Наукова стаття (Research article)
http://doi.org/10.32752/2786-5185-2022-2-5-6-53-64
УДК 004.051:351.746.1

ВИЗНАЧЕННЯ ЗАЛЕЖНОСТІ ПОКАЗНИКА ЕФЕКТИВНОСТІ ПРИКОРДОННОГО КОНТРОЛЮ ВІД СТАНУ ФУНКЦІОНУВАННЯ СИСТЕМИ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ

DETERMINING THE DEPENDENCE OF THE BORDER CONTROL EFFICIENCY INDICATOR ON THE STATE OF FUNCTIONING OF THE ELECTRONIC COMMUNICATIONS SYSTEM

Олександр Басараб[1], Ольга Басараб[2]
Національна академія Державної прикордонної служби України імені Б. Хмельницького (вул. Шевченка, 46, м. Хмельницький, Україна, 29003)

Oleksandr Basarab, Olga Basarab
Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine (46, Shevchenka, Khmelnytskyi, Ukraine, 29003)

Отримано: 13.12.2022. Затверджено: 30.01.2023

АНОТАЦІЯ
У статті запропоновано показник ефективності такого виду оперативно-службової діяльності Державної прикордонної служби України, як прикордонний контроль, а саме – ймовірність пропуску порушника в пункті пропуску через державний кордон. Визначено залежність зазначеного показника від стану функціонування системи електронних комунікацій відомства. Констатовано, що відповідно до законодавства Державна прикордонна служба України є суб'єктом інтегрованого управлінням кордонів. Для забезпечення виконання функцій, що покладені на відомство, в оперативно-службовій діяльності активно використовуються інформаційно-комунікаційні системи, зокрема, інформаційно-комунікаційна система прикордонного контролю. Ймовірність пропуску порушника в пункті пропуску через державний кордон залежить від багатьох факторів, у тому числі й фактору наявності запису про порушника в базі даних програмно-технічного комплексу «Гарт-1», що функціонує в пункті пропуску. Відсутність зазначеного запису може відбутися по різних причинах, таких як: помилка оператора при внесенні в базу даних, помилка інспектора при оформленні особи, несправність безпосередньо програмно-технічного комплексу, недоставлення запису з центрального сховища даних до бази даних комплексу через непрацездатність системи електронних комунікацій. У дослідженні проаналізовано стан функціонування системи електронних комунікацій в Державній прикордонній службі

[1] кандидат технічних наук, доцент; orcid 0000-0002-2852-9534; e-mail: a_basarab@ukr.net
[2] кандидат юридичних наук, доцент; orcid 0000-0001-7839-6955; e-mail: ot_basarab@ukr.net

України, та визначено аналітичний вираз для обчислення ймовірності відсутності у базі даних пункту пропуску інформації про правопорушника з урахуванням стану функціонування мережевої складової системи електронних комунікацій.
Ключові слова: Державна прикордонна служба України; інтегрована інформаційно-комунікаційна система «Гарт-1»; інформаційно-комунікаційна система; оперативно-службова діяльність; система електронних комунікацій.

ABSTRACT
The article proposes an indicator of the effectiveness of the border control as one of the types of operational and service activity of the State Border Guard Service of Ukraine, particularly it is about the probability of the violator passing through the checkpoint across the state border. It was determined the dependence of the above-mentioned indicator on the state of functioning of electronic communications system of the Agency. According to the current legislation, the State Border Service of Ukraine is a subject of integrated border management. In order to ensure the performance of assigned functions, in the operational and service activities of the State Border Guard Service of Ukraine are widely used information and communication systems, in particular, the information and communication system of border control. The probability of the violator passing through the checkpoint across the state border depends on many factors, including the presence of a record about the violator in the database of the "Hart-1" software and technical complex operating at the checkpoint. The absence of the specified record can occur for various reasons, such as: operator error when entering into the database, inspector's error when registering the identity, malfunction of the software and technical complex itself, failure to deliver the record from the central data storage to the database of the complex due to malfunction of the electronic communications system. The study analyzed the state of functioning of the electronic communications system in the State Border Guard Service of Ukraine, and it was defined the analytical expression for calculating the probability of the absence of information about the violator in the database, taking into account the state of functioning of the network component of the system of electronic communications.
Key words: State Border Guard Service of Ukraine; integrated information and communication system "Hart-1"; information and communication system; operational and service activity; electronic communications system.

I. ВСТУП

Однією зі стратегічних цілей з реалізації державної політики у сфері інтегрованого управління кордонами, що визначені розпорядженням Кабінету Міністрів України від 24 липня 2019 р. № 687-р «Про схвалення Стратегії інтегрованого управління кордонами на період до 2025 р.» є оптимізація контрольних процедур на кордоні із забезпеченням належного рівня безпеки. На виконання цієї цілі визначено ряд завдань, серед яких є запровадження сучасних ІТ-рішень під час проведення контрольних процедур[1].

[1] Про схвалення Стратегії інтегрованого управління кордонами на період до 2025 року: Розпорядження Кабінету Міністрів України від 24.07.2019 № 687-р. URL: https://zakon.rada.gov.ua/laws/show/687-2019-p#Text

У Державній прикордонній службі України (Держприкордонслужба), яка є суб'єктом інтегрованого управління кордонами, на виконання зазначеного завдання розгорнута, функціонує та постійно модернізується й вдосконалюється Інтегрована інформаційно-комунікаційна система «Гарт». Однією зі складових Інтегрованої інформаційно-комунікаційної системи «Гарт» є інформаційно-комунікаційна система «Гарт-1» (ІКС «Гарт-1»).

Система «Гарт-1» – це сукупність організаційно-розпорядчих заходів, програмно-технічних та телекомунікаційних засобів, що забезпечують обробку інформації (уведення, записування, зчитування, зберігання, знищення, приймання, передавання) щодо прикордонного контролю осіб і транспортних засобів, які перетинають державний кордон України, та автоматизований доступ до інформації, що зберігається в базах даних системи «Гарт-1»[1].

Застосування ІКС «Гарт-1» значно підвищує ефективність прикордонного контролю, проте, водночас, збільшує залежність ефективності даного виду оперативно-службової діяльності (ОСД) від працездатності ІКС «Гарт-1». Тому, важливо забезпечити високий рівень працездатності ІКС, який визначається вимогами до ефективності ОСД Держприкордонслужби.

Аналіз побудови та умов функціонування ІКС[2] дає підстави стверджувати, що важливим елементом системи, від якого залежить працездатність системи в цілому, є мережева складова системи електронних комунікацій ІКС «Гарт-1».

Питанням підвищення ефективності ОСД органів та підрозділів ДПСУ за рахунок вдосконалення мережевої складової системи електронних комунікацій присвячено дослідження таких вчених як І.С. Катеринчук, О.К. Юдін, Р.В. Рачок, Д.А. Мул та ін., однак у них не враховані особливості функціонування пунктів пропуску через державний кордон, та не визначені ймовірності пропуску порушників та/або фігурантів доручень правоохоронних органів в пунктах

[1] Про затвердження Положення про інформаційно-телекомунікаційну систему прикордонного контролю «Гарт-1» Державної прикордонної служби України: Наказ Адміністрації Державної прикордонної служби України від 30.09.2008 № 810-р. URL: https://zakon.rada.gov.ua/laws/show/z1086-08#Text

[2] Рачок Р.В., Лущик М.І. (2012). Підходи до вдосконалення оперативно-службової діяльності у відділах прикордонної служби шляхом модернізації інформаційно-телекомунікаційних систем. *Збірник наукових праць Національної академії Державної прикордонної служби України*. № 57. С. 63–67.

пропуску у зв'язку з відсутністю останніх в базах даних ІКС «Гарт-1», зокрема, через проблеми з мережевою складовою системи електронних комунікацій.

Тому, питання визначення аналітичних залежностей ефективності ОСД Держприкордонслужби від функціонування систем електронних комунікацій є актуальним.

II. МЕТА І МЕТОДОЛОГІЯ

Метою статті є визначення ймовірності відсутності в базі даних ІКС «Гарт-1» пункту пропуску інформації про правопорушника та впливу на неї стану функціонування мережевої складової системи електронних комунікацій.

При дослідженні використовувалися загальнонаукові та спеціалізовані методи досліджень. Методами спостереження та порівняння досліджувалися елементи ІКС «Гарт-1» органів та підрозділів охорони державного кордону та особливості побудови системи електронних комунікацій, їх вплив на ОСД Держприкордонслужби. Методом формалізації вивчалися та розроблювалися аналітичні та функціональні залежності, якими характеризувалися показники оцінки ефективності ОСД, при виконанні якої використовується система електронних комунікацій Держприкордонслужби.

III. ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Для забезпечення заданого рівня ефективності прикордонного контролю необхідно визначити показники, які будуть використовуватись для її оцінки[1]. Оскільки однією з основних задач ОСД у пунктах пропуску є недопущення незаконного перетину державного кордону, таким показником може бути імовірність цієї події. Визначимо імовірність незаконного перетину державного кордону у пунктах пропуску, як імовірність події, яка полягає у тому, що правопорушник незаконно перетинає кордон через пункт пропуску. Позначимо цю імовірність $P_{нпк}$. Оскільки нам завчасно невідомо, який саме напрям перетину кордону обере правопорушник, ця імовірність буде визначатись наступним чином:

[1] Литвин М.М., Єрошин Б.Ф. (2008). Методика вибору раціональних значень параметрів прикордонного контролю. *Збірник наукових праць Національної академії Державної прикордонної служби України*. № 42. Ч. ІІ. С. 26–30.

$$P_{нпк} = \sum_{i=1}^{N} P_{1i} \cdot P_{mpi}, \quad (1)$$

де: P_{1i} – імовірність того, що порушник кордону буде перетинати кордон у *i*-тому пункті пропуску; P_{nnpi} – імовірність незаконного перетину кордону у *i*-тому пункті пропуску; N – кількість пунктів пропуску.

Вираз (1) отриманий, виходячи з наступних міркувань. Порушник кордону, який знаходиться в Україні, або за її межами при перетині кордону через пункт пропуску має обрати один з N можливих варіантів, де N – кількість пунктів пропуску.

Оскільки порушником кордону буде обраний один з N можливих незалежних варіантів, остаточно $P_{нпк}$ буде обчислюватись як сума часткових ймовірностей незаконного перетину кордону у всіх пунктах пропуску. Ці часткові імовірності, в свою чергу, визначатимуться двома незалежними подіями: вибором порушником кордону певного пункту пропуску і незаконним перетином кордону у ньому. Відповідно до цього, для їх обчислення необхідно отримати добуток ймовірностей цих подій (P_{1i} *і* P_{nnpi}).

Оскільки порушником кордону буде обраний для перетину кордону один з N пунктів пропуску, справедливою є наступна нормуюча умова

$$\sum_{i=1}^{N} P_{1i} = 1, \quad (2)$$

Нормуюча умова (2) відображає той факт, що порушником робиться спроба перетину кордону і тому сума ймовірностей P_{1i} по всім пунктам пропуску має дорівнювати одиниці.

Враховуючи (2) можливо визначити різні підходи до обчислення P_{1i}. Якщо вважати, що порушник кордону не має ніяких преференцій щодо вибору певних пунктів пропуску і припустити, що усі P_{1i} рівні, для обчислення можливо використати наступний вираз:

$$P_{1i} = \frac{1}{N}.$$

Інший можливий підхід – припустити що P_{1i} пропорційна кількості осіб що перетинають пункт пропуску за достатній для статистичної обробки проміжок часу. Враховуючи це, отримуємо:

$$P_{1i} = \frac{w_i}{\sum_{i=1}^{N} w_i}, \quad (3)$$

де: N – кількість пунктів пропуску; w_i – кількість оформлених осіб у *i*-тому пункті пропуску за достатньо великий, для статистичної обробки проміжок часу.

Звичайно, більш точним є припущення, що різні пункти пропуску мають різну «привабливість» для порушників кордону. У такому випадку, можливо обчислити P_{1i} на основі статистичної інформації про затриманих порушників:

$$P_{1i} = \frac{a_i}{\sum_{i=1}^{N} a_i}, \qquad (4)$$

де: N – кількість пунктів пропуску; a_i – кількість порушень кордону у i-тому пункті пропуску за достатньо великий, для статистичної обробки проміжок часу.

Звичайно, імовірності визначені за виразами (3) та (4) відповідають умові нормування (2). На основі проведених досліджень було з'ясовано, що існує певна кореляція між (3) та (4), тобто чим більший потік осіб перетинає державний кордон у пункті пропуску, тим більше і затриманих порушників.

Слід відмітити, що незалежно від того, як проводити обчислення P_{1i}, ця величина залежить від вибору, який здійснює правопорушник, і ми не можемо безпосередньо на нього впливати. Тому, з точки зору визначення шляхів підвищення ефективності прикордонного контролю, доцільно звернути більшу увагу в (1) на імовірність незаконного перетину кордону у i-тому пункті пропуску ($P_{ппрі}$). У спрощеному вигляді її визначення розглянуто в дослідженні[1], однак при цьому зроблено ряд суттєвих обмежень. Аналіз факторів, які впливають на значення цього показника, дозволяє зробити висновок, що він є складною функцією, яка залежить від: людського фактору – імовірності помилки оператора при внесенні інформації до центрального сховища даних ($P_{по}$) та імовірності збою, внаслідок помилки інспектора прикордонної служби при оформленні особи ($P_{пк}$); імовірності збою у роботі програмно-технічного комплексу «Гарт-1/П» (ПТК «Гарт-1/П») зі складу ІКС «Гарт-1», що розгорнуто безпосередньо в пункті пропуску, без урахування мережевої складової ($P_{птк}$); імовірності того, що інформація про правопорушника не надійде до бази даних сервера пункту пропуску ($P_{бд}$). Таким чином для певного пункту пропуску:

[1] Лущик М.І. (2012). Методика вдосконалення оперативно-службової діяльності у відділах прикордонної служби типу А та Б шляхом модернізації інформаційно-телекомунікаційних систем з використанням новітніх технологій: магістерська робота. Хмельницький: Вид-во НАДПСУ. 77 с.

$$P_{\text{ппр}} = f(P_{по}, P_{пк}, P_{птк}, P_{бд}) \qquad (5)$$

Оскільки всі події, імовірності яких враховуються в (5) є незалежними, а виявлення порушника кордону здійсниться лише тоді, коли всі вони не відбудуться, $P_{ппр}$ можна знайти з наступного виразу:

$$P_{\text{ппр}} = (1 - (1 - P_{по}) \cdot (1 - P_{пк}) \cdot (1 - P_{птк}) \cdot (1 - P_{бд})). \qquad (6)$$

Для визначення основного показника ефективності $P_{нпк}$ підставимо (6) та (4) у (1).

$$P_{нпк} = \sum_{i=1}^{N} \frac{a_i}{\sum_{i=1}^{N} a_i} \cdot (1 - (1 - P_{поі}) \cdot (1 - P_{пкі}) \cdot (1 - P_{ткі}) \cdot (1 - P_{бді})). \qquad (7)$$

Аналіз статистичних даних, які дозволяють оцінити величини, потрібні для обчислення $P_{ппр}$ показує, що значну роль у (6) відіграє $P_{бд}$. Це пов'язано з тим, що для ефективного функціонування ПТК «Гарт-1/П» необхідний постійний зв'язок з центральним сервером передачі даних, з якого оновлюється інформація в базі даних комплексу в пункті пропуску. Причиною збільшення $P_{бд}$ є недостатня надійність функціонування мережевої складової системи електронних комунікацій Держприкордонслужби. В середньому, протягом року мережа є недоступною понад сто годин, що обумовлює достатньо низьке значення доступності мережі на рівні 98%, що не відповідає вимогам світових стандартів до високоефективних комп'ютерних мереж[1]. Все це приводить до зростання $P_{бд}$ і, відповідно, зростання $P_{ппр}$ і $P_{нпк}$ вище допустимого рівня.

Основою для функціонування системи передачі даних є система електронних комунікацій Держприкордонслужби. При виході її з ладу до бази даних пункту пропуску перестає надходити інформація про нові доручення та постановки на контроль і, відповідно, зростає (більше 0) ймовірність відсутності в ній інформації про правопорушника ($P_{бд}$). Розглянемо, який характер мають простої мережі.

Проміжки часу, протягом яких мережа не функціонує, для поломок різного характеру є різними. В основному можна виділити два класи проблемних ситуацій – коли відновлення працездатності мережі можливе дистанційно і коли вирішення проблеми потребує залучення фахівців та заміни елементів. В загальному випадку розглянемо K_p класів. При цьому

[1] Odom W., McDonald R. (2006). Routers and Routing Basics: CCNA 2 Companion Guide. Cisco; Kurose J.F., Ross K.W. (2013). Computer Networking: A Top-down Approach. Pearson.

$$P_{бд} = \sum_{j=1}^{Kp} P_{бдj}, \qquad (8)$$

де: $P_{бд.j}$ – ймовірність відсутності інформації у базі даних про правопорушника, спричинена поломкою мережі *j*-го типу.

В подальшому розглянемо визначення $P_{бд}$ для лише одного довільного класу проблемних ситуацій і не будемо використовувати індекс.

Введемо позначення: T_k – тривалість непрацездатності мережі; l – кількість виходів з ладу мережі протягом достатньо великого, для статистичної обробки, проміжку часу (одного року); M – загальна кількість записів у базі даних пункту пропуску; v_o – середня швидкість надходження записів з дорученнями до базі даних (кількість записів в одиницю часу); T_p – тривалість достатньо великого, для статистичної обробки, проміжку часу (одного року).

Відсутність запису про порушника в базі даних зумовлена тим, що при виході з ладу мережі і, відповідно, непрацездатності зв'язку з центральним сервером передачі даних, нові оновлення, які накопичились на ньому протягом певного часу, не отримуються. Чим більше часу відсутній зв'язок з цим сервером – тим більшою є кількість неприйнятих записів і більша ймовірність відсутності запису про правопорушника у базі даних. Однак система передачі даних функціонує таким чином, що при відновленні зв'язку всі непередані записи надходять до бази даних пункту пропуску, що приводить до зменшення імовірності відсутності запису до нуля. У зв'язку з цим, залежність імовірності відсутності запису про правопорушника в базі даних пункту пропуску ($P_{зап}$) від часу непрацездатності мережі має наступний вигляд:

$$P_{зап}(t) = \begin{cases} \frac{v_0 \cdot t}{M}, & 0 \le t \le T_к, \\ 0, & t > T_к \end{cases} \qquad (9)$$

Для визначення v_0 можна використати статистичні дані про надходження записів по системі передачі даних до бази даних комплексу.

Як було з'ясовано, $P_{зап}$ залежить від часу непрацездатності системи електронних комунікацій. Однак для визначення $P_{бд}$ необхідно врахувати імовірність непрацездатності мережі протягом часу t (P_M). Найбільшою ця імовірність буде для $t=0$. У цьому випадку P_M буде дорівнювати ймовірності виходу з ладу мережі, яка визначається наступним чином:

$$P_M(0) = P_0 = \frac{T_k \cdot l}{T_p}, \qquad (10)$$

При збільшенні t $P_M(t)$ буде поступово зменшуватись. Коли час непрацездатності мережі наближатиметься до максимально можливого – T_k, ймовірність перебування мережі в цьому стані прямуватиме до 0. Для $t > T_k$, P_M дорівнюватиме нулю. Причому характер зменшення імовірності буде лінійним. У зв'язку з цим:

$$P_M(t) = \begin{cases} \frac{P_0(T_k - t)}{T_k} & 0 \le t \le T_k, \\ 0 & t > T_k \end{cases} \qquad (11)$$

Таким чином, для довільного часу непрацездатності мережі відсутність інформації про особу буде визначатись двома подіями – знаходженням мережі в непрацездатному стані протягом цього часу, яке характеризується імовірністю (11) та, водночас, ненадходженням запису про правопорушника за той же час, що описується ймовірністю (9). Якби розглядались дискретні проміжки часу непрацездатності, результуючу імовірність можливо було б визначити як суму добутків (11) і (9) для всіх можливих дискретних значень часу. Однак у даному випадку час непрацездатності – неперервний. Тому для пошуку $P_{бд}$, визначимо нескінченно малий приріст $P_{бд}$ при збільшенні часу непрацездатності мережі.

$$dP_{бд} = P_c(t) \cdot dP_{зап} \qquad (12)$$

Підставивши (9) у (12) отримаємо:

$$dP_{бд} = P_M(t) \cdot \frac{v_0}{M} \cdot dt. \qquad (13)$$

Для визначення остаточної ймовірності $P_{бд}$, проінтегруємо (13) з урахуванням (11) на проміжку [0, T_k]:

$$P_{бд} = \int_0^{T_k} dP_{бд} = \int_0^{T_k} P_c(t) \cdot dP_{бд} = \int_0^{T_k} P_c(t) \cdot \frac{v_0}{M} dt = \int_0^{T_k} \frac{P_0 \cdot (T_k - t)}{T_k} \cdot \frac{v_0}{M} dt,$$

$$P_{бд} = \frac{P_0}{T_k} \cdot \frac{v_0}{M} \int_0^{T_k} (T_k - t) dt = \frac{P_0}{T_k} \cdot \frac{v_0}{M} \left(\int_0^{T_k} T_k dt - \int_0^{T_k} t dt \right),$$

$$P_{бд} = \frac{P_0}{T_k} \cdot \frac{v_0}{M} \left(T_k^2 - \frac{T_k^2}{2} \right) = \frac{P_0 \cdot v_0 \cdot T_k^2}{2 \cdot M \cdot T_k} = \frac{P_0 \cdot v_0}{2 \cdot M} \cdot T_k, \qquad (14)$$

Підставивши (10) у (14), отримуємо вираз для обчислення шуканої імовірності $P_{бд}$

$$P_{бд} = \frac{l \cdot v_0}{2 \cdot T_p \cdot M} \cdot T_k^2, \qquad (15)$$

Окремо слід відмітити, що для оцінки надійності функціонування мережі використовується також показник – доступність мережі D, який залежить від часу, протягом якого мережа не функціонує[1]:

$$D = \frac{T_p - t}{T_p} \cdot 100, \qquad (16)$$

де: T_p – тривалість року; t – час який мережа протягом року не функціонує.

Врахувавши, що $t=T_k \cdot l$, визначимо D через тривалість інтервалу непрацездатності мережі T_k:

$$D = 100 \cdot (1 - \frac{l \cdot T_k}{T_p}), \qquad (17)$$

З вигляду (17) можна зробити висновок про лінійну залежність між D і T_k. Визначивши з (17) T_k і підставивши у (15) отримаємо залежність імовірності $P_{бд}$ від доступності мережі:

$$P_{бд} = \frac{v_0 \cdot T_p}{20000 \cdot M \cdot l} \cdot (100 - D)^2,$$

Слід відзначити, що вираз (15) справедливий для різних типів несправності мережі. Необхідно лише для них враховувати різний час відновлення працездатності. В цьому, більш загальному випадку:

$$P_{бд.\ j} = \frac{l \cdot v_0}{2 \cdot T_p \cdot M} \cdot T_{kj}^2, \qquad (18)$$

де: $P_{бд.\ j}$ - ймовірність відсутності інформації в БД про правопорушника, спричинена поломкою мережі j – того типу; $T_{k.\ j}$ – час відновлення працездатності мережі при поломці j – того типу.

[1] Рачок Р.В., Лущик М.І. (2012). Підходи до вдосконалення оперативно-службової діяльності у відділах прикордонної служби шляхом модернізації інформаційно-телекомунікаційних систем. *Збірник наукових праць Національної академії Державної прикордонної служби України.* № 57. С. 63–67.

Підставивши (18) у (8) можливо отримати остаточну імовірність з урахуванням несправностей мережі різного типу:

$$P_{\text{од}} = \sum_{j=1}^{N_p} \frac{l \cdot v_0}{2 \cdot T_p \cdot M} \cdot T_{kj}^2, \qquad (19)$$

IV. ВИСНОВКИ

В результаті проведених досліджень отримано аналітичний вираз для обчислення показника ефективності прикордонного контролю – ймовірності відсутності у базі даних пункту пропуску інформації про правопорушника – з урахуванням стану функціонування мережевої складової системи електронних комунікацій.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Литвин М.М., Єрошин Б.Ф. (2008). Методика вибору раціональних значень параметрів прикордонного контролю. *Збірник наукових праць Національної академії Державної прикордонної служби України*. № 42. Ч. ІІ. С. 26–30.
2. Лущик М.І. (2012). Методика вдосконалення оперативно-службової діяльності у відділах прикордонної служби типу А та Б шляхом модернізації інформаційно-телекомунікаційних систем з використанням новітніх технологій: магістерська робота. Хмельницький: Вид-во НАДПСУ. 77 с.
3. Про схвалення Стратегії інтегрованого управління кордонами на період до 2025 року: Розпорядження Кабінету Міністрів України від 24.07.2019 № 687-р. URL: https://zakon.rada.gov.ua/laws/show/687-2019-p#Text
4. Про затвердження Положення про інформаційно-телекомунікаційну систему прикордонного контролю «Гарт-1» Державної прикордонної служби України: Наказ Адміністрації Державної прикордонної служби України від 30.09.2008 № 810-р. URL: https://zakon.rada.gov.ua/laws/show/z1086-08#Text
5. Рачок Р.В., Лущик М.І. (2012). Підходи до вдосконалення оперативно-службової діяльності у відділах прикордонної служби шляхом модернізації інформаційно-телекомунікаційних систем. *Збірник наукових праць Національної академії Державної прикордонної служби України*. № 57. С. 63–67.
6. Kurose J.F., Ross K.W. (2013). Computer Networking: A Top-down Approach. Pearson.
7. Odom W., McDonald R. (2006). Routers and Routing Basics: CCNA 2 Companion Guide. Cisco.

REFERENCES

1. Lytvyn M.M., Yeroshyn B.F. (2008). Metodyka vyboru ratsionalnykh znachen parametriv prykordonnoho kontroliu [Methodology for choosing rational values of border control parameters]. *Journal of scientific works*. No 42. Vol. II. pp. 26–30 [in Ukrainian].
2. Lushchyk M.I. (2012). Metodyka vdoskonalennya operatyvno-sluzhbovoyi diyal'nosti u viddilakh prykordonnoyi sluzhby typu A ta B shlyakhom modernizatsiyi informatsiyno-telekomunikatsiynykh system z vykorystannyam novitnikh tekhnolohiy [Methods of improving operational and service activities in the departments of the Border Guard Service of type A and B by modernizing information and telecommunication systems using the latest technologies]: master's thesis. Khmelnytsky. 77 p. [in Ukrainian].

3. Pro skhvalennia Stratehii intehrovanoho upravlinnia kordonamy na period do 2025 roku [On the approval of the Integrated Border Management Strategy for the period until 2025]: Order of Cabinet of Ministers of Ukraine No 687-p of Jul 24, 2019. URL: https://zakon.rada.gov.ua/laws/show/687-2019-%D1%80#Text [in Ukrainian].
4. Pro zatverdzhennya Polozhennya pro informatsiyno-telekomunikatsiynu systemu prykordonnoho kontrolyu "Hart-1" Derzhavnoyi prykordonnoyi sluzhby Ukrayiny [On Approval of the Regulation on the Information and Telecommunication System of Border Control "Hart-1" of the State Border Guard Service of Ukraine]: Order of the Administration of the State Border Guard Service of Ukraine dated 30.09.2008 No 810-p. URL: https://zakon.rada.gov.ua/laws/show/z1086-08#Text [in Ukrainian].
5. Rachok R.V., Lushchyk M.I. (2012). Pidkhody do vdoskonalennia operatyvno-sluzhbovoi diialnosti u viddilakh prykordonnoi sluzhby shliakhom modernizatsii informatsiino-telekomunikatsiinoi systemy [Approaches to the improvement of operational and service activities in the departments of the border service through the modernization of the information and telecommunications system]. *Journal of scientific works*. No 57. Vol. II. pp. 53–55 [in Ukrainian].
6. Kurose J.F., Ross K.W. (2013). Computer Networking: A Top-down Approach. Pearson.
7. Odom W., McDonald R. (2006). Routers and Routing Basics: CCNA 2 Companion Guide. Cisco.