DOI 10.37882/2223-2966.2026.03.07

БАЙЕСОВСКИЙ СЕТЕВОЙ ПОДХОД К ОЦЕНКЕ РИСКОВ КИБЕРБЕЗОПАСНОСТИ ВНЕДРЕНИЕ И РАСШИРЕНИЕ МОДЕЛИ FAIR

BAYESIAN NETWORK APPROACH TO CYBERSECURITY RISK ASSESSMENT IMPLEMENTATION AND EXPANSION OF THE FAIR MODEL

M. Zhelenkova
Ya. Goldovsky

Summary. Cybersecurity has become a critical issue for most organisations due to their growing dependence on IT systems and the increasing complexity of the network environment. The article discusses an approach to assessing cybersecurity risks based on the Bayesian network approach and the FAIR model. A comparative analysis of various methods for quantitative assessment and management of cyber risks is conducted. The author describes a methodology for adaptive stochastic cyber resilience management based on a hybrid architecture of dynamic Bayesian networks with continuous time. A mathematical formalisation of the methodology is also presented, based on stochastic differential equations describing the evolution of security parameters over time.

Keywords: information security, risks, model, Bayesian network, assessment, dynamics.

Желенкова Маргарита Борисовна
Ассистент, Российский университет транспорта (МИИТ), г. Москва
vfhujirf5@mail.ru
Голдовский Яков Михайлович
Кандидат технических наук, доцент, Российский университет транспорта (МИИТ), г. Москва
goldovsky_ym@mail.ru

Аннотация. Кибербезопасность стала критически важной проблемой для большинства организаций в связи с их растущей зависимостью от ИТ-систем и увеличением сложности сетевой среды. В статье рассмотрен подход к оценке рисков кибербезопасности на основе байесовского сетевого подхода и модели FAIR. Проведен сравнительный анализ различных методов количественной оценки и управления киберрисками. Описана разработанная автором методология адаптивного стохастического управления киберустойчивостью, базирующаяся на гибридной архитектуре динамических байесовских сетей с непрерывным временем. Представлена математическая формализация методологии, основу которой составляют стохастические дифференциальные уравнения, описывающие эволюцию параметров защищенности во времени.

Ключевые слова: информационная безопасность, риски, модель, байесовская сеть, оценка, динамика.

С ростом проникновения интернет-технологий во все сферы жизни и увеличением сложности сетевой среды, правительства и коммерческие организации стремятся защитить себя от разнообразных киберрисков. Эти риски обычно связаны с утечкой данных, взломом электронной почты, аномальными операциями в сети, такими как принудительные перерывы в работе онлайн-сервисов, которые зачастую приводят к экономическим потерям и другим серьезным последствиям.

Передовые практики кибербезопасности в значительной степени опираются на процесс управления рисками, который включает оценку и контроль различных угроз на информационные системы, подверженные атакам, повреждению или нарушению функционирования, а также обеспечение конфиденциальности, целостности и доступности обрабатываемой в них информации. Одним из общепризнанных процессов управления рисками кибербезопасности является подход, представленный в стандарте ISO/IEC 27005, ориентированный на непрерывную идентификацию, анализ, обработку и мониторинг рисков с целью достижения их приемлемого уровня (CRA) [1].

Факторный анализ информационных рисков (FAIR) является хорошо известной структурой CRA, которая широко применяется и признается, как в академических исследованиях, так и в практических приложениях. В то же время, нехватка данных, особенно исторических о нарушениях кибербезопасности, инцидентах и угрозах, препятствует разработке реалистичных моделей оценки рисков и уязвимости информационных систем. Кроме того, традиционные детерминированные и экспертно-ориентированные подходы характеризуются высокой долей субъективных оценок и ограниченным учетом причинно-следственных зависимостей. Это приводит к значительной погрешности и вариативности результатов при повторных анализах, особенно в динамически изменяющихся условиях [2]. Использование байесовского сетевого подхода в рамках расширения модели FAIR позволяет существенно увеличить число анализируемых факторов и сценариев риска, формализовать неопределённость и снизить среднюю погрешность оценки (см. табл. 1).

Таким образом, принимая во внимание вышеизложенное, задачи разработки модели оценки угроз сетевой безопасности на основе байесовского алгоритма

Таблица 1.

Сравнительный анализ традиционных и байесовских сетевых подходов к оценке рисков кибербезопасности

Показатель	Традиционные подходы	Байесовский сетевой подход
Тип математической модели	Детерминированная / полувероятностная	Вероятностная графовая
Число входных параметров в модели	8–15	20–50
Доля экспертных оценок в исходных данных, %	60–80	20–40
Число учитываемых причинно-следственных связей	≤10	40–120
Учет условных зависимостей	Отсутствует	Формализован
Возможность апостериорного обновления вероятностей	Отсутствует	Реализуется
Количество сценариев риска, анализируемых за один цикл	5–10	50–200
Средняя погрешность оценки годового риска, %	25–40	10–18
Дисперсия результатов при повторных оценках	Высокая	Низкая
Чувствительность к неполноте данных	Высокая	Умеренная
Минимальный объём наблюдений для устойчивой оценки	> 1 года	3–6 месяцев
Возможность учёта каскадных инцидентов	Не реализуется	Реализуется
Поддержка динамического мониторинга	Ограниченная	Полная
Временные затраты на обновление модели	Недели	Часы–дни
Применимость к сложным инфраструктурам	Ограниченная	Высокая

(составлено автором)

с учетом возможностей модели FAIR составляют перспективное направление научного поиска, что и предопределило выбор темы данной статьи.

Особенности факторного анализа информационных рисков, который предоставляет собой таксономическую структуру для классификации угроз кибербезопасности по набору количественно измеримых параметров и сочетает ее с количественными алгоритмами в форме симуляции Монте-Карло, описывают в своих трудах Вильховский Д.Э. [3], Piotr Żebrowski, Aitor Couce-Vieira, Alessandro Mancuso [4], Lei Wei [5].

Возможности динамических байесовских сетей обновлять апостериорные вероятности по мере появления новых записей в журналах или информации об угрозах, что позволяет прогнозировать краткосрочные риски, детально рассматривают Таупыкбай Е.Б. [6], Панилов П.А. [7], Ambairam Muthu Sivakrishna, R. Mohan, Valaparla Rohini [8], Danilo Bruschi [9].

В то же время, несмотря на развитость модели FAIR и активное внедрение байесовских сетей для оценки рисков кибербезопасности, в настоящее время сохраняются нерешённые вопросы, связанные с формализацией априорных распределений вероятностей при дефиците достоверных эмпирических данных и высокой неопределённостью исходных допущений. Кроме того, недостаточно проработаны методы динамического обновления байесовских моделей риска в условиях быстро меняющегося ландшафта угроз и их интеграции с количественными метриками FAIR для поддержки управленческих решений в режиме, близком к реальному времени.

Таким образом, цель статьи заключается в изучении возможностей использования байесовского сетевого подхода к оценке рисков кибербезопасности с расширением модели FAIR.

Традиционные подходы к анализу информационных рисков, включая модели на основе факторного анализа (FAIR) и их расширения через статические байесовские сети, обладают существенным методологическим недостатком — дискретностью и статичностью оценки. Как показано в работах ряда автором, применение байесовских сетей позволяет устранить жесткость распределений (например, треугольных), свойственную FAIR, и учесть причинно-следственные связи [1; 7; 10]. Однако данные модели рассматривают состояние системы как неизменный «снимок», игнорируя временную динамику развития кибератаки и деградацию защитных механизмов.

Очевидно, что в реальности процесс реализации угрозы является многостадийным и стохастическим. Вероятность успешной эксплуатации уязвимости в момент времени $t + \Delta t$ условно зависит от состояния системы в момент времени t. Следовательно, для адекватного моделирования необходимо перейти от статической оценки вероятности событий к оценке интенсивности переходов между состояниями защищенности. В данном контексте особого внимания заслуживают динамические байесовские сети с непрерывным временем, пред-

ставляющие собой направленные ациклические графы, обеспечивающие факторизацию совместного распределения вероятностей. Такие модели состоят из узлов, соответствующих случайным переменным, и дуг, отражающих причинно-следственные или вероятностные зависимости, параметры которых задаются вероятностными весами и в ряде случаев формализуются с использованием статистических либо детерминированных функций.

Для обоснования необходимости перехода к динамическому моделированию целесообразно провести сравнительный анализ эволюции методов оценки киберрисков. В таблице 2 представлено сопоставление классического метода FAIR, его реализации на базе статических байесовских сетей и предлагаемого метода адаптивного стохастического управления.

Итак, используя динамические байесовские сети, представляется возможным связать модель FAIR с другими передовыми моделями CRA для усовершенствования исходной модели оценки рисков кибербезопасности. Для реализации этого динамического подхода автором разработана структурно-функциональная схема, которая формализует контур адаптивного управления киберустойчивостью. Схема базируется на теории стохастического управления и включает объект защиты, подсистему наблюдения и адаптивный регулятор (см. рис. 1).

В рамках разработанного подхода таксономия FAIR трансформируется из статического дерева факторов в структурированное марковское пространство состояний, где каждый узел сети эволюционирует во времени под влиянием своих родителей.

Определим состояние информационной системы в момент времени t как факторизованный вектор $X(t)$, компоненты которого соответствуют ключевым узлам таксономии FAIR. Пусть граф байесовской сети $\mathcal{G} = (V, \mathcal{E})$ состоит из N узлов $X_1, \ldots, X_N$.

В контексте расширенной модели FAIR вектор состояния декомпозируется следующим образом:

$$X(t) = \{X_{TEF}(t), X_{Vuln}(t), X_{Asset}(t), X_{Control}(t)\}$$

где: $X_{TEF}(t)$ — стохастический процесс генерации угроз, принимающий значения из множества состояний активности, атакующего;

$X_{Vuln}(t)$ — текущий статус уязвимости, который изменяется во времени в зависимости от уровня технической реализуемости угрозы и применения обновлений;

$X_{Control}(t)$ — состояние контрмер, изменяемое управляющим воздействием $u(t)$;

$X_{Asset}(t)$ — состояние актива (целевая переменная), определяющая наличие ущерба.

В отличие от стандартных Марковских цепей, где задается одна глобальная матрица переходов, в дина-

Таблица 2.

Сравнительный анализ методов количественной оценки и управления киберрисками

Критерий сравнения	Классическая модель FAIR	Статические байесовские сети	Предлагаемый динамический метод
Учет временного фактора	Статический: оценка риска как «мгновенного снимка» состояния системы на фиксированный период.	Квази-статический: моделирование причинно-следственных связей, но без учета непрерывной эволюции атаки во времени.	Непрерывно-динамический: моделирование эволюции состояния системы $X(t)$ в реальном времени с использованием дифференциальных уравнений.
Математический базис	Арифметические операции над распределениями (Монте-Карло), приближенные методы (PERT).	Теория вероятностей, дискретный байесовский вывод на ациклических графах.	Стохастические дифференциальные уравнения, уравнения Колмогорова-Чепмена, теория оптимального управления.
Метрика риска	Произведение частоты на величину потерь.	Апостериорное распределение вероятностей потерь.	Интегральный функционал риска, учитывающий накопленный ущерб на горизонте планирования.
Моделирование защиты	Статический коэффициент сопротивления.	Условная вероятность блокировки угрозы.	Функция управления, динамически изменяющая матрицу интенсивностей переходов (адаптация).
Работа с неопределенностью	Субъективные экспертные оценки (калибровка).	Снижение энтропии за счет учета свидетельств.	Байесовская фильтрация: непрерывная коррекция оценки состояния на основе зашумленных данных мониторинга.
Тип управления	Реактивный (анализ постфактум).	Поддержка принятия решений «что-если».	Проактивный: автоматическая оптимизация стратегии защиты в замкнутом контуре управления.

(составлено автором)

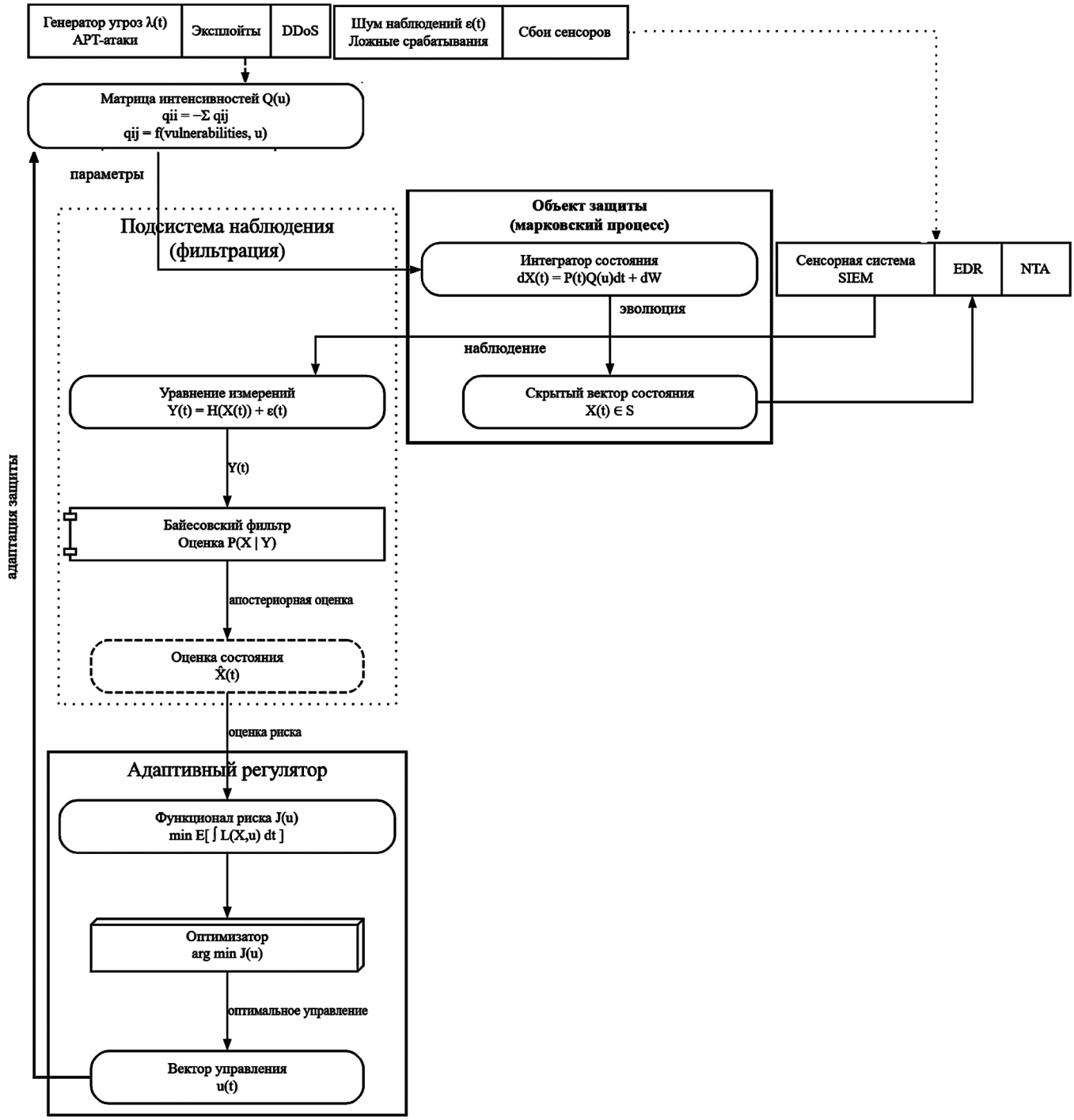

Рис. 1. Схема динамической оценки киберриска на основе гибридных стохастических сетей с непрерывным временем

(составлено автором)

мических байесовских сетях с непрерывным временем динамика определяется набором условных матриц интенсивностей. Для каждого узла X_i сети FAIR динамика изменения его состояния зависит от конфигурации родительских узлов $Pa(X_i)$.

Обозначим $Q_i(u_i)$ как семейство матриц интенсивностей для узла i, параметризованное состоянием родителей $u_i \in Val\left(Pa\left(X_i\right)\right)$. Элемент $q_{xy}^{i|u_i}$ определяет мгновенную вероятность перехода узла X_i из состояния x в состояние y при условии, что родители находятся в конфигурации u_i:

$$q_{xy}^{i|u_i} = \lim_{\Delta t \to 0} \frac{P(X_i(t+t) = y \mid X_i(t) = x, Pa(X_i)(t) = u_i)}{\Delta t}$$

В рамках предложенного подхода интеграция методологии FAIR в структуру динамичной байесовской сети с непрерывным временем реализуется посредством функционального преобразования статических оценок риска в кинетические параметры марковского процесса. Факторы таксономии FAIR (Частота угроз — TEF, уязвимость — Vuln) выступают в качестве аргументов функций, определяющих интенсивности переходов $\lambda(t)$ для целевых узлов сети.

Рассмотрим узел «Состояние актива» (X_{Asset}), родительскими узлами которого являются «Активность угрозы» (X_{TEF}) и «Уровень уязвимости» (X_{Vuln}). Интенсивность перехода актива из защищенного состояния в скомпрометированное ($\lambda_{compromise}$) формализуется как функция от состояний родительских узлов:

$$\lambda_{compromise}(t) = \Psi\left(X_{TEF}(t), X_{Vuln}(t), X_{Control}(t)\right)$$

где Ψ — отображение пространства состояний факторов риска в пространство положительных действительных чисел (интенсивностей).

Для случая, соответствующего логике FAIR (где риск является композицией частоты угроз и уязвимости), условная матрица интенсивностей Q_{Asset} для конфигурации родителей {Threat=активная}, {Vuln=высокая} принимает вид:

$$Q_{Asset} \mid \begin{matrix}\text{Threat} = \text{активная} \\ \text{Vuln} = \text{высокая}\end{matrix} = \begin{pmatrix} -\lambda_{attack} & \lambda_{attack} \\ \mu_{recover} & -\mu_{recover} \end{pmatrix}$$

где: λ_{attack} — параметр, численно равный оценке частоты успешных атак в модели FAIR для данных условий;

$\mu_{recover}$ — интенсивность восстановления работоспособности актива (обратная величина к среднему времени восстановления).

Глобальная динамика всей системы описывается путем амальгамации локальных матриц Q_i. Глобальный генератор Q_{global} формируется как сумма тензорных произведений локальных условных матриц интенсивностей:

$$Q_{global}(X) = \oplus_{i=1}^{N} Q_i\left(Pa(X_i)\right)$$

Эволюция совместного распределения вероятностей $P(X,t)$ описывается системой дифференциальных уравнений Колмогорова-Чепмена, которая в данной постановке приобретает структурный вид:

$$\frac{dP(X,t)}{dt} = P(X,t) \cdot Q_{global}$$

Это уравнение заменяет статичные таблицы вероятностей классических Байесовских сетей на дифференциальные операторы. Оно позволяет рассчитать вероятность реализации риска как мгновенную вероятность нахождения системы в состоянии X_{Asset}= Loss в любой момент времени t, учитывая инерционность процессов атаки и защиты.

Итак, в предлагаемой динамической модели риск трансформируется в функционал. Пусть $L(X_{Asset})$ — функция потерь, определенная на состояниях актива. Тогда мгновенное значение риска $Risk(t)$ представляет собой математическое ожидание потерь по всему ансамблю состояний:

$$Risk(t) = \sum_{x \in Val(X)} L(x) \cdot P(X(t) = x \mid Y_{0:t})$$

Задача управления киберустойчивостью сводится к минимизации интегрального риска на горизонте T путем выбора траектории управляющих параметров $u(t)$ (изменяющих матрицы $Q_{Control}$), что формализуется как вариационная задача:

$$J = \int_0^T e^{-\rho t} Risk\left(t, u(t)\right) dt \rightarrow min$$

Резюмируя вышеизложенное, отметим, что описанная математическая формализация осуществляет строгий перевод статической таксономии FAIR на язык стохастических дифференциальных уравнений на графах, позволяя применять мощный аппарат теории управления для решения задач классификации киберрисков и управления информационной безопасностью.

Таким образом, по результатам проведенного исследования можно сделать такие выводы.

Модель FAIR является эффективной методологией для анализа и расчета рисков кибербезопасности. Однако FAIR делает негибкие предположения, которые ограничивают как ее точность для ряда реальных сценариев, так и возможность интеграции в другие зрелые модели CRA. Кроме того, методология FAIR и ее расширения на базе статических байесовских сетей остаются дискретными инструментами, фиксирующими «мгновенный снимок» состояния системы. В условиях высокой динамики современных киберугроз, где процессы атаки и защиты развиваются непрерывно и стохастически, статичность моделей приводит к существенной недооценке накопленного риска и невозможности оперативного реагирования на изменения ландшафта угроз.

Учитывая отмеченное, в статье предложена методология адаптивного стохастического управления киберустойчивостью, которая базируется на гибридной архитектуре динамических байесовских сетей с непрерывным временем. В отличие от традиционных моделей, где факторы риска (частота событий, уязвимость) являются статичными параметрами, в разработанной методологии они трансформированы в переменные состояния, эволюция которых описывается системой дифференциальных уравнений Колмогорова-Чепмена.

ЛИТЕРАТУРА

1. Вильховский Д.Э. Возможности ИИ в сфере кибербезопасности: вопросы обнаружения, предотвращения и реагирования на SQL-инъекции, XSS- И CSRF-АТАКИ // Математические структуры и моделирование. 2024. № 4 (72). С. 111–124.
2. Володин Д.Н. Исследование подходов математического моделирования рисков в кибербезопасности // Научно-технический вестник Поволжья. 2025. № 6. С. 15–17.
3. Панилов П.А. Использование байесовских моделей и методов Монте-Карло для прогнозирования киберугроз // Вестник Астраханского государственного технического университета. 2024. № 4. С. 79–88.
4. Таупыкбай Е.Б. Особенности исследования и разработки алгоритмов обеспечения безопасности данных для защиты от спама в инфокоммуникационной сети // Интернаука. 2024. № 6. С. 28–31.
5. Хайруллин Э.Р., Вульфин А.М., Васильев В.И. Нейросетевая система обнаружения сетевых атак // Системная инженерия и информационные технологии. 2025. Т. 7. № 1 (20). С. 105–112.
6. Javorník M., Husák M. Mission-centric decision support in cybersecurity via Bayesian Privilege Attack Graph // Engineering Reports. 2022. Vol. 4. No. 12. P. 29–34.
7. Żebrowski P., Couce-Vieira A., Mancuso A. A Bayesian Framework for the Analysis and Optimal Mitigation of Cyber Threats to Cyber-Physical Systems // Risk Analysis. 2022. Vol. 42. No. 10. P. 70–76.
8. Wei L. Application of Bayesian Algorithm in Risk Quantification for Network Security // Computational Intelligence and Neuroscience. 2022. Vol. 19. No. 1. P. 129–134.
9. Muthu S.A., Mohan R., Rohini V. An Efficient Insider Threat Detection Framework Using Bayesian-Optimized XGBoost // Security and Privacy. 2025. Vol. 8. No. 6. P. 63–71.
10. Bruschi D. Ransomware Detection Using Sample Entropy and Graphical Models: A Methodology for Explainable Artificial Intelligence (XAI) in Cybersecurity // Applied Stochastic Models in Business and Industry. 2025. Vol. 41. No. 6. P. 11–18.