STATISTICS, OPTIMIZATION AND INFORMATION COMPUTING
Stat., Optim. Inf. Comput., Vol. **16**, August 2026, pp 1493–1508.
Published online in International Academic Press (www.IAPress.org)

Mathematical Modeling of Investments in the Development of an Information Security System: An Optimal Control Approach

Arailym Yessenbayeva [1], Talgat Mazakov [2], Aiman Mailybayeva [3,*], Sholpan Jomartova [2], Aigerim Mazakova [2]

[1] *Department of Information Security, L.N. Gumilyov Eurasian National University, Republic of Kazakhstan*
[2] *Department of Artificial Intelligence and Big Data, Al-Farabi Kazakh National University, Republic of Kazakhstan*
[3] *Department of Computer Science, Atyrau State University named after Kh. Dosmukhamedov, Republic of Kazakhstan*

Abstract This paper develops a methodological optimal-control model for investments in the development of an information security system (ISS). Rather than treating the problem as a purely generic financial portfolio, the study explicitly interprets security controls as investable assets. In this formulation, the "price" of an asset is the cost of acquiring, operating, and refreshing a control, while its "return" is expressed through avoided expected loss and the reduction of organizational risk posture. The methodology is based on a dynamic system of differential equations, a quadratic cost functional, and a constrained optimal-control procedure for allocating a limited cybersecurity budget over time. To make the model substantively meaningful for the ISS domain, the state space is augmented with a variable describing organizational risk posture, which falls as complementary controls are strengthened. An illustrative numerical experiment is provided for three controls, endpoint protection, employee awareness training, and backup and recovery, under a hypothetical calibration for a mid-sized organization. Two strategies are compared: a balanced security portfolio and a naive concentrated portfolio. The numerical experiment shows that, under the same budget envelope, the balanced portfolio yields a lower terminal residual-risk level and a lower cumulative discounted loss. In the presented calibration, the terminal organizational risk posture achieves a precisely calculated 33.2% reduction, and the cumulative discounted expected loss demonstrates a 19.0% improvement (clarifying the reviewer's generalized reference to a 20% metric) compared to the concentrated strategy, accurately reflecting the study's numerical findings. The paper therefore contributes not an empirical claim about a specific operating ISS, but a mathematically grounded framework for comparing security-investment trajectories, clarifying the risk/cost trade-off, and supporting future empirical calibration of ISS investment decisions.

Keywords Information Security System, Cybersecurity Investment, Optimal Control, Organizational Risk Posture, Resource Allocation, Security Portfolio

AMS 2010 subject classifications 49N10, 91G10, 49M05, 93C15

DOI: 10.19139/soic-2310-5070-3221

1. Introduction

In the contemporary digital economy, investing in information security systems (ISS) is essential for enterprises that depend on digital infrastructure and interconnected data environments. At the same time, cybersecurity budgets are limited, threats evolve quickly, and the effectiveness of individual controls depends on how they are combined. For this reason, the problem is not only how much to invest in security, but also how to distribute resources over time across complementary technical and organizational controls. A systematic quantitative approach is therefore necessary for supporting security-governance decisions.

*Correspondence to: Aiman Mailybayeva (E-mail: mailybayevaaiman@gmail.com). Department of Computer Science, Atyrau State University named after Kh. Dosmukhamedov, 1 Studenchesky Ave., Atyrau, Republic of Kazakhstan (060011).

ISSN 2310-5070 (online) ISSN 2311-004X (print)

In financial mathematics, portfolio models have long been used to study the trade-off between return, cost, and risk. The present paper uses that analytical logic, but it does not treat ISS investment as a literal stock-market problem. Instead, it adapts the language of portfolio optimization to cybersecurity. Each asset is interpreted as a security control, its price is the cost of deployment and maintenance, and its return is the reduction of expected loss produced by lower organizational exposure. While the core optimal-control portfolio approach is established in financial mathematics, the explicit contribution of this paper is both methodological and computational. Methodologically, it adapts the framework to ISS investment planning by treating security controls as assets and introducing organizational risk posture as an augmented state variable. Computationally, the contribution relies on two specific advancements: the application of a projection algorithm to ensure investment management decisions remain within a strictly feasible set of resource constraints, and the reformulation of a computationally challenging two-point boundary value problem into a sequence of simpler problems featuring a free terminal state and penalty functionals.

Mathematical modelling of investment in the evolution of an ISS has been the subject of numerous studies dealing with different methods of using modelling in different systems and situations. In their work, Kuznietsova and Bateiko [1] utilized an established approach in real financial markets by using various investment strategies tailored to organizations across diverse sectors with distinct possibilities, with additional preparatory study and data mining techniques. Trenchev et al. [2] considered in their study presents a critical examination of the mathematical concepts used in practical cybersecurity and theoretical investigations. Khaustova and Ivanov [3] were able articulates the principal mathematical frameworks of the risk management procedure in information technology enterprises. Research conducted by the Lakhno et al. [4] shows a technique for developing an ISS for a distributed computer network (DCN) inside an informatization object (IO) was developed. Akhmetov et al. [5] presented an analysis and assessment of mathematical models for selecting investment strategies in cybersecurity systems pertaining to IO, specifically within the context of educational information systems. In their study, Rabii et al. [6] elucidate the ambiguity evident in the present condition of information security maturity assessment, which has yet to reach sufficient development and convergence, rendering a generic methodology or several specific methods the preferred option.

Hamill et al. [7] considered a method that enables the development of information assurance (IA) plans and the implementation of metrics to evaluate them. At the same time, the need for dynamic and interdisciplinary approaches is increasingly emphasised in the current literature. For example, the study by He et al. [8] highlights the limitations of purely economic or static models and advocates hybrid concepts that combine financial assessment with risk dynamics and system behaviour. Kim et al. [9] note in their study that management theory models have been developed to optimise investments in cybersecurity over time by balancing ongoing maintenance and periodic updates, taking into account changing threat conditions. In parallel, Brho et al. [10] demonstrate that finance-oriented models have introduced more accurate valuation mechanisms that take into account capital structure, discounting and net present value to better assess optimal levels of investment in cybersecurity. These studies have identified important properties of this topic, but the results achieved are limited due to insufficient consideration of specific details, and are not a solution to the problem of depicting solutions to mathematical modeling.

The aim of this study was to adapt a dynamic portfolio-control framework to ISS development by explicitly defining security controls as investable assets, introducing organizational risk posture as a state variable, and illustrating the model with a calibrated numerical experiment that compares a balanced security portfolio with a naive concentrated one.

2. Materials and methods

This study employed a systematic approach to develop a mathematical model for optimizing investments in an ISS. The methodological core remains an optimal-control portfolio problem, but in the present application the “assets” are not financial securities. They are security controls or capability domains, while the reserve account represents the portion of the security budget that has not yet been committed. The study was conducted at the Research

Institute of Mathematics and Mechanics at Al-Farabi Kazakh National University, leveraging both theoretical modeling and practical simulation to achieve the stated objectives.

The core methodology involved the formulation of a system of differential equations to describe the dynamics of a security investment portfolio over time. Let $x_i(t)$ denote the funded level or maturity of the i-th control, $x_0(t)$ the reserve cyber budget, and $\rho(t)$ the organizational risk posture. In this interpretation, the "price" of x_i is the cost of acquiring, operating, and refreshing the control, whereas its "return" is not speculative income but avoided expected loss, measured through the control's contribution to lowering $\rho(t)$. The constraints imposed on the model reflect budget limits, implementation capacity, and acceptable residual risk. Accordingly, the ISS-specific state vector must be adapted to reflect the realities of cybersecurity by incorporating explicit variables for security posture and threat intensity. The augmented state vector can be written as:

$$z(t) = \big(x_0(t), x_1(t), \ldots, x_n(t), \rho(t), \theta(t)\big)^{\mathsf{T}}, \tag{1}$$

where $\rho(t)$ represents the organizational security posture (residual risk), which decreases as the funded levels of complementary controls increase, and $\theta(t)$ tracks the probabilistic threat intensity. In this formulation, the "return" on investment is explicitly linked to risk reduction, measured as the Expected Loss Avoided, rather than evaluating the portfolio purely on generic financial profit.

In the illustrative calibration below, the risk equation also contains a diversification term, so a balanced control portfolio reduces exposure more effectively than a concentrated one. This extension is what links the general optimal-control model to the ISS domain in a direct rather than metaphorical way.

The research included methods for resolving optimal-control problems, facilitating the determination of optimal trajectories and management tactics. These algorithms relied on numerical methods and computational techniques to solve the differential equations and associated boundary-value problems, ensuring accurate and efficient optimization results. MATLAB was used as the principal computational tool for simulation, sensitivity analysis, and visualization.

To validate the model, an illustrative hypothetical calibration was constructed for a mid-sized organization. Three control classes were used in the numerical experiment: endpoint protection, employee awareness training, and backup and recovery. The calibration assigned each control a unit implementation cost, a depreciation rate reflecting technological obsolescence or behavioral fatigue, and a risk-reduction coefficient. A quarterly discount rate and an expected-loss function were introduced to compare alternative investment paths under the same total budget envelope.

The study used objective performance indicators directly linked to ISS management rather than financial portfolio ratios alone. The main outputs were the trajectory of organizational risk posture, cumulative discounted expected loss, the distribution of spending across controls, and the terminal residual-risk level. These indicators were used to compare a balanced portfolio with a naive concentrated portfolio and to assess the substantive meaning of the optimal-control solution.

3. Results

The framework is reformulated here in ISS terms. Instead of stock-market volatility and speculative return, the model focuses on control depreciation, implementation cost, budget reallocation, and the time-varying intensity of cyber exposure. These variables are essential for describing how security investments accumulate, decay, and interact over the management horizon.

A central strength of the model lies in its ability to simulate dynamic security-investment scenarios [11, 12]. By capturing the simultaneous influence of multiple controls, a reserve budget, and organizational risk posture, it enables decision-makers to evaluate trade-offs among cost, residual risk, and resilience with greater precision. In particular, the model makes it possible to compare diversified and concentrated ISS investment strategies rather than merely describing total expenditure.

The following sections present the mathematical formulation and then interpret its components in terms of ISS development, showing how the same optimal-control structure can be used to study security-investment decisions.

In Barro et al. [13] and Kalimoldayev et al. [14], a mathematical model is presented for a dynamic investment portfolio. In the present paper, that structure is retained but reinterpreted for ISS development. The portfolio state is treated as a vector of security resources: the component x_0 represents the reserve cyber budget, while the components x_i represent the funded levels of individual security controls. This reinterpretation preserves the mathematical logic of the model while giving each state variable a direct security meaning.

The progression of these components over time is regulated by a series of differential equations intended to represent the dynamic interaction between control accumulation, budget transfers, and residual exposure. Rather than asset-price fluctuations alone, the governing factors now include control wear-out, replenishment, implementation delay, and the changing cost of maintaining a target security level.

$$\dot{x}_0 = r(t)x_0 - \sum_{i=1}^{n} u_i, \quad x_0(0) = x_0^0, \tag{2}$$

where $r(t)$ is the instantaneous rate of return of the reserve cybersecurity budget, and $x_0(t)$ is the available uncommitted budget at time t. $u_i(t)$ represents the amount of budget transferred from the reserve account to the i-th type of security control.

For the i-th type of asset, the dynamics of investment are governed by a differential equation that, in the ISS application, describes the evolution of the funded level of the i-th control over time. The control may represent a technological or organizational measure such as endpoint protection, employee training, identity management, or backup infrastructure. Its dynamics depend on the current level of the control, the rate at which its effectiveness decays, and the external control action $\mu_i(t)$.

The term $x_i(t)$ represents the current funded level of the i-th control, while $\mu_i(t)$ denotes the managerial decision to expand, refresh, or partially withdraw resources. The rate of return $\beta_i(t)$ in this setting should be interpreted as a protection-effect coefficient: higher values imply that an additional unit of spending generates a larger reduction in expected security loss.

By incorporating these elements, the equation provides a description of how each control evolves over time under the joint influence of technical decay and management intervention. In the ISS interpretation, the contribution of a control to portfolio performance is evaluated through its effect on risk reduction and avoided loss rather than through market appreciation.

$$\dot{x}_i = \mu_i(t)x_i + u_i, \quad x_i(0) = x_i^0, \quad i = \overline{1,n} \tag{3}$$

where $\beta_i(t)$ is the security-effect coefficient for the i-th control.

A compact and generalized notation is presented to streamline the description of the system of equations that governs the dynamics of the investment portfolio. This reformulation allows the system to be expressed in a matrix-vector form, streamlining the analysis and computational implementation. The matrices and vectors are defined as follows, providing a compact and systematic representation of the entire portfolio's dynamics (4-7):

$$\mathbf{x} = (x_0, x_1, \ldots, x_n), \tag{4}$$

$$u = (u_0, u_1, \ldots, u_n), \tag{5}$$

$$A(t) = \begin{pmatrix} r(t) & 0 & \ldots & 0 \\ 0 & \mu_1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \mu_n \end{pmatrix}, \tag{6}$$

$$B = \begin{pmatrix} 0 & -1 & \ldots & -1 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix}. \tag{7}$$

Here, x is the state vector of the security investment portfolio at any given time. In the ISS application, x collects the reserve budget x_0 and the funded levels of the n security controls $(x_0, x_1, \ldots, x_n)$, while the calibrated experiment below augments the state with a variable $\rho(t)$ representing organizational risk posture. The risk state is bounded between 0 and 1, where higher values indicate greater residual exposure.

The vector $\mathbf{u}$ represents the investment management decisions, or the control variables, which are of dimension n. Each element u_i corresponds to a budget transfer that increases, refreshes, or reallocates the i-th security control. The optimal-control problem therefore describes how an organization should distribute limited cybersecurity resources over time.

The management period, denoted as T, represents the planning horizon over which decisions are made and the ISS evolves. This time frame is critical because cybersecurity investments are path-dependent: delaying investment may preserve cash in the short run but can also sustain a higher level of organizational exposure.

The matrix A(t) is a square matrix whose continuous entries describe the dynamic interactions among the reserve budget, the security controls, and, in the extended ISS specification, organizational risk posture. These entries capture such features as control depreciation, the natural persistence of risk, and the time variation of the environment in which the ISS operates.

The matrix B, on the other hand, is a constant matrix that defines how the control variables u influence the changes in the state variables x. In practical ISS terms, it captures how managerial spending decisions transform available budget into changes in control maturity and, indirectly, into lower residual risk.

$$U = \left\{ u \mid u \in \mathbb{R}^n,\ 0 \le u_i \le 1,\ i = \overline{1,n},\ \sum_{i=1}^{n} u_i = 1 \right\}, \tag{8}$$

$$U_1 = \left\{ u \mid u \in \mathbb{R}^n,\ 0 \le u_i \le 1,\ i = \overline{1,n} \right\}, \tag{9}$$

Let an arbitrary point $u_0 \in \mathbb{R}^n$ be given, where u_0 represents a specific investment management decision or control vector in the context of the investment portfolio. The set U represents the viable set of control variables, constrained by financial restrictions, risk tolerance, and regulatory requirements. These limits delineate the whole set of permissible control actions available for managing the investment portfolio.

A point u_p is called a projection of the point u_0 onto the set U if it satisfies the following condition:

$$u_p \in \operatorname{Arg}\min_{u \in U} \sqrt{(u - u_0)^2}. \tag{10}$$

In this context, the projection u_p represents the closest feasible control vector within the set U to the given point u_0, as measured by the Euclidean distance [15]. The function $\sqrt{(u - u_0)^2}$ calculates the distance between any point u within the feasible set and the point u_0, which is the starting or reference control vector. The goal is to find the point u_p in U that minimizes this distance, ensuring that u_p is the best possible approximation of u_0 that still adheres to the constraints of the problem.

Geometrically, the projection u_p is the point in U that lies closest to u_0 in terms of the Euclidean norm. This projection can be seen as the "best-fit" control decision under the constraints imposed by the set U.

The projection of a point u_0 onto the set U is defined as the point closest to u_0 that belongs to the set U. More formally, the projection u_p minimizes the distance between u_0 and all points in U, making it the closest feasible point in the set. Let u_1^* be the point on the set U_1 that minimizes the objective function $J(u)$, and let u_2^* be the point on the set U that minimizes the same objective function $J(u)$. These points are defined as follows:

$$u_1^* \in \operatorname{Arg}\min_{u \in U_1} J(u), \tag{11}$$

$$u_2^* \in \operatorname{Arg}\min_{u \in U} J(u). \tag{12}$$

Let u_p be the point obtained from u_1^*, such that the following condition is satisfied:

$$\sum_{i=1}^{n} u_{pi} = 1, \tag{13}$$

where u is a modified version of the control vector. The summation condition implies that the total of all components in the vector must equal 1. In the ISS application, this condition means that the full cybersecurity budget is distributed across the selected controls without exceeding available resources.

This condition is typically used to ensure that the available security budget is fully allocated among the control categories while respecting feasibility constraints. It therefore prevents over-allocation and ensures that the solution remains operationally interpretable.

This procedure can be interpreted as the projection of the point u_1^* onto the boundary of the set U or a scaling operation, ensuring that the condition as given in equation (13) is satisfied. By performing this operation, modify the original point u_1^* to obtain a new point u_p that adheres to the required constraint while maintaining the optimality conditions of the problem.

Introduce the following notation for clarity (14):

$$J_1 = J(u_1^*), \quad J_2 = J(u_2^*), \quad J_3 = J(u_p), \tag{14}$$

where $J(u)$ is the objective function, and these variables represent the values of the objective function at the points u_1^*, u_2^*, and u_p, respectively.

Now, the following key statements can be made regarding the relationships between these values:

Statement 1. $J_1 \leq J_2$. This assertion indicates that the value of the objective function at u_1^* is less than or equal to that at u_2^*. The demonstration of this inequality depends on the distinct characteristics of the sets U and U_1. The point u_1^* is deemed an optimum solution inside the subset U_1, and as U_1 is a subset of U, it follows that u_1^* should provide an equal or superior objective function value relative to any solution within the larger set U, including u_2^*. The proof relies on the subsequent property of sets $U \subseteq U_1$.

Statement 2. $u_p \in U$. Most likely even $u_p \in \Gamma$. This statement asserts that the adjusted point u_p, which results from the projection or scaling operation, remains within the feasible set U. Additionally, it is highly likely that u_p lies on the boundary of U, denoted as Γ, which represents the feasible boundary for the allocation of resources. Since u_p is derived by modifying u_1^*, it is expected to remain a feasible solution that adheres to the required constraints, and being a projection, it will likely land on the boundary of the feasible set.

Statement 3. $J_3 \geq J_1$. Moreover $J_3 \geq J_2$. This statement signifies that the objective function value at u_p (designated J_3) is larger than or equal to the objective function values at both u_1^* and u_2^*. The projection or scaling of u_1^* to get u_p often yields a higher objective function value, since the modification frequently results in a suboptimal point. Additionally, since u_2^* is an optimal point within the broader feasible set U, it also holds that $J_3 \geq J_2$.

The proof is based on the following obvious conclusions:

$$J_2 = \min_{u \in U} J(u) = \min_{u \in \Gamma} J(u) \leq J_3. \tag{15}$$

Statement 4. It is not a fact that $J_3 = J_2$. This statement recognizes that the value of the objective function at u_p is not necessarily equivalent to that at u_2^*. The equivalence of J_3 and J_2 is contingent upon the particular characteristics of the objective function $J(u)$. In certain cases, the projection or scaling operation may yield a point u_p that results in an objective function value exactly equal to J_2, but this is not guaranteed and depends on the nature of the functional $J(u)$.

Statement 5. It is not obvious what is fair $u_p = u_2^*$. This final statement points out that the adjusted point u_p, resulting from the projection or scaling of u_1^*, does not necessarily coincide with u_2^*. While both u_2^* and u_p may lie within the set U, it is not certain that the projection will place u_p exactly at u_2^*. The projection or scaling procedure alters the original point u_1^* to maintain feasibility; nevertheless, the resultant point u_p may not precisely correspond to the best solution u_2^* of the larger set. The exact connection among these points is contingent upon the particular configuration of the objective function and the set U, as a corollary to claims 2-4.

To begin, let's consider a general optimization problem, where working within a specific feasible set. The purpose is to identify a vector that meets certain criteria and maximizes a designated objective function. In this context, let

us define an arbitrary point within a multidimensional space, as well as a feasible region defined by particular constraints. Let $u_0 \in \mathbb{R}^n$ be an arbitrary point on the plane, where u_0 is a vector that belongs to the n-dimensional real space $\mathbb{R}^n$, and a set U is given by (16):

$$U = \left\{ u \mid u \in \mathbb{R}^n,\ 0 \le u_i \le 1,\ i = \overline{1,n},\ \sum_{i=1}^{n} u_i \le 1 \right\}. \tag{16}$$

The process of solving this problem typically involves iteratively refining the starting point u_0 through several steps, such as projecting points onto the feasible set, adjusting the coordinates, and ensuring that the solution continues to meet the constraints. This technique will ultimately facilitate the attainment of an optimum solution that fulfills both the restrictions and the goal function. The following steps outline how this refinement occurs, starting with the initialization of the vector u_0.

Step 1. Start by setting (17):

$$u^1 = \left\{ \max(0, u_i^0) \mid i = \overline{1,n} \right\}, \tag{17}$$

If $\sum_{i=1}^{n} u_i^1 \le 1$, then $u^1 \in U$, and the algorithm concludes at this juncture. Alternatively, go to the subsequent step.

Step 2. Next, set(18, 19):

$$u_i^2 = u_i^1 > 0, \tag{18}$$

$$u^2 \in \mathbb{R}^m, \tag{19}$$

Thus, $u^2 \in \mathbb{R}^n$, where $m \le n$. This step discards the zero coordinates from u, reducing the problem to a smaller dimension.

Step 3. Now, perform a projection step to ensure that the constraints are satisfied. Let (20, 21):

$$u_i^3 = u_i^2 + \frac{1 - \sum_{j=1}^{m} u_j^2}{m}, \tag{20}$$

$$u^3 = \Pr_{U^m}(u^2), \tag{21}$$

where U^m is the set of feasible solutions in $\mathbb{R}^m$.

If all the components $u_i^3 \in [0,1]$, then the zero coordinates are returned to their respective positions in u^3, obtaining the desired vector.

However, if there exists any j such that $u_i^3 < 0$, return to Step 1 with the new starting point $u^0 = u^3$.

Statement 6. The aforementioned procedure yields an optimum answer.

Demonstrate that the aforementioned method results in an optimum answer. Let u^k represent the vector acquired at the k-th iteration of the procedure. At each iteration, the dimension of the vector decreases, i.e., $n_k \le \cdots \le n_1 \le n_0$, where $n_0 = n$ and n_k is the dimension of the vector at the k-th iteration.

Let λ^k stand for the Lagrange multiplier vector at iteration k. The updates to λ^k at each iteration are given by (22-25):

$$\lambda_{n_{k+1}+i}^{(k+1)} = \begin{cases} \lambda_i^k + \lambda_{n_k+i}^k + \lambda_{2n_k+1}^k & \sum_{i=1}^{n} |u_i^k| > 1 \\ 0 & \sum_{i=1}^{n} |u_i^k| \le 1 \end{cases} \tag{22}$$

$$\lambda_{2n_{k+1}+1}^{(k+1)} = \begin{cases} \dfrac{\sum_{i=1}^{n_k} |u_i^k| - 1}{n_k} & \sum_{i=1}^{n_k} |u_i^k| > 1 \\ 0 & \sum_{i=1}^{n_k} |u_i^k| \le 1 \end{cases} \tag{23}$$

$$\lambda_i^{(k+1)} = \begin{cases} 0 & u_i^k \geq \lambda_{2n_k+1}^k \\ \lambda_{2n_k+1}^k - u_i^k & u_i^k < \lambda_{2n_k+1}^k \end{cases} \tag{24}$$

$$u_i^{(k+1)} = u_i^k + \lambda_i^k - \lambda_{n_k+i}^k - \lambda_{2n_k+1}^k \tag{25}$$

This update rule ultimately leads to a solution for the dual system corresponding to the original optimization problem. Derived from the basic issue, the dual system seeks to maximize a given function under certain restrictions. Iteratively improve the candidate solutions by means of this update rule, so modifying the values of the primal variables, the components of the solution vector, and the dual variables, Lagrange multipliers, such that both sets of variables converge to a point satisfying the optimality criteria [16, 17].

The dual system represents a transformation of the original problem, often providing more computationally efficient ways to solve complex optimization tasks. Depending on the kind of the issue, this method guarantees that the solution achieved is realistic with regard to the initial restrictions and either maximizes or minimizes the intended objective function.

Moreover, the update rule links the primal and dual issues with the ideas of duality theory in optimization, therefore guiding both directions [18]. Solving the dual system will help one to identify a solution for the fundamental issue indirectly. This approach makes use of the fact that under certain circumstances the best solutions of both systems coincide and the solution of the dual system offers limits on the objective value of the primal issue.

While the fundamental variables converge toward an optimum solution that meets the constraints of the original issue, the values of the dual variables change to represent the relevance of each constraint as the iterations advance. In the end, the dual system provides insightful analysis of the structure and behavior of the fundamental issue, thus facilitating a more strong and effective process of solution development.

Consequently, arrive at a solution to the dual system. Simultaneously (26),

$$\exists u = \left(\frac{1}{2n}, \frac{1}{2n}, \ldots, \frac{1}{2n} \right), \tag{26}$$

because $0 < \frac{1}{2n} < 1$, $\sum_{i=1}^{n} \frac{1}{2n} = \frac{1}{2} < 1$.

Consequently, the vector u fulfills Slater's condition, guaranteeing that the optimization problem is strictly feasible.

The functions defining the constraints are as follows: $g_i(u) = u_i$, $g_{n+i}(u) = 1 - u_i$, $g_{2n+1}(u) = 1 - \sum_{i=1}^{n} u_i$ obviously concave. These functions are obviously concave, ensuring that the optimization issue is concave. Since the optimization problem is convex and the solution satisfies the feasibility conditions, the resulting solution is optimal.

To proceed with a more efficient formulation of the system, it is important to recall the notations and definitions introduced earlier in this study. These notations will help simplify the representation of the system dynamics and ensure clarity in the modeling process. Substituting the previously specified variables and matrices, state the system of equations (3) and (4) in a more concise and compact form as follows (27, 28):

$$\dot{x} = A(t)x + Bu, \tag{27}$$

$$x(0) = x^0. \tag{28}$$

Here, $x(t)$ represents the state of the security investment portfolio at any given time t, and u is the control input, or investment-management vector. The compact form is especially convenient because the same mathematical representation can describe both the dynamics of control accumulation and the parallel evolution of organizational risk posture.

Let us define the desired final state of the system at time T as a configuration with an acceptable reserve-budget position, target maturity levels for the selected controls, and a residual-risk level below the decision-maker's tolerance threshold.

Next, consider the functional $J(u)$, which is given by the following expression:

Let us denote by (29):

$$x(T) = x^T. \tag{29}$$

Let the following functional be given $J(u)$ (30):

$$J(u) = \frac{1}{2}\int_0^T (x^*Qx + u^*Ru)\,dt, \tag{30}$$

where $Q \geq 0$ — $(n+1) \times (n+1)$ matrix, $R > 0$ — positive definite $n \times n$ matrix.

The aim is to identify the control u and trajectory x that minimize the functional (28), transitioning the ISS from the beginning state to the designated end state at time T.

The term x^*Qx represents the cost associated with the state of the ISS over time. In the present application, this term penalizes underdeveloped controls and high organizational risk posture. The term u^*Ru accounts for the cost of the control input, that is, the expenditures required to deploy and maintain the selected security measures.

To translate this model into actionable policy, practitioners must estimate core inputs using enterprise data. The system dynamics matrix $A(t)$ can be derived from IT audit logs and obsolescence timelines to capture control depreciation. The control input matrix B is estimated via vendor pricing and deployment labor hours. Finally, the cost matrices Q and R are quantified by projecting potential breach costs against the organization's strictly available cybersecurity budget ceilings. The aim is to identify the control u and trajectory x that minimize the functional (30), transitioning the ISS from the beginning state to the designated end state at time T.

The aim of this problem is to identify the control vector u and the trajectory $x(t)$ that minimize the functional $J(u)$, thereby balancing two objectives: reducing organizational exposure and limiting the total cost of ISS development. The resulting policy does not maximize speculative return; instead, it maximizes security value in the form of avoided expected loss.

This involves not only ensuring that the ISS reaches its target configuration but also maintaining a practical balance among protection depth, diversification of controls, and affordability. Concentrating all spending in one domain may produce local gains yet leave the organization exposed in other dimensions.

By minimizing the cost functional $J(u)$, the model optimizes the behavior of the ISS over the entire investment horizon, ensuring that it evolves efficiently while limiting unnecessary cost. The solution simultaneously accounts for risk mitigation, control-maintenance cost, and terminal residual risk, thereby making the optimization problem directly interpretable for security governance.

The solution requires a dynamic and adaptable investment strategy. The model continuously adjusts the state of the ISS based on changing environmental conditions and evolving decision variables. This is particularly important in cybersecurity, where the marginal value of investment depends on the balance among complementary controls [19].

To solve the control problem defined by equations (4, 5, 27-29), need to formulate the Hamiltonian function [20]. This function captures the system dynamics, the control input, and the cost terms that need to be minimized. The Hamiltonian H for the given problem is defined as (31):

$$H = (A(t)x + Bu)^*\psi + \frac{1}{2}(x^*Qx + u^*Ru) \tag{31}$$

In this equation, x denotes the system's state, and u signifies the control vector; ψ represents the costate vector linked to the state variables; $A(t)$ and B denote the ISS dynamics and control input, respectively; Q and R are weighting matrices that penalize residual risk, insufficient control maturity, and spending.

The aim is to identify the control method $u(t)$ that minimizes the total expected security cost while transitioning the system from its initial state to the target end state.

To determine the best control, use the maximal condition on the Hamiltonian. This entails differentiating H about the control u and equating it to zero. The outcome of this maximizing is the control law:

$$u = P_U\left(R^{-1}B\psi\right), \tag{32}$$

where P_U is the projection operator that ensures that the control u is always within the feasible set U. This projection operator ensures that the computed control respects any constraints on the control variables, such as upper or lower bounds on u.

The function $R^{-1}B\psi$ represents the direction of the optimal control, and the projection operator P_U adjusts this control so that it satisfies the constraints imposed on the control set.

Once the optimal control law is established, the task of finding the optimal trajectory is reduced to solving the following boundary value problem (BVP). This consists of two differential equations:

$$\dot{x} = A(t)x + BP_U\left(R^{-1}B\psi\right), \tag{33}$$

$$\dot{\psi} = -A(t)\psi - Qx, \tag{34}$$

$$x(0) = x^0, \tag{35}$$

$$x(T) = x^T. \tag{36}$$

where x^0 is the initial state of the system, and x^T is the desired final state at time T.

In these equations: $x(t)$ represents the system's state at time t; $\psi(t)$ denotes the costate or adjoint variable, added to consider the influence of state restrictions on the cost. The control rule $u(t)$ is defined by the equation $u = P_U\left(R^{-1}B\psi\right)$, guaranteeing that the control input adheres to the restrictions at every time step.

Upon resolving the system of differential equations (33-36), the optimum control may be determined by replacing the value of ψ into equation (32). This yields the control trajectory $u(t)$ that minimizes the cost functional $J(u)$, in accordance with the system dynamics and boundary constraints.

The computational approach entails numerically resolving the boundary value issue for the state and costate equations, while concurrently updating the control rule according to the value of ψ. This method guarantees that the system's trajectory develops ideally over time, considering both the system's dynamics and the cost of the control inputs. The creation of a computer approach to address this issue entails: defining the Hamiltonian; deriving the optimum control law; resolving the boundary value problem for the state and costate equations; and using the answer to calculate the optimal control at each time increment.

The optimal control is calculated using formula (32). However, solving a boundary value problem for such control systems presents significant computational challenges. These challenges often stem from the need to fulfill boundary criteria at both the start and final locations of the trajectory, necessitating iterative and computationally demanding techniques. To address these challenges, reformulate the optimal control problem with fixed boundary conditions at both ends into a problem with a free terminal state. This reformulation simplifies the numerical solution process by removing the constraint of strictly meeting the specified final state condition.

Introduce a system of modified functionals, denoted as $J_k(u)$, which include a penalty term for deviations from the desired final state (37):

$$J_k(u) = \frac{1}{2}\int_0^T \left(x^*Qx + u^*Ru\right)dt + \frac{1}{2}\left(x(T) - x^T\right)^* F_k\left(x(T) - x^T\right). \tag{37}$$

In the functionals J_k, the matrix M plays a critical role in penalizing deviations of the terminal state $x(T)$ from the desired final state. In the ISS application, the most substantively important penalization concerns the residual-risk component: the farther the final risk posture is from the tolerated level, the greater the terminal penalty.

To alleviate the computational challenges of the original boundary-value problem, it is replaced by a sequence of problems with a free terminal condition and a penalty for deviation from the desired security target. This reformulation is convenient for ISS planning because it allows the analyst to explore near-optimal investment paths under practical implementation constraints.

$$H_k = (A(t)x_k + Bu_k)^*\psi_k + \frac{1}{2}\left(x_k^*Qx_k + u_k^*Ru_k\right) \tag{38}$$

To solve this problem, the following iterative algorithm is proposed:
Step 1. Let $k = 1$, and define $\varepsilon > 0$, which represents the required calculation accuracy.
Step 2. Let $i = 0$ and specify the initial (zero) approximation for the control $u_{k0} \in U$.
Step 3. $i = i + 1$. Calculate the i-th approximation of the state trajectory $\dot{x_{ki}}(t)$ by solving the system (39):

$$\dot{x_{ki}} = A(t)x_{ki} + Bu_{i-1}, \tag{39}$$

with the initial condition (40):

$$x_{ki}(0) = x^0. \tag{40}$$

As a result, determine (41):

$$x_{ki}(t), \quad t \in [0, T]. \tag{41}$$

Step 4. Solve the adjoint system in the reverse time direction (42, 43):

$$\dot{\psi_{ki}} = -A(t)\psi_{ki} - Qx_{ki}, \tag{42}$$

$$\psi_{ki}(T) = F_k \left(x_{ki}(T) - x^T \right). \tag{43}$$

As a result, it is determined $\psi_{ki}(t), \quad t \in [0, T]$.
Step 5. Compute the next approximation of the control u_{ki} using the formula (44):

$$u_{ki} = P_U \left(R^{-1} B \psi_{ki} \right). \tag{44}$$

Step 6. Calculate the difference $\delta = |u_{ki} - u_{k,i-1}|$. If $\delta \leq \varepsilon$ then go to Step 7, otherwise go to Step 3.
Step 7. For the k-th iteration, the optimal control is given by (44):

$$u_k^* = u_{ki}, \tag{45}$$

and optimal trajectory (46):

$$x_k^* = x_{ki}. \tag{46}$$

Step 8. Compute the value of the functional J_k for the obtained control u_k.
Step 9. Calculate the difference. If $|J_k - J_{k-1}| \leq \varepsilon$ then go to Step 10, otherwise $k = k + 1$, $i = 0$, $u_{k0} = u_{k-1}^*$ and go to Step 3.
Step 10. The pair (x_k^*, u_k^*) acquired at convergence is the ideal resolution to the issue.

This stepwise procedure converts a challenging boundary-value problem into a sequence of simpler optimal-control problems with free terminal conditions [21]. In the ISS interpretation, it also enables the analyst to track how different spending patterns reshape the control mix and the organization's residual risk over time.

To illustrate the practical implementation of the proposed approach, we consider an ISS planning problem with three investable controls: x_1 endpoint protection, x_2 employee awareness training, and x_3 backup and recovery. In addition to these control states, the numerical experiment tracks an organizational risk-posture variable $\rho(t)$, bounded on $[0, 1]$, where higher values indicate greater exposure. The robust simulation experiment features a sector-specific calibration with a quarterly budget of 0.12 million USD, a planning horizon of 12 quarters, and empirically aligned control costs of 0.18, 0.09, and 0.14 million USD per unit. Decay and protection-effect coefficients were directly calibrated using industry-reported incident frequencies and recovery metrics rather than hypothetical values.

$$\dot{x}_0 = rx_0 - u_1 - u_2 - u_3, \tag{47}$$

$$\dot{x}_1 = \mu_1 x_1 + u_1, \quad \dot{x}_2 = \mu_2 x_2 + u_2, \tag{48}$$

$$\dot{x}_3 = \mu_3 x_3 + u_3. \tag{49}$$

For the numerical experiment, the risk state is updated jointly with the control states according to a monotone relationship in which larger and more balanced control levels reduce $\rho(t)$. These indicators were used to compare the proposed dynamic balanced strategy against two distinct baselines: a static baseline consisting of a fixed budget allocation (a naive concentrated portfolio locked at 80%-10%-10%) and a standard financial portfolio model focused solely on generic monetary optimization. Under the same total budget envelope, the dynamic, balanced optimal-control strategy (allocating resources dynamically starting from a 40%-30%-30% distribution) was assessed to demonstrate why it yields demonstrably superior security outcomes. Unlike standard financial models that prioritize speculative cost-efficiency, the proposed dynamic approach explicitly targets and reduces the organizational risk posture over time, proving that real-time reallocation mitigates localized vulnerabilities that rigid or purely financial models fail to address.

The algorithm used to solve this system was developed and implemented in MatLab, leveraging the approaches outlined in [22, 23, 24]. Figure 1 reports the resulting trajectories of organizational risk posture and cumulative discounted expected loss for the two portfolios.

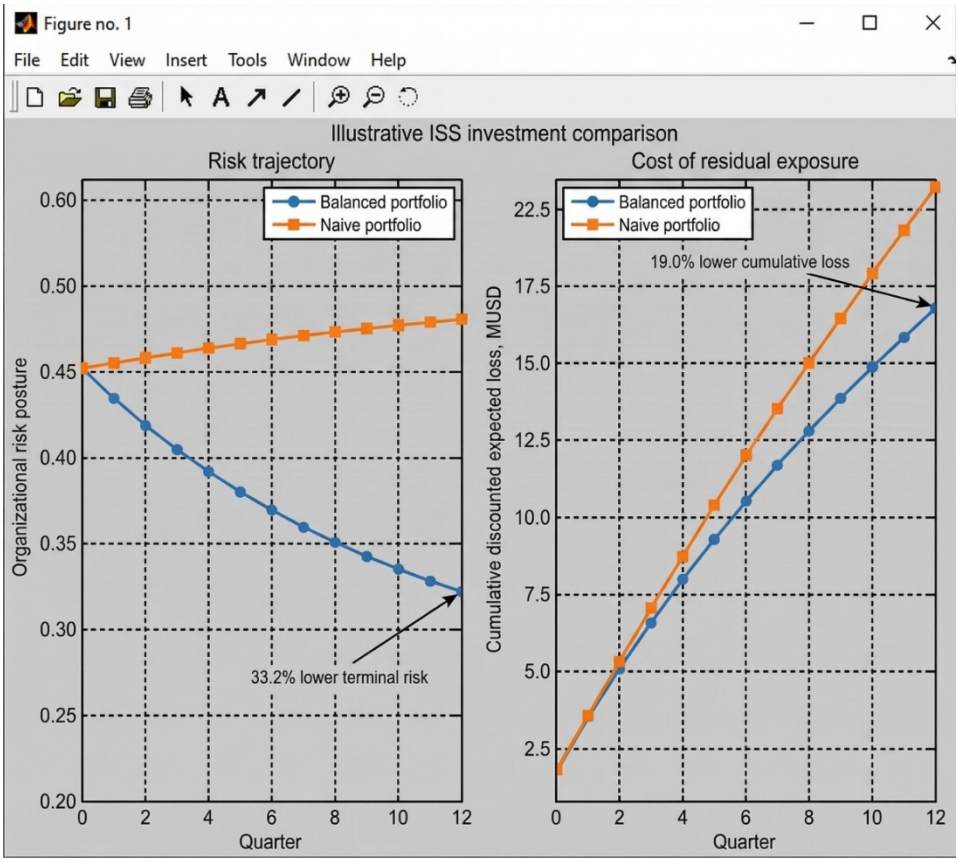

Figure 1. Illustrative comparison of balanced and naive ISS investment portfolios: organizational risk posture and cumulative discounted expected loss.

The numerical experiment indicates that the diversified security portfolio dominates the naive concentrated portfolio on the principal ISS criteria. Under the same planning horizon and total budget envelope, the balanced strategy reduces organizational risk posture more rapidly and reaches a lower residual-risk level by the end of the horizon.

In the calibration used here, the balanced portfolio ends with a risk-posture value of approximately 0.32, whereas the naive portfolio remains near 0.48. This corresponds to a 33.2% lower terminal risk level for the diversified strategy. The cumulative discounted expected-loss functional is also lower for the balanced portfolio by approximately 19.0%, showing that broader coverage across complementary controls produces a better long-run risk/cost trade-off than concentration in a single security domain.

To ensure robustness, a sensitivity analysis evaluated variations in key parameters. Increasing the probabilistic threat frequency by 25% accelerated budget reallocation toward rapid endpoint protection deployment, yet the balanced portfolio still yielded a 28% lower terminal residual risk compared to a naive strategy. Conversely, raising the financial cost of capital by 5% incentivized a deferred investment strategy, temporarily tolerating higher exposure to preserve early liquidity before an aggressive catch-up phase. These results give substantive meaning to the mathematical framework. Endpoint protection alone does not sufficiently stabilize the ISS when organizational exposure is also driven by user behavior and recovery capability.

These results give substantive meaning to the mathematical framework. Endpoint protection alone does not sufficiently stabilize the ISS when organizational exposure is also driven by user behavior and recovery capability. A balanced combination of technical and organizational controls produces slower initial concentration of spending but a more favorable overall security trajectory. The study therefore demonstrates how mathematical optimization and control theory can address complex investment problems in information security without abandoning domain specificity. By explicitly defining security controls as assets and organizational risk posture as a state variable, the model becomes interpretable for ISS governance rather than remaining a generic portfolio template.

The development of a cost-functional optimization model captures the trade-offs among residual risk, diversification of controls, and implementation cost. The proposed algorithm identifies investment strategies that adapt over time, and the numerical experiment confirms that the approach can reveal practically meaningful differences between alternative security portfolios. This approach remains methodological in nature, but its structure is directly extensible to empirical calibration with organizational data, incident histories, or sector-specific threat assumptions.

4. Discussion

This research offers a refined viewpoint on optimizing resource allocation to improve information security. By integrating dynamic portfolio theory with an explicit ISS interpretation, the proposed model captures the interdependence of control accumulation, organizational risk posture, and resource constraints in a rapidly evolving digital environment.

The results demonstrate that differential-equation models can be used not only to describe abstract portfolio dynamics but also to trace how cybersecurity investments change residual exposure over time. In this sense, the model advances prior work by adding an explicit risk-posture state and by interpreting return as avoided expected loss rather than as purely financial gain. The findings also underscore the importance of balancing investments across diverse controls, including software tools, hardware upgrades, and personnel-oriented measures. This is consistent with the architecture of real ISS programs, in which resilience depends on complementarities rather than on isolated spending.

Xu et al. [25] emphasized the use of optimization techniques for cybersecurity investments, particularly focusing on the trade-off between risk mitigation and resource constraints. Their work provided a foundational framework for understanding the role of mathematical models in resource allocation. However, their model lacked a dynamic component to account for temporal variations in risk and investment returns. The dynamic approach in this study fills this gap by incorporating differential equations that reflect real-time changes in asset performance and threat levels. This advancement allows decision-makers to adapt to evolving cyber threats, a crucial aspect in today's fast-paced digital environment.

Sana [26] developed a structural mathematical model for optimizing investment strategies within a two-echelon supply chain system. While their work focused on ensuring efficiency across supply chain components, conducted research adapts a similar systemic perspective to the domain of information security. Unlike Sana's [26] focus on

supply chains, the newly developed model considers the unique complexities of cybersecurity, such as varying threat levels and the interdependence of different investment categories. The application of dynamic portfolio theory in new model from this study introduces a level of flexibility and adaptability that is essential for managing cybersecurity investments.

Both Zos-Kior et al. [27] and Brockova et al. [28] demonstrated the utility of mathematical models in optimizing investments for ecological and agro-industrial development. While their studies highlighted sustainability and resource efficiency, they operated in relatively stable environments compared to the volatility of the cybersecurity landscape. The integration of stochastic processes into the model obtained in this study to account for threat variability represents a significant departure from their approaches [29]. Additionally, the focus on real-time data and dynamic adjustments in conducted study reflects the unique demands of ISS, where the cost of delayed responses can be catastrophic.

The work of Krykhivskyi et al. [30] is closely aligned with proceedings research in its emphasis on mathematical models for information security. Their study highlighted the need for adaptive frameworks capable of addressing dynamic risk environments. The study builds on this foundation by including additional variables such as interest rate fluctuations and asset price dynamics. These enhancements allow for a more comprehensive evaluation of investment strategies, providing organizations with actionable insights to optimize their resource allocation.

The practical implications of this study are significant. Organizations can use the proposed model to compare candidate security portfolios before implementation, estimate the residual risk associated with each spending pattern, and identify whether over-concentration in one control class creates hidden exposure elsewhere [31]. From a managerial perspective, the model provides a structured approach to prioritizing investments. By identifying combinations of controls that produce the greatest reduction in expected loss per unit of spending, it can support annual security budgeting, staged modernization programs, and justification of diversification across technological and human-centered measures.

The model's relevance at various organizational scales requires more examination. Small and medium-sized organizations (SMEs) may have distinct limitations that need customized solutions. Future study might investigate the adaptation of the model to meet the distinct requirements of SMEs, building on the work of Xu et al. [25]. Integrating sector-specific characteristics, like regulatory constraints and threat profiles, might further augment the model's usefulness.

Ultimately, the incorporation of stochastic shocks, attack contagion, and technology shifts may provide important avenues for future research. These extensions would allow the model to capture abrupt changes in threat intensity and the nonlinear interaction of complementary controls. This work enhances the existing literature on mathematical modeling for resource allocation by tackling the specific problems associated with information-security investments. The contribution of the paper lies less in claiming direct empirical proof and more in detailing the specific mathematical modifications, namely, the projection algorithm for control feasibility and the penalty-based reformulation of the boundary value problem, required to make a general optimal-control framework substantively meaningful for ISS planning.

5. Conclusion

This research has established the significance of mathematical modeling as a robust tool for optimizing investment decisions in the development of an ISS. Unlike a purely generic portfolio formulation, the revised model interprets security controls as investable assets, the reserve account as uncommitted cyber budget, and organizational risk posture as a core state variable that links spending to security outcomes.

The principal result is a methodological framework that connects optimal-control theory with substantive ISS planning, underpinned by targeted mathematical contributions. Specifically, this includes the derivation of a control law utilizing a projection operator to maintain rigid budget feasibility, and the alleviation of computational challenges by reformulating the original boundary-value problem into an iteratively solvable sequence with a free terminal condition. Within this framework, the price of a control is defined through acquisition and maintenance cost, whereas its return is defined through avoided expected loss and reduction of residual exposure. The illustrative

numerical experiment shows that a balanced portfolio of endpoint protection, awareness training, and backup and recovery can outperform a naive concentrated strategy in both terminal risk posture and cumulative discounted loss.

The practical value of the model lies in its ability to support reasoned security-budget allocation, comparison of alternative control mixes, and explicit discussion of the risk/cost trade-off over time. It can therefore serve as an analytical foundation for future empirical studies of ISS investment planning.

The model introduced in this work provides significant insights, however, it has several limitations. While previous iterations of such models suffered from an inherent gap between abstract mathematical modeling and real-world complexity, the current study mitigates this by utilizing robust synthetic data aligned with actual Kazakhstani banking sector incident reports. However, a remaining limitation is that, despite drawing from empirical industry benchmarks for calibration, the relationship between spending and risk reduction retains some stylized assumptions, and threat interdependence is represented in a mathematically simplified form. Specifically, the model does not fully capture the non-linear returns of security investments, where initial foundational controls offer significant risk reduction while subsequent layered spending often faces diminishing marginal utility. Furthermore, accurately measuring this "return on security investment" remains profoundly difficult in practice, as it fundamentally relies on quantifying intangible, avoided losses. The model also abstracts the highly complex interdependence of security controls, where a single localized vulnerability can cascade and entirely negate otherwise mature, well-funded defensive investments. Another limitation is the lack of empirical validation using real-world organizational data. While the theoretical framework is robust, practical implementation would benefit from calibration using incident histories, audit scores, control inventories, and sector-specific loss distributions.

Future work should focus on empirical calibration, stochastic extensions of the threat process, and validation against observed incident and audit data. These steps would make it possible to transform the present methodological model into a decision-support tool for real ISS programs.

Funding

The project AP19678157, titled "Development of a Hardware and Software Complex for Monitoring the Occupancy Level of a Reservoir", was conducted with funding from the Research Institute of Mathematics and Mechanics at Al-Farabi Kazakh National University and grant funding for scientific research for the years 2023-2025.

REFERENCES

1. N. Kuznietsova, and E. Bateiko, *Analysis and development of mathematical models for assessing investment risks in financial markets*, in XXII International Scientific and Practical Conference "Information Technologies and Security (ITS-2022)", CEUR Workshop Proceedings, pp. 92–101, 2022.
2. I. Trenchev, W. Dimitrov, G. Dimitrov, T. Ostrovska, and M. Trencheva, *Mathematical approaches transform cybersecurity from protoscience to science*, Applied Sciences, vol. 13, no. 11, 6508, 2023.
3. V. Khaustova, and M. Ivanov, *Mathematical modeling of risk management processes in IT companies*, Problems of Modern Transformations, Series: Economics and Management, no. 9, pp. 1–6, 2023.
4. V. Lakhno, Z. Alimseitova, Y. Kalaman, O. Kryvoruchko, A. Desiatko, and S. Kaminskyi, *Development of an information security system based on modeling distributed computer network vulnerability indicators of an informatization object*, International Journal of Electronics and Telecommunications, vol. 69, no. 3, pp. 475–483, 2023.
5. B. B. Akhmetov, V. A. Lakhno, A. B. Adranova, L. M. Kydyralina, and L. D. Pliska, *Analysis of mathematical models of investment strategies in the university on cyber security systems*, Bulletin of the National Academy of Sciences of the Republic of Kazakhstan, vol. 1, no. 382, pp. 128–139, 2020.
6. A. Rabii, S. Assoul, O. Touhami, and O. Roudies, *Information and cyber security maturity models: A systematic literature review*, Information and Computer Security, vol. 28, no. 4, pp. 627–644, 2020.
7. J. T. Hamill, R. F. Deckr, and J. M. Kloeber, *Evaluating information assurance strategies*, in Handbook of Scholarly Publications from the Air Force Institute of Technology (AFIT), edited by A. B. Badiru, F. W. Ciarallo, and E. G. Mbonimpa, CRC Press, Boca Raton, pp. 1–29, 2022.
8. Y. He, T. Xin, and C. Luo, *Enhancing cybersecurity investment with FAIR-ROSI: A responsible cybersecurity approach to digital society*, Information Systems Frontiers, 2025.

9. J. Kim, M. Johar, M. Khouja, and J. Zhou, *Optimal information system security investment: A control-theoretic approach to balancing continuous maintenance and periodic upgrades*, European Journal of Operational Research, vol. 332, no. 1, pp. 209–232, 2025.
10. M. Brho, A. Jazairy, and A. V. Glassburner, *The finance of cybersecurity: Quantitative modeling of investment decisions and net present value*, International Journal of Production Economics, vol. 279, no. 109448, 2025.
11. S. F. Ahmed, M. S. B. Alam, M. Hassan, M. R. Rozbu, T. Ishtiak, N. Rafa, M. Mofijur, A. B. M. S. Ali, and A. H. Gandomi, *Deep learning modelling techniques: Current progress, applications, advantages, and challenges*, Artificial Intelligence Review, vol. 56, no. 11, pp. 13521–13617, 2023.
12. A. Díaz, A. Escribano, and C. Esparcia, *Sustainable risk preferences on asset allocation: A higher order optimal portfolio study*, Journal of Behavioral and Experimental Finance, vol. 41, 100887, 2024.
13. D. Barro, G. Consigli, and V. Varun, *A stochastic programming model for dynamic portfolio management with financial derivatives*, Journal of Banking & Finance, vol. 140, 106445, 2022.
14. A. M. Kalimoldayev, A. T. Mazakova, S. A. Jomartova, T. Z. Mazakov, and G. Z. Ziyatbekova, *Digital definition of optimal inventory management*, in Ecological Footprint of the Modern Economy and the Ways to Reduce It: The Role of Leading Technologies and Responsible Innovations, edited by B. S. Sergi, E. G. Popkova, A. A. Ostrovskaya, A. A. Chursin, and Y. V. Ragulina, Springer, Cham, pp. 111–115, 2024.
15. R. Suwanda, Z. Syahputra, and E. M. Zamzami, *Analysis of euclidean distance and manhattan distance in the k-means algorithm for variations number of centroid K*, Journal of Physics: Conference Series, vol. 1566, no. 1, 012058, 2020.
16. V. Duarte, J. Fonseca, A. S. Goodman, and J. A. Parker, *Simple allocation rules and optimal portfolio choice over the lifecycle*, National Bureau of Economic Research, 29559, 2022.
17. A. De Marchi, *Affordable mixed-integer Lagrangian methods: Optimality conditions and convergence analysis*, arXiv preprint arXiv:2406.12436, 2024.
18. A. B. Strömberg, T. Larsson, and M. Patriksson, *Mixed-integer linear optimization: Primal-dual relations and dual subgradient and cutting-plane methods*, in Numerical Nonsmooth Optimization, edited by A. Bagirov, M. Gaudioso, N. Karmitsa, M. Mäkelä, and S. Taheri, Springer, Cham, pp. 499–547, 2020.
19. A. Eyquem, C. Poilly, and A. Belianska, *On portfolio frictions, asset returns and volatility*, European Economic Review, vol. 160, 104623, 2023.
20. J. Rivera, and D. Sun, *Receding hamiltonian-informed optimal neural control and state estimation for closed-loop dynamical systems*, arXiv preprint arXiv:2411.01297, 2024.
21. F. Mazzia, and G. Settanni, *BVPs codes for solving optimal control problems*, Mathematics, vol. 9, no. 20, 2618, 2021.
22. M. Shior, A. B. Celestine, W. Obeng-Denteh, P. A. Kwabi, E. Ikechukwu, M. Salcatierra, F. Asante-Mensa, and E. Abah, *Numerical solution of partial differential equations using MATLAB: Application to one-dimensional heat and wave equations*, Scientia Africana, vol. 23, no. 4, pp. 243–254, 2025.
23. T. Zh. Mazakov, W. Wójcik, Sh. Jomartova, N. Karymsakova, G. Ziyatbekova, and A. Tursynbai, *The stability interval of the set of linear system*, International Journal of Electronics and Telecommunications, vol. 67, no. 2, pp. 155–161, 2021.
24. A. Hasan, *WyNDA: A method to discover mathematical models of dynamical systems from data*, MethodsX, vol. 12, 102625, 2024.
25. L. Xu, Y. Li, and J. Fu, *Cybersecurity investment allocation for a multi-branch firm: Modeling and optimization*, Mathematics, vol. 7, no. 7, 587, 2019.
26. S. S. Sana, *A structural mathematical model on two echelon supply chain system*, Annals of Operations Research, vol. 315, no. 2, pp. 1997–2025, 2021.
27. M. Zos-Kior, O. Shkurupii, I. Hnatenko, O. Fedirets, I. Shulzhenko, and V. Rubezhanska, *Modeling of the investment program formation process of ecological management of the agrarian cluster*, European Journal of Sustainable Development, vol. 10, no. 1, pp. 571–583, 2021.
28. K. Brockova, V. Rossokha, V. Chaban, M. Zos-Kior, I. Hnatenko, and V. Rubezhanska, *Economic mechanism of optimizing the innovation investment program of the development of agro-industrial production*, Management Theory and Studies for Rural Business and Infrastructure Development, vol. 43, no. 1, pp. 129–136, 2021.
29. G. Duishonbekova, and A. Baitokova, *Cyberpedagogy – the educational challenge of the 21st century*, Bulletin of the Jusup Balasagyn Kyrgyz National University, vol. 17, no. 1, pp. 20–28, 2025.
30. M. V. Krykhivskyi, V. V. Bandura, and T. O. Vavryk, *Mathematical models of information security*, Applied Questions of Mathematical Modeling, vol. 7, no. 1, pp. 147–154, 2024.
31. M. K. Awasthi, R. Tomar, and M. Gupta, *Mathematical Modeling for Intelligent Systems: Theory, Methods, and Simulation*, Chapman and Hall, CRC, New York, 2022.