

DEVELOPMENT OF A METHODOLOGY FOR THE IMPLEMENTATION OF SECURE WEB APPLICATIONS IN BUSINESS ORGANIZATIONS

Rosen Ivanov Kirilov¹

Abstract: Background: Web application development is a difficult and complex task. The complexity is mostly expressed in the multitude of tasks that must be performed in the development life cycle. In today's environment, it is important that web applications prove their security and resilience in a changing cyber environment. For these reasons, web applications should meet a number of requirements in the process of their technological implementation, which is explored in the article. Methods: The methods used are related to a literature survey on the cyber security requirements of web applications and the characteristics of their life cycle. On this basis, basic key issues of vulnerability testing of developed systems in business organizations have also been studied. Results: As a result of the development of the methodology its main components have been tested in the development of web applications. The achieved application protection levels as a result of the implemented measures have been reported and analyzed. On this basis, some possibilities for improvement of the proposed methodological components are outlined. Conclusions: As a result of the studies and analyses basic conclusions have been drawn about the possibilities for developing and implementing secure web applications in business organizations.

Key words: cyber security, cyber threats, cyber security concept, technological protection measures

JEL: K24, L86, P46.

DOI: <https://doi.org/10.58861/tae.bm.2024.4.03>

Introduction

Issues of personal data protection have been a particular subject of interest in the last few years. In parallel with the strong development of

¹ Assoc. Prof. Phd, University of National and World Economy – Sofia, e-mail: rkirilov@unwe.bg, ORCID:0009-0005-3964-7586

Internet technologies and services in Internet space, the need for adequate protection of software applications and their data is also increasing. In its regulations, the European Union describes and specifies this issue in detail, noting that the effective protection of personal data within the Union requires strengthening and a detailed description of the rights of data subjects and the obligations of those who process and determine the processing of personal data (Regulation (EU) 2016/679, 2016). Compliance with these regulations, as well as the introduction of secure web platforms and applications, is the basis for the creation of a broad description of the technological control measures that are followed and monitored in the certification of organizations (ISO, 2023). These mechanisms impose an obligation on the developers of information systems, as well as the organizations that use them, to include specific algorithms and protection mechanisms.

Regular analyses by the European Union Agency for Cybersecurity state that network-related vulnerabilities include gaps affecting web applications, websites and the underlying internet infrastructure (ENISA, 2024). The analysed source details real cases and trends in the areas: Vulnerabilities Landscape, Ransomware, Malware, Social Engineering, Threats against Data, Threats against Availability: Denial of Service and Information Manipulation and Interference. There are also provisions in national legislation regarding the security of web platforms and applications. In particular, such are regulated in the Ordinance on minimum requirements for network information security (Ministry of Transport and Communications of the Republic of Bulgaria, 2024). There is a special section in the regulation governing the protection of web servers. In this part of the national legislation, the necessary measures for the protection of web applications are described in detail, and these measures can be increased in different organizations, in view of the specifics of their activity.

In practical terms, web application development has always been a complex and responsible task. Providing access to databases with sensitive data over a web environment has always posed the question of finding a secure way of communication. Potential and actual threats in this process can lead to misuse of data, thereby compromising the organization and its goals. For these reasons, theory and practice have always sought methods and ways to design, program and deploy applications that provide access to data in a web environment in a secure manner.

Literature review

These analyses and increasing regulatory requirements direct the attention of researchers in the direction of providing measures to guarantee the cyber security of web applications, already at the stage of their design. In this way, the creation of the applications will be realized with pre-planned algorithms for maximum protection against illegal access. Some of the researchers in this thematic area pay considerable attention to the construction of comprehensive concepts of cyber security in organizations, presenting conceptual models with functions at individual levels (Kirilova, 2024). These concepts should be taken critically at all times, both from the point of view of the scope and activity of the organization being studied, and also from the point of view of the role and use of web platforms and applications to serve business processes. Our understanding confirms the need for such comprehensive organizations of cyber security systems, but with the increased participation of methods, algorithms and approaches to ensure the security of information systems already in the process of their construction. Ensuring the necessary level of protection is complicated by the emergence and development of the concept of big data (Petrova et al., 2022). With the dynamism of these processes, individual authors are more and more persistently looking for approaches to guarantee the security of both the data stored and the data visualized by the applications. Other authors who consider the possibilities of building concepts in the field of web applications analyze in advance the issues of presenting textual data from web-based information systems in a structured form (Milev et al., 2022). On this basis, some security issues of these applications and platforms are also addressed. The strong development of web platforms and the entry of artificial intelligence into them also raises a number of new technological and ethical issues. Some of the researchers in this direction consider the protection of people's personal data and the observance of human rights as an important principle (Marinova, 2024). Asking cybersecurity questions when building software applications is key from a modern business perspective. It functions in an increasingly dynamic environment, and this imposes and requires the application of different approaches to identify the key steps and tools for the successful implementation of the digital platform integration strategy in line with the requirements of the dynamic business environment (Popova et al., 2024).

According to some other sources (Securelist, 2024), the main types of problems in the security of web applications can be summarized in the following groups:

- Broken Access Control;
- Sensitive Data Exposure;
- Server-Side Request Forgery (SSRF);
- SQL Injection;
- Cross Site Scripting (XSS);
- Broken Authentication;
- Security Misconfiguration;
- Insufficient Protection from Brute Force Attacks;
- Weak User Password;
- Using Components with Known Vulnerabilities.

As the performance of web applications depends to a certain extent on the browser used, according to some authors (Pan et al., 2023) it is important to investigate the issue of web tracking protection in different browsers. The protection that the browser provides at the lower abstraction layer of communication is quite important to the performance of the web applications being created. Other authors' research (Yadav et al., 2018) also discusses definitions and characteristics of Application Security risk. These authors define this type of risk as the likelihood that hackers will plan and create attacks against various types of web applications and resources in order to harm organizations. Other authors (Almutairi et al., 2021) draw attention to several groups of threats to applications, namely: SQL injection, operating system command injection, path traversal, and cross-site scripting vulnerabilities through dynamic and static approaches.

The literature review shows that there are a number of studies that discuss the security issues of web applications. This topic is relevant and important for the creation of safe information systems to ensure the activities of organizations in modern economic conditions. Without the provision of adequate measures to protect the web platforms, it may be impossible to fulfill the defined business goals.

Methodology

One of the serious challenges for organizations is the introduction of new digital platforms in the Internet environment. These applications may have different requirements, such as:

- To the maximum extent correspond to the business processes in the organizations;
- Provide secure data exchange with other platforms;
- Ensure interoperability of data and related information systems;
- To protect the users of the software to the maximum extent from errors in the work process, etc.

Our understanding is that ensuring secure web applications should be formed by a set of measures implemented throughout the application's development lifecycle. Allowing security compromises at any stage or task in the lifecycle can compromise the deployed application to the maximum extent. For these reasons, we also offer the methodology described below for the development and implementation of secure web applications in organizations. It is important to specify that in individual and specific cases of software development, this methodology can be parameterized and changed, depending on the specific features.

Research and analysis show that the methodology for deploying secure web applications and platforms should offer methods to ensure the protection of the software throughout its life cycle.

The main stages of the proposed methodology are (Figure 1):

- Analysis of the characteristics of the organization. At this stage, tasks related to a detailed analysis of the organization's activities are carried out. The main business processes and their relation to the individual components of the architecture of the created application are studied and modelled. So this phase should develop a detailed plan for implementing the application, as well as a corresponding budget;
- Development of the web application project. The development of an application project involves the detailed design of all its components. This includes the database, business logic, and web interface;
- Implementation of security components and methods. The implementation of security components and methods is the core of the proposed methodology. This refers to the development of specific algorithms, methods and program modules guaranteeing the security of the application. In particular, they are considered Multi-factor authentication (MFA), Injection-based vulnerability protection and Security header improvements;

- Application programming. Application programming represents a stage of its life cycle during which the actual implementation of all project components takes place;
- Implementation and real use. At this stage, the developed web application is put into real use. A mandatory component at this stage is conducting a Penetration test of the software being created.

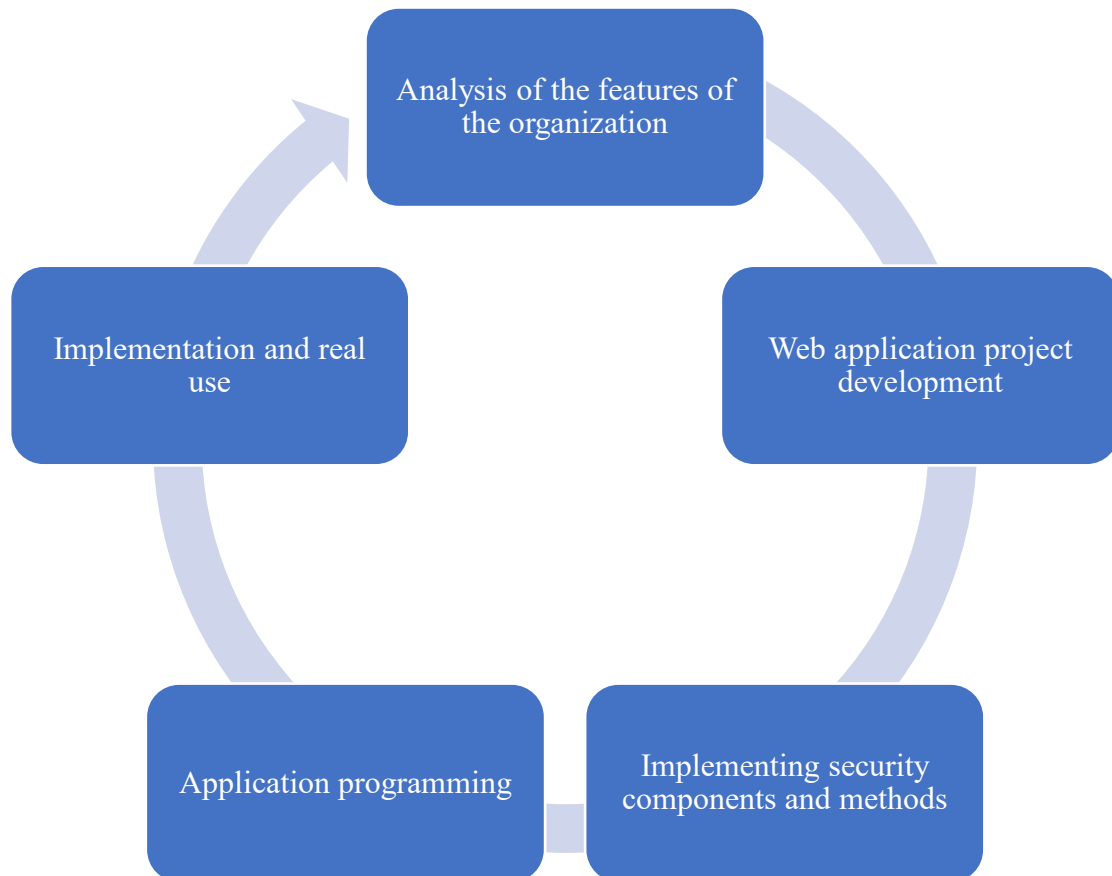


Figure 1. Components of the proposed methodology for deploying secure web applications in organizations.

The methodology can be implemented in the development process of web applications, as well as be a suitable adaptation for other similar types of software. It is important to emphasize that each individual business, as well as each individual organization, has its own characteristics. These features of business processes should be carefully studied and analysed as a basis for questioning and modifying the proposed methodology in each specific case.

Results

By adhering to the proposed security model, the following measures have been implemented (and afterwards, tested) to improve and strengthen the security of a student information system. The system is built with ASP.NET Core for the backend, React.js for the frontend and Microsoft SQL Server for the database. Some examples of the implementation of the individual methods and algorithms are presented below.

Authentication security mechanisms

Multi-factor authentication (MFA) has been implemented to enhance the security of the login for both students and staff. After entering their username and password, the system uses a Time-based One-Time Password (TOTP) for MFA. This involves generating a QR code during the setup phase that the user scans with the Google Authenticator app (or a similar one). Afterwards, they can use the app to generate a TOTP code every time they log in. When the user first enables MFA, we generate a QR code that they can scan:

```
var user = await _userManager.GetUserAsync(User);
var key = await _userManager.GetAuthenticatorKeyAsync(user);

if (string.IsNullOrEmpty(key))
{
    await _userManager.ResetAuthenticatorKeyAsync(user);
    key = await _userManager.GetAuthenticatorKeyAsync(user);
}

var authenticatorUri = GenerateQrCodeUri(user.Email, key);

return View(new EnableAuthenticatorViewModel { QrCodeUri =
authenticatorUri, SharedKey = key });

...

private string GenerateQrCodeUri(string email, string unformattedKey)
{
```

```
var formattedKey = FormatKey(unformattedKey);
return string.Format(
    "otpauth://totp/{0}?secret={1}&issuer={2}&digits=6",
    Uri.EscapeDataString(email),
    formattedKey,
    Uri.EscapeDataString("StudentInformationSystem"));
}
```

Once the user scans the QR code and starts using Google Authenticator, they will enter the code generated by the app during the login process.

```
var user = await _userManager.GetUserAsync(User);
var result = await _userManager.VerifyTwoFactorTokenAsync(user,
TokenOptions.DefaultAuthenticatorProvider, code);
if (result)
{
    await _signInManager.SignInAsync(user, isPersistent: false);
    return RedirectToAction ("Index", "Dashboard");
}
ModelState.AddModelError(string. Empty, "Invalid code.");
return View ();
```

Students and staff could also log in using their Microsoft 365 account, which would lead to a better overall authentication security, since the log in process is handled by Microsoft and they would be responsible for mitigating the security risks:

```
services.AddAuthentication()
    .AddMicrosoftAccount(microsoftOptions => {
        microsoftOptions.ClientId =
Configuration["Authentication:Microsoft:ClientId"];
        microsoftOptions.ClientSecret =
Configuration["Authentication:Microsoft:ClientSecret"];
    });
```

An example of the execution of the program code shown is given in Figure 2.

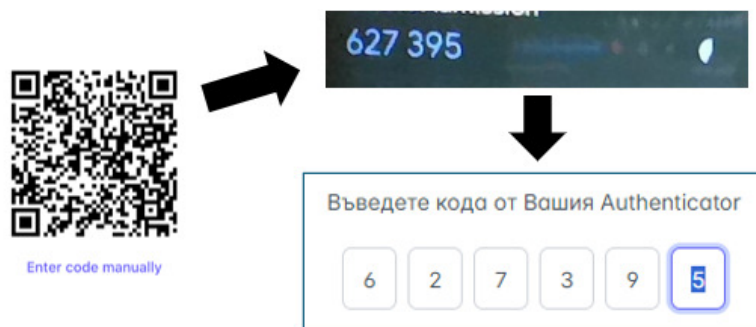


Figure 2. Using TOTP in three steps - QR scan, mobile authenticator app and entering the time-based code back in the web application

Injection-based vulnerability protection. To protect the system's MS SQL Server database from SQL injection, all queries use prepared statements, ensuring that inputs are properly escaped and can't be used for altering the query, for example:

```
var sql = "SELECT * FROM Students WHERE StudentId = @StudentId";
var student = await _context.Students.FromSqlRaw(sql, new SqlParameter("@StudentId", studentId)).FirstOrDefaultAsync();
```

Input sanitization is also an important preventive measure, for a better user experience, it should be handled in both frontend and backend.

In the frontend:

```
const emailRegex = /^[a-zA-Z0-9._%+-]+@[a-zA-Z0-9.-]+\.[a-zA-Z]{2,}$/;
if (!emailRegex.test(email)) {
  setError("Invalid email format");
}
```

In the backend:

```
[HttpPost]
public async Task<ActionResult> Register(StudentViewModel model)
{
  if(ModelState.IsValid) ...
  where StudentViewModel has the proper attributes.
```

Security header improvements

In the student information system, we have added HSTS to enforce HTTPS so that the browser wouldn't even attempt to use plain HTTP. This has been added to Program.cs:

```
app.UseHsts();  
app.UseHttpsRedirection();
```

To prevent clickjacking, where the student information system's pages are embedded in iframes on malicious sites, we have also added the X-Frame-Options header.

```
app.Use(async (context, next) =>  
{  
    context.Response.Headers.Add("X-Frame-Options", "DENY");  
    await next();  
});
```

An example of the execution of the program code shown is given in Figure 3.

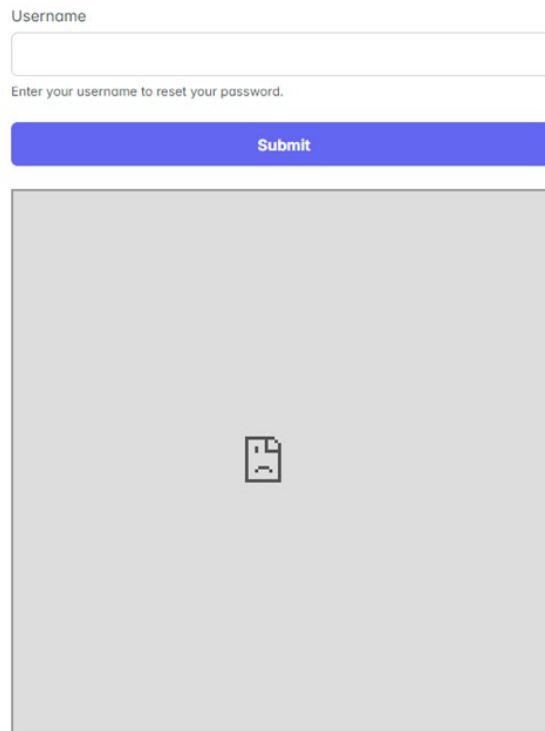


Figure 3. Using X-Frame-Options restricts other websites from embedding our site and therefore trying to confuse the user to perform an action on it

The X-Content-Type-Options header has been added to prevent browsers from interpreting files as a different MIME type, avoiding scenarios where students or staff accidentally download malicious files from the ones that have been uploaded to the system:

```
app.Use(async (context, next) =>  
{  
    context.Response.Headers.Add("X-Content-Type-Options",  
"nosniff");
```

```

    await next();
  });

```

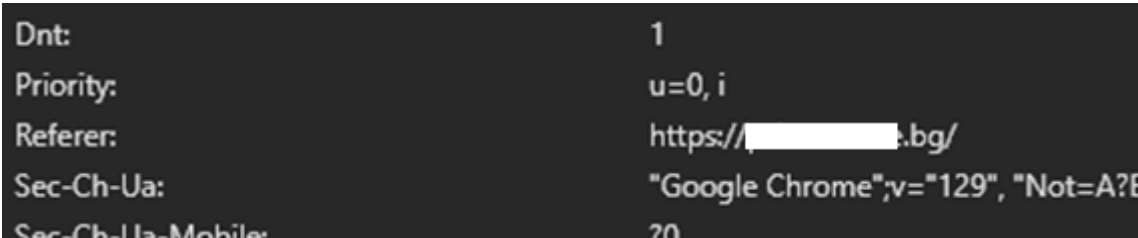
To protect students' privacy when they navigate between the portal and external services, the Referrer-Policy header has been set to limit the shared information to any outside services:

```

app.Use(async (context, next) =>
{
    context.Response.Headers.Add("Referrer-Policy", "no-referrer");
    await next();
});

```

An example of the execution of the program code shown is given in Figure 4.



The image shows a network request header with the following fields:

Dnt:	1
Priority:	u=0, i
Referer:	https://[REDACTED].bg/
Sec-Ch-Ua:	"Google Chrome";v="129", "Not=A?E
Sec-Ch-Ua-Mobile:	?0

Figure 4. Without a restrictive Referrer-Policy, the URL of the origin of the request is being shared with the target

These sample code snippets show the possibility of implementing the proposed methods and algorithms that improve the security of the web applications being created. In some specific cases of application, variants and modifications of this program algorithm can be developed in order to achieve higher efficiency.

Discussion

The study of this topic gives rise to many discussion questions. Some of them are related to the careful assessment of risk in the development of each web application. Carrying out this activity may also draw attention to an additional set of risk factors that should be addressed. In this sense, there is no single or definitive way to determine a set of algorithms to be applied in the development of all applications, but their specificity should be taken into account. Another important discussion point is related to finding the balance between the level of security of each application and the degree of complexity

in its implementation and maintenance. Our understanding is that absolute security does not exist, therefore every application should be approached with measures ensuring a balanced and appropriate level of protection. The question of how much this depends on the subject of the company itself, or rather, is related to the peculiarities of business processes and the stages of building the applications themselves, is debatable. The application of a mixed approach is also possible. All this shows that the proposed methodology is only one proven example of introducing cybersecurity measures to web applications, and alternative approaches are also possible.

Conclusions

Cybersecurity issues are becoming increasingly important to business organizations. In modern conditions, it is not enough to take some minimal measures, but a complex of interconnected components providing protection should be implemented. In this context, more and more importance is attached to the security of the main used information systems, web applications and services. In order for an application to be secure, the basic requirements should be implemented already at the stage of designing and programming the software solution itself. The article proposes and approves a methodology for providing secure applications for business needs, which can be expanded and adapted, according to the need and each specific case.

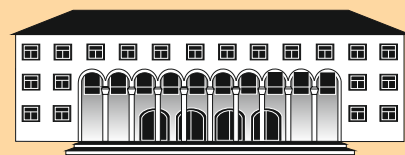
References

- Almutairi, A. & Mishra, S. & Alshehri, M. (2021). Web Security: Emerging Threats and Defense. *Computer Systems Science and Engineering*. 40. DOI: 10.32604/csse.2022.019427.
- Enisa. (n.d.). Available online: <https://www.enisa.europa.eu>.
- Eur-lex. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, Available online: <https://eur-lex.europa.eu/legal-content/bg/TXT/?uri=celex:32016R0679>.

- ISO. (n.d.). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection Information security management systems Requirements*. Available online: <https://www.iso.org/standard/27001>.
- Kirilova, K. (2024). Building a Concept for Cyber Security of an Educational Organization in Bulgaria. *Business Management*, (1), pp.85-100.
- Marinova, N. (2024). Advantages and Ethical Considerations of Industrial IoT Artificial Intelligence Solutions Usage. *Business Management*, (2), pp.43-58.
- Milev, P., & Tabov, Y. (2022). Conceptual Approach for Presenting Text Data from Web-Based Information Systems in Structured Form. *Business Management*, (1), pp.46-57.
- Mtc. government. (2019). *Naredba za minimalnite iziskvaniq za mrejova i informacionna sigurnost*. Available online: https://www.mtc.government.bg/sites/default/files/nar_minimalnite_iziskvaniq_mrejova_info_sigurnost-072019.pdf.
- Pan, R. & Ruiz-Martínez, A. (2023). Evolution of web tracking protection in Chrome. *Journal of Information Security and Applications*, (79), DOI:10.1016/j.jisa.2023.103643.
- Petrova, M., Popova, P., Popov, V., Shishmanov, K., Marinova, K. (2022). Potential of Big Data Analytics for Managing Value Creation. *International Conference on Communications, Information, Electronic and Energy Systems, CIEES 2022 - Proceedings*, DOI: 10.1109/CIEES55704.2022.9990882.
- Popova, P., Popov, V., Marinova, K., Petrova, M., & Shishmanov, K. (2024). The Digital Platform - New opportunities and implementation strategy. *Proceedings of the 16th International Conference on Electronics, Computers and Artificial Intelligence, ECAI 2024*, DOI: 10.1109/ECAI61503.2024.10607401.
- Securelist. (2024). *Top 10 web application vulnerabilities in 2021–2023*. Available online: <https://securelist.com/top-10-web-app-vulnerabilities/112144/>.
- Yadav, D., Gupta, D., Singh, D., Kumar, D., & Sharma, U. (2018). Vulnerabilities and Security of Web Applications. *2018 4th International Conference on Computing Communication and Automation (ICCCA)*, Greater Noida, India. pp.1-5. DOI:10.1109/CCAA.2018.8777558.

ISSN 0861 - 6604
ISSN 2534 - 8396

BUSINESS management



BUSINESS management 4/2024

PUBLISHED BY
D. A. TSENOV ACADEMY
OF ECONOMICS - SVISHTOV

4/2024

Editorial board:

Prof. Mariyana Bozhinova, Phd - Editor in Chief, Tsenov Academy of Economics, Svishtov, Bulgaria

Prof. Krasimir Shishmanov, Phd – Co-editor in Chief, Tsenov Academy of Economics, Svishtov, Bulgaria

Prof. Mariana Petrova, PhD - Managing Editor Tsenov Academy of Economics, Svishtov, Bulgaria

Prof. Borislav Borissov, DSc - Tsenov Academy of Economics, Svishtov, Bulgaria

Assoc. Prof. Aleksandar Ganchev, Phd - Tsenov Academy of Economics, Svishtov Bulgaria

Assoc. Prof. Irena Emilova, Phd - Tsenov Academy of Economics, Svishtov Bulgaria

Assoc. Prof. Ivan Marchevski, Phd - Tsenov Academy of Economics, Svishtov, Bulgaria

Assoc. Prof. Simeonka Petrova, Phd - Tsenov Academy of Economics, Svishtov Bulgaria

International editorial board:

Yuriy Dyachenko, Prof., DSc (Ukraine)

Olena Sushchenko, Prof., DSc (Ukraine)

Nurlan Kurmanov, Prof., PhD (Kazakhstan)

Dariusz Nowak, Prof., PhD (Poland)

Ryszard Pukala, Prof., PhD (Poland)

Yoto Yotov, Prof., PhD (USA)

Badri Gechbaia, Prof., PhD (Georgia)

Ioana Panagoret, Assoc. Prof., PhD (Romania)

Proofreader: Elka Uzunova

Technical Secretary: Zhivka Tananeeva

Web Manager: Martin Aleksandrov

The printing of the issue 4-2024 is funded with a grand from the Scientific Research Fund, Contract KP-06-NP5/42/30.11.2023 by the competition “Bulgarian Scientific Periodicals - 2024”.

Submitted for publishing on 28.11.2024, published on 29.11.2024, format 70x100/16, total print 80

© D. A. Tsenov Academy of Economics, Svishtov,

2 Emanuil Chakarov Str, telephone number: +359 631 66298

© Tsenov Academic Publishing House, Svishtov, 11A Tsanko Tserkovski Str

BUSINESS management

D. A. Tsenov Academy
of Economics, Svishtov

Year XXXIV * Book 4, 2024

CONTENTS

MANAGEMENT practice

BUSINESS INNOVATION SELF-ASSESSMENT WITH ARTIFICIAL INTELLIGENCE SUPPORT FOR SMALL AND MEDIUM-SIZED ENTERPRISES

Joaquim Jose Carvalho Proença 5

SOCIETAL IMPACTS AND ETHICAL CONSIDERATIONS OF AI IN THE BUSINESS

Reis Mulita, Zurab Nasaraia, Oksana Konarivska, Svitlana Boiko, Tetiana Paniuk18

DEVELOPMENT OF A METHODOLOGY FOR THE IMPLEMENTATION OF SECURE WEB APPLICATIONS IN BUSINESS ORGANIZATIONS

Rosen Ivanov Kirilov 38

MANAGERIAL TIES AND OPERATIONAL PERFORMANCE OF TOURISM BUSINESSES IN VIETNAM: THE MEDIATING ROLE OF RESOURCE ACCESS

Tran Nha Ghi, Nguyen Thanh Long, Nguyen Ngoc Thuc 51

ECONOMIC, SOCIAL AND ENVIRONMENTAL ANALYSIS OF THE DEVELOPMENT POTENTIAL OF NORTHWEST AND NORTH CENTRAL REGION IN BULGARIA

Marina Nikolova, Krasimira Slaveva, Pavlin Pavlov, Elitsa Lazarova 68

THE ROLE OF HUMAN RESOURCES MANAGEMENT IN ACHIEVING SUSTAINABLE DEVELOPMENT GOALS IN THE COMPANY

Badri Gechbaia, Ketevan Goletiani, Giorgi Abashidze, Zurab Nasaraia 97