СТОПАНСКА АКАДЕМИЯ

„Димитър А. Ценов" - Свищов

KreativEU
Knowledge & Creativity European University

Международна научно-практическа конференция

90 години дарителство, знание, иновации и устойчиво развитие в СА „Д. А. Ценов" – Свищов

Том II



5-7 ноември 2026 г.

СТОПАНСКА АКАДЕМИЯ „Д. А. ЦЕНОВ“ – СВИЩОВ

МЕЖДУНАРОДНА НАУЧНО-ПРАКТИЧЕСКА КОНФЕРЕНЦИЯ

90 ГОДИНИ ДАРИТЕЛСТВО, ЗНАНИЕ, ИНОВАЦИИ И УСТОЙЧИВО РАЗВИТИЕ В СА „Д. А. ЦЕНОВ“ – СВИЩОВ

Свищов, 5-7 ноември 2026 г.

Посветена на 90 години от създаването на Стопанска академия „Димитър А. Ценов“

Сборник с доклади

ТОМ II

Международната научно-практическа конференция е организирана при изпълнение на Административен договор № КП-06-МНФ/23 от 18.08.2026 г. (BNSF-1.010-0023-C01) на Фонд „Научни изследвания“ при МОН по Процедура за подкрепа на международни научни форуми, провеждани в Република България

Академично издателство „Ценов“
Свищов
2026

ПРОГРАМЕН КОМИТЕТ
Доц. д-р Марин Маринов
Ректор на Стопанска академия „Димитър А. Ценов“ – председател
Проф. д-р Красимир Шишманов
Проф. д. н. Божидар Божинов
Проф. д-р Любчо Варамезов
Доц. д-р Маргарита Шопова
Доц. д-р Ваня Григорова
Доц. д-р Румен Ерусалимов
Доц. д-р Пламен Йорданов
Доц. д-р Драгомир Илиев
Доц. д-р Иван Марчевски
Доц. д-р Ирена Емилова
Доц. д-р Сергей Найденов
Доц. д-р Катя Личева
Проф. д-р Пенка Шишманова
Доц. д-р Елена Йорданова
Доц. д-р Пламен Петков
Доц. д-р Пепа Стойкова
Доц. д-р Михаил Чиприянов
Доц. д-р Любка Илиева
Доц. д-р Теодора Филипова
Ст. преп. Елка Узунова
Ст. преп. д-р Радослав Николов

ОРГАНИЗАЦИОНЕН КОМИТЕТ
Доц. д-р Здравко Любенов – *председател*
Проф. д-р Светослав Илийчовски
Проф. д-р Атанас Атанасов
Доц. д-р Галина Чиприянова
Доц. д-р Маруся Смокова-Стефанова
Доц. д-р Красимира Славева
Гл. ас. д-р Асен Божиков
Ст. преп. д-р Венцислав Диков

РЕДАКЦИОНЕН СЪВЕТ
Проф. д-р Атанас Атанасов – *председател*
Проф. д-р Светослав Илийчовски
Проф. д-р Красимир Шишманов
Доц. д-р Искра Пантелеева
Доц. д-р Танер Исмаилов
Доц. д-р Здравко Любенов
Доц. д-р Галя Иванова-Кузманова
Доц. д-р Ирена Емилова
Доц. д-р Христо Сирашки
Доц. д-р Елена Йорданова
Доц. д-р Любка Илиева
Доц. д-р Валентин Милинов
Доц. д-р Красимира Славева
Доц. д-р Маруся Смокова-Стефанова
Доц. д-р Венцислав Василев
Доц. д-р Зорница Петкова

Публикуваните материали са рецензирани по метода на двойно сляпо рецензиране. Авторите носят отговорност за съдържанието на материалите, изразените мнения, използваните данни, цитираните източници и езиковото оформление на текстовете. Фонд „Научни изследвания“ не носи отговорност за съдържанието на докладите, представени на научния форум, както и за съдържанието на рекламните и други материали за него.

ISBN 978-954-23-2688-5 (print)
ISBN 978-954-23-2689-2 (online)

D. A. TSENOV ACADEMY OF ECONOMICS – SVISHTOV

INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE

90 YEARS OF CHARITY, KNOWLEDGE, INNOVATION AND SUSTAINABLE DEVELOPMENT IN D. A. TSENOV ACADEMY OF ECONOMICS - SVISHTOV

Svishtov, 5th - 7th November 2026

Dedicated to the 90th anniversary since the establishment of D. A. Tsenov Academy of Economics

Conference Proceedings

VOLUME II

The International Scientific and Practical Conference was organized in the implementation of Administrative Contract № КП-06-МНФ/23 of August 18, 2026 (BNSF-1.010-0023-C01), awarded by the Bulgarian National Science Fund at the Ministry of Education and Science under the Procedure for Support of International Scientific Forums Held in the Republic of Bulgaria

Tsenov Academic Publishing House
Svishtov
2026

PROGRAM COMMITTEE
Assoc. Prof. Marin Marinov, PhD
Rector of D. A. Tsenov Academy of Economics
Prof. Krasimir Shishmanov, PhD
Prof. Bozhidar Bozhinov, PhD
Prof. Lyubcho Varamezov, PhD
Assoc. Prof. Margarita Shopova, PhD
Assoc. Prof. Vanya Grigorova, PhD
Assoc. Prof. Rumen Jerusalemov, PhD
Assoc. Prof. Plamen Yordanov, PhD
Assoc. Prof. Dragomir Iliev, PhD
Assoc. Prof. Ivan Marchevski, PhD
Assoc. Prof. Irena Emilova, PhD
Assoc. Prof. Sergey Naydenov, PhD
Assoc. Prof. Katya Licheva, PhD
Prof. Penka Shishmanova, PhD
Assoc. Prof. Elena Yordanova, PhD
Assoc. Prof. Plamen Petkov, PhD
Assoc. Prof. Pepa Stoykova, PhD
Assoc. Prof. Mihail Chipriyanov, PhD
Assoc. Prof. Lyubka Ilieva, PhD
Assoc. Prof. Teodora Filipova, PhD
Senior Lecturer Elka Uzunova
Senior Lecturer Radoslav Nikolov, PhD

ORGANIZING COMMITTEE
Assoc. Prof. Zdravko Lyubenov. PhD, Chairman
Prof. Svetoslav Iliychovski, PhD
Prof. Atanas Atanasov, PhD
Assoc. Prof. Galina Chipriyanova, PhD
Assoc. Prof. Marusya Smokova-Stefanova, PhD
Assoc. Prof. Krasimira Slaveva, PhD
Ch. Assist. Prof. Asen Bozhikov, PhD
Sen. Lect. Ventsislav Dikov

EDITORIAL BOARD
Prof. Atanas Atanasov, PhD – Chair
Prof. Svetoslav Iliychovski, PhD
Assoc. Prof. Iskra Panteleeva, PhD
Prof. Krasimir Shishmanov, PhD
Assoc. Prof. Taner Ismailov, PhD
Assoc. Prof. Zdravko Lyubenov, PhD
Assoc. Prof. Galya Ivanova-Kuzmanova, PhD
Assoc. Prof. Irena Emilova, PhD
Assoc. Prof. Hristo Sirashki, PhD
Assoc. Prof. Elena Yordanova, PhD
Assoc. Prof. Lyubka Ilieva, PhD
Assoc. Prof. Valentin Milinov, PhD
Assoc. Prof. Krasimira Slaveva, PhD
Assoc. Prof. Marusya Smokova-Stefanova, PhD
Assoc. Prof. Ventsislav Vasilev, PhD
Assoc. Prof. Zornitsa Petkova, PhD

The published materials have been peer-reviewed using the double-blind review method. The authors are solely responsible for the content of the materials, the opinions expressed, the data used, the cited sources, and the linguistic formatting of the texts. The Bulgarian National Science Fund bears no responsibility for the content of the papers presented at the scientific forum, nor for the content of its promotional or other materials.

ISBN 978-954-23-2688-5 (print)
ISBN 978-954-23-2689-2 (online)

СЪДЪРЖАНИЕ

ТОМ II
МЕНИДЖМЪНТ, МАРКЕТИНГ, ПЛАНИРАНЕ, МЕЖДУНАРОДНА ИКОНОМИКА, БИЗНЕС ИНФОРМАТИКА

ИЗСЛЕДВАНЕ НА ГОТОВНОСТТА, НАГЛАСИТЕ И ПОТРЕБНОСТИТЕ НА ПРЕПОДАВАТЕЛИТЕ ОТ СТОПАНСКА АКАДЕМИЯ „Д. А. ЦЕНОВ“ ЗА ИЗПОЛЗВАНЕ НА ИЗКУСТВЕН ИНТЕЛЕКТ
Проф. д.н. Борислав Борисов, гл. ас. д-р Юлиян Господинов..... 9

THE PLACE AND ROLE OF UKRAINE IN ENSURING THE EU'S EXTERNAL ECONOMIC SECURITY
Prof. D.Sc. (Economics) Illya Khadzhynov..... 18

SHADOW DIGITAL ECONOMY AND SUSTAINABLE DEVELOPMENT
Prof. DSC Serghei Ohrimenco, Prof. DSC Dinara Orlova, Prof. PhD Tatiana Manasterska, Valeriu Cernei, Partner, IT Audit&Advisory..... 24

УПРАВЛЕНИЕТО НА ЗНАНИЕТО КАТО МЕХАНИЗЪМ ЗА ФОРМИРАНЕ НА ИНОВАЦИОННА СПОСОБНОСТ И ИНОВАЦИОННО ПРЕДСТАВЯНЕ НА ПРЕДПРИЯТИЕТО (ТЕОРЕТИЧЕН ПРЕГЛЕД И КОНЦЕПТУАЛНА РАМКА)
Проф. д-р Любчо Варамезов, докторант Стела Маринова..... 32

СТРАТЕГИЧЕСКАТА ДЪЛБОЧИНА (ВЪЗХОДЪТ) И НЕСТРАТЕГИЧЕСКАТА ПЛИТКОСТ (УПАДЪКЪТ) – КАЗУСЪТ НА СВИЩОВСКАТА АКАДЕМИЯ
Проф. д-р Никола Янков..... 40

LEAN MARKETING – СЪВРЕМЕНЕН ПОДХОД ЗА ТРАНСФОРМАЦИЯ НА МАРКЕТИНГОВАТА СТРАТЕГИЯ
Доц. д-р Ваня Григорова..... 48

ПОЗИЦИОНИРАНЕ НА ТЪРГОВСКА МАРКА В ДИГИТАЛНА СРЕДА
Доц. д-р Ваня Григорова, Александра Иванова, студент..... 56

СЪВРЕМЕННИ ПОДХОДИ ЗА ПРОДУКТОВА ИНОВАЦИЯ В КОЗМЕТИЧНИЯ СЕКТОР
Доц. д-р Ваня Григорова, Марая Драганова, студент..... 64

ДЕТЕРМИНАНТИ НА ТЪРСЕНЕТО НА ЗАСТРАХОВКИ СРЕЩУ ТЪРГОВСКИ РИСК
Доц. д-р Ваня Григорова, докторант Николай Марков,..... 71

ВЛИЯНИЕ НА ДИГИТАЛНИЯ БЪРНАУТ ВЪРХУ ПОТРЕБИТЕЛСКОТО ПОВЕДЕНИЕ
Доц. д-р Ваня Григорова, Пламена Жекова, студент..... 79

INTERNATIONAL ECONOMIC INTEGRATION AND STRUCTURAL RESILIENCE
Assoc. Prof., PhD Giga Abuseridze, Assoc. Prof. PhD Anatoliy Asenov..... 87

ПАРТИСИПАТИВНО ВЗАИМОДЕЙСТВИЕ В ИНОВАЦИОННИТЕ МРЕЖИ
Доц. д-р Евелина Парашкевова, проф. д-р Маргарита Богданова, доц. д-р Александра Пенишевич, проф. д-р Бранислав Санчанин" 93

ОСОБЕНОСТИ НА СЪВРЕМЕННИЯ МЕЖДУНАРОДЕН БИЗНЕС
Доц. д-р Здравко Любенов 101

CONVERGENCE OR DIVERGENCE? DIGITAL TRANSFORMATION AND EMERGING INTERNATIONAL MARKETING TRENDS IN ROMANIA AND BULGARIA
Assoc. Prof. Cătălin Deatcu-Gavril PhD, assoc. Prof. Alexander Ganchev PhD, Ivaylo Marinov PhD, Vlad-Mihai Panait PhD, Ec. Elena Deatcu-Gavril 108

CYBERSECURITY AND OPERATIONAL RISK IN THE ERA OF DIGITAL TRANSFORMATION: CHALLENGES FOR SUSTAINABLE DEVELOPMENT
Assoc. Prof. Habilitated Doctor Dorogaia Irina, Caminschi Olga, PhD student, Assistant Lecturer 122

MANAGING ORGANIZATIONAL STRUCTURE CHANGES IN AN UNSTABLE ENVIRONMENT
Assoc. Prof. Habilitated Doctor Dorogaia Irina, Coval Anastasia, Assistant Lecturer 129

ДИГИТАЛНОТО РАВЕНСТВО КАТО ФАКТОР В ПРОЦЕСА НА ДИГИТАЛНА ТРАНСФОРМАЦИЯ
Доц. д-р Кремена Маринова-Костова 139

ИНОВАЦИОННИ МРЕЖИ И МЕЖДУФИРМЕНО СЪТРУДНИЧЕСТВО: ФАКТОРИ, ВЗАИМОДЕЙСТВИЯ И РАЗВИТИЕ
Доц. д-р Любомир Тодоров, проф. д-р Дариуш Новак 146

СОЦИАЛНОМРЕЖОВИ ПОДХОД ЗА ИЗСЛЕДВАНЕ НА МЕЖДУУНИВЕРСИТЕТСКОТО СЪТРУДНИЧЕСТВО В РАМКИТЕ НА ИНИЦИАТИВАТА „ЕВРОПЕЙСКИ УНИВЕРСИТЕТ“: СРАВНИТЕЛЕН АНАЛИЗ ПО ПОКАНИ ЗА КАНДИДАТСТВАНЕ
Доц. д-р Маруся Смокова, гл. ас. д-р Галин Стефанов 155

ЕФЕКТИВНИ КОМУНИКАЦИОННИ СТРАТЕГИИ КАТО ФАКТОР ЗА ОРГАНИЗАЦИОННА УСТОЙЧИВОСТ
Доц. д-р Милен Динков 166

ESG ПОЛИТИКИ И РЕШЕНИЯ В СТРОИТЕЛНИЯ СЕКТОР
Доц. д-р Михаил Чиприянов 172

ВЪЗДЕЙСТВИЕ НА АГЕНТИТЕ С ИЗКУСТВЕН ИНТЕЛЕКТ ВЪРХУ СВЕТОВНАТА МРЕЖА
Доц. д-р Наталия Маринова 176

ASSESSING FACTORS AFFECTING AN ORGANIZATION’S INFORMATION SECURITY
Assoc. Prof. Olga Pugacheva, PhD 184

СТРАТЕГИЧЕСКИ АНАЛИЗ НА ПАЗАРА НА ЧУЖДОЕЗИКОВИ ОБРАЗОВАТЕЛНИ УСЛУГИ
Доц. д-р Пенка Горанова..... 192

ПРЕДИЗВИКАТЕЛСТВА И РИСКОВЕ ПРИ ВНЕДРЯВАНЕТО НА ИЗКУСТВЕН ИНТЕЛЕКТ И АНАЛИЗ НА ГОЛЕМИ ДАННИ ЗА УСТОЙЧИВИ ВЕРИГИ ЗА ДОСТАВКИ
Доц. д-р Петя Емилова, доц. д-р Веселин Попов 198

MANAGING RESEARCH–EDUCATION SYNERGIES FOR ENGINEERING AND SCIENCE CAREER DEVELOPMENT IN THE UNIVERSITY ENVIRONMENT: THE CASE OF VALAHIA UNIVERSITY OF TÂRGOVIȘTE
Assoc. Prof. Dr. Eng., Sălișteanu I.C., Professor, Dr. Eng., Dunea D.E.C. , Professor, Dr. Eng., Coandă H.G. , Assoc. Prof., Dr. Eng., Udroiu I.N. , Professor, Dr. Croitoru G., Senior Research Scientist, Dr. Eng., Nicolescu C.M., Assoc. Prof., Dr. Bumbac M., Assoc. Prof., Dr. Eng., Alexandrescu D.C., University Lecturer Dr., Hossu A.M., Assoc. Prof., Dr. Eng., Angelescu N., Assoc. Prof., Dr. Eng., Popa I.F., University Lecturer Dr., Catangiu A. 207

УПРАВЛЕНКСИ ИЗМЕРЕНИЯ НА КОНТИНУУМА „ПРОДУКТ – УСЛУГА“: ОПЕРАЦИОННА СИСТЕМА И ТРАНСФОРМАЦИОННИ ПРОЦЕСИ
Доц. д-р Силвия Благоева, доц. д-р Ирена Емилова 217

АСПЕКТИ НА УПРАВЛЕНИЕТО НА КАЧЕСТВОТО В ОРГАНИЗАЦИИТЕ ОТ ПУБЛИЧНИЯ СЕКТОР
Доц. д-р Христо Сирашки..... 224

НАУЧНАТА ПОЛИТИКА НА СТРАНИТЕ ОТ ЕВРОПЕЙСКИЯ СЪЮЗ И ВЛИЯНИЕТО НА ГЛОБАЛИЗАЦИЯТА
доц. д-р Цветан Дилков..... 230

ВЗЕМАНЕ НА РЕШЕНИЯ ЗА ПОКУПКА В СРЕДА НА ИЗКУСТВЕН ИНТЕЛЕКТ
Гл. ас. д-р Атанаска Решеткова..... 238

ОСОБЕНОСТИ В АНТИКРИЗИСНОТО УПРАВЛЕНИЕ
Гл. ас. д-р Валентин Панайотов 246

КОНВЕРГЕНЦИЯ НА ДОХОДИТЕ В РАМКИТЕ НА ЕВРОПЕЙСКИЯ СЪЮЗ: ДЕКОМПОЗИРАНЕ НА НАЦИОНАЛНО И РЕГИОНАЛНО НИВО
Гл. ас. д-р Галин Стефанов..... 253

АДМИНИСТРАТИВНИ РЕШЕНИЯ ЗА УСТОЙЧИВИ СОЦИАЛНИ ИНВЕСТИЦИ
Гл. ас. д-р Десислава Алексиева..... 262

ВАЛУТНА ЕКСПОЗИЦИЯ И ПОДХОДИ ЗА УПРАВЛЕНИЕ НА РИСКА: ИЗСЛЕДВАНЕ НА НАУЧНАТА ЛИТЕРАТУРА
Гл. ас. д-р Димитър Костов 268

СТРАТЕГИЧЕСКИ АСПЕКТИ НА СВИВАЩИТЕ СЕ ГРАДОВЕ
Гл. ас. д-р Елица Лазарова, Chrysostomos Roditis..... 281

ГЕОПОЛИТИЧЕСКИЯТ РИСК КАТО ФАКТОР ПРИ ИЗБОРА НА ЛОКАЦИЯ ЗА ПРЕКИ ЧУЖДЕСТРАННИ ИНВЕСТИЦИИ
Гл. ас. д-р Иван Ангелов 288

ПЕРИФЕРНИ ИЗЧИСЛЕНИЯ И ИНТЕРНЕТ НА НЕЩАТА: БЪДЕЩЕТО НА СВЪРЗАНИТЕ УСТРОЙСТВА
Гл. ас. д-р Искрен Таиров 296

ЕВРИСТИЧНИ СТРАТЕГИИ ЗА РЕДУКЦИЯ НА СЛОЖНОСТТА В ИКОНОМИЧЕСКОТО ПЛАНИРАНЕ ПРИ ОГРАНИЧЕНА ИНФОРМАЦИЯ
Гл. ас. д-р Надежда Веселинова 302

КАЧЕСТВО НА ТРУДОВИЯ ЖИВОТ: ОРГАНИЗАЦИОННО-ПОВЕДЕНЧЕСКИ АСПЕКТИ
Гл. ас. д-р Надежда Стефанова 310

АНАЛИЗ НА ЕФЕКТИВНОСТТА НА ОНЛАЙН МАРКЕТИНГА И KPI ПОКАЗАТЕЛИ
Гл. ас. д-р Пламен Петров 317

ТЕОРИЯ И ПРАКТИКА: ФАКТОРИ ЗА ИЗПОЛЗВАНЕ НА ИЗКУСТВЕН ИНТЕЛЕКТ ОТ СТУДЕНТИ ПО МАРКЕТИНГ
Гл. ас. д-р Светла Атанасова 325

ДОБРИ ПРАКТИКИ ПО ПРЕДОСТАВЯНЕ НА ДОБРО УПРАВЛЕНИЕ ОТ ДЪРЖАВНАТА АДМИНИСТРАЦИЯ
Гл. ас. д-р Юлиян Господинов 334

RETHINKING PLACE BRANDING: STRATEGIC FRAMEWORKS AND EXECUTION TOOLS
Senior Lecturer, PhD, Aliya Turganovna Baigarina, PhD student Anar Aliyeva, Head Assist.Prof., PhD Stanislava Stoyanova-Asenova, Assoc.prof. PhD Anatoliy Asenov ... 345

ЕЗИКОВА БЛИЗОСТ И ИНСТИТУЦИОНАЛНА ИНТЕГРАЦИЯ В МЕЖДУНАРОДНАТА ТЪРГОВИЯ: КОНЦЕПТУАЛЕН ПОДХОД
Ст. преп. д-р Маргарита Михайлова, доц. д-р Драгомир Илиев 350

ОТ КОНЦЕПЦИЯТА ДО ВЪЗДЕЙСТВИЕТО: ДИЗАЙН И ИЗПЪЛНЕНИЕ НА УСПЕШНИ ПРОЕКТИ ПО ПРОГРАМА „ИНТЕРРЕГ РУМЪНИЯ–БЪЛГАРИЯ“
Лектор, д-р Михаела Тинка Удриштиойу; професор, д-р Нику Джордже Биздоака 356

СТРАТЕГИЧЕСКО УПРАВЛЕНИЕ НА ЗАИНТЕРЕСОВАНИТЕ СТРАНИ ПРИ ПЛАНИРАНЕ НА ЕКОЛОГИЧНИ ПРОЕКТИ ЗА УПРАВЛЕНИЕ НА ОТПАДЪЦИ
Ас. д-р Димчо Шопов 362

MANAGERIAL STRATEGIES FOR MOTIVATING THE EMPLOYEES FROM ROMANIAN PUBLIC INSTITUTIONS
Assistant Professor, Ph.D, Miruna Angela Mutu, Senior Lecturer, Ph.D, Andreea Anamaria Panagoret, Senior Lecturer, Ph.D, Dragos Mihai Panagoret, Lecturer, Ph.D, Sorina Cernat 371

MAPPING AND MITIGATING CHILDREN'S DIGITAL FOOTPRINTS IN EGYPT
Assistant Professor Nehal Lotfy H. Khalil, PhD..... 384

ЕКСПЕРТНОТО ИНТЕРВЮ В ИЗСЛЕДВАНИЯТА ПО ДИГИТАЛЕН МАРКЕТИНГ: МЕТОДОЛОГИЧНИ НАСОКИ
Ас. д-р Спасимир Цветанов..... 392

МАРКЕТИНГ, ВОДЕН ОТ НОСТАЛГИЯТА В ЕРАТА НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ – ВЪЗМОЖНОСТИ, ПРЕДИЗВИКАТЕЛСТВА И ТЕНДЕНЦИИ
Ас. д-р Стелиана Василева 400

AI В ПОМОЩ НА СЕЛЕКЦИОНЕРИТЕ В ЖИВОТНОВЪДСТВОТО: ПРОТОТИП НА ИНТЕЛИГЕНТНА СИСТЕМА ЗА АНАЛИЗ НА РОДОСЛОВИЯ И ПОДПОМАГАНЕ НА РАЗВЪДНАТА ДЕЙНОСТ
Д-р инж. Пенка Чернаева, д-р инж. Петър Чернаев..... 411

АНАЛИЗ НА ПОТЕНЦИАЛА НА ИНОВАЦИОННИТЕ ПРОЕКТИ ЗА НАМАЛЯВАНЕ НА БЕДНОСТТА В СЕВЕРОЗАПАДНИЯ РАЙОН ЗА ПЛАНИРАНЕ БЪЛГАРИЯ
Д-р Таня Минкова Николова..... 418

УЧАСТИЕТО В ИНИЦИАТИВАТА ЗА НАСОЧЕНА ТЪРГОВИЯ И ВИЗОВАТА ОТВОРЕНОСТ В АФРИКА
Докторант Анита Йорданова 424

СТРАТЕГИЧЕСКО ПЛАНИРАНЕ НА РАБОТНАТА СИЛА В ЗДРАВНАТА СИСТЕМА НА ГЪРЦИЯ В КОНТЕКСТА НА ПРОФЕСИОНАЛНИТЕ ДИСБАЛАНСИ И РЕГИОНАЛНИТЕ НЕРАВЕНСТВА
Докторант Анна Коллару 432

СТРАТЕГИЧЕСКО ПЛАНИРАНЕ И УПРАВЛЕНИЕ НА КРИЗИ В АДМИНИСТРИРАНЕТО НА ОБЩЕСТВЕНОТО ЗДРАВЕОПАЗВАНЕ
Докторант Анна Коллару, докторант Алексиос Антониос Колларос..... 439

МОДЕЛИ НА ПУБЛИЧНО-ЧАСТНО ПАРТНЬОРСТВО ЗА ФИНАНСИРАНЕ НА ОБЩИНСКАТА ТРАНСПОРТНА ИНФРАСТРУКТУРА
Докторант Атанаска Василева 447

ИНТЕГРИРАН ПОДХОД ЗА ПОВИШАВАНЕ НА ЕФЕКТИВНОСТТА НА АДМИНИСТРАТИВНИТЕ ПРОЦЕСИ В ГЛОБАЛНИТЕ АУТСОРСИНГ СТРУКТУРИ
Докторант Веселин Василев Михайлов..... 451

СВЪРЗВАЩИТЕ СТРУКТУРИ В СИСТЕМАТА НА УПРАВЛЕНИЕ – МЯСТО И РОЛЯ
Докторант Галина Гатева-Христова..... 462

МЕЖДУНАРОДНА ТЪРГОВИЯ И ИКОНОМИЧЕСКИ БАРИЕРИ
Докторант Георги Спасов Витков 467

ДЕТЕРМИНАНТИ НА КЛИЕНТСКАТА УДОВЛЕТВОРЕНОСТ В ЗАСТРАХОВАНЕТО – ПОВЕДЕНЧЕСКИ И ДИГИТАЛНИ АСПЕКТИ
Докторант Десислава Кайрякова..... 474

ПРЕДИЗВИКАТЕЛСТВА ПРИ ИНТЕГРАЦИЯТА НА НЕСТРУКТУРИРАНИ И ПОЛУСТРУКТУРИРАНИ ДАННИ ВЪВ ФИНАНСОВО-СЧЕТОВОДНИТЕ СИСТЕМИ
Докторант Диян Николаев 482

WHO: TRANSFORMING ORGANIZATIONS THROUGH ESG CULTURE
PhD student Elton Rodrigo Titon 488

ВРЪЗКА МЕЖДУ ИНТЕГРИРАНОТО УПРАВЛЕНИЕ НА ОТПАДЪЦИТЕ И КРЪГОВИТЕ БИЗНЕС МОДЕЛИ
докторант Емил Найденов 496

ПРОГРАМНОТО БЮДЖЕТИРАНЕ КАТО ИНСТРУМЕНТ ЗА РЕАЛИЗАЦИЯ НА ОБЩИНСКИЯ ПЛАН ЗА РАЗВИТИЕ: МОДЕЛ ЗА ФИНАНСОВА УСТОЙЧИВОСТ
Докторант Емилия Върбанова 504

ТРАНСФОРМАЦИЯ НА БИЗНЕС МОДЕЛИТЕ В СЕКТОРА НА ВЪЗОБНОВЯЕМАТА ЕНЕРГИЯ В ЕВРОПЕЙСКИЯ СЪЮЗ В УСЛОВИЯТА НА ЗЕЛЕНИЯ ПРЕХОД
Докторант Жени Антонова 508

ИЗБОР МЕЖДУ ЛОКАЛЕН И ОБЛАЧНО БАЗИРАН ИЗКУСТВЕН ИНТЕЛЕКТ В СЪВРЕМЕННИТЕ БИЗНЕС ИНФОРМАЦИОННИ СИСТЕМИ
Докторант Зорница Иванова 516

ОТ ТЕОРИЯ КЪМ ПРАКТИКА: ИНТЕГРИРАНЕ НА УСТОЙЧИВОСТТА В УПРАВЛЕНИЕТО НА ПРОЕКТИ КАТО ФАКТОР ЗА КОНКУРЕНТОСПОСОБНОСТ НА БЪЛГАРСКАТА ИКОНОМИКА
Докторант Ивелина Станева 523

ВЪЗМОЖНОСТИ И ПРЕДИЗВИКАТЕЛСТВА ПРИ ИЗПОЛЗВАНЕТО НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ ЗА ОПТИМИЗАЦИЯ НА АДМИНИСТРАТИВНИТЕ ПРОЦЕСИ В ЗДРАВЕОПАЗВАНЕТО
докторант Йоан Парашкевов Денев 528

ВЪЗМОЖНОСТИ И ПРЕДИЗВИКАТЕЛСТВА ПРЕД ВНЕДРЯВАНЕТО НА ИЗКУСТВЕН ИНТЕЛЕКТ В МАЛКИ И СРЕДНИ ПРЕДПРИЯТИЯ
Докторант Йоанна Иванова Бакалова 536

ИНФОРМАЦИОННА СИГУРНОСТ В СЪВРЕМЕННИТЕ ОБУЧИТЕЛНИ ПЛАТФОРМИ
Докторант Лора Първанова 551

ДЕФИНИРАНЕ НА БЛОКЧЕЙН: ХАРАКТЕРИСТИКИ И КЛЮЧОВИ КОМПОНЕНТИ
Докторант Любен Кирев 551

ФАКТОРИ ЗА ВНЕДРЯВАНЕ НА ИНОВАЦИИ В ПУБЛИЧНИЯ СЕКТОР
Докторант Мария Савова 557

УПРАВЛЕНИЕ НА НЕФИНАНСОВИЯ РИСК ЧРЕЗ КСО В БЪЛГАРИЯ
Докторант Мария Цветанова 565

СРАВНИТЕЛНА ХАРАКТЕРИСТИКА НА МЕХАНИЗМИТЕ ЗА ВНЕДРЯВАНЕ НА КОМПЕТЕНТНОСТИ ПО ИКОНОМИКА
Докторант Милена Димитрова..... 569

СРАВНИТЕЛЕН АНАЛИЗ НА ДИГИТАЛНИ ПЛАТФОРМИ НА БЪЛГАРСКИЯ ПАЗАР ЧРЕЗ ИНДЕКС НА ПАЗАРНАТА ПРИВЛЕКАТЕЛНОСТ (MAS): NETFLIX, TRENDYOL И TEMU
Докторант Невин Ангелова..... 573

СТЕЙБЪЛКОЙНИТЕ В ТРАНСГРАНИЧНИТЕ РАЗПЛАЩАНИЯ: ПАЗАРНА КОНЦЕНТРАЦИЯ И РЕГУЛАТОРНИ ЕФЕКТИ ОТ MICA
Докторант Пенко Ангелов Бяливанов..... 580

ДЕТЕРМИНАНТИ НА КОРПОРАТИВНАТА СОЦИАЛНА ОТГОВОРНОСТ В МЕЖДУНАРОДНИ КОМПАНИИ ЗА БИЗНЕС УСЛУГИ
Докторант Петьо Божинов..... 588

КОНЦЕПТУАЛНА РАМКА НА ВНЕДРЯВАНЕТО НА ЗЕЛЕНИ ТЕХНОЛОГИИ В ПУБЛИЧНИЯ СЕКТОР
Докторант Радослав Асенов..... 596

УПРАВЛЕНСКИ ПРЕДИЗВИКАТЕЛСТВА ПРЕД ПУБЛИЧНИЯ СЕКТОР В УСЛОВИЯТА НА ДИГИТАЛНА ТРАНСФОРМАЦИЯ И ОТВОРЕНИ ИНОВАЦИИ
Докторант Сание Иса..... 604

TRANSFORMATIONAL LEADERSHIP AND AFFECTIVE ORGANIZATIONAL COMMITMENT: A FOCUSED NARRATIVE REVIEW
PhD student Slagjana Cvetkovska Mousa..... 611

ПРЕОДОЛЯВАНЕ НА ПРОПАСТТА В ЕКОЛОГИЧНИЯ ИНТЕГРИТЕТ: СРАВНИТЕЛЕН АНАЛИЗ НА РЕГУЛАТОРНАТА СТРОГОСТ НА СИСТЕМАТА ЗА ТЪРГОВИЯ С ЕМИСИИ НА ЕВРОПЕЙСКИЯ СЪЮЗ И ДОБРОВОЛНИТЕ ВЪГЛЕРОДНИ ПАЗАРИ
Докторант Стефани Георгиева, Докторант, Антони Георгиев..... 618

ВНЕДРЯВАНЕ НА ГЕНЕРАТИВЕН ИЗКУСТВЕН ИНТЕЛЕКТ И ИНТЕЛИГЕНТНИ АГЕНТИ В БИЗНЕС АНАЛИЗА: ТЕХНИЧЕСКИ ИЛИ ОРГАНИЗАЦИОНЕН ПРОБЛЕМ
Докторант Таньо Георгиев Георгиев..... 626

РЕШЕНИЯ ЗА ИНТЕЛИГЕНТНА МОБИЛНОСТ В СМАРТ ГРАДОВЕТЕ В БЪЛГАРИЯ
Докторант инж. Тихомир Панов..... 634

ГЕОГРАФСКА ЕКСПАНЗИЯ ЧРЕЗ МРЕЖОВИ СТРАТЕГИИ В СЕЛСКОСТОПАНСКАТА ТЪРГОВИЯ
Докторант Тотю Иванов..... 639

ПРИЛАГАНЕ НА АРХИТЕКТУРИ, УПРАВЛЯВАНИ ОТ СЪБИТИЯ, И МИКРОСЪРВИСИ ЗА ИНТЕЛИГЕНТНА АВТОМАТИЗАЦИЯ В ИНДУСТРИЯ 5.0
Докторант Яница Димитрова..... 643

ГЕНЕРАТИВНИЯТ ИЗКУСТВЕН ИНТЕЛЕКТ КАТО КАТАЛИЗАТОР НА ПЛАТФОРМЕНАТА ИНТЕРНАЦИОНАЛИЗАЦИЯ НА МАЛКИТЕ И СРЕДНИ ПРЕДПРИЯТИЯ
Докторант Юксела Шефкетева Брахимбашева..... 648

УЧИЛИЩЕТО КАТО СПЕЦИФИЧНА СРЕДА ЗА УПРАВЛЕНИЕ НА ПРОЕКТНАТА ДЕЙНОСТ
Магистър Лора Николова 656

PSYCHOLOGICAL METHODS FOR MARKETING INFLUENCE ON CONSUMER BEHAVIOR
Anna Grigorova, student 663

DIGITAL TRANSFORMATION AND CUSTOMER RELATIONSHIP MANAGEMENT IN SMES: A COMPARATIVE STUDY OF ROMANIA AND BULGARIA
Student Elena Deatcu – Gavril, Student Adriana – Daniela Urucu, Student Diana – Marina Vasile, Student Angelo – Patrick – Cosmin Baicu..... 670

СЪВРЕМЕННОТО ПРЕДПРИЯТИЕ В УСЛОВИЯ НА ГЛОБАЛИЗАЦИЯ И ДИГИТАЛИЗАЦИЯ
Студент Милена Христова 679

ОЦЕНКА ФАКТОРОВ, ВЛИЯЮЩИХ НА ИНФОРМАЦИОННАТА БЕЗОПАСНОСТ НА ОРГАНИЗАЦИЯТА

Доц. д-р Олга Пугачева[1]

Резюме: *Изследването включва анализ на съвременните заплахи за киберсигурността и експертна оценка на основните фактори, влияещи върху информационната сигурност на организациите: нивото на заплахите, човешкия фактор, технологичните промени, свързани с използването на технологии за изкуствен интелект, и други фактори, характеризиращи заплахите в дигиталния свят.*

Ключови думи: *информационна сигурност, заплахи, изкуствен интелект, експертни методи за оценка, организации*

JEL: A12, C8, O33, C45, Y10

ASSESSING FACTORS AFFECTING AN ORGANIZATION'S INFORMATION SECURITY

Associate Professor, PhD, Olga Pugacheva

Abstract: *The study includes an analysis of modern cybersecurity threats and an expert assessment of the main factors influencing the information security of organizations: the level of threats, the human factor, technological changes associated with the use of artificial intelligence technologies, and other factors characterizing threats in the digital world.*

Keywords: *information security, threats, artificial intelligence, expert assessment methods, organizations*

JEL: A12, C8, O33, C45, Y10

1. Introduction

Analyzing the main cybersecurity threats is a crucial part of an information security strategy and an asset for any organization seeking to ensure its security in the digital world.

Assessing the factors affecting an organization's information security is important for the following key reasons (Pugacheva, 2025):

– increasing number of cyberattacks. Each year, we see an increase in the number and complexity of cyberattacks. Hackers are using increasingly sophisticated methods, making continuous threat monitoring and analysis essential;

[1] OPugacheva@gsu.by, Гомелски държавен университет на името на Франциск Скарина, Република Беларус

– threat diversity. Threats can range from simple viruses and malware to complex attacks such as phishing, DDoS attacks, supply chain attacks, and more. Understanding these threats allows organizations to better prepare and protect themselves;

– economic impact. Cyberattacks can have serious financial consequences for organizations, including data loss, reputational damage, and fines. Threat analysis helps minimize risks and losses for organizations;

– regulatory com

– pliance. Many industries are subject to strict cybersecurity regulations. Threat analysis helps organizations meet these requirements and avoid legal consequences;

– technological change. The rapid advancement of technologies such as cloud computing, IoT (Internet of Things), and artificial intelligence (AI) creates new vulnerabilities. Threat analysis enables the timely identification and remediation of these vulnerabilities;

– raising awareness. Threat analysis helps increase employee and management awareness of cybersecurity risks, leading to a more responsible security culture within the organization;

– forecasting and preventative measures. Understanding current and potential threats allows organizations not only to respond to incidents but also to take proactive measures to prevent them.

The purpose of this study is to analyze the factors that pose the main threats to organizational information security so that they can build a robust defense system, which is impossible without up-to-date knowledge of current cyberattack trends.

2. Research into the main threats in the field of information security

Cybersecurity research shows that government agencies, industry, defense enterprises, and the financial sector will be the most frequently targeted by malicious campaigns in 2025 (Figure 1).

As a result of such attacks, organizations and government agencies lose confidential information (personal data, trade secrets, documents), suffer direct financial losses, experience downtime of critical services, and even risk human life (for example, during attacks on healthcare facilities, energy systems, and transportation).

Experts point to a variety of threats: theft of military secrets, disruption of vital facilities, large-scale hacker campaigns, and long-term espionage. The main consequences of cyberattacks (the percentage of successful attacks) worldwide in 2025 are shown in Figure 2.

Data on the main consequences of cyberattacks worldwide in 2025 shows that almost two-thirds (64%) of successful attacks on organizations resulted in leaks of confidential information, while disruptions to the organizations' core business accounted for 47%.

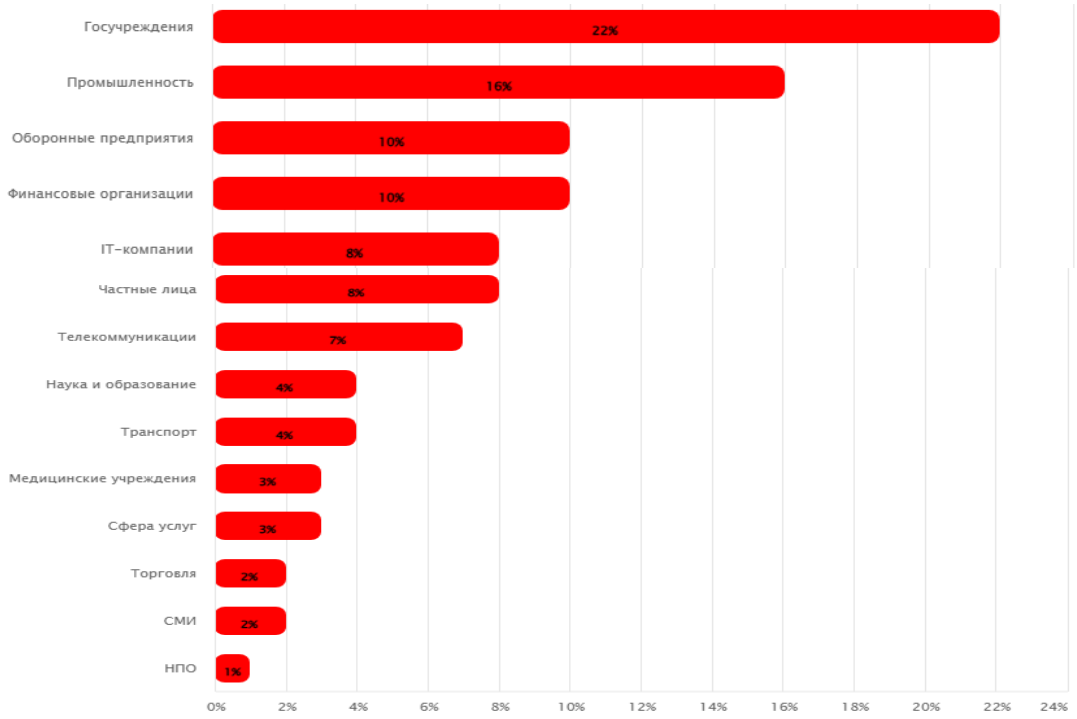


Figure. 1. The areas of activity of organizations around the world that are subject to cyberattacks by malicious campaigns in 2025

Source: Attack trends in 2026

Other consequences (use of organizational resources, damage to state interests, direct financial losses to the organization, and others) together accounted for 27%.

Technological changes associated with the use of artificial intelligence (AI) tools are among the main threats to information security.

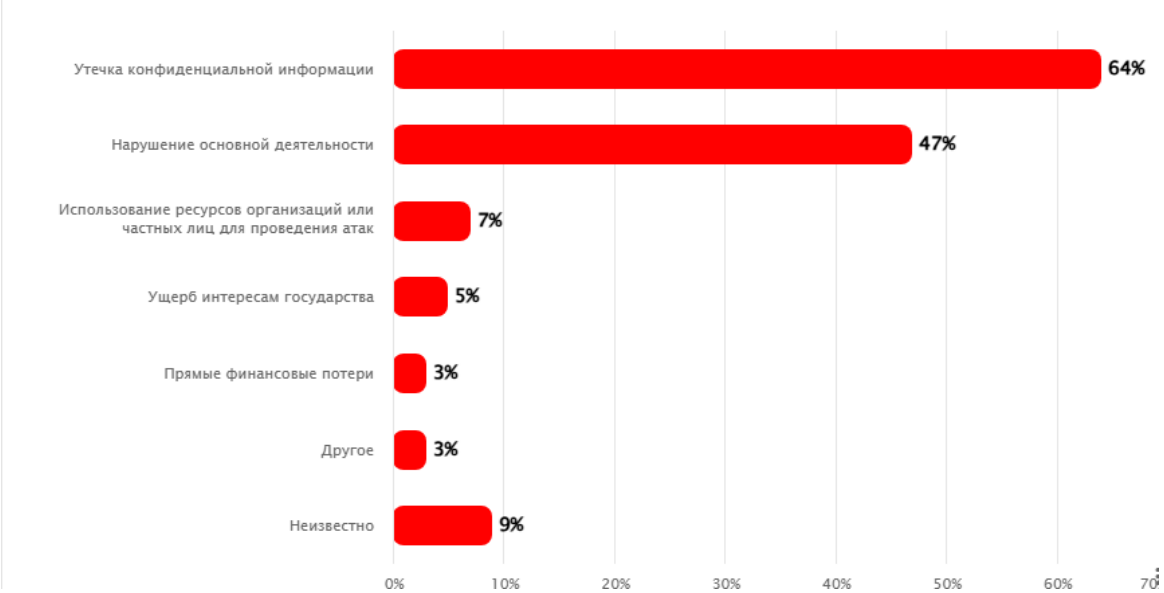


Figure. 2. The main consequences of cyberattacks (the share of successful attacks) in the world in 2025

Source: Attack trends in 2026

Artificial intelligence is not only a tool for business and science, but also a new resource in the arsenal of cybercriminals. The main risks of using AI, the directions of AI use in the development and evolution of malware, and important aspects of using AI in social engineering are presented in Table 1.

Table 1. Threats associated with the use of AI technologies

Type of threat	Characteristics
1. Risks of using AI and their characteristics	1. Attack automation. AI can be used to automate cyberattacks such as phishing, password cracking, or distributed denial-of-service (DDoS) attacks. Algorithms can analyze vulnerabilities and find ways to exploit them faster and more efficiently than humans could. 2. Advanced data analysis. AI can process and analyze large volumes of data, which can be used by attackers to identify vulnerabilities in security systems or to create targeted attacks based on collected user information. 3. Creating fake content. Using technologies such as generative neural networks, it's possible to create fake images, videos, or text, which can lead to disinformation and manipulation. 4. Circumventing security systems. AI can be used to develop methods to bypass intrusion detection systems and other defense mechanisms, making them less effective.
2. Directions for the use of AI in the development and evolution of malware	1. Adaptive attacks. AI can be used to create malware that can adapt to different conditions and systems. For example, such programs can analyze the defenses on the target system and modify their attack methods to bypass these defenses. 2. Phishing automation. AI can be used to automate phishing attacks. Algorithms can analyze social media and other information sources to create convincing fake messages that are sent to specific users based on their interests and behavior. 3. Malicious code generation. Using generative neural network technologies, it is possible to create new malicious code that is unique and less detectable by antivirus programs. This can significantly increase the effectiveness of malware. 4. Targeted learning. AI can be used to gather information about targets by analyzing data from open sources such as social media, websites, and databases. This allows attackers to better understand their victims and plan more effective attacks.
3. Basic aspects of using AI in social engineering	1. Attack personalization. AI allows attackers to collect and analyze data about their victims, such as their interests, behavior, and social connections. This allows them to create personalized messages that are more convincing and believable, increasing the likelihood of an attack's success. 2. Behavioral analysis. AI can be used to analyze user behavior online, identifying patterns and anomalies. This helps attackers understand when and how best to attack, as well as predict how victims will react to certain actions. 3. Content generation. AI-based text generation technologies, such as GPT, can create plausible and well-formed messages. This allows attackers to generate fake messages from trusted sources, such as colleagues or well-known companies

Source: Pugacheva, O. (2024)

An analysis of the table's information allows us to draw the following conclusions:

– taking into account the identified risks, it is important to develop strategies to minimize them and ensure the safe use of AI technologies in information security;

– AI significantly enhances the capabilities of malware, making it more complex, adaptive, and difficult to detect, creating significant challenges for cybersecurity professionals, who must constantly update their defenses and respond to new threats;

– AI significantly expands the capabilities of social engineering, making attacks more targeted and effective. This creates significant challenges for organizations and individuals, who must be more aware of potential threats and develop critical thinking skills to protect against manipulation.

Thus, the threat of cyberattacks affects national security, the economy, and society, making cybersecurity and the fight against these threats an urgent priority.

3. Analysis of factors posing the main threats in the field of information security of organizations

Let us consider the main factors that have the greatest impact on the information security of organizations (Table 2).

Table 2. List of factors, their designation and characteristics

Factor	Designation	Characteristic
1. Human factor	x_1	Employee errors, lack of awareness of cyber threats, and a lack of security culture can lead to data breaches and other incidents.
2. Technological infrastructure	x_2	Outdated systems, software, and poorly secured networks can become vulnerabilities to attack.
3. Security policies and procedures	x_3	Having clear security management policies and adhering to standards is critical to protecting information.
4. Threat level	x_4	Constantly evolving cyber threats, including malware, phishing, and zero-day attacks, require constant monitoring and adaptation of security measures.
5. Regulatory compliance	x_5	Organizations must follow legal and industry standards (e.g., GDPR, HIPAA) to avoid legal consequences and penalties.
6. Access control system	x_6	Effective management of access rights to data and systems helps prevent unauthorized access and information leaks.
7. Incident planning	x_7	Having an incident response plan allows you to respond quickly and effectively to cyberattacks, minimizing damage and downtime.

Expert methods can be used to study the factors that pose the main threats to organizational information security. One such method is ranking, which involves arranging objects (factors) according to their significance or influence. Each object is assigned a unique rank: from 1 (most important) to n (least important). This method is convenient for subsequently calculating the Kendall Concordance Coefficient (W), a statistical indicator reflecting the degree of consistency in the ranks assigned by experts to the same objects (Grachev, 2018). Ranking may vary depending on the specific organization and its specifics, but in general, the factors presented have a given degree of importance.

To assess the factors that have the greatest impact on organizational information security, in the case of unrelated ranks, the experts assigned them as follows (Figure 1).

	Факторы							
Эксперты	x1	x2	x3	x4	x5	x6	x7	$\Sigma (j=1,m)\ x_{ij}$
1	3	6	7	2	5	1	4	28
2	4	5	6	3	7	2	1	28
3	2	7	5	4	6	1	3	28
4	5	4	6	1	7	3	2	28
5	1	6	7	3	5	2	4	28
$\Sigma (i=1, n)\ x_{ij}$	15	28	31	13	30	9	14	140
Отклонение от средней	-5	8	11	-7	10	-11	-6	0
Квадрат отклонения от ср.	25	64	121	49	100	121	36	**516**

Figure 1. Matrix of unrelated ranks assigned by experts to factors influencing an organization's information security

The following formula is used to calculate the coefficient of concordance:

$$W = \frac{12 \cdot S}{m^2(n^3 - n)}, \quad (1)$$

where:
S – is the sum of squared deviations of the sum of ranks from the mean value,
m is the number of experts,
m – is the number of experts,
n – is the number of factors.

Substituting the corresponding values from the table in Figure 1 into formula 1, we obtain:

$$W = \frac{12 \cdot 516}{5^2(7^3 - 7)} = 0{,}737$$

The obtained value of W = 0.737 indicates a high level of agreement between expert opinions regarding the ranked factor scores.

To test the statistical significance of the obtained value of the concordance coefficient W, the Pearson goodness-of-fit test is used:

$$\chi^2 = m(n-1)W \quad (2)$$

Substituting the obtained value W into formula 2, we obtain:

$$\chi^2 = 5(7-1) * 0{,}737 = 22{,}114$$

Thus, the calculated value of the Pearson goodness-of-fit criterion is $\chi^2 = 22{,}114$, and its tabular value is $\chi^2 = 12{,}59$. Since the calculated value of the criterion is greater than its tabulated value, the hypothesis about the randomness of expert opinions is rejected with a probability of 0,95.

As a result, a factor rank chart can be constructed based on their impact on an organization's information security (Figure 2).

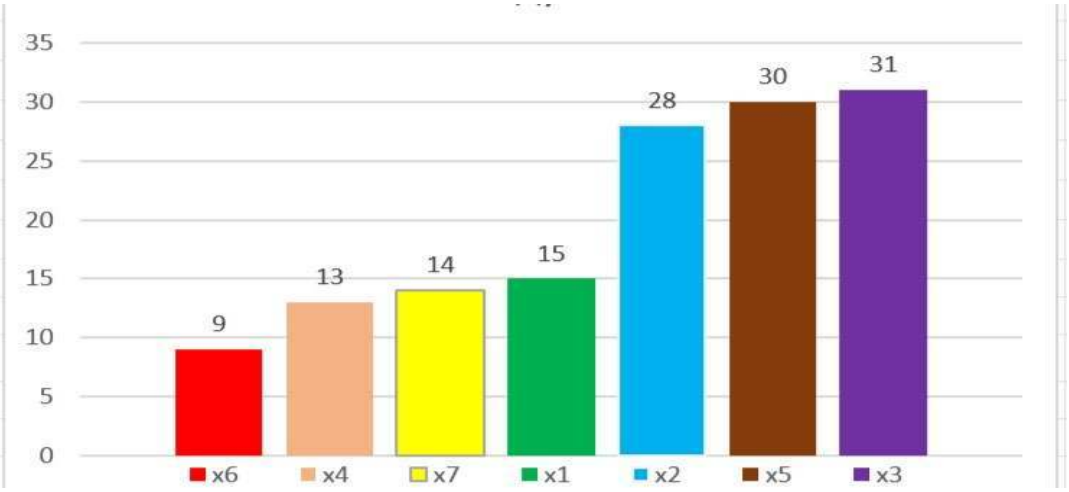


Figure. 2. Diagram of factor ranks according to their impact on an organization's information security

The results show that factor x_6 (access control system) exerts the greatest influence, demonstrating that effective access control that prevents unauthorized access to data is considered the most critical factor in establishing an organization's information security system. This is followed by factor x_4 (threat level), indicating that understanding and adapting to constantly changing threats is crucial for an organization's information protection. Next come factors x_7 (incident planning), as having a response plan helps minimize damage during incidents, and x_1 (human factor), as employee errors and insufficient awareness can lead to serious incidents. This suggests that experts primarily consider the need for effective access control, as well as the threat level, incident planning, and human factor when assessing factors affecting an organization's information security.

The next levels of significance, according to the experts, are observed for factor x_2 (technological infrastructure), as outdated systems and insufficient security create vulnerabilities, and factor x_5 (regulatory compliance), which is important as it is primarily aimed at preventing incidents.

Factor x_3 (security policies and procedures) was found to be the least signifycant, according to the experts, indicating that having clear security management policies and adhering to standards is essential for information protection. However, they consider it a less critical factor in developing an organization's information security system.

Conclusion

Thus, recent years have seen a significant increase in the number, diversity, and distribution channels of cyberattacks, reinforcing the need for continuous improvement of security systems.

Analysis of threat landscapes shows that the main areas of cyberattacks span both the corporate and personal sectors, including stolen data, financial losses, reputational damage, and the loss of confidential information.

One of the current trends is the use of artificial intelligence by cybercriminals, enabling them to automate and sophisticate attacks, as well as create new types of malware and employ social engineering techniques.

To counter new types of threats and minimize risks, organizations must consider the factors that pose the main threats to information security and, based on these factors, develop and implement comprehensive strategies that include constantly updating protection and response methods, as well as training specialists.

References

Attack trends in 2026 (2026). (Access Date 10.06.2026) from: https://ptsecurity.com/research/analytics/trendy-atak-v-2026-godu/#id8 (2026, January 23)

Grachev, A. (2018). Methods of Expert Assessments in Management / A. V. Grachev. – St. Petersburg: Piter.

Pugacheva, O. (2025). Innovative technologies in educational activities and ensuring digital security. *Technological innovations in digital security», international conference* (May 15-16; 2025). Chişinău: SEP ASEM, 168-175.

Pugacheva, O. (2024). Use of artificial intelligence in the economy and society: directions, problems and regulation. *Proceedings of the F. Skorina Gomel State University* (5), 136-141.