутковості інвестицій (ROI), чистої приведеної вартості (NPV) і внутрішньої норми прибутку (IRR), і управлінські підходи , засновані на теорії прийняття рішень, управління ризиками та теорії організації. Об'єднання різних теорій і підходів призводить до формування мультитеоретичної моделі, яка дозволяє об'єднати методи зазначених напрямків досліджень в рамках комплексної моделі, засновану на ресурсному поданні та теорії організаційного навчання. Вказані складності розробки теоретичної моделі для інвестицій в інформаційну безпеку, а саме: різноманітність природи контрзаходів, що охоплюють стратегічні та операційні питання з урахуванням правових, технічних і організаційних аспектів; цільове призначення інвестицій в інформаційну безпеку (зниження ризику, а не отримання прибутку); взаємодоповнюваність перспектив оперативного і стратегічного періодів. Представлені різні точки зору на проблеми інвестицій, а саме ресурсне уявлення і уявлення в рамках теорії організаційного навчання. Пропонований підхід дозволив побудувати інтегральну модель інвестицій в інформаційну безпеку. Відповіді на питання, що випливають з аналізу інтегральної моделі інвестицій в інформаційну безпеку можуть не тільки визначати майбутні дослідження, а й мати управлінські наслідки, які допоможуть фірмам приймати обґрунтовані інвестиційні рішення в області інформаційної безпеки.

Ключові слова: інформаційна безпека; інвестиції; ресурсне уявлення; організаційна теорія навчання; інтегральна модель інвестицій.

Модель инвестиций в информационную безопасность: ресурсное представление и организационное обучение

А. В. Милов, М. Ю. Костяк, С. В. Милевский, Х. Н. Рзаев

Аннотация. Защита информационных технологий (ИТ) является ключевой экономической проблемой для организаций. В то время как исследования в области инвестиций в ИТ-безопасность быстро растут, у них отсутствуют теоретические основы для объединения экономических и технологических явлений и направлений исследований. Предлагаемая теоретическая модель основана на использовании теории организационного поведения и ресурсного представления. Совместное применение этих теорий позволяет в рамках одной модели представить организационные эффекты обучения, возникающие при разработке защиты организационных ресурсов с помощью контрмер ИТ-безопасности. Определены подходы к изучению инвестиций в информационную безопасность, которые сводятся к следующим: микроэкономические подходы, основанные на теории игр, финансовый анализ, основанный на доходности инвестиций (ROI), чистой приведенной стоимости (NPV) и внутренней норме прибыли (IRR), и управленческие подходы, основанные на теории принятия решений, управлении рисками и теории организации. Объединение различных теорий и подходов приводит к формированию мульти-теоретической модели, которая позволяет объединить методы указанных направлений исследований в рамках комплексной модели, основанную на ресурсном представлении и теории организационного обучения. Указаны сложности разработки теоретической модели для инвестиций в информационную безопасность, а именно: разнообразие природы контрмер, охватывающих стратегические и операционные вопросы с учетом правовых, технических и организационных аспектов; целевое назначение инвестиций в информационную безопасность (снижение риска, а не получение прибыли); взаимодополняемость перспектив оперативного и стратегического периодов. Представлены различные точки зрения на проблемы инвестиций, а именно ресурсное представление и представление в рамках теории организационного обучения. Предлагаемый подход позволил построить интегральную модель инвестиций в информационную безопасность. Ответы на вопросы, вытекающие из анализа интегральной модели инвестиций в информационную безопасность могут не только определять будущие исследования, но и иметь управленческие последствия, которые помогут фирмам принимать обоснованные инвестиционные решения в области информационной безопасности.

Ключевые слова: информационная безопасность; инвестиции; ресурсное представление; организационная теория обучения; интегральная модель инвестиций.