

СИСТЕМА ПОКАЗНИКІВ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ

Національна академія Державної прикордонної служби України
імені Богдана Хмельницького

У роботі визначені підходи до формування системи показників ефективності функціонування телекомунікаційної системи Державної прикордонної служби України. Отримано вираз для обчислення важливої складової показника ефективності прикордонного контролю

Вступ

Державна прикордонна служба України (ДПСУ) в своїй діяльності активно застосовує інформаційно-телекомунікаційні системи (ІТС), основою яких є телекомунікаційна система (ТКС).

Аналіз праць [1-2], що присвячені оцінці ефективності функціонування ТКС, показав, що для її оцінки використовують наступні показники:

- продуктивність;
- стійкість;
- достовірність передачі;
- безпечність передачі даних.

Наведений вище перелік показників дає можливість оцінити ефективність функціонування ТКС з точки зору ефективності технічних рішень, що реалізовані в конкретній телекомунікаційній системі.

Разом з тим ТКС ДПСУ є системою спеціального призначення, яка використовується для забезпечення оперативно-службової діяльності (ОСД) ДПСУ. Враховуючи сказане вище в систему показників оцінки ефективності функціонування ТКС ДПСУ слід ввести показник, який би дозволив оцінити вплив ТКС на ефективність ОСД.

Мета статті

Визначити підходи до формування системи показників ефективності функціонування ТКС ДПСУ з визначенням показника ефективності прикордонного контролю – ймовірності відсутності у БД пун-

кту пропуску інформації про правопорушника, яка зумовлена непрацездатністю мережі.

Результати дослідження

Показники оцінки ефективності функціонування ТКС ДПСУ представляють множину (1):

$$S = \langle S1, S2, S3, S4, S5 \rangle \quad (1)$$

де $S1$ – продуктивність ТКС;

$S2$ – стійкість ТКС;

$S3$ – достовірність передачі даних в ТКС;

$S4$ – безпечність передачі даних в ТКС;

$S5$ – ефективність оперативно-службових дій, які виконуються з використанням ТКС.

Існуюча система показників $S1$ – $S4$ дозволить оцінити ефективність функціонування ТКС. Разом з тим, ці показники не дають можливість оцінити вплив функціонування ТКС на ОСД, при здійсненні яких обов'язково використовується телекомунікаційна система ДПСУ та її елементи. Враховуючи сказане вище, слід сформулювати комплексний показник оцінки ефективності ОСД, які виконуються з використанням ТКС.

Найбільш активно ТКС ДПСУ використовується під час здійснення прикордонного контролю (ПК) та прикордонної служби (ПС). Тому, для оцінки впливу функціонування ТКС на ОСД у подальшому дослідженні будемо оцінювати вплив ефективного функціонування ТКС

на прикордонний контроль і прикордонну службу та визначимо результируючий комплексний імовірнісний показник ефективності ОСД. Визначення цього комплексного показника розпочнемо з дослідження ПК.

Оскільки однією з основних задач ОСД у пунктах пропуску є недопущення незаконного перетинання державного кордону, то таким показником може бути імовірність цієї події. Визначимо імовірність незаконного перетинання державного кордону у пунктах пропуску, як імовірність події, яка полягає у тому, що правопорушник незаконно перетинає кордон через пункт пропуску. Позначимо цю імовірність $P_{\text{ппр}}$. Оскільки нам завчасно невідомо, який саме напрям перетину кордону обере правопорушник, цю імовірність пропонуємо визначити наступним чином:

$$P_{\text{ппр}} = \sum_{i=1}^N P_{li} \cdot P_{\text{ппр}i} \quad (2)$$

де: P_{li} – імовірність того, що порушник кордону буде перетинати кордон у i -тому пункті пропуску;

$P_{\text{ппр}i}$ – імовірність незаконного перетину кордону у i -тому пункті пропуску; N – кількість пунктів пропуску.

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

$$\sum_{i=1}^N P_{li} = 1 \quad (3)$$

Звичайно, різні пункти пропуску мають різну «привабливість» для порушників кордону. У такому випадку, можливо обчислити P_{li} на основі статистичної інформації про затриманих порушників:

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

де: N – кількість пунктів пропуску;

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

Слід відмітити, що величина P_{li} залежить від вибору який здійснює правопорушник, і ми не можемо безпосередньо

на нього впливати. Тому, з точки зору визначення шляхів підвищення ефективності ПК доцільно звернути більшу увагу в (2) на імовірність незаконного перетину кордону у i -тому пункті пропуску (). В спрощеному вигляді її визначення розглянуто у [3], 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 ЦСД () та імовірності збою, внаслідок помилки контролера при оформленні особи (); імовірності збою у роботі програмно-технічного комплексу автоматизації ПК «Гарт-1/П» без урахування мережевої складової (); імовірності того, що інформація про правопорушника не надійде до бази даних (БД) сервера пункту пропуску () за причини виходу з ладу мережевої складової ТКС. Таким чином для конкретного пункту пропуску імовірність визначається за формулою:

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

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

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

Остаточний показник ефективності з урахуванням (2), (4) та (6) визначатиметься за такою аналітичною залежністю:

$$P_{\text{ппр}} = \sum_{i=1}^N \frac{\alpha_i}{\sum_{i=1}^N \alpha_i} \cdot [1 - (1 - P_{\text{по}i}) \cdot (1 - P_{\text{пк}i}) \cdot (1 - P_{\text{птк}i}) \cdot (1 - P_{\text{бд}i})] \quad (7)$$

Аналіз статистичних даних, які дозволяють оцінити величини, потрібні для обчислення показує, що значну роль у (6) відіграє $P_{\text{пк}}$. Причиною збільшення є виходи з ладу та недостатня надійність роботи мережевої складової ТКС. В середньому, протягом року мережа є недоступною понад сто годин, що обумовлює достатньо

низьке значення доступності мережі на рівні 98% [3].

Проміжки часу, протягом яких мережа не функціонує, для полумок різного характеру є різними. Хоча в основному можливо виділити два класи проблемних ситуацій (коли можливо відновити працездатність мережі дистанційно і коли вирішення проблеми потребує заміни блоків та, відповідно, приїзду ремонтної групи) розглянемо в загальному випадку K_p класів. При цьому:

$$P_{\text{бд}} = \sum_{j=1}^{K_p} P_{\text{бд}j}, \quad (8)$$

де: $P_{\text{бд}j}$ - ймовірність відсутності інформації в БД про правопорушника, спричинена полумкою мережі j - того типу.

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 БД пункту пропуску;
- v_0 - середня швидкість надходження записів з дорученнями до БД (кількість записів в одиницю часу);
- T_p - тривалість достатньо великого, для статистичної обробки, проміжку часу (одного року).

Відсутність запису про порушника в БД зумовлена тим, що при виході з ладу мережі і, відповідно, непрацездатності зв'язку з центральним сервером передачі даних нові оновлення, які накопичилися на ньому протягом певного часу не отримуються. Чим більше часу відсутній зв'язок з цим сервером - тим більшою є кількість неприйнятих записів і більшою ймовірність відсутності запису про правопорушника у БД. Однак система передачі даних функціонує таким чином, що при відновленні зв'язку всі непередані записи надходять до БД пункту пропуску, що приводить до зменшення ймовірності відсутності запису до нуля. У зв'язку з цим, залежність ймовірності відсутності запису про правопорушника в БД пункту пропус-

ку () від часу непрацездатності мережі має наступний вигляд:

$$P_{\text{зан}}(t) = \begin{cases} v_0 \cdot t & 0 \leq t \leq T_k \\ M & \\ 0 & t > T_k \end{cases}, \quad (9)$$

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

Як було з'ясовано, залежить від часу непрацездатності комп'ютерної мережі. Однак для визначення необхідно врахувати ймовірність непрацездатності мережі протягом часу t (P_M). Найбільшою ця ймовірність буде для $t=0$. У цьому випадку P_M буде дорівнювати ймовірності виходу з ладу мережі, яка визначається наступним чином [3]:

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

При збільшенні тривалості непрацездатності мережі (t) буде поступово зменшуватись. Коли час непрацездатності мережі наблизитиметься до максимально можливого - T_k , ймовірність перебування мережі у цьому стані буде наблизитися до 0. Для $t > T_k$, P_M дорівнюватиме нулю. Причому, характер зменшення ймовірності буде лінійним. У зв'язку з цим:

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

Таким чином для довільного часу непрацездатності мережі відсутність інформації про особу буде визначатись двома подіями - знаходженням мережі в непрацездатному стані протягом цього часу, яка характеризується ймовірністю (11) і одночасно ненадходженням запису про правопорушника за цей час, що описується ймовірністю (9). Якби розглядали дискретні проміжки часу непрацездатності, результуючу ймовірність можливо було б визначити як суму добутоків (11) і (9) для всіх можливих дискретних значень часу. Однак, у даному випадку, час непрацездатності неперервний, тому для пошуку визначимо нескінченно ма-

лий приріст при збільшенні часу непрацездатності мережі:

$$dP_{\delta\delta} = P_c(t) \cdot dP_{зан}, \quad (12)$$

Підставивши (9) у (12) отримуємо:

$$dP_{\delta\delta} = P_c(t) \cdot \frac{v_0}{M} \cdot dt, \quad (13)$$

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

$$\begin{aligned} P_{\delta\delta} &= \int_0^{T_k} dP_{\delta\delta} = \int_0^{T_k} P_c(t) \cdot dP_{\delta\delta} = \int_0^{T_k} P_c(t) \cdot \frac{v_0}{M} dt = \\ &= \int_0^{T_k} \frac{P_0 \cdot (T_k - t)}{T_k} \cdot \frac{v_0}{M} dt = \frac{P_0}{T_k} \cdot \frac{v_0}{M} \int_0^{T_k} (T_k - t) dt = \\ &= \frac{P_0}{T_k} \cdot \frac{v_0}{M} \left(\int_0^{T_k} T_k dt - \int_0^{T_k} t dt \right) = \frac{P_0}{T_k} \cdot \frac{v_0}{M} \left(T_k^2 - \frac{T_k^2}{2} \right) =, \quad (14) \\ &= \frac{P_0 \cdot v_0 \cdot T_k^2}{2 \cdot M \cdot T_k} = \frac{P_0 \cdot v_0}{2 \cdot M} \cdot T_k \end{aligned}$$

Підставивши (10) у (14), отримуємо вираз для обчислення шуканої ймовірності

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

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:

$$P_{\delta\delta j} = \frac{l v_0}{2 \cdot T_p \cdot M} \cdot T_{kj}^2, \quad (16)$$

де: $P_{\delta\delta j}$ - ймовірність відсутності інформації в БД про правопорушника, спричинена поломкою мережі j - того типу;

T_{kj} - час відновлення працездатності мережі при поломці j - того типу.

Підставивши (16) у (8) можливо отримати остаточно ймовірність з урахуванням несправностей мережі різного типу. На основі (8) та (7) і статистичних да-

них для обчислення $P_{по}$, $P_{пк}$ та $P_{птк}$ отримується $P_{пнк}$. Однак, оскільки нас цікавить оптимізація мережевої складової, від якої в (7) залежить лише $P_{бд}$, цей показник і буде використовуватись для оцінки впливу на ефективність прикордонного контролю мережевої складової ІТС «Гарт-1».

Висновок

В результаті проведених досліджень визначені підходи до формування системи показників ефективності функціонування ТКС ДПСУ та отримано вираз для обчислення важливої складової показника ефективності прикордонного контролю – ймовірності відсутності у БД пункту пропуску інформації про правопорушника, зумовлена непрацездатністю мережі.

Квадратична залежність цієї ймовірності від часу, який витрачається на відновлення мережі робить актуальним пошук шляхів суттєвого зменшення цього часу.

Список літератури

1. Проектирование и диагностика компьютерных систем и сетей / [М. Ф. Бондаренко, Г. Ф. Кривуля, В. Г. Рябцев и др.]. – К.: НМЦ ВО, 2000. – 306 с.
2. Короуз Дж., Росс К. Компьютерные сети / Дж. Короуз, К. Росс. – [3-е изд.]. – СПб.: Питер, 2004. – 765 с.
3. Лушик, М.І. Методика вдосконалення оперативно-службової діяльності у відділах прикордонної служби типу А та Б шляхом модернізації інформаційно-телекомунікаційних систем з використанням новітніх технологій : магістерська робота, видавництво – Хмельницький: НАДПСУ, 2012 – с. 58-77