Peer Reviewed, Open Access, Free Online Journal
Published monthly : ISSN: 2308-832X
Issue 5(14); May 2014

Original Article: APPROCCIO ALLE INFORMAZIONI E TUTELA DEI SISTEMI DI TELECOMUNICAZIONE BASATA RICONFIGURAZIONE PROATTIVA

Citation
Korsunsky A.S., Maslennikova T.N., Shumilov S.S., Eryshov V.G. Approccio alle informazioni e tutela dei sistemi di telecomunicazione basata riconfigurazione proattiva. *Italian Science Review.* 2014; 5(14). PP. 26-30.
Available at URL: http://www.ias-journal.org/archive/2014/may/Korsunsky.pdf

Authors
Andrey S. Korsunsky, FRPC OJSC RPA "Mars", Russia.
Tatyana N. Maslennikova, FRPC OJSC RPA "Mars", Russia.
Sergey S. Shumilov, FRPC OJSC RPA "Mars", Russia.
Vadim G. Eryshov, Military Academy of Communications, Russia.

Submitted: May 1, 2014; Accepted: May 10, 2014; Published: May 15, 2014

Creazione e massiccia introduzione di tecnologie moderne e Veda di guerra ha una significativa influenza sullo sviluppo di sistemi di difesa infotelecommunication (ITCS).

All'interno di questo articolo, discuteremo il processo di protezione del software contro gli urti, interferenza e la distruzione delle armi homing radiazioni.

Uno degli svantaggi degli approcci esistenti per la tutela dei ITCS effetti di cui sopra è che quando sono usati non sono considerati un ITCS consapevolezza nemico (ITCS intelligence - security) o creduto che il nemico ha la piena consapevolezza di esso. Valutazione ricognizione sicurezza ITCS si basa sull'analisi del nemico, colpendo le sue strutture per quanto riguarda la loro reale importanza. [1]

L' analisi ha mostrato che la strategia e la tattica della sconfitta del nemico implica in primo luogo i più importanti oggetti ITCS. Tuttavia, l'avversario non può sempre corretto nella scelta degli elementi più importanti della ITCS per la soppressione e distruzione. Con questo in mente, l'approccio proposto per la tutela della ITCS compito importante è la sua riconfigurazione proattiva, che prende una decisione sul corpo di gestione sulla base di analizzare e valutare la correttezza della scelta degli oggetti nemici ITCS per la loro soppressione e di riflessione.

La principale fonte di dati sono: $D_{ИТКС}$ - l'accuratezza della valutazione del sistema di struttura di controllo ITCS (CS); D_{nop} - Un livello di soglia predeterminato di struttura ITCS valutazione dell'affidabilità; N - Il numero di elementi ITCS; N_B - Il numero di elementi ITCS esposto al nemico; ε - Precisione della struttura stima ITCS CS; σ - La deviazione standard di una variabile casuale; M - numero totale di azioni nemiche su tutti gli elementi ITCS; m_n - Il numero medio degli impatti sulle ITCS elemento nemico n-esimo ($n = 1,2...N$); $\Delta t_j^{\text{в}}$ - L'intervallo di tempo medio tra le esposizioni del nemico; $t_j^{\text{рек}}$ - ITCS intervalli di riconfigurazione

dopo la prima esposizione al nemico ($j = 1, 2...M$); Δt_j^{ϕ} - Intervalli funzionanti minuti ITCS dopo riconfigurazione per la prima azione di un nemico; K - Numero di intervalli di tempo tra le azioni del nemico.

Con i dati iniziali sono calcolate utilizzando le seguenti figure. Riconfigurazione media Tempo $\overline{T}_{рек}$: (1)

Media ITCS tempo di funzionamento: (2)

Tempo tra influenze distruttive esterne media: (3)

Considerate le disposizioni di base dell'approccio proposto. All'inizio dell'operazione viene modellato ITCS dagli effetti del nemico. I risultati della simulazione di riconfigurazione modello di simulazione e calcolare la probabilità di violazione ITCS del suo funzionamento contro gli effetti destabilizzanti del nemico.

Durante il funzionamento, le ITCS in condizioni operative reali e sotto l'influenza del nemico catturato i dati sugli elementi ITCS interessati (tempo e grado di lesione, l'importanza della categoria). Dato questo spettacolo classifiche sono calcolate per ciascuna delle ITCS elementi interessati: (4)

dove K_1 - coefficiente di intensità di esposizione, calcolato dalla seguente formula: $K_1 = \frac{m_i}{M}$; K_2 - Coefficiente di elementi ITCS downtime, calcolato secondo la formula: $K_2 = 1 - \frac{\overline{T}_{\text{функ}}}{\overline{T}_{\text{функ}} + \overline{T}_{\text{рек}}}$.

Ulteriori elementi colpiti ITCS ordinati per valore massimo calcolato in classifica metrica. Per fare questo, scegliere il valore minimo $R_{\min}$ e massimo $R_{\max}$ degli elementi interessati classifica ITCS. Calcolare i valori di scala degli indicatori ranking elementi interessati ITCS: (5)

Classifica passo deciso: (6)

dove Z - il numero di categorie di elementi di importanza ITCS, ad esempio, Z = 3.

Intervalli calcolati ranking: (7), (8), (9)

Quindi, classifichiamo gli elementi interessati ITCS sulla loro appartenenza ad una determinata categoria di importanza. Quando questo viene confrontato con gli indicatori e gli intervalli di classifica. Se la condizione (7), l'elemento interessato è assegnato alla terza categoria ITCS torio. Se la condizione (8), l'elemento interessato è assegnato alla seconda categoria di ITCS. Se la condizione (9), l'elemento interessato è assegnato alla prima categoria ITCS.

I valori di esempio di reale importanza degli elementi di categorie e si ITCS - rappresentati negli impatti laterali, che caratterizza la precisione della struttura stime ITCS mostrato in Figura 1.

Successivamente, calcolare la classifica affidabilità impatto elementi ITCS lato dalla formula: (10)

dove Q - errore nel determinare l'elemento di impatto laterale ITCS rango.

Formazione di un modello di simulazione di ITCS sui dati ricevuti è una procedura nota e viene eseguita secondo le regole stabilite in un certo numero di fonti note [2].

Modellazione influenze esterne distruttive effettuate con metodi noti di generazione (simulazione), a seconda del tipo di quantitativi distribuzione emanato caratterizzano le aspettative di tempo influenze esterne [2]. Allo stesso tempo, a seconda dell'ambiente esterno mentre simulazione può utilizzare i seguenti metodi di generazione (disegno) di variabili casuali:

Metodo di elaborazione numeri casuali per le distribuzioni uniformi discrete;

Metodo di elaborazione numeri casuali per le distribuzioni non uniformi discrete;

Metodo di elaborazione numeri casuali per le distribuzioni continue uniformi;

Metodo di elaborazione numeri casuali per le distribuzioni continue non uniformi.

I risultati della simulazione sono calcolati affidabilità apertura ITCS struttura di impatto laterale: (11)

Poi calcola l'affidabilità dei autopsia ITCS partito -esposizione ing: (12)

Successivamente, il valore calcolato l'impatto affidabilità di aprire ITCS la parte interessata viene confrontata con un livello di soglia predeterminato di fiducia $D^{\text{пор}}_{\text{вскр ИТКС}}$. Se il valore calcolato supera il valore $D_{\text{вскр ИТКС}}$ di soglia di affidabilità che l'avversario $D^{\text{пор}}_{\text{вскр ИТКС}}$ ha una conoscenza sufficiente circa la struttura di un ITCS funzionanti. In queste condizioni la riconfigurazione viene effettuata prelazione ITCS di lavoro reali. Quando riconfigurazione proattiva ITCS la seguente condizione: (13)

Quando riconfigurazione proattiva ITCS ITCS aumenta anche la sopravvivenza. Dipendenza della probabilità di sopravvivenza a ITCS attuazione delle attività di riconfigurazione proattiva di apertura urto laterale ITCS affidabilità è illustrato nella Figura 2.

I risultati delle simulazioni hanno mostrato che quando svolgere attività tempestiva efficacia riconfigurazione ITCS del suo impatto lato di apertura è ridotto al 60% e aumenta sopravvivenza ITCS al 20 %.

Pertanto, l'approccio proposto per la tutela della ITCS nella guerra informazione permette proattiva ITCS riconfigurazione, sulla base di un'analisi degli impatti del nemico, che ha portato in efficienza ridotta impatti laterali ITCS autopsia, così come aumenta la sua capacità di sopravvivenza di intelligence sicurezza e. L'attuazione di questo approccio sarà in grado di fornire la necessaria tempestività le prestazioni di servizio al cliente ITCS, la sua sicurezza e sopravvivenza.

References:

1. Men'shakov Yu.K. 2002. protection of communication facilities and information from technical means of intelligence. 399 p.
2. Korsunsky A.S., Eryshov V.G. 2011. Infotelecommunication protection systems in terms of information warfare. Process Automation control. Pp. 82-85.

Fig. 1. Valori di reale importanza degli elementi di categorie ITCS ($Z_{\text{реал}}$) e voi rappresentate in urto laterale (del nemico) ($Z_{\text{расч}}$)

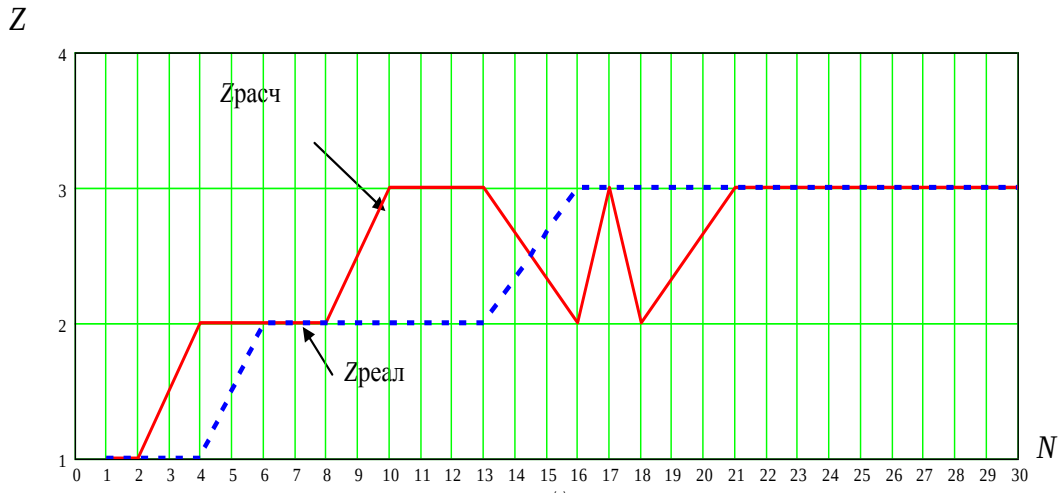
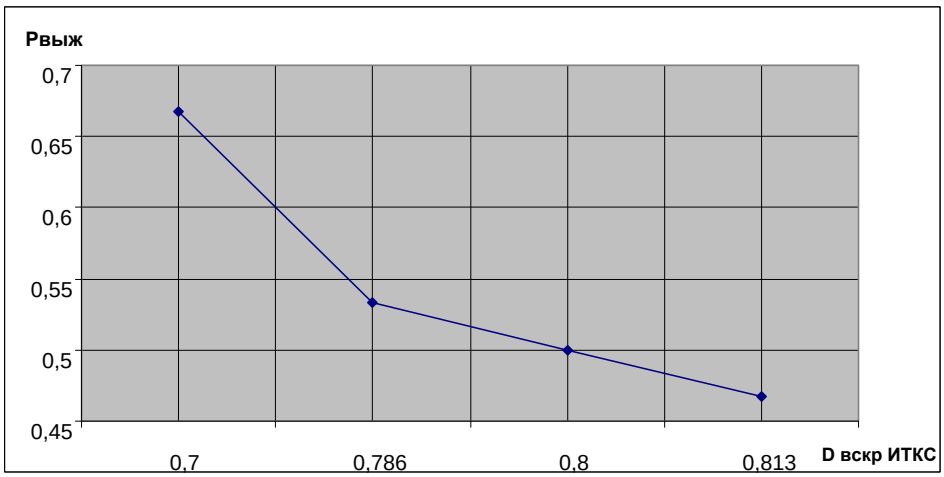


Fig. 2. Probabilità di sopravvivenza ($P_{\text{выж}}$) ITCS (ИТКС) quando le misure preventive per la riconfigurazione della veridicità di apertura ITCS (ИТКС) ($D_{\text{вскрт сс}}$) impatto laterale



$$\overline{T}_{\text{рек}} = \frac{\sum_{j=1}^{m} t_j^{\text{рек}}}{M} \tag{1}$$

$$\overline{T}_{\text{функ}} = \frac{\sum_{j=1}^{m} \Delta t_j^{\text{ф}}}{M} \tag{2}$$

$$\overline{T}_{\text{дв}} = \frac{1}{K} \sum_{j=1}^{K} \Delta t_j^{\text{в}} \tag{3}$$

$$R = \frac{K_2}{K_1} \tag{4}$$

$$\Delta R = R_{\max} - R_{\min} \tag{5}$$

$$R_{\Delta} = \frac{\Delta R}{Z} \quad (6)$$

$$R_i \le R_{\min} + R_{\Delta} \quad (7)$$

$$R_{\min} + R_{\Delta} \le R_j \le R_{\min} + 2R_{\Delta}, \quad (8)$$

$$R_j \ge R_{\min} + 2R_{\Delta}, \quad (9)$$

$$D_{\text{ранж ИТКС}} = 1 - \frac{Q}{N_B} \quad (10)$$

$$D_{\text{в иткс}} = 1 - \frac{\sigma^2}{N_{\text{в}} \cdot \varepsilon^2} \cdot \quad (11)$$

$$D_{\text{вскр иткс}} = D_{\text{ранж иткс}} \cdot D_{\text{в иткс}}. \quad (12)$$

$$2t_j^{\text{рек}} + t_j^{\text{ф}} \le \Delta t_j^{\text{в}} \quad (13)$$