© Shevchenko A., Kokotov O. Method of risk assessment considering the security mechanism influence on parameters of the wireless information & telecommunication systems in the information operations // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 1, p. 7-11.

МЕТОД ОЦІНЮВАННЯ РИЗИКІВ З УРАХУВАННЯМ ВПЛИВУ МЕХАНІЗМІВ ЗАХИСТУ ІНФОРМАЦІЇ НА ПАРАМЕТРИ БЕЗПРОВОДОВИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ПІД ЧАС ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ

Андрій Шевченко, Олег Кокотов

Військовий інститут телекомунікацій та інформатизації Державного університету телекомунікацій, Україна

ШЕВЧЕНКО Андрій Сергійович

Рік та місце народження: 1983 рік, м. Ташкент, Узбекистан.
Освіта: Полтавський військовий інститут зв'язку, 2005 рік.
Посада: старший викладач Військового інституту телекомунікацій та інформатизації Державного університету телекомунікацій.
Наукові інтереси: інформаційна безпека інформаційно-телекомунікаційних систем, інформаційні операції.
Публікації: більше 30 наукових публікацій, серед яких наукові статті, матеріали і тези доповідей на конференціях, науково-дослідні роботи.
E-mail: assheva@gmail.com

КОКОТОВ Олег Вікторович, к.т.н.

Рік та місце народження: 1966 рік, м. Ізмаїл, Україна.
Освіта: Київське вище інженерне радіотехнічне училище протиповітряної оборони імені маршала авіації О. І. Покришкіна.
Посада: викладач Військового інституту телекомунікацій та інформатизації Державного університету телекомунікацій.
Наукові інтереси: інформаційна безпека безпроводових інформаційно-телекомунікаційних систем, інформаційні операції, когнітивні радіосистеми.
Публікації: більше 40 наукових публікацій, серед яких наукові статті, матеріали і тези доповідей на конференціях, науково-дослідні роботи.
E-mail: skat256@bigmir.net

Анотація. *У статті розглядається метод оцінювання ризиків з урахуванням впливу механізмів захисту інформації на параметри безпроводових інформаційно-телекомунікаційних систем, які функціонують в умовах реалізації атак інформаційних операцій. Метод враховує додатковий ризик, який виникає при застосуванні механізмів захисту інформації, під час інформаційного конфлікту, що призводить до зниження параметрів спеціальних безпроводових інформаційно-телекомунікаційних систем: пропускної спроможності, швидкості передачі, дальності зв'язку, часу передачі повідомлень, що є додатковим ризиком під час бойових дій. При застосуванні приведеного методу у статті представлені результати моделювання впливу зменшення швидкості передачі даних ультракороткохвильовою станцією при застосуванні завадозахищеного режиму в різних завадових станах на зміну загального ризику та зв'язок з результатами попередніх досліджень.*

Ключові слова: *безпроводові інформаційно-телекомунікаційні системи, інформаційні операції, методи оцінювання ризиків, рівень ризику, параметри безпроводових інформаційно-телекомунікаційних систем, пропускна спроможність, швидкість передачі, дальність зв'язку.*

Вступ

Попереднім етапом ведення сучасних бойових дій є інформаційні операції, що представляють собою узгоджені за часом, напрямом та цілями комплексні інформаційні впливи, які спрямовані на порушення, зрив, узурпацію прийняття рішення противником з одночасним захистом власних процесів управління.

Засобом проведення інформаційних операцій і одночасно об'єктом їх атак є інформаційно-телекомунікаційні системи, найбільш уразливою частиною якої є безпроводові інформаційно-телекомунікаційні системи (БІТС).

Застосування БІТС спеціального призначення під час інформаційних операцій викликає велику кількістю ризиків отримання збитків, які пов'язані з реалізацією противником інформаційних атак на критичну інформацію, що передається радіоканалами. В умовах ведення інформаційної операції суттєво обмежується час на прийняття рішення для вибору та застосовування механізмів захисту інформації (МЗІ), які б перекривали вразливості БІТС. Результатом цього може бути неоптимальне застосування МЗІ, яке призведе до зниження параметрів БІТС, що в свою чергу, вплине на доступність інформації, а відповідно і на загальний рівень ризику отримання збитку внаслідок атак.

Аналіз останніх досліджень та публікацій

Згідно міжнародного стандарту ISO 27001 [1] оцінювання стану інформаційної безпеки здійснюється на основі ризиків. Огляд останніх публікацій [2–4] показав, що при аналізі інформаційних операцій не враховується ризик отримання збитку від реалізації атак на критичну інформацію, що передається через радіоканали спеціальних БІТС, а також вплив на нього результатів зниження параметрів БІТС при застосуванні МЗІ.

На сьогоднішній час існує велика кількість методів оцінювання ризиків, включаючи і найбільш широко розповсюджені: OCTAVE, CRAMM, Risk Watch, COBRA, RA2, ГРИФ тощо [5]. Вказані методи базуються на схожих етапах оцінювання ризиків, але вони безпосередньо не враховують вплив МЗІ на зниження параметрів БІТС при функціонуванні в умовах ведення інформаційних операцій.

Мета. У роботі ставиться за мету розглянути метод оцінювання ризиків з урахуванням впливу зниження параметрів БІТС при зміні МЗІ в ході інформаційних операцій та провести моделювання зміни рівня ризику з відображенням впливу МЗІ на параметри системи.

Постановка завдання

Для досягнення мети при оцінюванні ризиків необхідно врахувати відносні значення зниження параметрів БІТС при застосуванні МЗІ. На основі отриманого методу провести моделювання впливу зниження параметрів БІТС на зміну загального ризику.

Обмеження. Розглядається функціонування БІТС спеціального призначення в умовах інформаційних операцій. В роботі не розглядаються питання визначення важливості параметрів БІТС, розміру та градацій збитку.

Викладення основного матеріалу дослідження

У процесі розробки захищених БІТС, які передбачається використовувати в критичних умовах впливу навмисних атак противника (порушника), необхідно враховувати всі можливі ризики, включаючи і ризики від обмеження параметрів БІТС, при застосуванні певних МЗІ в ході інформаційних операцій.

Суть заходів з управління ризиками полягає в оцінюванні їх величини, виборі ефективних підходів зниження величини ризиків та визначення залишкового ризику [1].

Оцінювання ризиків є ключовим етапом процесу управління інформаційною безпекою. На сьогоднішній час методи оцінювання ризиків здебільшого спираються на методи, що основані на врахуванні імовірність загроз ($P_{\text{загр}}$) [5]:

$$R = \sum_i P_{\text{загр}\,i} \cdot Z_i \ ,$$

та імовірність події ($P_{\text{под}}$) [5]:

$$R = \sum_i P_{\text{под}\,i} \cdot Z_i = \sum_i P_{\text{загр}\,i} P_{\text{вр}\,i} \cdot Z_i \ , \qquad (1)$$

де R – загальний ризик отримання збитку; $P_{\text{под}\,i} = P_{\text{загр}\,i} P_{\text{вр}\,i}$, $P_{\text{вр}}$ – імовірність виникнення вразливості системи захисту інформації (СЗІ);
Z_i – величина збитку від реалізації i-ої загрози;
i – порядковий номер загрози, $i \in [1, n]$;
n – загальна кількість загроз.

Використання МЗІ призводить до обмеження параметрів БІТС відносно того стану, коли МЗІ відсутні. Пов'язано це, здебільшого, з особливістю реалізації захисних функцій.

Кінцевим результатом загрози є нанесення збитку внаслідок успішної реалізації атак. Таким чином, можна зробити висновок, що $P_{\text{под}\,i} = P_{\text{зб}\,i}$.

Для визначення рівня ризику з урахуванням зниження параметрів БІТС введемо показник зниження параметру L_i. В результаті функція (1) видозміниться і отримає наступний вигляд:

$$R = \sum_i (P_{\text{зб}\,i} \cdot Z_i + L_i) \ . \qquad (2)$$

Величина збитку Z_i від реалізації атак визначається за ступенем важливості параметра для обробки і передачі інформації та його критичності, відповідно до відомих методів оцінювання збитків [5].

Показник зниження параметру L_i БІТС внаслідок застосування МЗІ є відносним значення величини параметра без впровадження засобів захисту та після впровадження МЗІ, і розраховується за вдосконаленим виразом, що приводиться в статті [6]:

$$L_i = \sum_{j=1}^{n} l_{ji} = \sum_{j=1}^{n} \left(1 - \alpha_{ji}\right) \cdot W_{ji}\,, \qquad (3)$$

де l_{ji} – показник зниження j-го параметру, α_{ji} – відносне значення зміни j-го параметру системи, $\alpha_{ji} \in [0,1)$; W_{ji} – коефіцієнт важливості параметру БІТС; j – порядковий номер параметра, $j \in [1, m]$; m – загальна кількість параметрів БІТС.

Відносне значення зміни параметру БІТС, внаслідок впровадження МЗІ, розраховується як відношення:

$$\alpha_{ji} = \frac{Q_{\text{рп}}}{Q_0}\,, \qquad (4)$$

де $Q_{\text{рп}}$ – значення результуючого параметру, після впровадження МЗІ, Q_0 – величина параметру без використання МЗІ.

Відповідно до виду, технології та стандарту БІТС, механізмів захисту інформації, атаки, загальний показник зниження параметру L_i може бути сумою показників l_{ji} в залежності від типу параметру, які взяті з різними коефіцієнтами важливості параметру W_{ji}, що і враховано в формулі (3).

Зазвичай, зниження параметру БІТС проявляється як зниження продуктивності системи в процесі обробки і передачі інформації. З точки зору інформаційної безпеки, зниження параметрів БІТС еквівалентне порушенню доступності інформації, а показник зниження параметру системи відповідає величині збитку Z_i від реалізації атаки. Тому L_i та Z_i в формулі (2) повинні мати однакову розмірність.

На етапах проектування і експлуатації СЗІ ці показники повинні бути пов'язані з відповідними технічними параметрами БІТС.

До параметрів БІТС відносяться:

– пропускна спроможність (C);

– швидкість передачі (V);

– зона покриття (дальність зв'язку D);

– час передачі повідомлення (Δt).

Розглянемо більш детально суть впливу зниження параметрів БІТС при впровадженні МЗІ на зміну ризику під час інформаційного конфлікту.

Першим з параметрів БІТС розглянемо пропускну спроможність.

Пропускна спроможність залежить від відношення сигнал/шум та змінюється в результаті зниження потужності сигналу, як заходу захисту для зменшення зони перехоплення сигналу радіорозвідкою, чи збільшення рівня шуму в ході радіоелектронної боротьби.

Відповідно до теореми Шенона-Хартлі, пропускна спроможність розраховується за формулою [7]:

$$C = B \log_2 \left(1 - \frac{P_{\text{с}}}{P_{\text{ш}}}\right),$$

де $P_{\text{с}}$ – рівень потужність сигналу, $P_{\text{ш}}$ – рівень потужності шуму, B – смуга пропускання каналу зв'язку.

Відповідно до виразу (4) показник зниження пропускної спроможності матиме вигляд:

$$\alpha_{\text{пз}} = C_1 / C_0\,, \qquad (5)$$

де C_0, C_1 – пропускні спроможності БІТС без впливу МЗІ та з врахуванням обмеження МЗІ відповідно.

Наступним показником, що характеризує БІТС, є швидкість передачі. Зниження номінальної швидкості передачі БІТС, як правило, обумовлене появою надлишкової інформації. Прикладом може бути застосування криптографічних алгоритмів захисту інформації, методів автентифікації, контролю цілісності, що призводять до збільшення службової інформації, яка в свою чергу впливає на зменшення частини корисного навантаження та зниження швидкості передачі.

Як відомо, швидкість передачі розраховується за формулою [7]:

$$V = k/T\,, \qquad (6)$$

де k – кількість символів, T – тривалість k-бітового символу.

При впровадженні МЗІ об'єм інформації, що передається, збільшується, а звідси збільшується і кількість символів k, яку необхідно буде передати. При цьому тривалість бітового символу T залишиться постійною.

Для розрахунку відносного значення швидкості передачі інформації $\alpha_{\text{шп}}$, відповідно до виразу (4), приймемо значення відносного зниження швидкості передачі інформації, що буде розраховуватись за формулою:

$$\alpha_{\text{шп}} = V_1 / V_0\,, \qquad (7)$$

де V_1 – швидкість передачі інформації з урахуванням надлишкової службової інформації МЗІ; V_0 – швидкість передачі інформації без використання МЗІ.

В результаті, виходячи з виразу (7), після підстановки відношення (6) отримаємо:

$$\alpha_{\text{шп}} = \frac{V_1}{V_0} = \frac{k_1/T_1}{k_0/T_0} = \frac{k_1 T_0}{k_0 T_1}\,. \qquad (8)$$

Врахуємо те, що при збільшенні надлишкової службової інформації в результаті застосування МЗІ, технічні характеристики системи передачі не змінюються і довжина імпульсу залишається сталою. Відповідно $T_1 = T_0$ вираз (8) прийме кінцеве значення:

$$\alpha_{\text{шп}} = k_1 / k_0\,, \qquad (9)$$

який показує достатність порівняння лише обсяг інформації, що передається через радіоканал БІТС.

В умовах ведення маневрених бойових дій, критичним параметром БІТС спеціального призначення, є дальність зв'язку. Зона покриття радіозв'язку БІТС зменшується внаслідок зниження потужності передавача та визначається відношенням дальностей зв'язку:

$$\alpha_{\text{зп}} = D_1 / D_0\,, \qquad (10)$$

де D_1 – дальність радіозв'язку з урахуванням обмеження в результаті застосування МЗІ; D_0 – дальність радіозв'язку БІТС без впливу МЗІ.

Дальність радіозв'язку враховує характеристики приймального та передавального пристроїв, діапазону частот та втрат потужності

радіосигналу на трасі розповсюдження радіохвиль [7]:

$$D = \sqrt{\frac{P_{\text{прд}} G_{\text{прд}} G_{\text{прм}} \lambda_{\text{прд}}^2 L^2}{(4\pi)^2 P_{\text{с min}}}}, \qquad (11)$$

де $P_{\text{прд}}$ – потужність передавача, що підводиться до антени, $G_{\text{прд}}$ та $G_{\text{прм}}$ – коефіцієнти підсилення передавальної та приймальної антен, $\lambda_{\text{прд}}$ – довжина хвилі радіосигналу, L – множник ослаблення радіо хвиль на трасі розповсюдження, $P_{\text{с min}}$ – мінімально необхідна потужність сигналу на вході приймача (чутливість приймача).

Розглянемо ситуацію зменшення зони радіоперехоплення для підвищення розвідзахищеності БІТС від засобів радіорозвідки. Кореспондент вдається до зменшення потужності передавача, при цьому інші характеристики БІТС залишаються сталими. В результаті, вираз (10) після підстановки формули розрахунку дальності радіозв'язку (11) та скорочення, прийме вигляд:

$$\alpha_{\text{зп}} = P_{\text{прд 1}} / P_{\text{прд 0}}, \qquad (12)$$

де $P_{\text{прд 1}}$ – знижена потужність передавача після реалізації захисних заходів, $P_{\text{прд 0}}$ – максимальна потужність передавача.

Важливим критерієм для БІТС, що функціонують в умовах інформаційних операцій, є доступність інформації. Від швидкості передачі команд управління залежить успіх виконання завдань, тому час передачі повідомлення напряму пов'язаний з доступністю інформації.

В якості показника зміни параметру БІТС системи управління, можна використовувати час передачі (обробки) інформації. Відповідно показник зміни часу обробки інформації прийме вигляд:

$$\alpha_{\text{ч}} = \Delta t_0 / \Delta t_1, \qquad (13)$$

де Δt_1 – час передачі (обробки) інформації з урахуванням затрат на обробку МЗІ; Δt_0 – час передачі інформації без затрат на обробку МЗІ.

Час передачі інформації Δt не повинен перевищувати час старіння інформації $\Delta t_{\max}$, коли інформація перестає бути актуальною та адекватною дійсному стану: $\Delta t < \Delta t_{\max}$. Час старіння інформації або максимально дозволений час передачі інформації може визначатись нормативно (передача повідомлень з різною категорією терміновості) або обмежуватись технічними показниками БІТС (в цьому випадку тісно пов'язаний з пропускною спроможністю).

Проведемо моделювання зміни рівня ризику БІТС відносно значення обмеження параметру БІТС, на прикладі, швидкості передачі даних ультракороткохвильовою (УКХ) радіостанцією Р-005У. Розглянемо динаміку зміни ризику БІТС під час придушення радіолінії. Нехай в ході інформаційної операції станція УКХ радіозв'язку перейшла на завадозахищений режим з використанням псевдовипадкової перестройки радіочастоти. В результаті, швидкість передачі інформації знизилась з 16 до 9.6, 4.8, 2.4, 1.2 кбіт/с, відповідно до різних завадових станів [8].

Таблиця 1
Початкові дані стану БІТС під час атаки радіоелектронного придушення

	Інтенсивність атак придушення радіолінії, λ				
	$0{,}2\cdot\lambda^{opt}$	$0{,}4\cdot\lambda^{opt}$	$0{,}6\cdot\lambda^{opt}$	$0{,}8\cdot\lambda^{opt}$	λ^{opt}
$P_{\text{зб}}$	0,4105	0,4142	0,4177	0,4203	0,4249

Використовуючи вираз (4) та вихідні дані, що отримані за результатами диференційно-ігрового моделювання поведінки БІТС під час встановлення активних радіоелектронних завад в ході інформаційних операцій [9], які представлені в таблиці 1, та попередні дані зміни швидкості передачі, розрахуємо зміну рівнів ризику БІТС в ході інформаційної операції.

Результати моделювання рівня ризику для станції УКХ радіозв'язку, в залежності від зміни швидкості передачі, представлені на рис. 1.

За результатами моделювання можна бачити, що при постійній активності противника (інтенсивність атак) рівень ризику БІТС змінюється, відповідно до зниження параметру БІТС – швидкості передачі інформації внаслідок застосування завадозахищеного режиму.

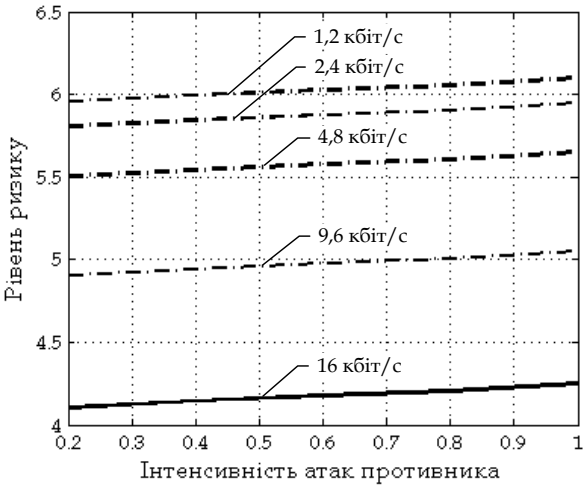

Рис. 1. Залежність рівня ризику від показника зниження швидкості передачі УКХ радіостанції при застосуванні завадо захищеного режиму

Висновки

Метод оцінювання ризиків спеціальних БІТС з урахуванням зміни параметрів БІТС, дозволяє враховувати вплив МЗІ на збільшення ризику внаслідок зменшення таких параметрів БІТС, як пропускна спроможність, швидкість передачі, дальність зв'язку, час передачі повідомлення, що відбувається внаслідок оперативної зміни МЗІ під час інформаційних операцій.

В роботі було проведено моделювання, що показало динаміку зміни рівня ризику при зниженні швидкості передачі інформації БІТС. За результатами моделювання можна зробити висновок про необхідність вибору МЗІ адекватних існуючим загрозам з мінімальним впливом на параметри безпроводових інформаційно-телекомунікаційних

систем. Надлишковість МЗІ може призвести до суттєвого погіршення параметрів продуктивності БІТС, що, в свою чергу, еквівалентно результату атаки на доступність інформації і відповідно повинно враховуватись при оцінці величини збитку.

Представлений метод, може застосовуватись під час проектування СЗІ для БІТС, що дозволить досягти рівноваги між такими показниками системи, як продуктивність та захищеність. Крім того, метод оцінювання ризиків з урахуванням зниження параметрів БІТС може бути використаний для оцінювання ефективності СЗІ.

Література

[1] ISO/IEC 27001:2013 Information technology — Security techniques — Information security management.

[2] Information Operations / Joint Publication 3-13. — DOD, 2012. — p. 69.

[3] Daniel Wentre. Information warfare. — San Francisco, Wiley-ISTE, 2012. — p. 320.

[4] Толубко В.Б. Інформаційна безпека держави у контексті протидії інформаційним війнам: навч. пос. // За заг. ред. В.Б. Толубка. — К. : НАОУ. — 2004. — 315 с.

[5] Астахов А.М. Искусство управления информационными рисками. — М.: ДМК Пресс, 2010. — 312 с.

[6] Скоробагатько Е.А. Методика количественной оценки защищенности телекоммуникационных систем / Е.А. Скоробагатько // Захист інформації. — 2011. — № 3. — С. 9-13.

[7] Скляр Б. Цифровая связь. Теоретические основы и практическое применение. [изд. 2-е испр.] / Б. Скляр: пер. с англ. — М.: Издательский дом «Вильямс». — 2003. — 1104 с.

[8] УКВ радиостанция Р-005У [Электр. ресурс] // официальный сайт ООО «Телекарт-Прибор» — Режим доступу: http://telecard.odessa.ua/production/dlya_silovyh_struktur/sredstva_svyazi/6

[9] Шевченко А.С. Модель процесу придушення радіоліній безпроводових інформаційно-телекомунікаційних систем під час інформаційної боротьби / А.С. Шевченко, О.Є. Мазулевський // Сучасний захист інформації. — 2012. — № 4. — С. 35-40.

УДК 621.396+654.16 (045)

Шевченко А. С., Кокотов О. В. Метод оценивания рисков с учетом влияния механизмов защиты на параметры беспроводных информационно-телекоммуникационных систем во время информационных операций

Аннотация. *В статье рассматривается метод оценки рисков с учетом влияния механизмов защиты на параметры беспроводных информационно-телекоммуникационных систем, функционирующих в условиях реализации атак информационных операций. Метод учитывает дополнительный риск, возникающий при уменьшении параметров беспроводных информационно-телекоммуникационных систем: пропускной способности, скорости передачи, дальности связи, времени передачи сообщений, вследствие применения механизмов защиты информации во время информационных операций, что является дополнительным риском во время боевых действий. При применении приведенного метода в статье представлены результаты моделирования влияния уменьшения скорости передачи данных ультракоротковолновой станцией при применении помехозащищенных режимов в различных помеховых состояниях на изменение общего риска и связь с результатами предыдущих исследований.*

Ключевые слова: *беспроводные информационно-телекоммуникационные системы, информационные операции, методы оценки рисков, уровень риска, параметры беспроводных информационно-телекоммуникационных систем, пропускная способность, скорость передачи, дальность связи.*

Shevchenko A., Kokotov O. Method of risk assessment considering the security mechanism influence on parameters of the wireless information & telecommunication systems in the information operations

Abstract. *In this paper the method of risk assessment for the effects of protection mechanisms in the wireless information & telecommunication systems, which operate in the implementation of information operations attacks. The method takes into account the additional risk that arises in the application of mechanisms to protect information when information conflicts, which reduces the specific parameters of wireless information & telecommunication systems: its handling capacity, transmission speed, communication range, time of communication, which is an additional risk under the fighting. In applying the method reduced the article presents the results of modeling of reducing the data rate UV station in the application of noise -interference regime in different states to change the overall risk and relation with the results of previous studies.*

Key words: *wireless information & telecommunication systems, information operations, methods of risk assessment, risk level, options of wireless information & telecommunication systems, handling capacity, transmission speed, communication range.*

Отримано *13 січня 2014 року*, затверджено редколегією *30 січня 2014 року*