

Gerasymchuk M.V., Grycyuk Yu.I. Encryption of information by the method of transposition

The classic methods of encryption/decryption of information a method transpositions which are basis of modern cryptography. Described that cryptographic methods of priv used only for that information, which contains secret or confidential information, not intended for wide publicity. Without regard to their availability and clearness of exposition in other educational literature, majority from the examples resulted there touch the English and Russian alphabets. In this work the examples of implementation of tasks are developed to laboratory works on discipline "Cryptographic transformations" with the use of the only Ukrainian alphabet.

Keywords: methods of priv, cryptography, encryption/decryption of information, method of transposition, enciphering table, magic square.

УДК (656.22+656.212):656.2.08 Доц. Я.В. Болжеларський, канд. техн. наук;
доц. В.С. Джус, канд. техн. наук; доц. О.М. Баль, канд. техн. наук –
Дніпропетровський НУ залізничного транспорту

**АНАЛІЗ ТРАНСПОРТНИХ ПОДІЙ НА ЗАЛІЗНИЧНИХ
ПЕРЕЇЗДАХ ЛЬВІВСЬКОЇ ЗАЛІЗНИЦІ**

Здійснено аналіз та прогнозування кількості зіткнень на залізничних переїздах Львівської залізниці. Встановлено відсоткове співвідношення між переїздами різних типів, за яких спостерігається найменша кількість зіткнень. Встановлено, що найбільша кількість зіткнень в абсолютних, питомих (на 100 переїздів) показниках та у відсотковому відношенні до інших типів переїздів стається на переїздах без чергового з сигналізацією.

Постановка задачі. Залізничні переїзди, що є пересіченнями залізничних колій та автомобільних доріг на одному рівні – це зони підвищеної небезпеки. На залізничних переїздах трапляється значна кількість транспортних подій, більшість з яких мають важкі наслідки – травмування та смерть людей. Ситуація, яка складається на залізничних переїздах, знаходиться під постійним контролем ревізорського апарату залізниць [1-4], її аналізують науковці [5-7] та правоохоронні органи.

Згідно з інструкцією з улаштування та експлуатації залізничних переїздів [8], переїзди поділяються на регульовані та ті, що не регулюються. До регульованих належать переїзди, які обладнані пристроями переїзної сигналізації для водіїв транспортних засобів або такі, які обслуговуються черговим працівником та обладнані шлагбаумами.

До нерегульованих належать переїзди, які не обладнані пристроями переїзної сигналізації і які не обслуговує черговий працівник. Можливість безпечного проїзду або проходження через такі переїзди визначає водій транспортного засобу або пішохід. Завдання дослідження полягає у встановленні основних закономірностей настання транспортних подій на залізничних переїздах Львівської залізниці з метою пошуку шляхів підвищення безпеки руху на цих об'єктах.

Методи дослідження. Аналіз транспортних подій на залізничних переїздах здійснено шляхом побудови двомірних рядів динаміки [9, 10]. Ряди динаміки дають змогу отримати аналітичний вигляд моделей і на основі них

проводити розрахунок, встановлювати та аналізувати тенденції розвитку і прогнозувати. Зазвичай, ряди динаміки задаються у вигляді таблиць або графічно. Під час графічного зображення на осі абсцис будується рівномірна шкала часу, а на осі ординат – шкала значень рівнів ряду в рівномірному чи логарифмічному масштабі.

Аналізуючи ряди динаміки, спочатку необхідно виявити закономірність в зміні рівнів ряду. В одних випадках ця закономірність проявляється доволі чітко, в інших вона прихована внаслідок випадкових відхилень і коливань. Тому одним з перших завдань є виявлення тренду, тобто основної тенденції зміни ряду. Власне тренд – це лінія регресії ряду динаміки. Термін "регрес", на противагу прогресу, означає рух назад, – у цьому випадку в минуле, на основі якого планують оцінювати майбутнє. Для побудови лінії тренду потрібно підібрати математичну функцію, яка якомога точніше відображає тенденцію зміни показника і потім використовувати цю функцію для оцінки та аналізу.

У фізичних закономірностях між змінними діють функціональні зв'язки, за яких кожному значенню однієї змінної x відповідає чітко визначене значення іншої змінної, тобто $y = f(x)$. Але детермінована функціональна залежність на практиці трапляється рідко, або взагалі відсутня, оскільки під час вимірювання величин x та y завжди є помилки і вплив випадкових факторів. При цьому кожна з цих величин може залежати від одних і тих самих, або від різних, випадкових факторів.

Кількісні оцінки зв'язку між величинами випадкового процесу встановлює регресійний аналіз. У загальному випадку, коли є результат певних експериментальних досліджень або спостережень, що задані у вигляді таблиці, зв'язок між змінними апроксимується або інтерполюється аналітичними залежностями найпростішого вигляду. Під апроксимацією розуміється знаходження аналітичного виразу відомого вигляду, який би максимально наближався до цієї функції. Інтерполювання ж передбачає знаходження виразу для функції, що задана в табличній формі таким чином, щоб отримані за інтерполяційною формулою значення в точках, де задана початкова функція, збіглися зі значеннями самої функції в цих же точках.

Зв'язки між змінними можуть бути лінійними і нелінійними. Перші мають місце, коли з ростом величини x значення y збільшуються більш-менш рівномірно, утворюючи на графіку пряму лінію. У найпростішому випадку ряд динаміки може бути апроксимований у вигляді лінійної залежності виду:

$$y = a + bx, \quad (1)$$

Якщо під час рівномірного збільшення x значення y зростають прискорено, то в такому випадку залежність y від x найчастіше може бути виражена у вигляді параболи:

$$y = a + bx + cx^2, \quad (2)$$

де: y – показник; a, b, c – коефіцієнти апроксимуючих функцій; x – аргумент, хоча можуть також застосовуватись криві інших видів.

Коли вид функції хоча б приблизно буде відомий, потрібно знайти числові значення параметрів. Для цього потрібно прийняти деякий критерій "найкращого наближення", який був би об'єктивним, відповідав би нашому інтуїтивному поняттю прийнятного і мав би порівняно просте математичне вираження. Найчастіше з цією метою використовується метод найменших квадратів, за якого отримують мінімум суми квадратів відхилень між фактичним значенням показника y_i та теоретичним значенням показника (на лінії тренду) $\bar{y}_i$:

$$S = \sum_{i=1}^n [y_i - \bar{y}_i]^2 \rightarrow \min. \quad (3)$$

Критерій мінімуму суми квадратів застосовується з кількох причин. По-перше, при цьому велику кількість задач можливо розв'язати аналітично. По-друге, за квадратичної залежності вплив малих похибок незначний, а з їхнім збільшенням різко зростає; ця обставина правильно відображає практичну ситуацію, оскільки незначні похибки менш небезпечні, ніж великі. І, по-третє, за такого критерію задовольняється вимога максимуму правдоподібності для випадку, коли відхилення підлягають нормальному закону розподілу. По суті, метод найменших квадратів просто формалізує процедуру підбору апроксимуючої кривої "на око", коли ми намагаємося звести до мінімуму відхилення експериментальних точок від кривої, яку ми підбираємо.

Для обчислення параметрів за методом найменших квадратів підставимо рівняння лінійної регресії в (1):

$$S = \sum_{i=1}^n [y_i - (a + bx)]^2. \quad (4)$$

Мінімізація суми S проводиться шляхом взяття часткових похідних по a і b і прирівнювання їх до нуля. Після спрощення отримуємо систему так званих нормальних рівнянь [9], розв'язок якої дає шукані значення коефіцієнтів a та b .

Оцінку близькості значень лінії тренда до фактичних значень можна здійснити шляхом обчислення показника змішаної кореляції R^2 , значення якого визначаємо за формулою

$$R^2 = 1 - \frac{\sum_{i=1}^n (y_i - \bar{y}_i)^2}{\sum_{i=1}^n y_i^2 - \frac{1}{n} \left(\sum_{i=1}^n y_i \right)^2}. \quad (5)$$

Цей показник може приймати значення від 0 до 1. Лінія тренду найбільш відповідає дійсності, коли значення R^2 близьке до 1, тобто найбільш вірогідною буде модель, для якої значення показника змішаної кореляції R^2 буде найбільшим.

Результати дослідження. На основі даних, що наведені в [1-4], ми проаналізували дані з кількості діючих залізничних переїздів Львівської залізниці впродовж 2007-2010 рр. (табл. 1, 2) та з кількості допущених на них

транспортних подій (табл. 3, 4). З використанням методики, що наведена вище, побудовано лінії трендів та виконано прогнозування зазначених показників на 2011 р. (рис. 1-4).

Табл. 1. Кількість діючих залізничних переїздів Львівської залізниці

Тип переїзду та спосіб регулювання	Кількість переїздів за роками				
	2007	2008	2009	2010	2011 (прогноз)
Регульований (з черговим та сигналізацією)	352	349	349	344	342
Регульований (з черговим без сигналізації)	10	9	9	9	9
Регульований (без чергового з сигналізацією)	791	791	785	793	800
Нерегульований (без чергового та сигналізації)	667	645	624	572	512
Всього	1820	1794	1767	1718	1663

Табл. 2. Кількість діючих залізничних переїздів Львівської залізниці

Тип переїзду та спосіб регулювання	Кількість переїздів, $\bar{N}$ % за роками				
	2007	2008	2009	2010	2011 (прогноз)
Регульований (з черговим та сигналізацією)	19,34	19,45	19,75	20,02	20,43
Регульований (з черговим без сигналізації)	0,55	0,50	0,51	0,52	0,58
Регульований (без чергового з сигналізацією)	43,46	44,09	44,43	46,16	48,02
Нерегульований (без чергового та сигналізації)	36,65	35,95	35,31	33,29	30,97

Табл. 3. Кількість допущених на діючих залізничних переїздах Львівської залізниці транспортних подій

Тип переїзду та спосіб регулювання	Кількість зіткнень на переїздах K вип, за роками				
	2007	2008	2009	2010	2011 (прогноз)
Регульований (з черговим та сигналізацією)	8	2	2	4	11
Регульований (з черговим без сигналізації)	0	0	0	0	-
Регульований (без чергового з сигналізацією)	35	21	15	18	29
Нерегульований (без чергового та сигналізації)	7	5	6	6	8
Всього на переїздах	50	28	23	28	48
Поза переїздами	2	0	1	1	3

Табл. 4. Кількість допущених на діючих залізничних переїздах Львівської залізниці транспортних подій

Тип переїзду та спосіб регулювання	Кількість зіткнень на переїздах, % за роками				
	2007	2008	2009	2010	2011 (прогноз)
Регульований (з черговим та сигналізацією)	16,00	7,14	8,70	14,29	16,83
Регульований (з черговим без сигналізації)	0	0	0	0	-
Регульований (без чергового з сигналізацією)	70,00	75,00	65,22	64,29	54,48
Нерегульований (без чергового та сигналізації)	14,00	17,86	26,09	21,43	28,69

Як видно з табл. 3 і 4, упродовж останніх чотирьох років на регульованих переїздах, регулювання на яких здійснює черговий працівник без сигналізації, транспортних подій не спостерігалось. Це пов'язано з незначною кільк-

кістю таких переїздів (табл. 1, 2) та їх специфікою (переїзди четвертої категорії з незначними відстанями руху поїздів та автотранспорту).

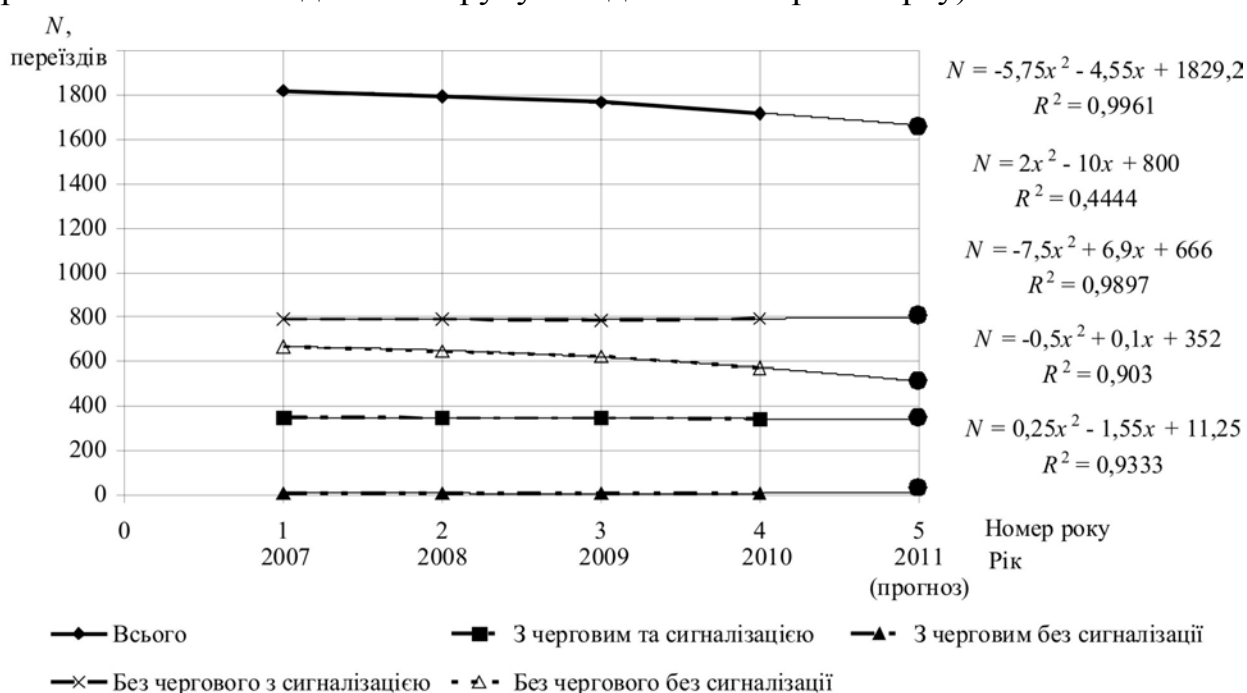


Рис. 1. Кількість переїздів на Львівській залізниці без чергового з сигналізацією

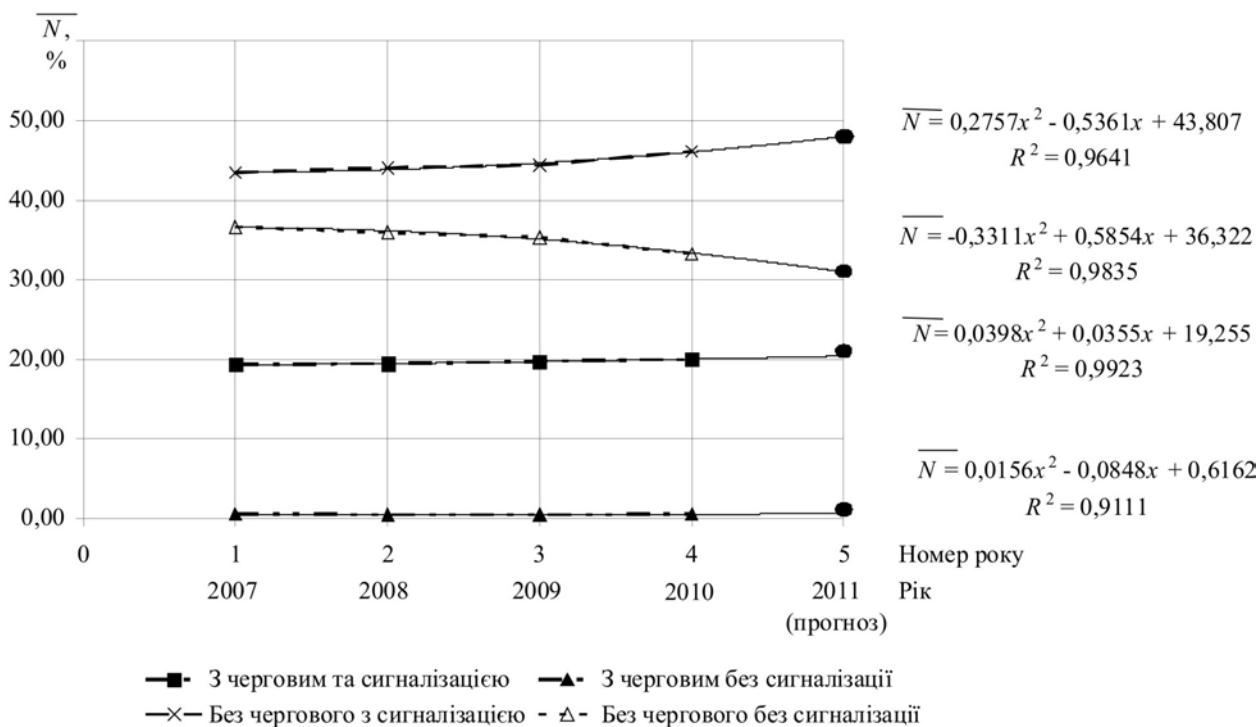


Рис. 2. Кількість переїздів на Львівській залізниці без чергового з сигналізацією

Подальший аналіз буде здійснено без урахування зіткнень, що сталися на переїздах із черговим без сигналізації та зіткнень поза переїздами, поодинокі випадки яких траплялись впродовж 2007-2010 рр. Як видно з рис. 1-4, на Львівській залізниці найбільшу кількість становлять переїзди без чергового з сигналізацією. В останні роки спостерігається стійка тенденція до скорочення загальної кількості переїздів, переважно через закриття нерегульованих (без чергового та без сигналізації) переїздів.

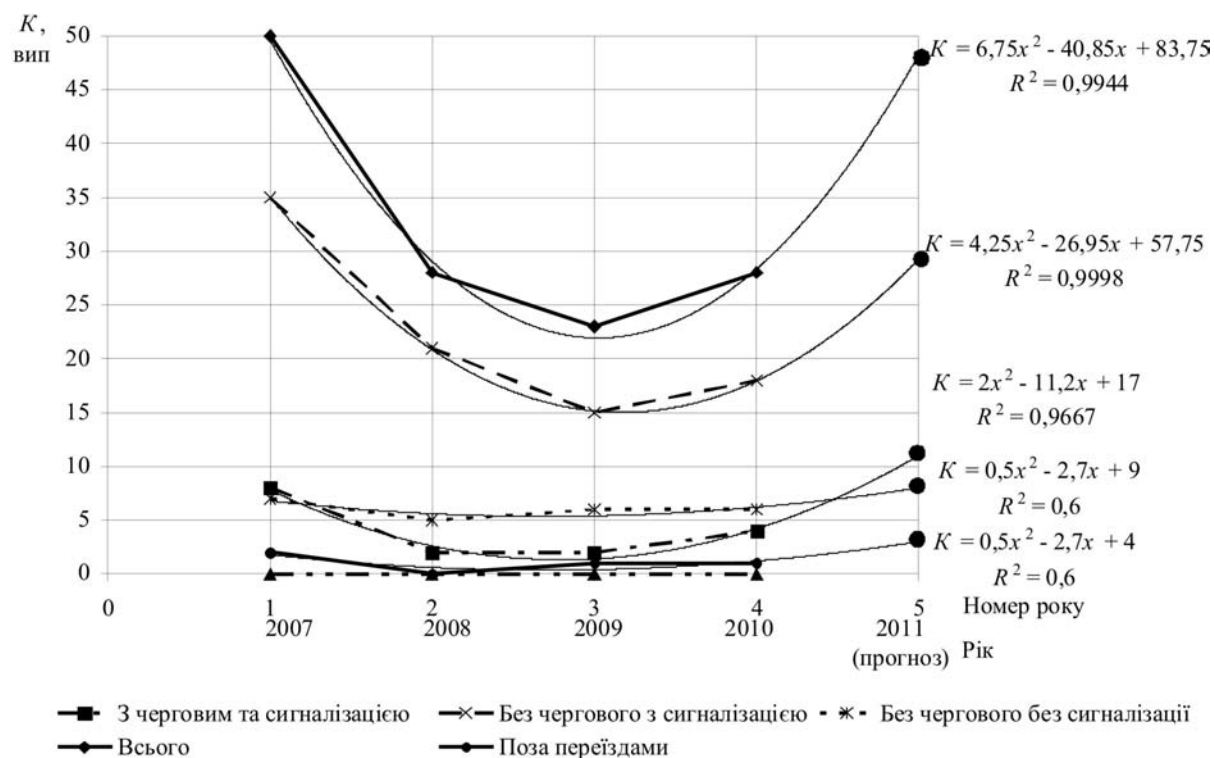


Рис. 3. Кількість зіткнень в абсолютних показниках та у відсотковому відношенні на переїздах Львівській залізниці

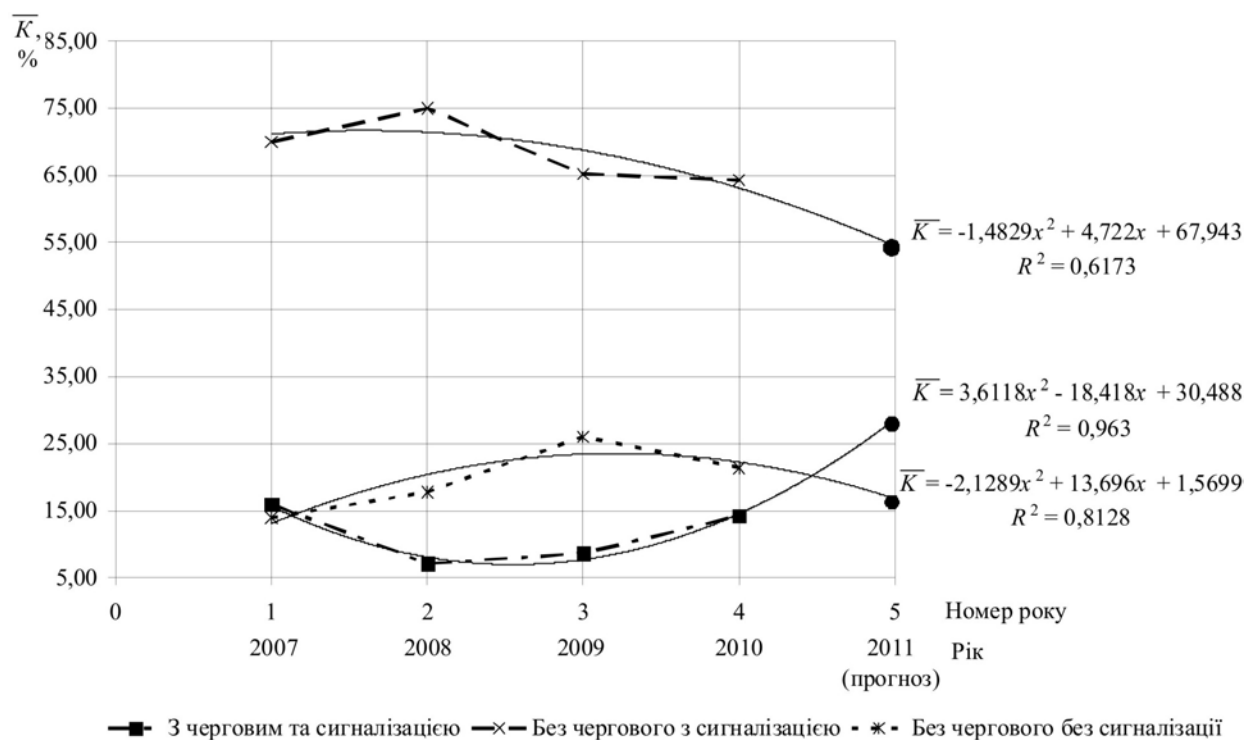


Рис. 4. Кількість зіткнень в абсолютних показниках та у відсотковому відношенні на переїздах Львівській залізниці

У 2010 р. спостерігається зростання кількості зіткнень на переїздах у абсолютних показниках, порівняно з 2009 р. Необхідно зазначити, що напрямок тренду кількості зіткнень в абсолютних показниках та у відсотковому відношенні може не збігатися внаслідок зміни загальної кількості переїздів і перерозподілу між їх типами (рис. 3, 4). На нашу думку, більш інформативним є аналіз динаміки *питомої* (на 100 переїздів) *кількості зіткнень*. Вказа-

ний показник ревізорським апаратом Львівської залізниці на сьогодні не аналізується. Ми виконали розрахунок питомої кількості зіткнень (на 100 залізничних переїздів) за 2007-2010 рр. (табл. 5), побудовано лінії трендів та спрогнозовано значення цього показника на 2011 р. (рис. 5).

Табл. 5. Питома кількість зіткнень на переїздах Львівської залізниці

Тип переїзду та спосіб регулювання	Питома кількість зіткнень на переїздах k , випадків/100 переїздів за роками				
	2007	2008	2009	2010	2011 (прогноз)
Регульований (з черговим та сигналізацією)	2,27	0,57	0,57	1,16	3,17
Регульований (без чергового з сигналізацією)	4,42	2,65	1,91	2,27	3,67
Нерегульований (без чергового та сигналізації)	1,05	0,78	0,96	1,05	1,46
Середнє значення	2,75	1,56	1,30	1,63	2,8

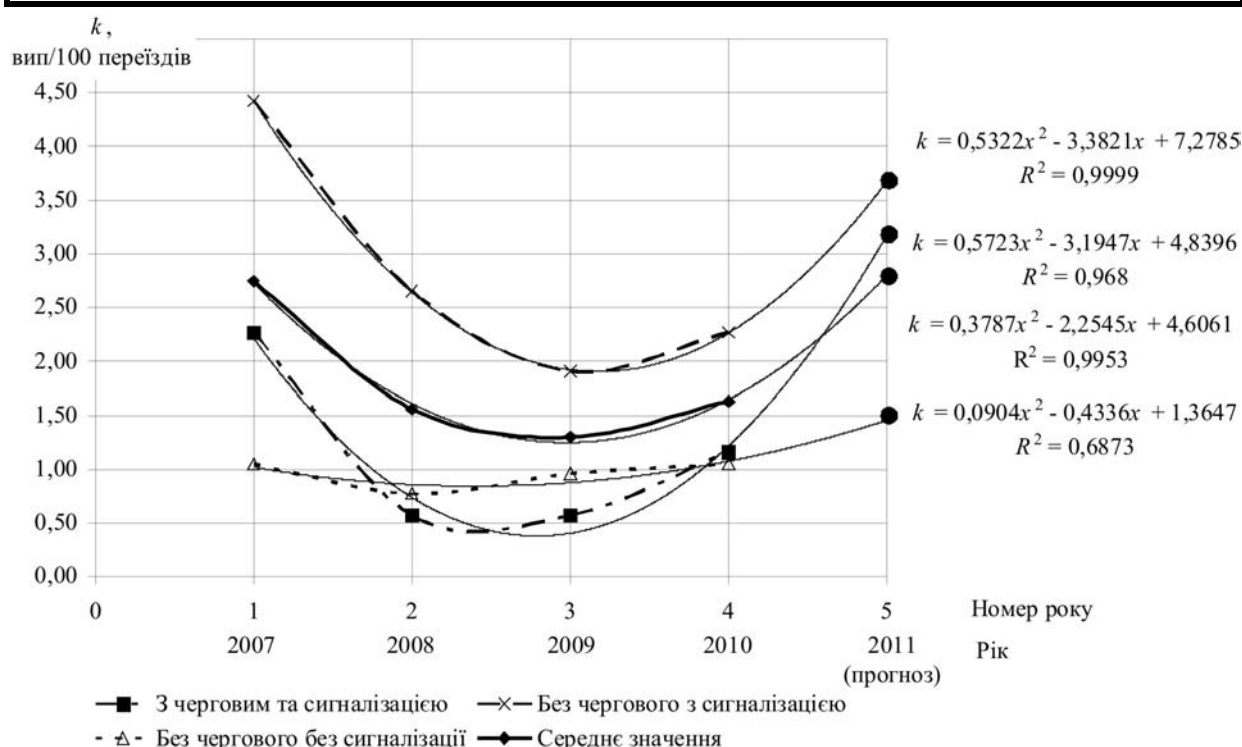


Рис. 5. Прогнозування питомої кількості зіткнень на переїздах Львівської залізниці

Як видно з рис. 3, найбільша кількість зіткнень стається саме на регульованих залізничних переїздах без чергового, які обладнані сигналізацією. Необхідно зазначити, що саме ці переїзди займають найбільшу частку в загальній кількості переїздів, причому вона стійко зростає (рис. 2).

На основі виконаних досліджень можна стверджувати, що визначальним фактором гарантування безпеки руху на залізничних переїздах Львівської залізниці є наявність на них чергового працівника. Збільшення кількості регульованих залізничних переїздів із світлофорною сигналізацією, але без чергового працівника не виправдано стосовно гарантування безпеки руху. Водночас зрозуміло, що переведення усіх залізничних переїздів із сигналізацією без чергового на обслуговування черговим працівником пов'язано зі значними матеріальними затратами.

З метою встановлення відсоткового розподілу між кількістю залізничних переїздів різних типів та питомою кількістю зіткнень на них ми побудували залежності $k = f(\bar{N})$ (рис. 6-8), які мають такий вигляд:

- для переїздів з черговим та сигналізацією

$$k = 11,355 \cdot \bar{N}^2 - 448 \cdot \bar{N} + 4419; \quad (6)$$

- для переїздів без чергового з сигналізацією

$$k = 1,0233 \cdot \bar{N}^2 - 92,509 \cdot \bar{N} + 2092,2; \quad (7)$$

- для переїздів без чергового та без сигналізації

$$k = 0,0563 \cdot \bar{N}^2 - 3,9529 \cdot \bar{N} + 70,294. \quad (8)$$

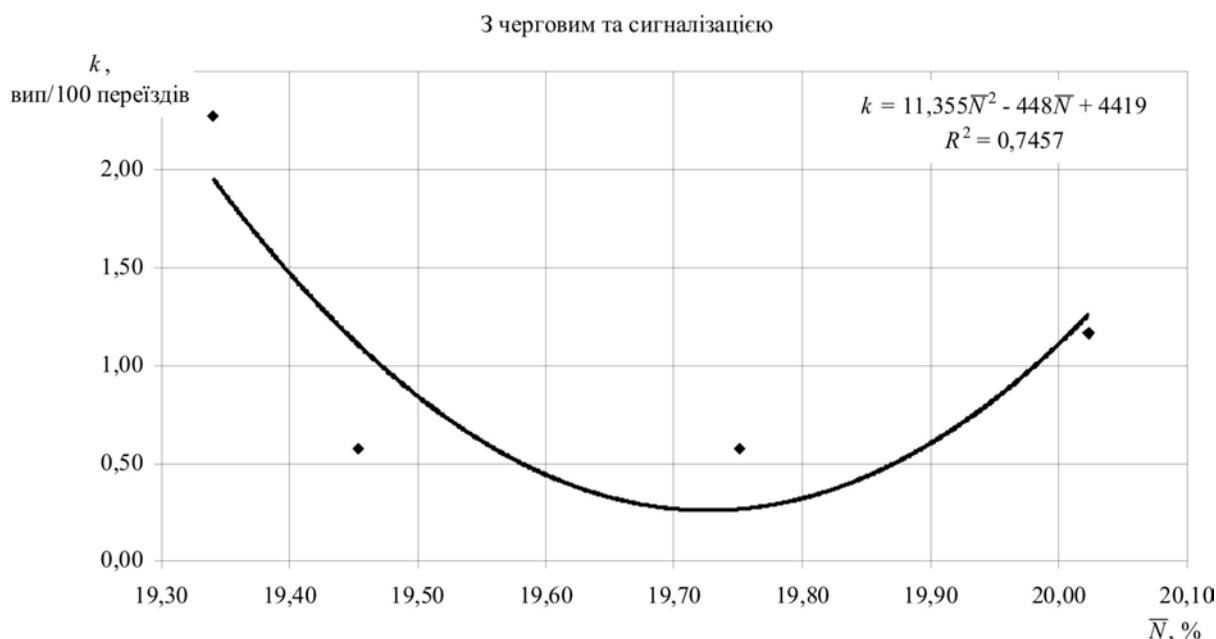


Рис. 6. Розподіл між кількістю залізничних переїздів Львівської залізниці різних типів та питомою кількістю зіткнень на них

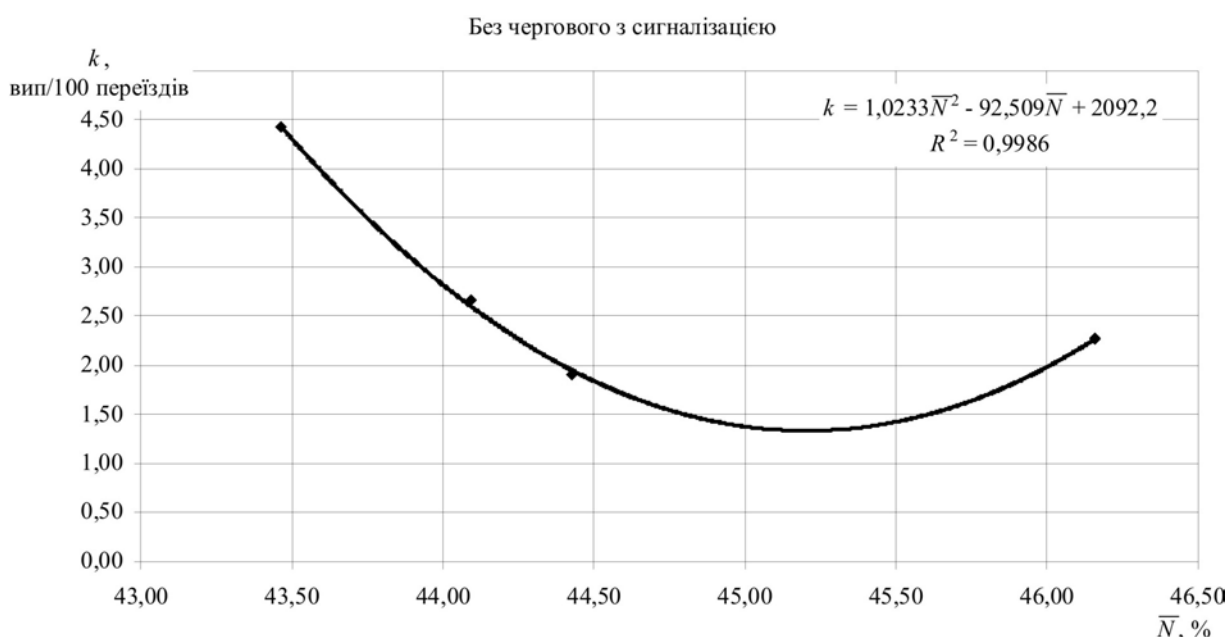


Рис. 7. Розподіл між кількістю залізничних переїздів Львівської залізниці різних типів та питомою кількістю зіткнень на них

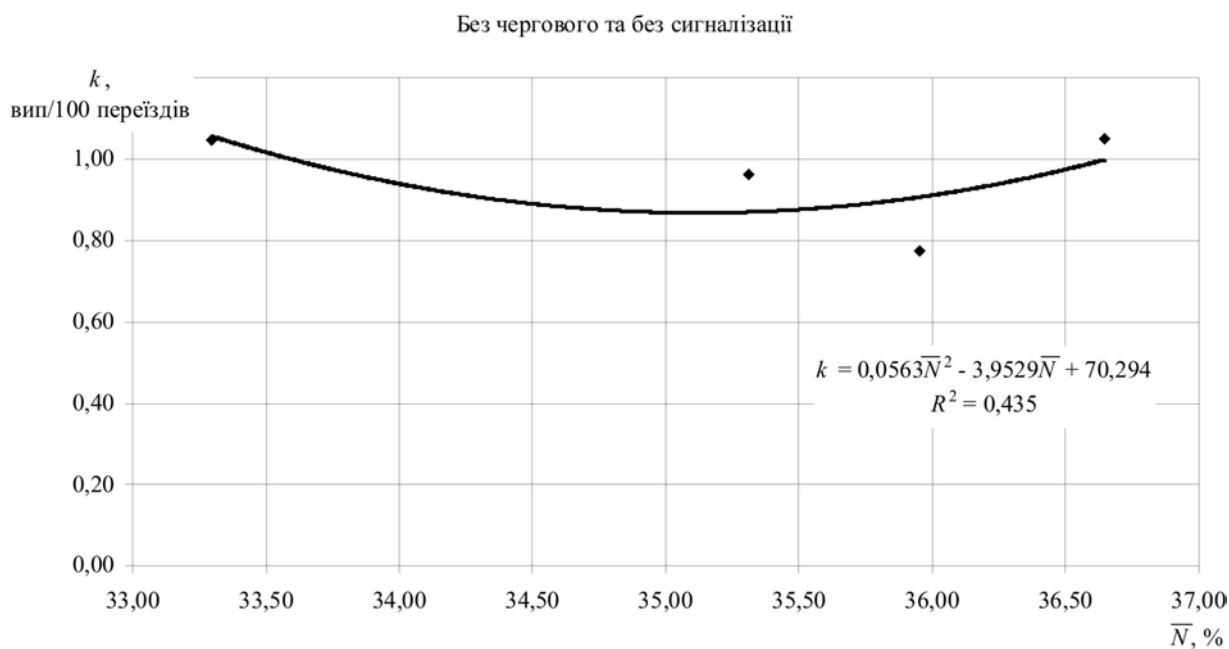


Рис. 8. Розподіл між кількістю залізничних переїздів Львівської залізниці різних типів та питомою кількістю зіткнень на них

Взявши похідні виразів (6-8) та прирівнявши їх до 0, отримаємо значення $\bar{N}$, для якого $k \rightarrow \min$. Підставивши отримане значення N у вирази (6-8), отримаємо мінімальне значення k .

Результати розрахунків зведені до табл. 6.

Табл. 6. Результати розрахунку кількості залізничних переїздів Львівської залізниці різних типів та питомою кількістю зіткнень на них

Тип переїзду та спосіб регулювання	Значення показника	
	$\bar{N}$, %	k , вип/100 переїздів
Регульований (з черговим та сигналізацією)	19,727	0,1537
Регульований (без чергового з сигналізацією)	45,201	1,436
Нерегульований (без чергового та сигналізації)	35,106	0,9094

За отриманими значеннями $\bar{N}$ питома кількість зіткнень на переїздах є мінімальною. Проведемо розрахунок кількості зіткнень на переїздах у 2010 р. за умови, що значення $\bar{N}$ відповідали б розрахованим. Результати розрахунку зведено в табл. 7.

Табл. 7. Результати розрахунку питомої кількості залізничних переїздів Львівської залізниці різних типів та питомою кількістю зіткнень на них

Тип переїзду та спосіб регулювання	Значення показника			
	$\bar{N}$, %	N , шт.	k , вип/100 переїздів	K , вип
Регульований (з черговим та сигналізацією)	19,727	337	0,1537	1
Регульований (без чергового з сигналізацією)	45,201	772	1,436	11
Нерегульований (без чергового та сигналізації)	35,106	600	0,9094	5
Всього (для k – середнє значення)	100	1709	-	17

Як видно з результатів розрахунку, в разі дотримання рекомендованого перерозподілу між типами переїздів у 2010 р. можна було б очікувати 17 випадків зіткнень, що менше, ніж у 2009 р. Фактично ж у 2010 р. сталося 28

зіткнень на залізничних переїздах, При цьому була б збережена позитивна динаміка скорочення кількості зіткнень, яка намітилась у 2007-2008 рр.

Необхідно зазначити, що на кількість зіткнень на залізничних переїздах також впливає інтенсивність руху автотранспорту та поїздів, технічний стан дорожнього покриття на переїздах та на підходах до них і технічний стан систем запобігання зіткненням.

Залежно від інтенсивності руху автотранспорту та поїздів, через залізничний переїзд визначається його категорія, за якою встановлюється тип переїзду, тому вказаний фактор у наведеному аналізі частково врахований. Хоча необхідно зазначити, що переїзди однакової категорії можуть мати різну інтенсивність руху поїздів та автотранспорту. Кількісна оцінка впливу цього фактора, а також технічного стану дорожнього покриття та стану систем запобігання зіткнень на гарантування безпеки руху потребує подальших досліджень.

Висновки. На основі аналізу статистичних даних встановлено, що найбільша кількість зіткнень в абсолютних, питомих (на 100 переїздів) показниках та у відсотковому відношенні до інших типів переїздів стається на переїздах без чергового з сигналізацією. Вказаних переїздів є найбільша кількість і їхня частка постійно зростає, незважаючи на динаміку зменшення загальної кількості переїздів.

Аналіз *загальної* кількості зіткнень, який проводиться ревізорським апаратом залізниці, недостатньо інформативний, оскільки тренди загальної кількості зіткнень на переїздах та питомої їх кількості можуть мати різний напрямок із причини зміни кількості переїздів та відсоткового перерозподілу між їх типами, тому більш інформативним є аналіз *питомої* кількості зіткнень, яких враховує зміну кількості переїздів та відсоткового перерозподілу між їх типами.

Запропонований метод аналізу з врахуванням питомої кількості зіткнень може бути використаний ревізорським апаратом залізниць для оцінки стану безпеки руху, а також удосконалений шляхом врахування впливу інших факторів.

Література

1. **Аналіз стану** безпеки руху поїздів і автотранспорту на Львівській залізниці за підсумками роботи у 2007 році.
2. **Аналіз стану** безпеки руху поїздів і автотранспорту на Львівській залізниці за підсумками роботи у 2008 році.
3. **Аналіз стану** безпеки руху поїздів і автотранспорту на Львівській залізниці за підсумками роботи у 2009 році.
4. **Аналіз стану** безпеки руху поїздів і автотранспорту на Львівській залізниці за підсумками роботи у 2010 році.
5. **Бойник А.Б.** Безопасность на переездах магистрального железнодорожного транспорта (история и анализ) / А.Б. Бойник // Залізничний транспорт України. – 2001. – № 2. – С. 29-32.
6. **Бойник А.Б.** Вероятностная модель функционирования железнодорожных переездов по критерию безопасности / А.Б. Бойник // Залізничний транспорт України. – 2003. – № 1. – С. 29-31.
7. **Сокол Э.Н.** Сходы с рельсов и столкновения подвижного состава (Судебная экспертиза. Элементы теории и практики) / Э.Н. Сокол. – К. : Вид-во "Транспорт України", 2004. – 386 с.

8. Інструкція з улаштування та експлуатації залізничних переїздів. ЦП-0174. Затверджена наказом Міністерства транспорту та зв'язку України від 26.01.2007 р., № 54.

9. Федорец В.А. Методические указания к применению регрессионного анализа в задачах исследования многофакторных процессов / В.А. Федорец. – Харьков : Изд-во ХИИТ, 1986. – 18 с.

10. Вайну Я.Я.-Ф. Корреляция рядов динамики / Я.Я.-Ф. Вайну. – М. : Изд-во "Статистика", 1977. – 119 с.

Болжеларский Я.В., Джус В.С., Баль О.М. Анализ транспортных событий на железнодорожных переездах Львовской железной дороги

Проведен анализ и прогнозирование количества столкновений на железнодорожных переездах Львовской железной дороги. Установлено процентное соотношение между переездами различных типов, при котором наблюдается минимальное количество столкновений. Установлено, что наибольшее количество столкновений в абсолютных, удельных (на 100 переездов) показателях и в процентном отношении к другим типам переездов происходит на переездах без дежурного с сигнализацией.

Bolzhelarsky Ya.V., Dzhus V.S., Bal' O.M. An analysis of transport events is on railway cross of Lviv railway

The analysis and prognostication of amount of collisions on the railway crossings at the Lviv railway was resulted. The between's relation by the different types of railway crossings, at which the minimum of collisions was rated. It is set that most of collisions in absolute, specific (on 100 railway cross) indexes and in a percentage ratio to other types of moves takes a place on railway cross non-attended with signaling.

УДК 629.1

Доц. Л.Д. Величко, канд. фіз.-мат. наук; ад'юнкт

Ю.А. Чаган – Академія сухопутних військ ім. гетьмана Петра Сагайдачного

ДИНАМІКА ГУСЕНИЧНИХ ТРАНСПОРТНИХ ЗАСОБІВ ПО ПЕРЕСІЧЕНІЙ МІСЦЕВОСТІ

Для плоскої моделі гусеничних транспортних засобів побудовано математичну модель її руху, яка враховує нелінійні пружні характеристики підвіски та профіль дороги, по якій вона рухається.

Ключові слова: гусеничний транспортний засіб, система підресорювання, рівняння руху, амплітуда коливань.

Актуальність досліджень та огляд основних результатів. У сучасній промисловості багато уваги приділяється розробці й удосконаленню силових установок і трансмісій транспортних засобів. Однак з тих чи інших причин цей процес недостатньо торкнувся систем підресорювання гусеничних транспортних засобів (ГТЗ) [1-4]. Як показали дослідження та випробування, існуюча система підресорювання ГТЗ не завжди дає змогу повною мірою реалізувати їхні можливості, що зростають, завдяки вдосконаленню інших вузлів чи механізмів. ГТЗ можна розглядати як коливальні системи із багатьма ступенями вільності, які здебільшого призначені для руху по пересіченій місцевості. Саме в цих умовах велике значення надається системі підресорювання, від якої залежить комфортабельність водія та перевезень, а значною мірою і термін їх експлуатації. Система підресорювання під час руху ГТЗ по пересіченій місцевості безперервно сприймає дії нерівностей та передає їх корпусу, що приводить до коливань останнього. Коливання корпусу шкідливо впливають на водія та пасажирів, спричиняють значні динамічні