

Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Департамент економічного розвитку, торгівлі та залучення інвестицій
Полтавської обласної військової адміністрації
Полтавська торгово-промислова палата
Університет Флорида (США)
“1 DECEMBRIE 1918” University of Alba Iulia (Румунія)
Білостоцький технологічний університет (Польща)
Вільнюський університет прикладних наук (VIKO) (Литва)
London Metropolitan University (Велика Британія)
Словацький технологічний університет (Словаччина)
Рада молодих вчених Національної академії наук України
Рада молодих вчених Національного університету «Запорізька політехніка»
Рада молодих вчених Національного технічного університету «Дніпровська політехніка»
Рада молодих вчених Національного університету «Чернігівська політехніка»
Рада молодих вчених Національного університету «Одеська політехніка»
Рада молодих вчених Одеського національного університету імені І.І. Мечникова
Рада молодих вчених Ізмаїльського державного гуманітарного університету
Рада молодих вчених Глухівського національного педагогічного університету
імені Олександра Довженка
Рада молодих вчених Сумського національного аграрного університету
Рада молодих вчених Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»
Рада молодих вчених Харківського національного педагогічного університету імені Г.С. Сковороди
Рада молодих вчених Чернівецького національного університету імені Юрія Федьковича
Наукове товариство студентів та молодих вчених Хмельницького національного університету
Рада молодих вчених Київського національного університету будівництва та архітектури
Рада молодих вчених Херсонського державного аграрно-економічного університету

МОЛОДІЖНА НАУКА: ІННОВАЦІЇ ТА ГЛОБАЛЬНІ ВИКЛИКИ

ЗБІРНИК ТЕЗ

Міжнародної науково-практичної конференції студентів,
аспірантів та молодих вчених



Полтава, 06 листопада 2024 року

age=175

4. Літинський Л.К. Розвиток системи управління конфліктними ситуаціями та стресами у робочому середовищі. 2024. URL: <http://surl.li/rqalpn>

5. Сухоребра М.В. Функціональне призначення стрес-менеджменту на підприємствах. *Світове господарство і міжнародні економічні відносини*. 2020. № 27. URL: <https://financial.lnu.edu.ua/wp-content/uploads/2015/11/19.pdf#page=27>

6. Чайкіна Н.О. Психологічні особливості сприйняття ризику життєвих ситуацій під час військових дій в Україні. *In The 10th International scientific and practical conference "Modern methods of applying scientific theories" (March 14–17, 2023) Lisbon, Portugal*. International Science Group. 2023. P. 382.

UDC 330.4

Kudinova Alina

PhD in Economics, Associate Professor

Pikalov Oleksii

Master's Degree student

National University «Yuri Kondratyuk Poltava Polytechnic»

Kuchka Daiana

student

“1 Decembrie 1918” University of Alba Iulia (Romania)

MANAGEMENT OF ENTERPRISE INFORMATION SECURITY IN MODERN BUSINESS CONDITIONS

The successful functioning of an enterprise depends on making high-quality and timely management decisions based on a thorough analysis of information coming from the internal and external environment. In recent years, with the development of information technologies and the general computerization of socio-economic relations, the importance of information has increased in the economy and society as a whole. Information has become one of the most important management resources and human, financial and material resources. The growing role of information has created an information space that must be protected from unauthorized or unwanted interference at the national, regional, and individual levels. In commercial activities, information protection can bring significant revenue, ensure the conclusion of profitable contracts with counterparties, significantly increase the competitiveness of enterprises, and increase the efficiency of business processes [1, 4].

The purpose of information protection is to preserve the value of information assets for their owners. Based on this, direct protection measures

support certain technologies for creating, processing, storing, searching, and providing information resources to users, not the information sources themselves. Such technologies not only take into account the characteristics of the information to be evaluated but also ensure the effective use of information resources. Therefore, it is desirable to consider the information security system of an enterprise as a model of conducting information warfare under the influence of internal and external environmental factors. The content of the information conflict consists of 2 components associated with various actions that can benefit from the information.

The first element (information attack) is to combat the violation of the integrity of the provision of corporate information by the external environment, including measures aimed at violating the confidentiality of corporate information, providing false information, blocking data reception, information processing, and information exchange (including physical destruction of information carriers) and information support at all stages of disinformation management [5].

Response to information is carried out in several ways, including technical reconnaissance of communication and management systems, as well as interception of information through communication channels.

The second element (information protection) includes corporate information, storage, processing, transmission, and automated measures to protect these processes from external influence, including the definition of information policy, and information dissemination measures necessary to solve administrative tasks (including the protection of information carriers from destruction). dissemination and penetration of disinformation information into corporate management systems [2].

The main goal of the information security system is to ensure the sustainable development of the enterprise, prevent security threats, protect legitimate interests from illegal violations, prevent disclosure, loss, leakage, falsification and destruction of information, as well as ensure the effective operation of all structural divisions of the enterprise. In addition, the system must provide constant risk monitoring for the timely detection of threats.

The structure of the information security system depends on the goals, objectives, methods and means of the enterprise, the nature (quantity, value) of the information itself, the nature of possible threats and the required level of security. A standard corporate information security management system includes all the key components inherent in management systems. Experience in using standardized requirements for such systems helps to identify the main factors that ensure information security in modern enterprises:

- information security policies, objectives and measures that reflect the company's business strategy;

- an approach to implementing, monitoring, maintaining and improving information security that is consistent with the corporate culture;

support and active participation of management at all levels;
understanding of information security requirements, risk assessment and availability of tools to manage them;
effective measures to increase awareness in the field of information security;
clear guidelines for information security policies and standards;
ensuring adequate funding for information security management activities;
creating an effective process for responding to information security incidents;
assessing the system to increase management effectiveness and provide recommendations for its improvement [3].

Therefore, the management of the enterprise's information security system should cover all elements of the information and communication environment and implement effective measures to protect it. The basis of this management is the definition of goals, objectives, methods, principles, and means of information protection. Maintaining confidentiality, integrity, and availability of data contributes to improving the effectiveness of the enterprise's information security, which allows the protecting of information from internal and external threats, creates favorable conditions for the effective operation of the enterprise, and increases its competitiveness.

Reference

1. Босак А.О., Вержиковський В.П., Калінін І.Є., Максимів І. Д., Приступа Д. А., Ривак О.І. Засади формування інформаційної безпеки підприємства. *Міжнародний науковий журнал "Інтернаука". Серія: "Економічні науки"*. 2023. URL: <https://www.inter-nauka.com/uploads/public/16944126635036.pdf>
2. Маркіна І. А., Дячков Д. В. Основи формування системи менеджменту інформаційної безпеки підприємства. *Проблеми і перспективи розвитку підприємництва*. 2016. № 3(1). С. 80–88.
3. Смачило Т. В., Кахній М. І. Теоретичні засади управління системою інформаційної безпеки підприємства. *Молодий вчений*. 2016. № 12.1(40). С. 969–972.
4. Комеліна О.В. Інформаційно-аналітичне забезпечення інвестиційного менеджменту в сучасних умовах. *Майбутнє економіки в епоху інформаційного суспільства*. № 81. URL: <http://socrates.vsau.org/b04213/html/cards/getfile.php/13060.pdf#page=81>
5. Чайкіна А., Маслій О., Черв'як А. Сучасні драйвери підвищення економічної безпеки країни в умовах цифрової трансформації. *Сталий розвиток економіки*. 2024. №. 2 (49). С. 307–313.