КРЪГЛА МАСА С МЕЖДУНАРОДНО УЧАСТИЕ

ТЪРГОВИЯТА – НАУЧНО ЗНАНИЕ И БИЗНЕС РЕАЛНОСТ

Сборник с доклади

АКАДЕМИЧНО ИЗДАТЕЛСТВО „ЦЕНОВ" СВИЩОВ

ОРГАНИЗАЦИОНЕН КОМИТЕТ

доц. д-р Теодора Филипова
доц. д-р Петранка Мидова
доц. д-р Симеонка Петрова
доц. д-р Венцислав Перков
гл. ас. д-р Зоя Иванова
гл. ас. д-р Иван Маринов
докт. Никола Илчев

РЕДАКЦИОНЕН СЪВЕТ

Председател:
Доц. д-р Светослав Илийчовски

Членове:
проф. д-р Анета Денева
проф. д-р Теодора Димитрова
проф. д-р Атанас Атанасов
доц. д-р Теодора Филипова
доц. д-р Петранка Мидова
доц. д-р Симеонка Петрова
доц. д-р Венцислав Перков



ISBN 978-954-23-2005-0

СЪДЪРЖАНИЕ

Катедра „Търговски бизнес“: 30 години обучение, академична мисия и проекции на бъдещето
Доц. д-р Теодора Филипова 5

Пленарни доклади

Новата „реалност“ в търговския бизнес
Проф. д-р Данчо Данчев 32

Омниканалното асортиментно планиране и потребителското поведение
Доц. д-р Симеонка Петрова 42

Някои моменти от развитието на корпоративната социална отговорност
Доц. д-р Иванка Николова 52

Тематично направление: Предприемачество и мениджмънт на ресурсите в търговията

Перспективы производства безопасных продуктов питания в условиях организационно-экономической модернизации предприятий пищевой промышленности Украины
Проф. Наталья Валинкевич, д.э.н. 60

Бранд мениджмънт на търговците на дребно
Доц. д-р Виолета Гълъбова 66

Търговски мениджмънт и аспекти на личността
Доц. д-р Явор Янкулов..... 73

Проблемы и перспективы развития коммерческой деятельности торговых предприятий в Украине
Доц. Ангелина Сотник, к.э.н. 81

Офшорните зони като алтернатива за алокация на капитала
Доц. д-р Донка Желязкова 87
Доц. д-р Михал Стоянов

Текстилната индустрия в България – състояние и перспективи
Доц. д-р Сергей Найденов 93
Докторант Калин Киряков

Дефиниране целите на сектор пчеларство от област Русе
Доц. д-р Любомир Любенов..... 99

Антикризисното управление в процеса на глобалната промяна
Доц. д-р Ирена Емилова 107

Иновации и иновационен процес в търговския бизнес
Доц. д-р Анатолий Асенов 112

Елементи и същност на организацията и организации от публичния сектор
Доц. д-р Христо Сирашки 120

HRM системите в търговските предприятия – ключът за успешно управление
Гл. ас. д-р Зоя Иванова..... 128

Глобален недостиг в търговията с графични карти – фактори и тенденции
Гл. ас. д-р Иван Маринов..... 136

Управленски аспекти на търговията в новата дигитална реалност
Гл. ас. д-р Станислава Стоянова..... 144

Въздействие от употребата на пестициди в селското стопанство
Гл. ас. д-р Илияна Кръстева 152

Култура и мениджмънт на ресурсите при търговията с луксозни стоки
Гл. ас. д-р Иво Велинов 159

Предизвикателства пред виртуалното управление на търговския екип
Ас. д-р Надежда Стефанова..... 168

Основные направления развития перспективы „клиенты“ для потребностей стоимостно-ориентированного управления клиентским капиталом
Татьяна Завалий..... 176

Модели на ситуационно лидерство
Синан Пехливанов..... 181

Тематично направление: Иновации и дигитализация в търговията

Cooperation of Business and Science in the Frames of Technology Parks: Cases of Cee Countries
Prof., DSc. Ihor Lishchynskyy 186
Prof., DSc. Mariia Lyzun

Substantiation of Prospects for Trade Development in the Post-Pandemic Period
Doctor of Economic Sciences, Professor, Maryna Baldzhy 195
PhD in Economics, Victoria Odnolko

Start-up проекты в ритейле
Доц. Светлана Бирюченко, к.э.н. 202

Иновации и дигитализация в сектора на търговията
Доц. д-р Искра Пантелеева..... 206

Роля и влияние на изкуствения интелект върху търговията на дребно
Доц. д-р Надежда Димова 214

Завладени от интернет-на-нещата
Доц. д-р Михал Стоянов 220
Гл. ас. д-р Десислава Гроздева

Форми на проявление на дигитализацията на електроенергетиката – икономически аспекти
Доц. д-р Цветелина Ганкова - Иванова 229

Дигитални решения за реализация на земеделска продукция
Доц. д-р Марина Николова 237

„Системните молове“ и дигиталната революция
Доц. д-р Цветнен Цветков 247

Сравнителен анализ на електронната търговия в Европейския съюз
Доц. д-р Маргарита Шопова 251
Гл. ас. д-р Евгени Овчинников

За продоволствието и продоволствената сигурност – от научното знание до бизнес реалността
Доц. д-р Виолета Блажева 259

Изследване на потенциала за развитие на иновативни форми туризъм в България
Доц. д-р Любка Илиева 265
Сиана Спасова

Управление на складовете – процеси, предизвикателства, практики
Гл. ас. д-р Марияна Кътева 272

Марковата активност – индикатор за иновации
Гл. ас. д-р Венцислава Николова-Минкова 279

Пост-кризисното състояние и проблеми на хотелиерския бизнес в България
Гл. ас. д-р Любомира Тодорова 287

Блокчейн в агробизнеса
Гл. ас. д-р Радка Ненова 293

Дигитални решения в туристическия бизнес
Гл. ас д-р Павлин Павлов 301

Тематично направление:
Моделиране и инвестиционни проекти в търговията

Проектный подход как инструмент реализации политики управлении торгово-обменными операциями
Доц. Мария Плотникова, к.э.н. 306
Доц. Оксана Присяжнюк, к.э.н.

Различни възможности за прогнозиране и планиране на застрахователната дейност
Проф. д-р Росен Тодоров 310

Възможности за определяне на ликвидационната стойност
Доц. д-р Светослав Илийчовски 319

Въздействие на преките чуждестранни инвестиции върху вземанията по лизингови договори – нов бизнес в търговията
Доц. д-р Венцислав Перков 327

Преките чуждестранни инвестиции в икономическите сектори на страната
Доц. д-р Добрин Ганчев 335
Доц. дмн Милена Рачева

Организиране на мърчандайзинговите стокови запаси посредством Economic Order Quantity Model – EOQ
Хон. ас. д-р Светла Атанасова 342

A Model for Internet Payment Systems: Qualitative Risk Assessment
PhD Student Valeriu Cernei 351

Производство и търговия с етерични масла – традиция, бъдеще и здраве
Мая Алексиева 358

Тематично направление: Пазарни проучвания и конкурентоспособност в търговията

Increasing the Competitiveness of Ukrainian and Bulgarian Food Industry Enterprises
Doctor of Economic Sciences, Professor, Maryna Baldzhy 367
Graduate student, Aleksandra Nosachenko

The Trade Sector's Response to the Crisis Caused by the Covid 19 Pandemic
Professor Sreten Ćuzović, PhD 375
Associate Professor Svetlana Sokolov Mladenović, PhD
Đorđe Ćuzović, PhD

Конвергенция между омниканалния ритейлинг, маркетинг и логистика
Доц. д-р Виолета Димитрова 385

Състояние и тенденции на пазара на месо в България
Доц. д-р Петранка Мидова 393

Тенденции в заявителската активност и регистрирането на марки със закрила в България за периода от март 2019 г. до март 2021 г.
Гл. ас. д-р Мариела Димитрова 400

Фрагменти от търговията с хранителни добавки и Covid-19
Гл. ас. д-р Борислав Атанасов 407

Приложение на комуникационни инструменти в хипермаркети „Зора“
Гл. ас. д-р Цветелина Кабакчиева 413

Регионални аспекти и проблеми на търговията със селскостопанска продукция
д-р Валери Велковски 422

Инвестиционна активност и търговски възможности пред общините от поречието на река Дунав
Гл. ас. д-р Милен Динков 432

Анализ на улова на калкан (Psetta Maxima) в Черно море
Гл. ас. д-р Георги Русенов 439
Доц. д-р Ангелина Иванова
Гл. ас. д-р Мария Янкова
Ас. д-р Василка Кръстева

Здравният туризъм – елемент на продуктовия портфейл на дестинация България
Д-р Кристина Георгиева 443

Проблеми и възможности пред развитието на интермодалния транспорт в България
Докторант Елена Вълчева..... 451

Ценообразуването като конкурентно предимство
Докторант Илияна Дикова..... 459

Дали бъдещето е тук с иновативните 5G технологии в търговията с услуги?
Милан Чернев 466

Футуристичните доставки като конкурентно предимство на WALMART
Милчо Милчев..... 474

Социално-икономическото присъствие на „Загорка“ ад на пазара
Деница Стоянова 480

Тематично направление: Ефективност и социална отговорност в търговията

Съвременни тенденции и предизвикателства в развитието на кооперативната търговия в България
Доц. д-р Бисер Петков..... 489

Кратки бележки по историята за началото на застраховането в България
Проф. д-р Росен Тодоров..... 496

Sustainability Logistics Infrastructure: Conceptual Considerations and Possible Application
Docent, Candidate of Economic Sciences, Alexander Tanichev..... 501

Съвременни аспекти на търговията с пощенски услуги в България
Доц. д-р Теодора Филипова 512

Съвременните потребители, потребителският активизъм и гражданското общество
Гл. ас. д-р Виолета Петева 520

Сдруженията за защита на потребителите – взаимодействия и ползи
Гл. ас. д-р Миглена Душкова 528

Оценка на рентабилността в търговията
Гл. ас. д-р Николинка Игнатова 536

Организационно развитие чрез социално-отговорно поведение
Гл. ас. д-р Десислава Алексиева 544

Липсата на контрол – предпоставка за фалит на търговска верига (по примера на „Пикадили“ ЕАД)
Д-р Цветан Димов 549

Възможности за оценяване ефективността на дистрибуционните канали
Докторант Велизар Йорданов 557

Тематично направление: Стопанска отчетност и финансиране в търговията

Направления формирования учетного обеспечения системы управления земельными ресурсами
Проф. Татьяна Остапчук, д.э.н. 565

Проблеми при счетоводното отчитане на ДДС при продажбата на стоки в условията на Covid 19
Доц. д-р Галя Иванова-Кузманова 570

Изследване влиянието от прилагането на МСФО 15 приходи от договори с клиенти върху дейността на търговските предприятия
Доц. д-р Иван Андреев 576

Структура на продажбите на дребно – състояние и тенденции
Доц. д-р Красимира Славева 582

Изисквания към документирането на търговските сделки
Доц. д-р Славена Стоянова 589

Приложни аспекти на финансовия контрол при стопанската отчетност
Гл. ас. д-р Надежда Цветкова 597

A MODEL FOR INTERNET PAYMENT SYSTEMS: QUALITATIVE RISK ASSESSMENT

PhD Student Valeriu Cernei
Academy of Economic Studies of Moldova

Abstract: *The Financial Services Sector represents a component of Republic of Moldova Critical Infrastructure (CI) as it had been documented in the Government Decision no. HG701/2018 (The Government, 2018). Power outages, natural disasters, pandemic, sabotage, and an increased number of cyberattacks demonstrate the wide range of potential risks facing the financial sector. It is to mention that the financial sector is a component of the CI in most of the countries and, once banks opened their systems to clients, had been continuously exposed various cyber risks. Failure to protect the financial sector may lead to unpredictable events, up to crashing of the country's financial system.*

At the European level, new standards have been developed and put in practice. One is the PSD2, which requires that the payment service providers (PSPs) shall establish a framework with appropriate mitigation measures and control mechanisms to manage operational and security risks relating to the payment services they provide. (EBA, 2018)

The current work is presenting the pillars of the qualitative cyber and information security risk assessment for the internet payment systems (incl. mobile applications). The article presents main elements and components of the model with a focus on the final output – the reporting and monitoring of risk profile.

Key words: *Critical Infrastructure, Cyberattacks, Information Security, Risk Assessment, Risk Management Model.*

JEL: *G21 L81 M15*

Introduction

According to Cybersecurity & Infrastructure Security Agency, the Financial Services Sector includes thousands of depository institutions, providers of investment products, insurance companies, other credit and financing organizations, and the providers of the critical financial utilities and services that support these functions. Financial institutions vary widely in size and presence, ranging from some of the world's largest global companies with thousands of employees and many billions of dollars in assets, to community banks and credit unions with a small number of employees serving individual communities.

Whether an individual savings account, financial derivatives, credit extended to a large organization, or investments made to a foreign country, these products allow customers to:

- Deposit funds and make payments to other parties.
- Provide credit and liquidity to customers.
- Invest funds for both long and short periods.
- Transfer financial risks between customers. (The Government, 2018)

The banking sector, as part of the financial system of the country, has a significant role in establishing and maintaining the cyber security resilience.

Before COVID 19, the digitization of banking services was slow; banks were adopting online services, however, the adoption speed was dictated by rigid legal changes. During the last period, the banking sector had a significant support from the National Bank in the process of switching from traditional banking services to online banking services.

Banks are opening their systems to their clients by implementing internet – banking systems for individuals and for legal entities. They are coming closer to their clients by developing internet and mobile applications, meant to offer diverse banking services remotely.

At the same time, there is a strong need of complex approaches to securing the remote systems, as they become a direct target for bad intentioned persons. Banking Security remains actual in every country and Republic of Moldova is not an exception. The National Bank of Moldova had developed and approved for implementation a number of measures and requirements in order to consolidate the internet – banking systems. Specifically, the a regulation had been developed SADD (ISO, 2018) specifies certain requirements as bi-factorial authentication, logging and monitoring, digital signatures, the necessity to conduct a detailed risk analysis, conducting of external third-party audits, etc.

There are several banks in Republic of Moldova that started to issue retail loans through their internet – banking systems. More, there are initiatives related to creating of specific marketplaces, where a client, by using its internet/mobile system, is proposed diverse services and products as well as conducting commercial operations like payments for services and goods.

This implies additional, client cyber security risks. It can be concluded that attackers target not the banks directly – they invest in information security significant resources, but the clients. More, in spite of the fact that the responsibility for ensuring the user security falls on the Banks, banking institutions are not ready to assume the entire responsibility. The contractual terms are mentioning that the responsibility for client`s account operations remain to be on the client's side.

As it had been mentioned earlier, a holistic approach to cyber security is to be applied for these systems. The Risk Management helps to define different perspectives and have a 360 degrees analysis: technical vs organizational, internal vs external, manual (human) vs automated, etc.

By conducting of a complex cyber risk analysis, the people in charge of security within the organizations will have a consistent range of tools to minimize the identified cyber risks that could affect the internet – banking and mobile – banking systems. The process should take into consideration the nature of the organization as well as the context of business operations in relation to legal, regulatory and contractual obligations.

A consistent risk management framework can be considered the ISO 31000 and ISO 27005 Standards, which can help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats and

effectively allocate and use resources for risk treatment (ISO, 2018). In the traditional understanding, the risk is defined by the likelihood of the occurrence of an unwanted event and the consequences that would follow from that event.

In practice, we realize that available and accepted risk management frameworks (e.g. ISO 31000, Open FAIR™, NIST RMF, COSO, etc.) remain very general and specify mostly what is to be done but not how to conduct a holistic cyber and information security risk analysis. They act as a skeleton and give directions for the risk management strategy of the company. Each framework approaches their way to risk assessment; however, they support organizations in achieving of the same objectives – identify and mitigate risks.

1. Internet – Banking Risk Management Model

1.1. Decomposition and Analysis

To have an acceptable coverage of the all aspects of an internet – banking information system there is a need to ensure that all the system's components are included in the cyber and information security risk management scope. Thus, the system has to be decomposed by its components. The decomposition will depend on the system's architecture and relevant modules of the system. It is very important that, because of decomposition, all the components placed on the logical path (components, which are not directly linked to the functioning of system: e.g. AD services, DMZ, DNS Services, PKI, etc.), are identified, documented and analysed.

The identified components are to be analysed from different points of view like people, processes, operating systems, application and network layers, data and database management systems, hardware and utilities, locations, etc. From experience, grouping threats and risks by relevant components allows identifying the most critical areas related to the system. More, this grouping may support in identifying risks which may affect an entire category (e.g. hardware, DBMS, etc.). The proposed classification can be extended and/or be narrowed. This will be done based on the current needs and requirements (e.g. legal). It is to point that the cyber and information security risks manager has to adjust the approach in certain aspects according to change of the internal/external factors.

1.2. Risks Matrix for qualitative analysis

Use of risk matrixes for risk evaluation is commonly accepted for the qualitative risk analysis. It is important to consider and decide on the size of the matrix. Less size (e.g. a 3x3-risk matrix) of a risk matrix is easier to understand and use. By the other side, it is difficult to truly determine where the boundary between acceptable and unacceptable truths/lies are. By using a 3x3 matrix, the risk management specialist has only three categories of risks — low, medium and high and this will give him less flexibility and granularity in decisions.

A bigger in size risk matrix (e.g. 5x5 or more) is more difficult to use, as it requires a specific discussion and decision of how severe hazardous scenarios can

be. By the other side, they allow for more detailed risk assessments. Each organization has to decide the risk matrix size. Selection of the risk matrix size may be done based on different aspects like the experience of the risk manager, the complexity of the project, external and internal limitations, etc. However, for an internet – banking system the recommended size is 5x5 or more as it is exposed in the Internet and if compromised, and then the overall impact may be significant.

The matrix will have five levels for the probability and five levels for the impact as presented in the image.



Figure 1. Risk Matrix.
Source: ISO 31000:2018 Risk management – Guidelines

1.3. Threats and Risks

One cannot identify all the risks at a time and cannot minimize risks to zero. To conduct the risk analysis there is a need to make sure that there is a continuous process, which is run periodically, or every time when the environment changes (legal changes, new configurations, new components, etc.). In addition, to ensure a holistic approach, main threats are to be considered. The security manager will consider available tools as a starting point. One of the example is ENISA Threats Taxonomy (EBA, 2018), which provides a classification of main threats by threats categories. It cannot be said that the list is full; however, it is a good starting point. Risks are being identified by conducting detailed analysis of each component. The analysis is linked to the threats categories. The starting point is to identify best practices (e.g. hardening standards, frameworks, etc.) and specific legal and contractual requirements, if any. The analysis includes a mix of automatic tools versus manual checks of system configuration and operational procedures. The

risks manager will consider each implemented security measure and their efficiency, as well as the extent of final objective achievement.

The risk evaluation will be done according to the risks matrix, by assessing the probability and the impact of a specific risk on the system. Evaluation of the probability and the impact, in most cases of a qualitative risk assessment, is a subjective process. The accuracy of the evaluation significantly depends on the experience of the risk manager as well as on his capacity to explore and identify statistic information, which is relevant. The security risk manager will compare the risk level against the organization's risk appetite.

All the identified risks are to be documented in the Risks Register, which represents the historical risks database. Because the environment changes continuously, there is a strong recommendation that periodic reviews of part risks are being conducted - some of the risks, which had been evaluated as being low, may change their impact and/or probability.

1.4. Risks mitigation

As there is no 100% security, there is no measure or control that will reduce the risks level to zero. For each risk, the security risk manager will select the appropriate risk mitigation strategy, depending on the nature and complexity. To minimize the risk to an acceptable level, the risk manager will select one or several mitigation strategies. The most applied strategy is to control risks – meaning that the organization will implement security controls that have the objective to minimize the risk probability or the impact. Along with the control strategy and depending on the risk nature (probability and/or impact level), the security risk manager will consider other risk mitigation strategies like transfer, contingency, tolerate, communicate, compliance check, etc.

Control measures will be designed for each risk. First, an analysis of the current control mechanisms should be conducted. Different type and categories of controls will be considered, specifically preventing/detecting and/or recovery. In addition, a mix of technical and organizational controls shall be designed. The risk manager has to make sure that the designed controls will minimize risks to an acceptable level. Otherwise, additional measures have to be implemented. Along with diverse technical and organizational security measures, it is important that banks include in their agenda client-related training activities in the field of cyber and information security.

The system's owner will approve all the risks and designed control mechanisms.

1.5. Reporting and Risk profile

In order to achieve the reporting objectives, each identified risk will be linked to a specific component or process. This will allow the bank management to elaborate correct and relevant decisions. The COO dashboard should be easy

adjustable and present high-level information, like risks by domains, risks by resources, top 5 resources at risk, residual risks no versus total risks no, etc.

Selection and establishment of Key Risk Indicators (KRI) will help the top management to remain focused on most critical and those areas that are of most interest. For example, for an internet-banking system the availability of the services has a very high importance. Accordingly, a KRI related to the system availability would help to identify deviations from the set threshold (e.g. 1% of total monthly time, no of interruptions, etc.). In addition, in case that the organization is implementing major changes, then a KRI threshold for the change management process can be established. Other relevant KRIs like access control or data integrity may be set.

KRIs are very useful as they help to link the previous organization's experience to the risk estimations and by doing so, KRIs act as a correction indicator. For example, if, for the continuity domain, we estimate an aggregate risk level as being Medium, but during the last period (e.g. 1 year) we exceeded the set threshold, then the aggregate risk level for this specific category may be increased and set to Major. By this, the management can ask questions and decide on specific actions to be undertaken.

The overall risk profile is formed as a sum of the risk levels by category and corrected by KRIs. The risk profile itself for a single resource does not bring much value-added, however, it helps when we have complex infrastructures and there is a need to have the big picture.

1.6. Conclusions

We manage risks every second, hour, day, year and so on in our lives. By applying of a risk management model in a structured and holistic way may help organizations to not only save, but also to earn money. Implementation of a systematic cyber security risk management process for the internet and mobile payment systems should be mandatory. The National Bank of Moldova has improved its practices and requirements, but at the same time, they have to implement supervising tools that would be efficient.

In Republic of Moldova, there is no consolidated, actual information related to systems risk profiles. Moreover, we suppose that the case is applicable for other countries from the region. The next important task, which is under study, is to aggregate risks related information by sector and by industry and even more, consolidate this information at the country level in order to plan relevant actions at the macro level.

References:

1. CISA (Cybersecurity & Infrastructure Security Agency). (October 21, 2020). *Financial Services Sector*. Retrieved 27 August, 2021, from https://www.cisa.gov/financial-services-sector

2. EBA, (2018). Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2), https://www.eba.europa.eu/

3. ENISA. (2016). *Threats Taxonomy.* Retrieved 26 August, 2021, from https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view

4. Executive Committee of the National Bank of Moldova (NBM). (18.04.2017). *Regulation on the provision of payment services through automated remote service systems, approved by HCE of the NBM no. 62 from 09.03.2017.* Retrieved 26 August, 2021, from https://www.bnm.md/ru/content/reglament-o-predostavlenii-platezhnyh-uslug-posredstvom-avtomatizirovannyh-sistem

5. ISO, (2018). *ISO 31000:2018(en) Risk management — Guidelines.* Retrieved 27 August, 2021, from https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

6. The Government, (11.07.2018). *HG 701/2018 din 11.07.2018, Regulamentul privind protecția antiteroristă a infrastructurii critice.* Retrieved 26 August, 2021, from https://www.legis.md/cautare/getResults?doc_id=108835&lang=ru