P. V. Afanasiev, M. P. Trembovetskyi, V. N. Bondarenko, N. A. Trintina, M. N. Sedchenko

COMPARATIVE DESCRIPTION OF SOURCES OF TROUBLE-FREE FEED OF DPCS

All topologies of sources of trouble-free feed that have the applications in DPCS are considered. The advantages of sources of trouble-free feed considered in the «on-line» topology in details. In case of anomalous electric digits the presence of galvanic upshot between an entrance and exit results in a volume, that the action of electric peak of digit is assumed by the rectifier of source of trouble-free feed, and the feed of loading proceeds swimmingly and failures.

The fundamental features of topology of «off-line» are considered with modern modernization. It is indicated on a limit application of this technology, as cheap sources of trouble-free feed. These recommendations on application of sources of trouble-free feed after the topology of «on-line» with double transformation of tension. Considered sources of «line-interactive» of the improved modification with delta transformations in that more exact regulative element-compensative transformer is used, with the aim of reduction of hindrances, improvement of work and expansion of range of initial tension different additional devices are used.

With the aim of realization of commutation for the receipt of the step stabilizing of initial tension an autotransformer is used, that promotes or reduces initial tension on 12%, extending the limits of range of this tension the same. Due to commutation of winding of autotransformer in the interactive sources of trouble-free feed in case of transition of feed from a network on a feed from a storage battery salutatory treason of tension, frequency and form of initial tension takes place far fewer, than in the sources of trouble-free feed as «off-line», in that commutation is absent.

It follows from resulted, that the sources of trouble-free feed with double transformation of tension are most perfect, especially from delta transformations that are most reliable. The sources of trouble-free feed of this type it is expedient to apply for the feed of DPCS, stations of the local calculated networks, file servers, in those cases, when quality of power supply is qualificatory for computer centers.

Keywords: trouble-free feed; off-line; on-line; DPC; Delta Conversion On-line.

УДК 004.048

І. М. ГАМАНЮК,
Державний університет телекомунікацій, Київ

Варіант застосування байєсівських методів для машинного навчання штучного інтелекту системи підтримки прийняття рішень у боротьбі зі спамом

Запропоновано варіант застосування байєсівських методів для машинного навчання штучного інтелекту системи підтримки прийняття рішень у боротьбі зі спамом.

Ключові слова: байєсівські методи; машинне навчання; штучний інтелект; системи підтримки прийняття рішень; спам.

Вступ

Уявімо собі, що система підтримки прийняття рішень (далі — СППР) приймає рішення, чи можна використовувати отримане повідомлення, що надійшло електронною поштою, чи його потрібно віднести до спаму. Іншими словами, система тестує повідомлення і за позитивного результату відсортовує це повідомлення до таких, що підлягають використанню, а за негативного результату відносить його до спаму.

Спам — це електронні, текстові і/або мультимедійні повідомлення, які без попередньої згоди (замовлення) споживача умисно масово надсилаються на адресу його електронної пошти або кінцеве обладнання абонента, крім повідомлень оператора, провайдера з надання послуг [4].

Розглянемо, що таке тестування повідомлення в даному досліджені.

Приклад тестування повідомлення: СППР отримує повідомлення, сканує його і за відсутності певної ознаки спаму ухвалює рішення, що тестування пройшло позитивно, тобто це повідомлення можна використовувати. У разі наявності певної ознаки спаму система приймає рішення про негативне тестування, і це повідомлення розміщується серед таких, що належать до спаму.

Користувач переглядає перелік повідомлень спаму, з деякими ознайомлюється, і якщо вирішує, що певне повідомлення не є спамом, то переносить його до переліку працездатних повідомлень.

Також користувач ознайомлюється з працездатними повідомленнями і при вирішенні, що певне повідомлення є спамом, переносить його до переліку повідомлень спаму.

Під час тестування виникають помилки 1-го роду — визнання повідомлення таким, що належить до спаму, тоді як воно є функціонально придатним. Помилка 2-го роду — визнання повідомлення функціонально придатним, тоді як воно належить до спаму [3].

Метою дослідження є опис моделі СППР, що відсіює певні повідомлення з ознаками спаму і в процесі роботи здійснює навчання штучного інтелекту щодо ознак спаму.

Основна частина

Широкий клас методів моделювання, прогнозування і керування, які спрямовані на боротьбу з невизначеностями, ґрунтується на байєсівському підході. Використання байєсових мереж для аналізу процесів різної природи, діяльності людини та функціонування технічних систем дозволяє враховувати та використовувати будь-які вхідні дані — експертні оцінки і статистичну інформацію. Мережі Байєса — це високоресурсний метод імовірнісного моделювання процесів довільної природи з невизначеностями різних типів, який забезпечує можливість достатньо точного опису їх функціонування, оцінювання прогнозів та побудову системи управління [2].

Формула Байеса:

$$P(A|B) = P(B|A)\,P(A)/P(B),$$

де P(A) — апріорна ймовірність гіпотези A;

P(A|B) — імовірність гіпотези A при настанні події B (апостеріорна ймовірність);

P(B|A) — імовірність настання події B при істинності гіпотези A;

P(B) — повна ймовірність настання події B.

Було проведено 1000 тестів. Один тест — одне повідомлення (табл. 1).

360 тестів показало, що повідомлення придатні і вони дійсно виявилися придатними в ході роботи. 440 тестів показало, що повідомлення непридатні і вони дійсно виявилися непридатними в ході роботи.

Але 60 тестів показало, що повідомлення непридатні, але вони виявилися придатними в ході роботи (помилка 1-го роду). Та 80 тестів показало, що повідомлення придатні, але вони виявилися непридатними (помилка 2-го роду).

Таблиця 1

Історична інформація

		Тестування		
		Позитивне	Негативне	Сума
Працездатність повідомлення	Працездатне	360	60	420
	Непрацездатне	80	500	580
	Сума	440	560	1000

Далі обчислюємо частотну ймовірність. Для цього кількість кожного виду результатів тестування поділемо на загальну кількість тестів.

Здобуті результати наведено в табл. 2.

Таблиця 2

Частотна ймовірність

		Тестування		
		T_1 = «+»	T_2 = «–»	Сума
Працездатність повідомлення	D_1 = Так	0,36	0,06	0,42
	D_2 = Ні	0,08	0,50	0,58
	Сума	0,44	0,56	1

Визначаємо умовну ймовірність отриманих позитивних значень тестів у придатних повідомлень:

$$0{,}36/0{,}42 = 0{,}8571,$$

та частку отриманих негативних значень тестів у придатних до роботи повідомлень:

$$0{,}06/0{,}42 = 0{,}1428.$$

Відповідно здійснюємо підрахунок у непридатних до роботи повідомлень.

Результати зазначених обчислень подано в табл. 3

Таблиця 3

Історичне подання

		P(T|D) = P(D,T)/P(D)		
		Тестування		
P(T|D)		T_1 = «+»	T_2 = «–»	Сума
Працездатність повідомлення	D_1 = Так	0,8571	0,1428	1
	D_2 = Ні	0,1379	0,8620	1

Далі розраховуємо умовну ймовірність отримання придатних до роботи повідомлень серед повідомлень, що дістали позитивний результат тестування

$$0{,}36/0{,}44 = 0{,}81818,$$

а також умовну ймовірність отримання непридатних до роботи повідомлень серед повідомлень з позитивним результатом тестування:

$$0{,}06/0{,}56 = 0{,}1071.$$

Відповідно здійснюємо обчислення у повідомлень, що дістали негативний результат.

Результати зазначених підрахунків наведено в табл. 4

Таблиця 4

Майбутнє передбачення

		P(T|D) = P(D,T)/P(D)	
		Тестування	
P(T|D)		T_1 = «+»	T_2 = «–»
Працездатність повідомлення	D_1 = Так	0,81818	0,1071
	D_2 = Ні	0,1818	0,8928
	Сума	1	1

Відповідно до здобутих результатів можна стверджувати таке:

- після отримання позитивного результату тестування ймовірність того, що повідомлення працездатне дорівнює $P(D_1|T_1) = P(D_1,T_1)/P(T_1) = 0{,}81818$;
- імовірність того, що після отримання позитивного результату тестування стверджується, що повідомлення придатне до роботи, а воно в процесі роботи виявилось непрацездатним (помилка 2-го роду), а також $P(D_2|T_1) = P(D_2,T_1)/P(T_1) = 0{,}1818$;
- після отримання негативного результату тестування ймовірність того, що повідомлення непрацездатне дорівнює $P(D_2|T_2) = P(D_2,T_2)/P(T_2) = 0{,}8928$;
- імовірність того, що після отримання негативного результату тестування стверджується, що повідомлення буде непрацездатним, а воно в процесі

роботи виявилось працездатним (помилка 1-го роду), а також $P(D_1|T_2) = P(D_1,T_2)/P(T_2) = 0{,}1071$.

Постає питання: як діяти, якщо процес тестування нових повідомлень триває і статистичні дані оновлюються? У такому разі необхідно вносити зміни до таблиці. Отже, ми здійснюємо навчання штучного інтелекту системи підтримки прийняття рішень у боротьбі зі спамом. Якщо це робити в автоматичному режимі, отримаємо автоматичне навчання.

Наприклад, було протестовано нове повідомлення і отримано позитивний результат, а також за результатами роботи підтверджено працездатність повідомлення (табл. 5).

Таблиця 5

Історична інформація

		Тестування		
		Позитивне	Негативне	Сума
Працездатність повідомлення	Працездатне	361	60	421
	Непрацездатне	80	500	580
	Сума	441	560	1001

Тут 361 — новий результат (було 360). Також збільшилася кількість тестів із позитивним результатом до 441 і загальна кількість тестів до 1001.

Нові значення ймовірностей ілюструє табл. 6.

Таблиця 6

Частотна ймовірність

		Тестування		
		T_1 = «+»	T_2 = «–»	Сума
Працездатність повідомлення	D_1 = Так	0,3606	0,0599	0,4206
	D_2 = Ні	0,0799	0,4995	0,5794
	Сума	0,4405	0,5594	1

Розрахуємо умовну ймовірність отриманих позитивних значень тестів у придатних до функціонування повідомлень 0,3606 / 0,4206 = 0,8575, а також частку отриманих негативних значень тестів у придатних до функціонування повідомлень 0,0599/0,4206 = 0,1425.

Відповідно визначаємо у непридатних до функціювання повідомлень (табл. 7).

Таблиця 7

Історичне подання

		P(T|D) = P(D,T)/P(D)		
		Тестування		
P(T|D)		T_1 = «+»	T_2 = «–»	Сума
Працездатність повідомлення	D_1 = Так	0,8575	0,1425	1
	D_2 = Ні	0,1379	0,8621	1

Обчислюємо умовну ймовірність отримання придатних до функціонування повідомлень серед тих, що дістали позитивний результат тестування:

$$0{,}3606/0{,}4405 = 0{,}8186,$$

та умовну ймовірність отримання непридатних до функціонування повідомлень серед тих, що дістали позитивний результат тестування:

$$0{,}0599/0{,}5594 = 0{,}1071.$$

Відповідно здійснюємо підрахунок у повідомлень, що дістали негативний результат (табл. 8).

Таблиця 8

Майбутнє передбачення

		P(T|D) = P(D,T)/P(D)	
		Тестування	
P(T|D)		T_1 = «+»	T_2 = «–»
Працездатність повідомлення	D_1 = Так	0,8186	0,1071
	D_2 = Ні	0,1814	0,8929
	Сума	1	1

Порівнюючи з попередніми результатами, маємо:

- було значення $P(D_1|T_1) = 0{,}81818$, стало $P(D_1|T_1) = 0{,}8186$. Це означає, що збільшується ймовірність отримання працездатного повідомлення при отриманні позитивного значення тестування нового повідомлення;
- було значення $P(D_2|T_1) = 0{,}1818$, стало $P(D_2|T_1) = 0{,}1814$. Це означає, що зменшується ймовірність отримання непрацездатного повідомлення при отриманні позитивного значення тестування нового повідомлення (помилка 2-го роду);
- інші значення, а саме $P(D_1|T_2) = 0{,}1071$ — імовірність отримання працездатного повідомлення при отриманні негативного значення тестування (помилка 1-го роду) та $P(D_2|T_2) = 0{,}8929$ — імовірність отримання непрацездатного повідомлення при отриманні негативного значення тестування залишилися без змін.

Уявімо, що результати постійно накопичуються, але технології створення тест-систем весь час змінюються. Отже, виникає стара статистика, яка негативно впливає на отримання відповідних імовірностей.

Так, наприклад, якщо перше повідомлення із попереднього прикладу було протестовано за застарілою технологією, можна спробувати відкинути перший результат тестування (загальна кількість результатів стала 1000). Нехай це був позитивний результат тестування з отриманням непрацездатного повідомлення.

Тоді дістанемо такі результати на основі байєсівських методів (табл. 9).

Таблиця 9

Майбутнє передбачення

		P(T|D) = P(D,T)/P(D)	
		Тестування	
P(T|D)		T_1 = «+»	T_2 = «–»
Працездатність повідомлення	D_1 = Так	0,8205	0,1071
	D_2 = Ні	0,1795	0,8929
	Сума	1	1

Якщо їх порівняти із попередніми результатами, поданими в табл. 4, побачимо, що змінилися значення, а саме:

$P(D_1|T_1) = 0{,}81818$ на 0,8205 — імовірність отримання працездатного повідомлення при здобутті

позитивного значення тестування та $P(D_2|T_1)$ = = 0,1818 на 0,1795 — імовірність отримання непрацездатного повідомлення при здобутті позитивного значення тестування (помилка 2-го роду).

Висновки

♦ Накопичення результатів тестування та їх урахування в таблиці, що грунтується на байєсівських методах, позитивно впливає на точність отримання відповідних імовірностей.

♦ Ті чи інші значення ймовірностей характеризують ознаку, за якою здійснюється тестування на спам. А отже, при великих значеннях помилок 1-го і 2-го роду можна дійти висновку щодо низької якості ознаки, за якою здійснюється тестування, а також про виключення її з переліку ознак.

♦ Зміни технологій тестування можуть впливати на результати отримання відповідних імовірностей. При зміні технологій тестування повідомлень необхідно відкидати застарілі значення статистичних даних.

♦ Якщо накопичувати нові дані та відкидати застарілі, обробляти дані за допомогою байєсівських методів, оцінювати дані, то можна вважати, що цим описано модель СППР зі штучним інтелектом, який здійснює машинне навчання.

Список використаної літератури

*1. **Гаманюк І. М.** Методи розрахунку помилок 1-го та 2-го роду при прийнятті рішення про функціональний стан системи підтримки прийняття рішень // Зв'язок. 2018. № 4. С. 25–27.*

*2. **Байєсівські** мережі в системах підтримки прийняття рішень: навч. посіб. / М. З. Згуровський, П. І. Бідюк, О. М. Терентьєв, Т. І. Просянкіна-Жарова. Київ, 2015. 300 с.*

*3. **Горбань І. І.** Теорія ймовірностей і математична статистика для наукових працівників та інженерів: монографія. Київ, 2014. 244 с.*

*4. **Постанова** Кабінету Міністрів України від 11 квітня 2012 р. № 295 «Про затвердження Правил надання та отримання телекомунікаційних послуг».*

*5. **Chiang S. Jao.** Decision Support Systems // Intech, 2010. 406 p.*

Рецензент: доктор техн. наук, професор **В. В. Вишнівський**, Державний університет телекомунікацій, Київ.

И. М. Гаманюк

ВАРИАНТ ПРИМЕНЕНИЯ БАЙЕСОВСКИХ МЕТОДОВ ДЛЯ МАШИННОГО ОБУЧЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В БОРЬБЕ СО СПАМОМ

Предложен вариант применение байесовских методов для машинного обучения искусственного интеллекта системы поддержки принятия решений в борьбе со спамом.

Ключевые слова: байесовские методы; машинное обучение; искусственный интеллект; системы поддержки принятия решений; спам.

I. M. Gamaniuk

USAGE OPTION OF BAYESIAN METHODS FOR MACHINE LEARNING OF ARTIFICIAL INTELLIGENCE OF DECISION SUPPORT SYSTEM IN THE FIGHT AGAINST SPAM

This article offers an option for using Bayesian methods to determine if sign of spam is present in a message. This is taken into account during machine learning of artificial intelligence.

A message test is considered as a process when a decision support system (further — DSS) receives a message, scans it and, in the absence of a certain sign of spam, makes a decision that the test has passed positively, and this message can be used. If there is a certain sign of spam, it makes a decision that the test was negative and this message can be placed among messages related to spam.

The user scans the list of spam messages, reviews some of them, and when he decides that a message is not spam, it moves it to the list of workable messages. Also, the user is familiar with working messages, and when it is determined that a message is spam, it transfers it to the list of spam messages.

The purpose of the study is to describe a DSS model based on Bayesian methods that takes away the messages with signs of spam and, in the process of work provides artificial intelligence machine learning on the signs of spam.

During the conduct of 1000 tests (one test — one message), 360 tests showed that the messages were suitable and they were really useful during the work. 440 tests showed that the messages were unsuitable and they really were not suitable during the work. 60 tests showed that the messages were unsuitable, but they were suitable in the course of work (error of type I). 80 tests showed that the messages were suitable, but they were not suitable (error of type II).

According to the results, it was stated that:

- after receiving a positive test result, the probability, that we will receive a suitable message, is $P(D_1|T_1) = P(D_1, T_1)/P(T_1) = 0{,}81818$;

- the probability that after receiving a positive test result we will get an unsuitable message (error of type II) is $P(D_2|T_1) = P(D_2, T_1)/P(T_1) = 0.1818$;

- after receiving the negative test result, the probability that we will receive an unsuitable message $P(D_2|T_2) = P(D_2, T_2)/P(T_2) = 0,8928$;

- the probability that after receiving the negative test result, we will get a suitable message (error of type I) is $P(D_1|T_2) = P(D_1, T_2)/P(T_2) = 0.1071$.

According to the results of the research, the following conclusions were drawn:

- the accumulation of test results and their inclusion in a tables based on Bayesian methods positively affects on the accuracy of obtaining the appropriate probabilities;

- different probabilities characterize the sign on which spam testing is performed. At large values of type I and II errors it is possible to draw a conclusion regarding the quality of the test is low. So the sign could be excluded from the list of signs;

- changes in testing technology can affect the results of obtaining the appropriate probabilities. When changing the testing technology it is necessary to reject the outdated values of statistical data;

- accumulating new data and rejecting outdated, processing data using Bayesian methods, evaluating data — we can assume that this is a described model of DSS with artificial intelligence that carries out artificial intelligence machine learning on the signs of spam.

Keywords: Bayesian methods; machine learning; artificial intelligence; decision support systems; spam.

УДК 658.5+681.51

Ю. І. КАТКОВ, канд. техн. наук, доцент;
М. В. ХОМЕНКО,
Державний університет телекомунікацій, Київ

ЗАГРОЗИ ВІД ІНТЕЛЕКТУАЛЬНИХ ІНФОРМАЦІЙНИХ СИСТЕМ ПОШУКУ ДЛЯ КРИТИЧНИХ ІНФРАСТРУКТУР

Розглянуто питання прояву уразливості елементів інтелектуальної інформаційної системи пошуку інформації. Інтелектуальна інформаційна система пошуку інформації розглядається як складова частина критичної інфраструктури системи управління в складній організаційній системі. Критична інфраструктура — це система, в якій відмова (повністю або частково) уразливого елемента може спричинити ланцюжок відмов у складній організаційній системі взаємопов'язаних інших елементів і тому значно впливає на безпеку і добробут у різних сферах забезпечення основних людських потреб. У XXI столітті критичні інфраструктури стають все більш залежними від нового виду загроз — упровадження сучасних технологій на основі штучного інтелекту. Грунтуючись на цих технологіях, створюються інтелектуальні системи, від яких залежить основна функціональність критичної інфраструктури. Виникає питання: чи можна довіряти інтелектуальним системам автоматично приймати рішення, якщо в них є уразливі елементи і присутній людський фактор? Тому залежність критичних інфраструктур від інтелектуальних систем проявляється не тільки в тому, які технології на основі штучного інтелекту використовуються, а й у тому, яка організація управління прийнята самими інфраструктурами. Аналіз залежності критичних інфраструктур від загроз є складною обчислювальною проблемою. У цьому дослідженні подано опис проблеми прояву уразливості елементів інтелектуальної інформаційної системи пошуку інформації, яка входить до складу інфраструктури системи управління складної організаційної системи. Метою цієї статті є виявлення уразливих елементів інтелектуальних інформаційних систем пошуку, а також визначення їх наслідків для забезпечення безпеки і стабільності інфраструктури та окреслення заходів щодо захисту.

Ключові слова: інтелектуальна інформаційна система пошуку інформації; критична інфраструктура; вразливі елементи.

ВСТУП

У сучасному світі мережу Інтернет використовують як довідковий інструмент. Досить згадати сленгові слова «прогугліть питання». Засобом отримання інформації слугують пошукові системи, наприклад Google, Bing, Yahoo!, Baidu, Yandex та ін., які є невід'ємною частиною інтернету. Пошук інформації виконують інформаційно-пошукові системи із застосуванням технологій штучного інтелекту (ШІ), які сьогодні мають назву ***інтелектуальні інформаційні системі пошуку***.

Інтелектуальна інформаційна система пошуку (ІІСП) — це один із видів автоматизованих інформаційних систем, заснованих на знаннях. ІІСП є комплексом програмних, лінгвістичних і логіко-математичних засобів для підтримання діяльності людини і пошуку інформації у режимі розширеного діалогу на природній мові з використанням технологій ШІ. Результатом упровадження ІІСП є пошук і аналіз інформації, відкритої в публічному інформаційному просторі; виявлення згадок (натяків, непрямих доказів та ін.) заданих об'єктів спостережень (персони, організації, факти, події); здатність обробляти великі обсяги даних і отримувати необхідну релевантну інформацію; створення різних інтерактивних звітів потрібної тематики, з можливістю приведення їх до необхідних стандартизованих форм звітів потрібних типів, наприклад аналіз активності джерел із досліджуваних тем, аналіз популярності персон (організації) та ін.