УДК 004.896:681.5.015.23
doi: 10.21685/2307-4205-2024-4-8

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ МАШИННОГО ОБУЧЕНИЯ В ЗАДАЧАХ ОЦЕНКИ И ОБЕСПЕЧЕНИИ НАДЕЖНОСТИ ТЕХНИЧЕСКИХ СИСТЕМ С УЧЕТОМ БЕЗОПАСНОСТИ ИХ РАБОТЫ

Е. А. Воронин

Федеральный исследовательский центр «Информатика и управление» РАН, Москва, Россия
e.voronin1@gmail.com

Аннотация. *Актуальность и цели.* Учет внешних угроз и воздействий при оценке надежности технических и информационных систем является критически важным для обеспечения их устойчивости и безопасности. Внешние угрозы могут быть разнообразными: от природных катастроф (землетрясения, пожары, наводнения) до действий злоумышленников (кибератаки, саботаж, вандализм). Учет этих угроз позволяет разработать системы с повышенной устойчивостью к внешним факторам, минимизируя риск сбоев и потерь. Актуальность оценки надежности технических систем в условиях безопасности в последние годы значительно возросла из-за увеличения сложности систем и повышенных требований к их устойчивости перед внешними угрозами и неисправностями. Цель работы – выбрать, разработать и обосновать методы и информационные технологии оценки безопасности сложных систем с учетом их безопасности эксплуатации. *Материалы и методы.* В работе изучены и представлены основные направления исследований в этой области: моделирование надежности, интеграция безопасности и надежности, методы анализа рисков, а также статистические методы и машинное обучение. Рассмотрены основные подходы к решению этой задачи. Показано, что оценка надежности технических систем, учитывающая риски внешних воздействий, требует комплексного подхода, который включает не только анализ собственных свойств системы, но и оценку влияния внешних факторов, нарушающих ее работоспособность. На основании изучения и анализа математических методов решения этой задачи разработаны и представлены математический метод «наивного» Байеса и метод машинного обучения сложной Байесовской сети для оценки вероятности безотказной работы сложных систем с учетом их безопасности. *Результаты и выводы.* Учет внешних угроз и воздействий при оценке надежности технических и информационных систем является критически важным для обеспечения их устойчивости и безопасности. Интеграция машинного обучения Байесовских сетей значительно повышает точность и оперативность оценки их надежности с учетом безопасности.

Ключевые слова: оценка, методы, обеспечение, надежность, достоверность, отказы, вероятность, безотказность, риски, алгоритмы, угрозы, безопасность, искусственный интеллект, машинное обучение, Байесовские сети доверия, ациклические графы

Для цитирования: Воронин Е. А. Применение технологий машинного обучения в задачах оценки и обеспечении надежности технических систем с учетом безопасности их работы // Надежность и качество сложных систем. 2024. № 4. С. 75–84. doi: 10.21685/2307-4205-2024-4-8

THE USE OF MACHINE LEARNING TECHNOLOGIES IN THE TASKS OF EVALUATING AND ENSURING THE RELIABILITY OF TECHNICAL SYSTEMS, TAKING INTO ACCOUNT THE SAFETY OF THEIR OPERATION

E.A. Voronin

Federal Research Center "Computer Science and Control" of the RAS, Moscow, Russia
e.voronin1@gmail.com

Abstract. *Background.* Taking into account external threats and impacts when assessing the reliability of technical and information systems is critical to ensuring their sustainability and security. External threats can be varied: from natural disasters (earthquakes, fires, floods) to actions of intruders (cyberattacks, sabotage, vandalism). Taking these threats into account allows developing systems with increased resistance to external factors, minimizing the risk of failures and losses. The relevance of assessing the reliability of technical systems in a safe environment has increased significantly in recent years due to the increasing complexity of systems and increased requirements for their resistance to external threats and malfunctions. Purpose of the work. Select, develop and justify the methods and information

technologies for assessing the safety of complex systems, taking into account their operational safety. *Materials and methods.* The paper studies and presents the main directions of research in this area. These are: reliability modeling, integration of safety and reliability, risk analysis methods, as well as statistical methods and machine learning. The main approaches to solving this problem are considered. It is shown that the assessment of the reliability of technical systems, taking into account the risks of external influences, requires a comprehensive approach that includes not only the analysis of the system's own properties, but also an assessment of the influence of external factors that disrupt its performance. Based on the study and analysis of mathematical methods for solving this problem, the mathematical method of naive Bayes and the machine learning method of a complex Bayesian network for assessing the probability of failure-free operation of complex systems taking into account their safety are developed and presented. *Results and conclusions.* Taking into account external threats and impacts when assessing the reliability of technical and information systems is critical to ensuring their sustainability and safety. The integration of machine learning in Bayesian networks significantly increases the accuracy and efficiency of assessing their reliability taking into account safety.

Keywords: assessment, methods, provision, reliability, authenticity, failures, probability, reliability, risks, algorithms, threats, security, artificial intelligence, machine learning, Bayesian belief networks, acyclic graphs

For citation: Voronin E.A. The use of machine learning technologies in the tasks of evaluating and ensuring the reliability of technical systems, taking into account the safety of their operation. *Nadezhnost' i kachestvo slozhnykh sistem = Reliability and quality of complex systems.* 2024;(4):75–84. (In Russ.). doi: 10.21685/2307-4205-2024-4-8

Введение

Учет внешних угроз и воздействий при оценке надежности технических и информационных систем является критически важным для обеспечения их устойчивости и безопасности. Это необходимо для повышения уровня защищенности. Внешние угрозы могут быть разнообразными: от природных катастроф (землетрясения, пожары, наводнения) до действий злоумышленников (кибератаки, саботаж, вандализм). Учет этих угроз позволяет разработать системы с повышенной устойчивостью к внешним факторам, минимизируя риск сбоев и потерь.

Сбои в работе технических систем могут иметь серьезные последствия, например, отключение электроэнергии, аварии на транспорте, нарушение работы инфраструктуры. Учет внешних угроз позволяет предусмотреть меры для предотвращения подобных событий, минимизируя потенциальный ущерб.

В условиях внешних воздействий важно обеспечить непрерывность работы систем. Учет угроз позволяет разработать меры, которые позволят системе оставаться работоспособной даже в неблагоприятных условиях.

Сбои в работе технических и информационных систем могут привести к значительным финансовым потерям из-за простоя производства, потери данных, репутационных ущербов и других факторов. Учет угроз позволяет снизить эти риски.

Обзор состояния вопроса [1–26] показал, что оценка надежности с учетом безопасности сложная, многоэтапная задача системного анализа. Для ее решения необходимо знать:

1) методологию системного анализа и общий подход к ее решению;
2) алгоритм оценки безопасности технических систем с учетом их безопасности;
3) математические методы оценки надежности технических систем с учетом рисков внешних воздействий;
4) численные методы, математические модели и программное обеспечение для их реализации.

Уточненная постановка задачи оценки и обеспечения надежности технических систем с учетом их безопасности

Актуальность оценки надежности технических систем (ТС) в условиях безопасности в последние годы значительно возросла из-за увеличения сложности систем и повышенных требований к их устойчивости перед внешними угрозами и неисправностями. Основные направления исследований в этой области:

1. Моделирование надежности: исследования на тему моделирования надежности рассматривают различные подходы, включая стохастические модели, модели на основе событий и структурные модели. Эти методы позволяют учитывать влияние внешних факторов на работу системы [1–3].

2. Интеграция безопасности и надежности: существуют работы, которые исследуют связь между надежностью и безопасностью. Это направление акцентирует внимание на том, как высокая надежность системы может снижать вероятность инцидентов безопасности, и наоборот [2].

3. Методы анализа рисков: методы количественной и качественной оценки рисков, такие как FMEA (анализ видов и последствий отказов) и FTA (анализ деревьев отказов), широко применяются для оценки надежности в контексте безопасности [3, 4].

4. Статистические методы и машинное обучение: использование статистических методов и алгоритмов машинного обучения для прогнозирования отказов и анализа надежности становится все более актуальным. Эти методы позволяют обрабатывать большие объемы данных и выявлять скрытые зависимости [4, 5].

Подходы и рекомендации:

1. Системный подход: необходимо рассматривать оценку надежности и безопасности в рамках целостной системы, учитывая взаимодействие всех компонентов и внешних факторов [1, 2].

2. Мультидисциплинарное исследование: использование знаний из различных областей, таких как механика, электроника и информационная безопасность, может привести к более точным оценкам надежности [2, 3].

3. Применение современных технологий: внедрение машинного обучения и анализа больших данных может значительно улучшить качество оценок надежности и помочь выявить новые уязвимости и риски [4, 5].

4. Постоянное обновление данных: регулярный анализ и обновление данных о состоянии системы и ее окружении помогут лучше предсказывать потенциальные отказы и угрозы [5].

Современные исследования в области оценки надежности технических систем с учетом условий безопасности ставят перед собой важные задачи адаптации к изменяющимся условиям и угрозам. Интеграция различных подходов и использование новых технологий обещают улучшить процедуры оценки надежности, что критично для обеспечения безопасной и устойчивой работы технических систем.

Оценка надежности технических систем, учитывающая риски внешних воздействий, требует комплексного подхода, который включает не только анализ собственных свойств системы, но и оценку влияния внешних факторов, которые могут нарушить ее работоспособность.

1. Идентификация и классификация внешних воздействий:

– анализ окружающей среды: определение климатических условий (температура, влажность, осадки), сейсмической активности, электромагнитных помех, уровня загрязнения и т.д., которые могут воздействовать на систему;

– анализ человеческого фактора: учет потенциальных ошибок операторов, неправильного обслуживания, несоблюдения инструкций и т.д.;

– анализ социальных и политических факторов: оценка рисков, связанных с терактами, саботажем, политическими потрясениями, конфликтами и т.д.;

– анализ технологических факторов: учет влияния других систем, с которыми взаимодействует данная система, внешних источников питания, сетевых сбоев, киберугроз и т.д.

2. Оценка вероятности и последствий внешних воздействий:

– анализ исторических данных: изучение данных о предыдущих инцидентах, связанных с воздействием подобных факторов, для оценки вероятности и серьезности возможных последствий;

– моделирование и прогнозирование: использование математических моделей для прогнозирования вероятности возникновения внешних воздействий и оценки их влияния на систему;

– экспертная оценка: привлечение экспертов в соответствующих областях для оценки вероятности и последствий внешних воздействий.

3. Анализ уязвимости системы к внешним воздействиям:

– анализ чувствительности: определение компонентов и функций системы наиболее чувствительных к внешним воздействиям;

– имитационное моделирование: проведение имитационного моделирования для оценки влияния внешних воздействий на функционирование системы в различных сценариях;

– анализ режимов отказа: идентификация возможных режимов отказа системы под воздействием внешних факторов и оценка их последствий.

4. Внедрение мер по минимизации рисков:

– проектирование для безопасности: включение в конструкцию системы мер по минимизации уязвимости к внешним воздействиям (например, защита от погодных условий, электромагнитных помех, механических повреждений);

– резервирование: внедрение резервных систем или компонентов, которые могут заменить основную систему в случае ее выхода из строя;

– системы раннего оповещения: разработка систем раннего оповещения о неблагоприятных внешних воздействиях для своевременного принятия мер;

– управление рисками: разработка планов реагирования на различные внешние воздействия, обучение персонала, управление информацией и контроль доступа.

5. Постоянный мониторинг и оценка:

– сбор данных о внешних воздействиях: отслеживание изменений в окружающей среде, деятельности человека, технологических условиях;

– обновление оценок рисков: пересмотр оценок вероятности и последствий внешних воздействий с учетом новых данных и изменений в обстановке;

– адаптация мер по минимизации рисков: введение корректировок в конструкцию, эксплуатацию или управление системой с учетом изменений в рисках.

Внедрение вышеизложенного комплексного подхода к оценке и обеспечению надежности технических систем с учетом рисков внешних воздействий позволит повысить их устойчивость и обеспечить непрерывность функционирования в сложных условиях.

Методология обеспечения и оценки надежности технических систем с учетом их безопасности предлагает системный подход.

1. Определение системы и ее контекста:

– идентификация системы: четкое определение границы системы, ее компоненты, функции и взаимодействие с другими системами;

– определение контекста: описание окружающей среды, в которой функционирует система, включая людей, процессы, другие системы и потенциальные угрозы;

– формулировка целей безопасности: установка ясной и измеримыой цели безопасности для системы, которые отражают ее критичность и потенциальные риски.

2. Анализ рисков:

– идентификация опасностей: выявление всех потенциальных опасностей, которые могут привести к нарушению безопасности системы;

– оценка вероятности каждой опасности, учитывая ее источник, частоту и условия возникновения;

– оценка тяжести последствий каждого риска, исходя из потенциального ущерба, который может быть нанесен системе, людям и окружающей среде;

– оценка уровня риска для каждой опасности, используя комбинацию вероятности и тяжести последствий.

3. Анализ безопасности: определяет, как система функционирует в нормальном и аварийном режимах. Проверяется соответствие системы требованиям безопасности, нормативам и стандартам.

4. Меры по снижению рисков:

– разрабатываются меры по снижению выявленных рисков до приемлемого уровня;

– выбираются меры, которые являются эффективными и практичными, учитывая их стоимость, сложность и влияние на производительность системы;

– реализуются выбранные меры, проверяется их правильная работа и тестирование для подтверждения их эффективности.

5. Мониторинг и оценка:

– мониторинг безопасности. Регулярно отслеживается безопасность системы, чтобы выявить изменения в рисках, уязвимостях и угрозах;

– оценка эффективности. Оценивается эффективность реализованных мер по снижению рисков, и при необходимости вносятся коррективы в план безопасности;

– постоянно совершенствование системы безопасности на основе полученных данных и опыта.

Дополнительные шаги:

– документирование. Все этапы оценки безопасности должны быть задокументированы, чтобы обеспечить прозрачность и отслеживаемость процесса;

– обучение. Сотрудники, работающие с системой, должны быть обучены правилам безопасности и процедурам в случае возникновения инцидентов.

Важно отметить, что эта методология является общей схемой, и его конкретные этапы и методы могут варьироваться в зависимости от конкретной технической системы, ее критических функций и контекста использования.

Методика решения задачи оценки надежности технических систем с учетом безопасности

Математические методы играют ключевую роль в разработке надежных и безопасных систем.

Основные математические методы оценки надежности:

1. Вероятностные модели. Вероятностные модели основываются на использовании конечных и бесконечных вероятностных пространств для описания поведения систем, их компонентов и взаимодействий. Эти модели позволяют рассчитывать вероятности отказа, выполнения заданных функций и других характеристик надежности [6, 10].

2. Теория надежности включает такие концепции, как функция надежности, функция распределения времени до отказа, а также модели, основанные на времени до первой неисправности. Здесь же используются также методы анализа временных рядов для оценки надежности систем [7, 8–10].

3. Симуляционные методы, такие как Монте-Карло, позволяют моделировать поведение сложных систем с целью оценки их надежности и устойчивости к сбоям [11].

Наиболее распространенные математические методы:

1) анализ деревьев отказов (FTA);

2) анализ режимов отказов и их последствий (FMEA);

3) моделирование цепей Маркова;

4) метод Байесовских сетей.

Первые три метода фактически являются вариантами представления Байесовских сетей.

Общие определения и математический формализм объединения теории надежности и теории безопасности

По функциональному определению безопасность системы характеризуется отсутствием угроз и способностью ее противостоять внешним угрозам.

Формально ее определяют как вероятность отсутствия угроз и вероятность успешного противодействия им:

$$P_s(t) = 1 - P_u(t) + P_u(t)P(c), \tag{1}$$

где $P(t)-$ вероятность угрозы; $P(c)$ – вероятность успешного противодействия угрозе.

Очевидно, что вероятность отказа системы под воздействием угрозы будет равна

$$P_{ou}(t) = P(o \mid u)P_{ru}(t), \tag{2}$$

где $P(o \mid u)-$ условная вероятность отказа при реализации угрозы.

Вероятность реализации угрозы равна

$$P_{ru}(t) = 1 - P_s(t) = P_u(t)(1 - P(c)). \tag{3}$$

Естественно предположить, что отказы происходят как от внешних воздействий (угроз), так и внутренним причинам, обусловленным собственными особенностями системы. Вероятность такого типа отказов определяется на этапах производства, испытаний и эксплуатации. Обозначим ее как вероятность безотказной работы $P_z(t)$.

Тогда вероятность безотказной работы системы с учетом безопасности ее работы будет равна

$$P_r(t) = P_z(t)(1 - P_{ou}(t)) = P_z(t)(1 - P(o \mid u)P_{ru}(t)) \tag{4}$$

или

$$P_r(t) = P_z(t)(1 - P(o \mid u)P_u(t)(1 - P(c)). \tag{5}$$

Если система состоит из множества $\{e_i, i = 1...n\}$ элементов, на нее действует набор угроз $\{u_j, j = 1...m\}$, вероятность безотказной работы i-го элемента будет равна

$$P_{ri}(t) = P_{zi}(t)\prod_j (1 - P(o_i \mid u_j)P_{uj}(t)(1 - P(c_j)), \tag{6}$$

где $P(o_i \mid c_j)$ – вероятность отказа *i*-го элемента при воздействии *j*-й угрозы; $P_{ri}(t)$ – вероятность безотказной работы *i*-го элемента; $P_{zi}(t)$ – вероятность безотказной работы *i*-го элемента при отсутствии угроз; $P_{uj}(t)$ – вероятность *j*-й угрозы; $P(u_j)$ – вероятность отражения *j*-й угрозы.

Если принять допущение, что отказ любого элемента приводит к отказу системы и угрозы имеют независимое действие, то ее вероятность безотказной работы будет равна

$$P(t) = \prod_i P_{ri}(t) = \prod_i P_{zi}(t) \prod_j (1 - P(o_i \mid u_j) P_{uj}(t)(1 - P(c_j)). \quad (7)$$

Однако это допущение не всегда возможно. Часто угрозы имеют эффект только при совместном действии, а отказ системы происходит при отказе нескольких элементов. В этом случае необходимо изучать и моделировать сложную схему событий, т.е. строить многомерное распределение $P(t) = P(t, u_1, u_2, u_3 .... u_m)$. Лучшим методом решения этой задачи является Байесовская модель в виде Байесовской сети.

Байесовские сети (БС) становятся все более популярными в области оценки надежности технических систем, и это объясняется их важными прикладными возможностями:

1) моделирование неопределенности: БС позволяют эффективно представлять и обрабатывать неопределенности, возникающие в сложных системах;

2) учет взаимосвязей: БС обеспечивают возможность анализа зависимостей между различными компонентами системы, что помогает оценить их влияние на надежность;

3) моделирование вероятности неисправностей отдельных компонентов системы в зависимости от их состояния и внешних факторов [12, 14];

4) анализ уязвимостей: оценка вероятности успешного осуществления атак на технические системы и определение их влияния на общую надежность [13, 15, 16].

Байесовская сеть – это вероятностная модель, которая использует граф для представления наборов переменных и их условных зависимостей.

В ее логической основе лежит цепное разложение многомерного распределения вероятностей, т.е.

$$P(u_1, u_2, u_3 .... u_m, t) = P(u_1, t) P(u_2 \mid u_1, t) P(u_3 \mid u_1, u_2, t) ... P(u_m \mid u_1, u_2 ... u_{m-1}, t). \quad (8)$$

Оно после оценки значений условных вероятностей и отбрасывания их не значимых значений легко представляется в виде ациклического графа, который будет реальной вероятностной моделью исходного многомерного распределения вероятностей.

Важной особенностью ее будет значительное снижение энтропии по мере Шеннона, т.е. неопределенности состояний наблюдаемой системы, а следовательно, объема информации для получения искомых закономерностей наблюдаемого процесса.

В многообразии Байесовских сетей для поставленной задачи наиболее подходящими будут Байесовские сети доверия.

Байесовские сети доверия (БСД), также известные как Bayesian Belief Networks (BBN), представляют собой графические модели, которые используются для отображения вероятностных зависимостей между переменными. Эти сети широко применяются в различных областях, таких как диагностика, принятие решений в условиях неопределенности, прогнозирование и обнаружение аномалий.

Байесовская сеть доверия состоит из следующих основных компонентов:

– **вершины (узлы)** представляют случайные переменные, которые могут быть дискретными или непрерывными;

– **ребра (дуги)** – направленные связи между вершинами, которые указывают на условные зависимости между переменными;

– **условные вероятностные таблицы (CPT)**. Для каждой вершины определяется таблица, которая описывает вероятности различных состояний этой вершины в зависимости от состояний ее родительских вершин.

Для оценки надежности с учетом безопасности эта сеть представляется из четырех уровней: уровня свидетельства угроз, уровня действия угроз, уровня отказов элементов системы и уровня отказа всей системы (рис. 1).

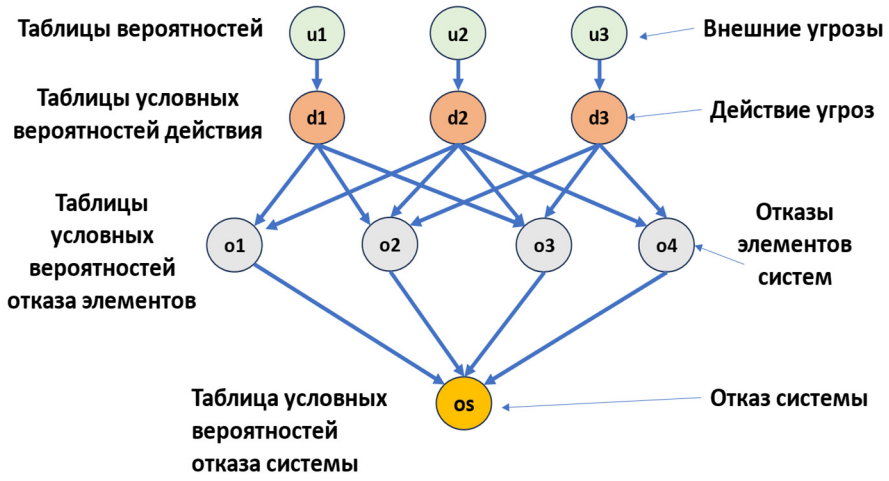

Рис. 1. Структура Байесовской сети оценки и прогнозирования надежности технических систем с учетом их безопасности

Уровень угроз представляется таблицей вероятностей угроз, а эту таблицу можно обозначить как вектор угроз $P(u_j, j=1...m)$.

Уровень действия представляется вектором вероятностей реализации угроз после преодоления средств защиты от них $P(d_j, j=1...m)$, где

$$P(d_j) = P(u_j)(1 - P_z(c_j)). \quad (9)$$

Уровень отказа элементов характеризуется вектором вероятностей отказов, где каждая компонента вычисляется как произведение матрицы условных вероятностей элемента на вектор угроз

$$P(o_i) = A(o_i \mid d_j)P(d_j, j=1...m), \quad (10)$$

где $P(o_i \mid d_j, j=1...m)$ – таблица (матрица) условных вероятностей отказа i-го элемента от j-го вредоносного действия.

Уровень отказа системы характеризуется вероятностью ее отказа при всех возможных комбинациях отказов элементов соответствующей таблицей условных вероятностей ее отказа при отказах элементов $P(o \mid P(o_i, i=1...n)$.

Вероятность отказа системы вычисляется как произведение матрицы условных вероятностей от отказов элементов на вектор отказов элементов

$$P(o) = P(o \mid P(o_i, i=1...n)P(o_i, i=1...n). \quad (12)$$

Этот порядок расчетов называется проходом вниз. Существует также проход вверх, который позволяет уточнить свидетельства угроз.

Основные шаги алгоритма обучения Байесовской сети:

1) сбор данных, которые будут использоваться для обучения. Это могут быть таблицы с угрозами и соответствующими им отказами элементов и всей системы;

2) определение структуры сети или как переменные в базе данных связаны друг с другом. Это может быть сделано вручную или с помощью алгоритмов, таких как PC, Grow-Shrink или др. [17, 22];

3) оценка параметров в виде вероятностных зависимостей, основываясь на имеющихся данных. Обычно это делается с использованием максимального правдоподобия или Байесовского вывода [18, 19, 23–25];

4) валидация модели. Проверяется, насколько хорошо модель предсказывает данные, используя тестовый набор данных [20, 25, 26];

5) совмещение БС с методами онлайн-обучения позволяет динамически адаптировать модель по мере поступления новых данных;

6) алгоритмы формирования и обучения Байесовских сетей доверия реализованы в виде прикладных библиотек на языках Python и Julia [21, 23].

Заключение

Учет внешних угроз и воздействий при оценке надежности технических и информационных систем является критически важным для обеспечения их устойчивости и безопасности.

Интеграция машинного обучения в процесс построения и улучшения вероятностных оценок Байесовских сетей открывает новые горизонты в анализе данных и принятии решений. С помощью МЛ можно значительно повысить точность и надежность модели, что делает ее полезной в самых различных областях техники и безопасности.

Байесовские сети доверия, реализуемые методами машинного обучения, являются мощным аппаратом оценки, мониторинга и обеспечения надежности технических систем на всех этапах их жизненного цикла.

Представленный математический аппарат в сочетании с существующими алгоритмами и программами на языках Python и Julia позволяет оперативно и эффективно решать задачи обеспечения и оценки надежности разнообразных сложных систем.

Список литературы

1. Lee K. L. Reliability assessment of complex systems with cybersecurity considerations // Reliability Engineering & System Safety. 2018. P. 22–28.
2. Simon P. K., Hoyt, R. A. Integrating safety and reliability assessments in engineering practices // Engineering Management Journal. 2019. P. 11–16.
3. Zhao T. A review of risk analysis methodologies in system reliability // Journal of Loss Prevention in the Process Industries. 2020. P. 64–73.
4. Martin S. Data analytics for reliability assessment of safety-critical systems // Safety Science. 2021. P. 234–239.
5. Bobrov A. N., Silin E. V. Probabilistic safety assessment for complex engineering systems // International Journal of Engineering Science. 2022. P. 111–120.
6. Koller D., Friedman N. Probabilistic Graphical Models: Principles and Techniques. 2009. P. 76–85.
7. Cox D. R., Oakes D. Analysis of survival data. Chapman & Hall, 1995. P. 45–50.
8. Gnedenko B. V., Kovalenko A. L. The theory of reliability. Wiley, 1998. P. 61–67.
9. Maleeva M. A. A. O. S. L. Risk analysis and reliability assessment in engineering // Safety Science. 2016. P. 23–30.
10. Zhang X. Q., Liu Y. S. Probabilistic models for evaluating safety and reliability in engineering systems // Reliability Engineering and System Safety. 2020. P. 99–107.
11. Zaitsev D. V., Ivchenko S. G. Optimization of reliability and safety of technical systems based on simulation methods // Journal of Quality in Maintenance Engineering. 2021. P. 42–49.
12. Patterson S. Using Bayesian Networks for Reliability Assessment of Complex Technical Systems // IEEE Transactions on Reliability. 2020. P. 33–38.
13. Fernandez D. Bayesian Networks for Vulnerability Analysis in Cybersecurity // International Journal of Information Security. 2019. P. 76–84.
14. Smirnov A., Kuznetsov I. Reliability Assessment of Systems Considering External Impacts Using Bayesian Networks // Journal of Reliability Engineering. 2021. P. 55–61.
15. City T., Gulevsky A. Integrating Bayesian Networks with Risk Analysis Methods in Engineering Systems // Nature Scientific Reports. 2022. P. 63–67.
16. Li M. Development of a Security Model for Critical Infrastructures Based on Bayesian Networks // Computers & Security. 2020. P. 41–46.
17. Heckerman D. A Tutorial on Learning with Bayesian Networks // Technical Report MSR-TR-95-06. 1995. 57 p.
18. Neapolitan R. Learning Bayesian Networks. 2004. 693 p.
19. Friedman N., Goldszmidt M. Learning Bayesian networks with local structure // Artificial Intelligence. 1996. № 85 (2). P. 241–294.
20. Koller D., Friedman N. Probabilistic Graphical Models: Principles and Techniques. 2009. 1233 p.
21. Ghaddar B., Jebara T. Bayesian Network Structure Learning via Neural Networks // Proceedings of the AAAI Conference on Artificial Intelligence. 2019. № 33. P. 178–185.
22. Klienets S. Structure learning in Bayesian networks using machine learning methods // Machine Learning. 2020. № 109 (3). P. 124–130.
23. Agarwal R. An enhanced Bayesian parameter learning method using neural networks // IEEE Transactions on Neural Networks and Learning Systems. 2019. P. 361–368.
24. Ivanova A. Using ensemble methods for predicting probabilities in Bayesian networks // Journal of Computational and Graphical Statistics. 2021.
25. Lee M. Contextual learning for adaptive Bayesian networks // Artificial Intelligence Review. 2022. P. 202–210.
26. Shapiro S. Interpretable Machine Learning in Bayesian Networks // Journal of Machine Learning Research. 2019. P. 130–139.

27. Voronin E. A. Assessing and optimizing the security of development strategies for small industries and agriculture in Russia in a market economy // Reliability and quality of a complex system. 2023. P. 123–128.
28. Voronin E. A. Assessment and selection of food safety systems // Reliability and quality of a complex system. 2020. P. 228–236.

References

1. Lee K.L. Reliability assessment of complex systems with cybersecurity considerations. *Reliability Engi-neering & System Safety*. 2018:22–28.
2. Simon P.K., Hoyt R.A. Integrating safety and reliability assessments in engineering practices. *Engineering Management Journal*. 2019:11–16.
3. Zhao T. A review of risk analysis methodologies in system reliability. *Journal of Loss Prevention in the Process Industries*. 2020:64–73.
4. Martin S. Data analytics for reliability assessment of safety-critical systems. *Safety Science*. 2021:234–239.
5. Bobrov A.N., Silin E.V. Probabilistic safety assessment for complex engineering systems. *International Journal of Engineering Science*. 2022:111–120.
6. Koller D., Friedman N. *Probabilistic Graphical Models: Principles and Techniques*. 2009:76–85.
7. Cox D.R., Oakes D. *Analysis of survival data*. Chapman & Hall, 1995:45–50.
8. Gnedenko B.V., Kovalenko A.L. *The theory of reliability*. Wiley, 1998:61–67.
9. Maleeva M.A. Risk analysis and reliability assessment in engineering. *Safety Science*. 2016:23–30.
10. Zhang X.Q., Liu Y.S. Probabilistic models for evaluating safety and reliability in engineering systems. *Reliabil-ity Engineering and System Safety*. 2020:99–107.
11. Zaitsev D.V., Ivchenko S.G. Optimization of reliability and safety of technical systems based on simulation methods. *Journal of Quality in Maintenance Engineering*. 2021:42–49.
12. Patterson S. Using Bayesian Networks for Reliability Assessment of Complex Technical Systems. *IEEE Transactions on Reliability*. 2020:33–38.
13. Fernandez D. Bayesian Networks for Vulnerability Analysis in Cybersecurity. *International Journal of Information Security*. 2019:76–84.
14. Smirnov A., Kuznetsov I. Reliability Assessment of Systems Considering External Impacts Using Bayesian Networks. *Journal of Reliability Engineering*. 2021:55–61.
15. City T., Gulevsky A. Integrating Bayesian Networks with Risk Analysis Methods in Engineering Systems. *Nature Scientific Reports*. 2022:63–67.
16. Li M. Development of a Security Model for Critical Infrastructures Based on Bayesian Networks. *Computers & Security*. 2020:41–46.
17. Heckerman D.A Tutorial on Learning with Bayesian Networks. *Technical Report MSR-TR-95-06*. 1995:57.
18. Neapolitan R. *Learning Bayesian Networks*. 2004:693.
19. Friedman N., Goldszmidt M. Learning Bayesian networks with local structure. *Artificial Intelligence*. 1996; (85):241–294.
20. Koller D., Friedman N. *Probabilistic Graphical Models: Principles and Techniques*. 2009:1233.
21. Ghaddar B., Jebara T. Bayesian Network Structure Learning via Neural Networks. *Proceedings of the AAAI Conference on Artificial Intelligence*. 2019;(33):178–185.
22. Klienets S. Structure learning in Bayesian networks using machine learning methods. *Machine Learning*. 2020;(109):124–130.
23. Agarwal R. An enhanced Bayesian parameter learning method using neural networks. *IEEE Transactions on Neural Networks and Learning Systems*. 2019:361–368.
24. Ivanova A. Using ensemble methods for predicting probabilities in Bayesian networks. *Journal of Computational and Graphical Statistics*. 2021.
25. Lee M. Contextual learning for adaptive Bayesian networks. *Artificial Intelligence Review*. 2022:202–210.
26. Shapiro S. Interpretable Machine Learning in Bayesian Networks. *Journal of Machine Learning Research*. 2019:130–139.
27. Voronin E.A. Assessing and optimizing the security of development strategies for small industries and agriculture in Russia in a market economy. *Reliability and quality of a complex system*. 2023:123–128.
28. Voronin E.A. Assessment and selection of food safety systems. *Reliability and quality of a complex system*. 2020:228–236.

Информация об авторах / Information about the authors

Евгений Алексеевич Воронин
доктор технических наук, профессор,
ведущий научный сотрудник,
Федеральный исследовательский центр
«Информатика и управление» РАН
(Россия, г. Москва, ул. Вавилова, 44)
E-mail: e.voronin1@gmail.com

Evgeny A. Voronin
Doctor of technical sciences, professor,
leading researcher,
Federal Research Center "Computer Science
and Control" of the RAS
(44 Vavilova street, Moscow, Russia)

Автор заявляет об отсутствии конфликта интересов /
The author declares no conflicts of interests.
Поступила в редакцию/Received 10.09.2024
Поступила после рецензирования/Revised 27.09.2024
Принята к публикации/Accepted 07.10.2024