Міністерство освіти і науки України
Одеська національна академія зв'язку ім. О.С. Попова

Третя всеукраїнська науково-практична конференція

"ПЕРСПЕКТИВНІ НАПРЯМИ ЗАХИСТУ ІНФОРМАЦІЇ"

02 – 06 вересня 2017 року

Збірник тез

Одеса
ОНАЗ
2017

УДК 004.056.5

Перспективні няпрями захисту інформації: матеріали третьої всеукраїнської наук.-пр. конф. – м. Одеса, 02-06 вересня 2017 р. – Одеса: ОНАЗ, 2017. – 104 с.

Даний збірник містить тези матеріалів, що представлені на третю всеукраїнську науково-практичну конференцію "**Перспективні няпрями захисту інформації**", що проводиться 02-06 вересня 2017 р. в Одеській національній академії зв′язку ім. О.С. Попова.

У збірник включені тези доповідей за такими напрямками:

- організаційно-правові методи захисту інформації;
- системи ідентифікації і обробки персональних даних;
- системи квантової криптографії;
- технічні засоби виявлення каналів витоку інформації;
- засоби захисту інформації в інформаційних і телекомунікаційних системах;
- елементи і компоненти для систем захисту інформації;
- методи та засоби захисту господарських об'єктів.

Робочі мови конференції – українська, російська, англійська.

Програмний комітет

Воробієнко П.П.	голова, д.т.н., проф., ректор ОНАЗ ім. О.С. Попова
Каптур В.А.	заступник голови, к.т.н., с. н. с., проректор з наукової роботи ОНАЗ ім. О.С. Попова
Васіліу Є.В.	д.т.н., проф., директор Навчально-наукового інституту Радіо, телебачення та інформаційної безпеки ОНАЗ ім. О.С. Попова
Гнатюк С.О.	к.т.н., доц. каф. безпеки інформаційних технологій, Національний авіаційний університет
Захарченко М.В.	д.т.н., проф., зав. каф. інформаційної безпеки та передачі даних, ОНАЗ ім. О.С. Попова
Кільдішев В.Й.	к.т.н., доц. каф. інформаційної безпеки та передачі даних, ОНАЗ ім. О.С. Попова
Корченко О.Г.	д.т.н., проф., зав. каф. безпеки інформаційних технологій, Національний авіаційний університет
Корчинський В.В.	д.т.н., проф. каф. інформаційної безпеки та передачі даних, ОНАЗ ім. О.С. Попова
Ніколаєнко С.В.	к.т.н., доц. каф. інформаційних технологій, ОНАЗ ім. О.С. Попова;
Оксіюк О.Г.	д.т.н., проф., зав. каф. кібербезпеки та захисту інформації, Київський національний університет ім. Тараса Шевченко
Онацький О.В.	к.т.н., доц. каф. інформаційної безпеки та передачі даних, ОНАЗ ім. О.С. Попова
Рудницький В.М.	д.т.н., проф., зав. каф. системного програмування, Черкаський державний технологічний університет

Організаційний комітет

Васіліу Є.В.	д.т.н., проф., директор навчально-наукового інституту радіо, телебачення та інформаційної безпеки, ОНАЗ ім. О.С. Попова
Пилявський В.В.	к.т.н., відповід. за навчальну та наукову роботу навчально-наукового інституту радіо, телебачення та інформаційної безпеки, ОНАЗ ім. О.С. Попова
Марколенко П.Ю.	к.т.н., доц., відповід. за профорієнтаційну роботу навчально-наукового інституту радіо, телебачення та інформаційної безпеки, ОНАЗ ім. О.С. Попова
Рябуха О.М.	к.т.н., викл. каф. інформаційної безпеки та передачі даних, ОНАЗ ім. О.С. Попова
Кільдішев В.Й.	к.т.н., доц. каф. інформаційної безпеки та передачі даних, ОНАЗ ім. О.С. Попова
Севастєєв Є.О.	ст. викл. каф. інформаційної безпеки та передачі даних, ОНАЗ ім. О.С. Попова;
Михайлова Л.В.	викл. каф. інформаційної безпеки та передачі даних, ОНАЗ ім. О.С. Попова
Лімарь І.В.	ст. наук. співробітник, ОНАЗ ім. О.С. Попова
Лазукін В.О.	директор бази відпочинку «Електрон»

УДК 512.77+004.056.5+003.26

Беспалов О.Ю.
Аспірантура НТУУ «КПІ імені Ігоря Сікорського»
alexb5dh@gmail.com
Панасюк І.І.
Компанія «ДЕПС Україна»
igor.panassiouk@gmail.com

МЕТОД ЛЄНСТРА ТА ОСОБЛИВОСТІ ЙОГО ЗАСТОСУВАННЯ НА КРИВИХ ЕДВАРДСА

Анотація. *У роботі вперше запропоновано метод факторизації чисел, який є аналогом методу Лєнстра на кривих Едвардса. Всі твердження, які необхідні для обґрунтування цього методу, є строго доведеними. Розроблено відповідний алгоритм та проведено порівняльний аналіз нового та класичного алгоритмів. Показано, що новий алгоритм має переваги як у швидкодії, так і в імовірності успіху у порівнянні з класичним алгоритмом Лєнстра.*

Вступ. Метод Лєнстра [1-4, 6] є одним з найшвидших загальних методів факторизації цілих чисел. Він використовує еліптичну криву над полем раціональних чисел і деяку її редукцію за цілим модулем і потребує близько $2\log_2 k$ додавань точок цієї кривої, де k – параметр алгоритму, вибір якого впливає на імовірність успіху алгоритму. Отже, час роботи алгоритму Лєнстра пропорційний часу додавання точок кривої. Цей факт природно наводить на думку використовувати для реалізації цього методу такі еліптичні криві, на яких операція додавання точок виконується найшвидше, а саме – криві Едвардса.

Проте слід зазначити, що класичний алгоритм Лєнстра базується на деякій властивості еліптичних кривих у формі Вейєрштраса, якої немає у кривої Едвардса. Ця властивість – наявність нескінченно віддаленої точки, яка не має координат і, отже, не є розв'язком рівняння відповідної кривої. Тому безпосередньо перенести метод Лєнстра на криві Едвардса не можна.

У цій роботі буде показано, як можна модифікувати метод Лєнстра, щоб його можна було застосувати до кривої Едвардса.

Також на початку роботи буде наведено огляд "прообразів" методу Лєнстра на еліптичних кривих, потім класичний алгоритм, а потім алгоритм, модифікований для кривої Едвардса, а також оцінки часу його роботи та імовірність успіху.

Також буде показано, що умови його успішного застосування є більш широкими, ніж це описано у класичних роботах, тому і імовірність успіху буде більшою, ніж там зазначено.

1. Прообраз класичного методу Лєнстра – $p-1$ метод Поларда. Ми почнемо з опису $p-1$ методу Поларда [4-6], який можна вважати прообразом методу Лєнстра. Успішне застосування методу Поларда можливе не для всіх чисел, а лише до чисел певного виду. У таких випадках він є досить ефективним. Далі коротко пояснимо ідею цього методу.

Нехай нам треба знайти прості дільники складеного числа n. Припустимо, що один з простих дільників p цього числа має таку властивість: всі прості дільники числа $p-1$ **є** "малими" – наприклад, не перевищують деякого числа B.

Нехай a – деяке натуральне число, таке, що (a, p)=1. Тоді за малою теоремою Ферма, $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$, тобто $p \mid a^{p-1}-1$, отже $\left(n, a^p-1\right) = p$.

Але число p нам невідоме, тому ми діємо наступним чином. Нехай $s_1, s_2, ..., s_r$ – перші r простих чисел, $e_1, e_2, ..., e_r$ – невеликі прості числа. Обчислимо

$$k = \prod_{i=1}^{r} s_i^{e_i} . \tag{1}$$

Робота алгоритму буде успішною, якщо

$$p-1 \mid k . \tag{2}$$

Дійсно, за умови (2) виконується рівність $a^k \equiv 1 (\mathrm{mod}\, p)$, тому

$$\left(n, a^p - 1\right) = p . \tag{3}$$

Слід зазначити, що рівність (2) не є необхідною умовою виконання рівності (3). Дійсно, нехай $(a, p) = 1$, тоді $ord\left(a \bmod p\right) = l \mid p-1$. Тоді для того, щоб виконувалась умова (3), достатньо, щоб виконувалась умова

$$ord\left(a \bmod p\right) \mid k . \tag{4}$$

2. Класичний алгоритм Лєнстра. Метод, запропонований Лєнстра [1-3], позбавлений цього недоліку. Причиною цього є те, що група, у якій працює метод Лєнстра, для одного і того ж числа p може бути побудована багатьма різними способами, і наявність у ній елементів малих порядків не залежить від розкладу числа $p-1$ на множники (на відміну від методу Поларда, який може працювати лише у групі Z_p^*).

Основна ідея методу Лєнстра полягає у тому, щоб замість групи Z_p^* використовувати групу E_p точок деякої еліптичної кривої над полем F_p, а замість числа a – деяку точку P цієї кривої.

Час роботи алгоритму, за оцінками з тієї ж роботи, є

$$\mathrm{O}\left(2^{\lambda(\log n)^{\frac{1}{2}}(\log\log n)^{\frac{1}{2}}}\right) \tag{5}$$

для деякого $\lambda > 0$, де параметр λ залежить від часу виконання додавання точок на кривій.

3. Алгоритм Лєнстра на кривих Едвардса. Вперше рівняння еліптичної кривої у формі, яка згодом дістала назву "форма Едвардса", було запропоновано у роботі [7]. У цій же роботі був доведений ізоморфізм (за певних умов) між кривими у формі Вейєрштраса та у формі Едвардса. Проте криві, запропоновані у [7], були слабкими з криптографічної точки зору. Але після роботи [7] швидко з'явилась робота [8], де криві Едвардса були модифіковані шляхом введення деякого параметра. Рівняння кривих, запропонованих у [8], над скінченнім полем характеристики $p > 2$ мають вигляд:

$$E:\ x^2 + y^2 = e^2\left(1 + dx^2y^2\right),$$

де параметр d є квадратичним нелишком за модулем p.

Тут і далі для спрощення ми будемо вважати $e = 1$ і розглянемо криву E_p, задану над простим полем F_p рівнянням

$$x^2 + y^2 = 1 + dx^2y^2,\ \left(\frac{d}{p}\right) = -1 . \tag{6}$$

Основними відмінностями (майже всі з яких є перевагами) кривої Едвардса у порівнянні з кривою Вейєрштраса є наступні.

1. Універсальність закону додавання. Дійсно, операції додавання різних точок різних точок та подвоєння точки звдвються одними й тими ж формулами:

$$\left(x_1, y_1\right) + \left(x_2, y_2\right) = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}\right). \tag{7}$$

2. Відсутність "точки на нескінченості". Так, нейтральним елементом є звичайна точка кривої Едвардса з координатами $(0,1)$, які, очевидно, задовольняють рівнянню (7).

3. Група E_p завжди циклічна.

4. Порядок групи E_p завжди ділиться на 4.

5. Рекордна швидкість додавання точок. Ця властивість є основною перевагою кривої Едвардса. Так, при додаванні двох (різних) точок кривої Едвардса потрібно приблизно у 1,4 рази менше бітових операцій, ніж при додаванні точок кривої у формі Вейєрштраса Особливо значний виграш у швидкодії для так званих скручених кривих Едвардса, рівняння яких відрізняється від рівняння (7) наявністю деякого додаткового параметра [9, 10].

Теорема 1.

Нехай

$$d \in Q_p \tag{8}$$

і деяка крива задана рівнянням

$$\widetilde{E}_p:\ x^2 + y^2 = 1 + dx^2 y^2 \tag{9}$$

над F_p. Тоді для будь-якої точки $(x_1, y_1) \in \widetilde{E}_p$ знайдеться така точка $(x_2, y_2) \in \widetilde{E}_p$, що

$$dx_1 x_2 y_1 y_2 \equiv 1 (\mathrm{mod}\ p). \tag{10}$$

Аналогічно, для будь-якої точки $(x_1, y_1) \in \widetilde{E}_p$ знайдеться така точка $(x_2, y_2) \in \widetilde{E}_p$, що

$$dx_1 x_2 y_1 y_2 \equiv -1 (\mathrm{mod}\ p). \tag{11}$$

Виходячи з викладеного вище, можна побудувати наступний алгоритм Лєнстра для кривої Едвардса.

Алгоритм Лєнстра на кривих Едвардса

Вхід: n – складене.

1. Випадково вибираємо x_0, y_0 від 2 до n.

2. Обчислюємо $D_1 = (x_0, n)$ та $D_2 = (y_0, n)$. Якщо $1 < D_i < n$, $i = 1, 2$, то $p = D_i$. Алгоритм виводить значення p і завершує роботу.

3. Обчислюємо $x_0^{\,2} + y_0^{\,2} - 1$.

4. Обчислюємо $D_3 = (x_0^{\,2} + y_0^{\,2} - 1, n)$. Якщо $1 < D_3 < n$, то $p = D_3$. Алгоритм виводить значення p і завершує роботу. Якщо $D_3 = n$, то повертаємось до кроку 1.

5. Якщо $\left(\dfrac{x_0^{\,2} + y_0^{\,2} - 1}{n}\right) = 1$, то повертаємось до кроку 1 і обираємо нові значення.

6. Обчислити $d = (x_0^{\,2} + y_0^{\,2} - 1)(x_0^{\,2} y_0^{\,2})^{-1}$.

7. Далі розглядаємо еліптичну криву у формі Едвардса $\widetilde{E}_n:\ x^2 + y^2 = 1 + dx^2 y^2$ та точку на ній $P(x_0, y_0)$.

8. Обираємо k, що має вигляд (1) (або обираємо будь-яким іншим чином, так, щоб k мало багато невеликих простих дільників).

9. Послідовно з використанням схеми Горнера обчислюємо kP за формулами (7). При цьому кожного разу при додаванні точок $P_1(x_1, y_1)$ та $P_2(x_2, y_2)$ обчислюємо D_i, $i = 4, 5, 6, 7$ за формулами:

$$D_4 = (1 + dx_1 y_1 x_2 y_2, n),\ D_5 = (1 + dx_1 y_1 x_2 y_2, n),$$
$$D_6 = (x_1 y_2 + x_2 y_1, n),\ D_7 = (y_1 y_2 - x_1 x_2, n).$$

10. Якщо в ході обчислень виникла ситуація, коли при додаванні точок $P_1(x_1, y_1)$ та $P_2(x_2, y_2)$ для деякого $i = 4, 5, 6, 7$ $1 < D_i < n$, то $p = D_i$. Алгоритм виводить значення p і завершує роботу.

11. Якщо ж при обчисленні kP не вдалося знайти нетривіальний дільник числа n, то повертаємось до кроку 1 і перевибираємо x_0, y_0, або ж збільшуємо значення.

Висновки. У цій роботі наведено новий алгоритм, що є аналогом алгоритму Лєнстра на кривих Едвардса. Показано, що перевагою цього алгоритму є не лише підвищення швидкодії, але і збільшення імовірності його успіху.

Література

1. Lenstra A.K., Lenstra H. W.Jr. Algorithms in number theory. – Technical Report 87-008. Chicago: University of Chicago, 1987.

2. Lenstra H. W. Jr. Elliptic curves and number-theoretic algorithms. – Report 86-19. Amsterdam: Mathematisch Instituut, Universiteit van Amsterdam, 1986.

3. Lenstra H. W. Jr. Factoring integers with elliptic curves. – Ann. Math., 1987, v. 126, p. 649-673.

4. Koblitz N. A Course of Number Theory and Cryptography.- Berlin: Springer, 1994.-231p.

5. Pollard J. M. Theorems on factorization and primality testing. – Proc. Cambridge Phil. Soc, 1974, v. 76, p. 521-528**.**

6. Ю.П. Соловьёв, В.А. Садовничий, Е.Т. Шавгурлидзе, В.В. Белокуров. – Эллиптические кривые и современные алгоритмы теории чисел. – М.: Ижевск, 2003. – 192 с.

7. Edwards H.M. A normal form for elliptic curves. Bulletin of the American Mathematical Society, Volume 44, Number 3, July 2007, PP. 393-422.

8. Berstein D.J., Lange T. Faster Addition and Doubling on Elliptic Curves // Advanced in Cruptology – ASIACRYPT'2007 (Proc. 13th Int. Conf. On the Theory and Application of Cryptology and Information Security. Kuching, Malaysia. December 2-6, 2007). LNCS, V 4833. Berlin: Springer, 2007, PP. 29-50.

9. Бессалов А.В. Эллиптические кривые в форме Едвардса и криптография: монография. – Киев, КПИ им. Игоря Сикорского, изд. «Политехника», 2017. – 272 с.

10. Berstein Daniel J., Birkner Peter, Joye Marc, Lange Tanya, Peters Christiane. Twisted Edwards Curves. // IST-2002-507932 ESRYPT, and in part by the National Science Foundation under grant ITR-0716498, 2008, PP. 1-17.

11. L Kovalchuk, A. Bessalov. Exact Number of Elliptic Curves in the Canonical Form, Which are Isomorphic to Edvards Curves Over Prime Field // Cybernetics and Systems Analysis, volume 51, issue 2, 2015, p. 165-172.

12. Бессалов А.В., Дихтенко А.А. Киптостойкие кривые Эдвардса над простыми полями // Прикладная радиоэлектроника. – 2013. – Том 12. – № 2. – С. 285-291.

УДК 004.056

Бондар І.С.
Національний авіаційний університет
6ira.bondar6@gmail.com
Лозова І.Л.
Національний авіаційний університет

СИСТЕМА МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИВАТНОГО ПІДПРИЄМСТВА

Анотація. *Успіх сучасного підприємства та його розвиток, перш за все, залежать від ступеня захищеності та забезпечення інформаційної безпеки(ІБ). В даний час, підприємство, що знаходиться в умовах жорсткої конкуренції, потребує побудови ефективної системи менеджменту інформаційної безпеки (СМІБ). З швидким розвитком інформаційних систем, проблема забезпечення безпеки загострюється. СМІБ, у свою чергу, несе відповідальність за безпеку інформаційно-важливих активів підприємства, а також забезпечення цілісності та доступності працездатності високотехнологічного обладнання.*

З кожним днем з'являються нові загрози, які здатні нанести збитків організації. Це зокрема хакерські дії, соціальна інженерія, втручання до системи, злом, несанкціонований доступ до системи, комп'ютерні злочини, продаж інформації, атаки на систему, перегляд інформації з обмеженим доступом, фальсифікація та підроблення даних, зловмисні коди (віруси, логічні бомби, "троянські коні"), продаж персональної інформації, дефекти системи тощо. Можна стверджувати, що такі загрози з часом набуватимуть все більшого поширення [1].

СМІБ - одна з основ життєдіяльності організації. Побудова СМІБ дозволяє описати, як пов'язані процеси і підсистеми ІБ на підприємстві, хто є відповідальний за них, які фінансові та трудові ресурси необхідні для їх ефективного функціонування. Система управління інформаційною безпекою на підприємстві об'єднує всі організаційні та захисні заходи, що використовуються в єдиний комплекс, який адекватний реальним загрозам і дозволяє досягати корпоративних цілей інформаційної безпеки на рівні всього підприємства.

Метою роботи є підвищення рівня захищеності активів приватного підприємства (ПП), шляхом розробки та впровадження системи менеджменту інформаційної безпеки.

«Загальна система менеджменту» компанії включає в себе набагато більше, ніж просто безпеку. Існує декілька стандартів по системах менеджменту у відповідності з ISO. Сімейство ISO 9000 включає в себе серію стандартів,які відносяться до систем менеджменту якості. Сімейство ISO 14000 - набір стандартів з систем екологічного менеджменту. ISO 27000 – це сімейство стандартів на системи менеджменту безпеки. Тому ISO може використовуватись для всіх систем менеджменту, а також визначити дії, необхідні для створення, підтримки та поліпшення менеджменту інформаційної безпеки [2].

З 4 по 8 розділів стандарту ISO 27001 випливає, що компанія повинна побудувати і впровадити свою СМІБ, включаючи основні вимоги щодо створення, управління, моніторингу і підтримки. Після впровадження СМІБ, компанія може офіційно забезпечувати безпеку інформації і продовжувати виконувати вимоги клієнтів, законодавств, регуляторів і акціонерів [3].

Варто згадати модель PDCA, що існує для впровадження СМІБ на основі стандарту ISO 27001. Етапи PDCA дозволяють встановити політику, цілі, процеси та процедури, відповідні оброблюваним ризиків (етап планування – Plan), впровадити і використовувати (етап виконання – Do), оцінювати і вимірювати результати процесу з точки зору політики (етап перевірки – Check), виконувати коригувальні та превентивні дії (етап поліпшення – Act).

Для даного ПП, СМІБ впроваджується за рахунок чотирнадцяти етапів, відповідно до вимог міжнародного стандарту ISO / IEC 27001.

У зв'язку з великими об'ємами конфіденційної інформації, що циркулює на підприємстві, питання інформаційної безпеки повинне розглядатися гостро. Щодо захисту інформаційних ресурсів, їх циркулювання у мережі та на програмному рівні, використовуються стандарти ISO 27001/27002. Оскільки організація керується стандартами у своїй роботі, її діяльність задокументована, завдання організації процесу захисту інформації цілком усвідомлене керівництвом, та ставиться задача розробки документації, і впровадження її в дію, а також зниження ризиків інформаційним активам.

Оцінка можливих ризиків ПП здійснюється за допомогою програмного засобу Microsoft Security Assessment Tool. Засіб включає в себе опитувальник із більше ніж 200 питань, в результаті яких формується загальна картина процесу організації безпеки на підприємстві. Оцінка призначена для виявлення ризику для бізнесу організації і визначення заходів безпеки, що існують для зниження ризику.

Після впровадження всіх етапів СМІБ на ПП, та побудови порівняльних діаграм за допомогою MSAT, було зроблено висновок, що за рахунок розробки та впровадження СМІБ: захищеність активів ПП зросла на 47%, а рівень ризику зменшився на 18%.

Таким чином підприємство отримує такі вигоди:

- Інформаційні активи стали зрозумілими для менеджменту компанії.
- Загрози та вразливості безпеки регулярно виявляються.
- Ризики прораховуються і рішення приймаються на основі бізнес-цілей компанії.

– Ефективне управління інформаційними активами в критичних ситуаціях.
– Проводиться процес виконання політики безпеки (знаходити і виправляти слабкі місця в системі інформаційної безпеки в регулярному режимі).

Література

1. Вяткин В.Н. Риск-менеджмент / И.В. Вяткин, В.А. Гамза, Ю.Ю. Екатериносла-вский, Дж.Дж Хэмптон; И. Юргенс. – М: Дашков и К. – 2003. – 494 с.
2. Нестеров С. А. Информационная безопасность и защита информации: учеб. пособие / С.А. Нестеров. – СПб.: Изд-во Политехн. ун-та. – 2009. – 126 с.
3. Информационная безопасность. Система менеджмента информационной безопасности. [Електронний ресурс]. – Режим доступу до ресурсу:http://dorlov.blogspot.com/2011/06/iso-27001-2.html

УДК 003.26:621.39+530.145

Василиу Е.В.
д.т.н, профессор,
директор УНИ РТиИБ ОНАС им. А.С. Попова
irte@onat.edu.ua
Лимарь И. В.
ОНАС им. А.С. Попова, научный сотрудник
quantum.biology@outlook.com

АТАКИ НА КВАНТОВЫЕ СИСТЕМЫ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ, ЭКСПЛУАТИРУЮЩИЕ УЯЗВИМОСТЬ ОБОРУДОВАНИЯ

Аннотация. *Рассматриваются некоторые основные угрозы для конфиденциальной передачи данных с использованием квантовых криптосистем. Показывается роль уязвимостей аппаратуры в реализации нападений (хакинга) на системы квантовой криптографии. Описывается концепция атаки «Троянский конь» а также атаки «ослепления» систем квантового распределения ключей, конструкция детекторов которых основана на использовании лавинных фотодиодов нескольких различных типов. Анализируется ряд современных средств и методов противодействия данным видам хакинга*

Введение. Главным критерием, по которому оценивается приемлемость использования средств защищенной передачи данных, является, как известно, стойкость к различного рода атакам. Применительно к квантовым криптосистемам следует констатировать, что к настоящему времени уже предложены протоколы [1], для которых существуют формальные доказательства теоретико-информационной стойкости, позволяющие приравнивать их по критерию криптоанализа к шифру одноразового блокнота (шифру Вернама) [2]. В то же время, использование абсолютно стойких шифров, как в классической, так и в квантовой криптографии само по себе еще не дает полной гарантии успешного обеспечения секретной связи. И в первом и во втором случае злоумышленник может попытаться использовать для несанкционированного получения информации конструктивные особенности аппаратуры и физические принципы лежащие в основе функционирования её устройств. В силу того, что промышленный выпуск коммерчески доступных систем квантового распределения ключей начался лишь немногим более 10-ти лет назад, существующие уязвимости выявляются именно на данном этапе развития квантовой криптографии [3].

Атака «Торянский конь». Одной из самых эффективных атак, использующих уязвимости аппаратуры в настоящее время является атака «Троянский конь». Рассмотрим установку квантового распределения ключей с модуляцией фазы, частью которой является

модуль передатчика. Злоумышленник (Ева) вводит свет в аппаратуру легитимного пользователя-отправителя (Алиса) через то же оптоволокно которое служит квантовым каналом между пользователями. Цель злоумышленника состоит в том, чтобы достигнуть фазового модулятора, который кодирует секретную информацию φ_A. Ева может использовать испускаемые лазером импульсы со средним числом фотонов μ_{in} , которые находятся к когерентном состоянии $\left|\sqrt{\mu_{in}}\right\rangle$. Импульсы приобретают информацию о фазовой модуляции φ_A и возвращаются к Еве как $\left|e^{i\varphi_A}\sqrt{\mu_{out}}\right\rangle$, где $\mu_{out}=\gamma\mu_{in}$ со значением оптической изоляции передающего модуля $\gamma << 1$. Световой импульс полученный Евой коррелирует с фазой φ_A и это ставит под угрозу безопасность системы.

Чтобы предотвратить атаку троянского коня Алиса может скорректировать величину оптической изоляции γ , чтобы сделать μ_{out} и, следовательно, информацию, ушедшую к Еве произвольно малой.

Авторы работы [4] обозначают через *N* максимальное число фотонов, которое система защиты позволяет ввести Еве в модуль передатчика легитимного пользователя за один такт без нарушения целостности оптоволоконного кабеля.

При осуществлении атаки Троянского коня Ева сначала приготавливает *M* групп фотонов, а затем использует каждую группу для различных величин фазового модулятора Алисы. Предполагается [4], что каждая группа фотонов соответствует одному импульсу источника света Евы и что каждый импульс приготовлен в чистом когерентном состоянии. В итоге система характеризуется тензорным произведением когерентных состояний:

$$\left|\sqrt{\mu_1}\right\rangle\otimes\left|\sqrt{\mu_1}\right\rangle\otimes\ldots\otimes\left|\sqrt{\mu_M}\right\rangle \tag{1}$$

где $\mu_i\left(i=1,\ldots,M\right)$ – среднее число фотонов *i*-го когерентного состояния. Чтобы не преодолеть порог нарушения целостности оптоволокна Ева вынуждена соблюдать следующее условие:

$$\sum_{i=1}^{M}\mu_i = M\mu_{in} < N \tag{2}$$

которым вводится общее среднее число фотонов Евы μ_{in}. В работе [4] показано, что варьирование Евой значений μ_i не дает ей преимуществ в ходе атаки.

Каждый из троянских импульсов Евы отправляется в модуль передачи, чтобы зондировать различные величины фазы φ_A фазового модулятора Алисы. После этого импульсы получаются Евой, для них среднее число фотонов составляет $\mu_{out}=\gamma\mu_{in}$. В работе [4] через f_A называется общее число значений фазы закодированных фазовым модулятором Алисы за 1 секунду. Это равно тактовой частоте фазового модулятора, выраженной в Гц. Поскольку Алиса знает f_A, максимальное количество троянских фотонов в секунду *N* и степень оптической изоляции (γ), она может ограничивать среднее число фотонов троянских импульсов, выходящих из ее модуля. В свою очередь через μ_{out} обозначается [4] верхняя граница. Она составляет

$$\mu_{out}=\frac{N\gamma}{f_A}, \tag{3}$$

μ_{out} – решающий параметр в аргументации безопасности, потому что он непосредственно управляем Алисой. Это может быть интерпретировано как среднее количество фотонов троянских импульсов, полученных Евой.

Атаки «ослепления». Наряду с нападением Троянского коня другой значимой угрозой системам квантового распределения ключей, в том числе выпускаемых промышленно, являются выделяемые в отдельный класс атаки, получивший в литературе название «удаленное управление детекторами единичных фотонов с использованием адаптированного яркого освещения». В силу характерной стратегии используемой при осуществлении нападения такого типа мы полагаем, что этот вид атак следует также относить к уже существующему и хорошо известному классу «атака человек посредине». Для краткости мы также далее будем именовать такое нападение «атака ослепления», основываясь на основном методе передаче легитимной стороне ложной информации – управлении злоумышленником приемными детекторами путем направления через коммуникационный канал интенсивных импульсов света.

При осуществлении атак на криптосистемы в криптографии хорошо известен подход, именуемый «человек посредине». Суть его заключается в установке на коммуникационном канале между легитимными пользователями оборудования злоумышленника. Такое техническое устройство предназначено для перехвата информации направленной легитимным пользователем отправителем Алисой и, по возможности, криптоанализу этих данных. Кроме того, далее злоумышленник может сформировать поддельный, нужной ему конфигурации набор данных и отправляет его легитимному получателю – Бобу. Таким образом Ева осуществляет перехват с последующим криптоанализом и/или манипулирование информацией которой обмениваются легитимные пользователи с искажением её необходимым ей (Еве) образом.

Аналогичный подход был предложен в свое время и для нападения на системы квантового распределения ключей [5]. В литературе он получил название «атаки с использованием «фальшивых состояний».

Изначально в работе [5] нападение на квантовую криптосистему с использованием фальшивых состояний позиционировалось как разновидность атаки «человек посредине», в ходе которой Ева не пытается восстановить исходные состояния, но генерирует вместо этого световые импульсы, которые обнаруживаются легитимными сторонами, которыми Ева манипулирует, не повышая в коммуникационном канале уровня ошибок которые бы говорили Алисе и Бобу об опасности.

Известно, что нападение «человек посредине» - стратегия, обреченная на неудачу, если Ева попытается просто, без каких-либо дополнительных мероприятий, направить Бобу такие же квантовые состояния которые обнаружены ею при перехвате сообщения Алисы. Однако легитимные стороны можно было бы попытаться ввести в заблуждение применяя определенные методики. используя недостатки их оборудования. То есть, задача заключается в том, чтобы, чтобы легитимные пользователи полагали, что они обнаруживают исходные квантовые состояния, в то время как они на самом деле ими бы обнаруживались световые импульсы, сгенерированные Евой. Эти световые импульсы называются фальшивыми состояниями.

Во всех разработанных в последствии атаках ослепления нападение Евы успешно тогда, когда она вынуждает Боба обнаружить фотоны не в случайным образом выбранном основании, а в основании, выбранном и диктуемым Бобу Евой. Ева осуществляет подключение к участку оптоволокна, соединяющего аппаратуру Алису и Боба. Затем Ева, фиксируя свои измерительные базисы накапливает значение для каждого квантового состояния, которое она обнаруживает. После чего она отправляет фальшивое состояние Бобу для каждого обнаруженного квантового состояния, обеспечивая выбор Бобом базис обнаружения. Боб всегда обнаруживает состояние в основании, запрограммированном Евой. Присутствие Евы остается скрытым, потому что после шага просеивания все биты в сыром ключе были обнаружены ею в надлежащем основании, и последующая проверка Алисой и Бобом не показывает увеличения квантового коэффициента битовых ошибок (QBER).

Вопросом оставалось как именно вынудить Боба считать, что он выполнил измерение в том или ином базисе. Техническое решение было найдено путем использования некоторых особенностей детекторов систем квантового распределения ключей. В значительной части

промышленно выпускаемых квантовых криптосистем для регистрации фотонов используются лавинные фотодиоды – твердотельные аналоги фотоэлектронных умножителей. Они различаются по способу подавления «лавины» – гашения тока возникающего при регистрации фотона. В устройствах квантового распределения ключей используются детекторы с активным и пассивным подавлением, а также со стробирующим импульсом – «стробом».

Детекторы единичных фотонов на основе лавинных фотодиодов могут быть временно ослеплены относительно ярким светом. Режим яркого света, очень хорошо подходит для нападения на систему квантового распределения ключей, содержащую такие детекторы. В этом режиме, все детекторы в приемнике Боба одинаково ослеплены непрерывным освещением, прибывающим от злоумышленника Евы. Ева отправляет импульсы яркого света, чтобы перевести детекторы из режима Гейгера в линейный режим, в котором детекторы ведут себя как классические детекторы [6-8]. Затем через адаптированные яркие импульсы (называемыми также запускающими импульсами), Ева может управлять функциями отклика детекторов. Так, например, она может обеспечить такую конфигурацию фальшивых состояний, что «щелчки» в соответствующих детекторах Боба происходят, только если являются одинаковыми соответствующие измерительные базисы Евы и Боба, и, как следствие, отсутствует повышение уровня ошибок. То есть цель состоит в том, чтобы преобразовать ответ устройства измерения Боба в то, которое зависит от стратегий нападения Евы. Когда Еве нужен определенный детектор Боба, чтобы произвести «щелчок» (регистрацию фотона), она изменяет поляризацию (или другие параметры, используемые, чтобы закодировать квантовые состояния) света, который она отправляет Бобу, таким образом, что целевой детектор прекращает получать свет, в то время как другой детектор (детекторы) продолжает освещаться. Ева возвращает целевому детектору способность регистрировать единичные фотоны и, когда Ева изменяет поляризацию снова, происходит единственный (отдельный) «щелчок». Таким образом Ева имеет полный контроль над Бобом и может успешно выполнить атаку «человек посредине».

Эффективное осуществление нескольких видов атак ослепления, в том числе, на промышленно выпускаемые образцы квантовых систем распределения ключей, вызвало необходимость разработки соответствующих контрмер. Одним из наиболее удачных протоколов, препятствующих нападениям, использующим несовершенство оборудования, признано решение, предложенное в работе [9]. В данной публикации описан оригинальный протокол, который не только позволяет бороться с атаками ослепления, но также и в два раза увеличивает возможное расстояние между пользователями, осуществляющими распределение ключей шифрования. Это становится возможным в силу того, что в установке используется два лазерных источника – по одному у каждого пользователя, а сама процедура квантового измерения осуществляется между пользователями на равном удалении от каждого из них.

Выводы. Устройства квантового распределения ключей, выпускаемые промышленностью на ранних этапах развития рынка данного оборудования оказались подвержены атакам использующим уязвимость аппаратуры. Наиболее известными из них являются атаки «Троянского коня» и «ослепление». С целью обеспечения приемлемой с точки зрения безопасности работы устройств квантовой криптографии для противодействия указанным видам нападений были разработаны соответствующие контрмеры.

Публикация содержит результаты исследований, проведенных при грантовой поддержке Государственного фонда фундаментальных исследований Украины по конкурсному проекту Ф73/49-2017.

Литература

1. Lum D.J. Quantum enigma machine: Experimentally demonstrating quantum data locking / D.J. Lum, J.C. Howell, M.S. Allman, T. Gerrits, V.B. Verma, S.W. Nam, C. Lupo, and S. Lloyd // Physical Review A. – 2016. – Vol. 94, Issue 2. – 022315.

2. Зубов, А. Ю. Совершенные шифры / А. Ю. Зубов. - М.: Гелиос АРВ, 2003. –160 с.

3. Jain N. Attacks on practical quantum key distribution systems (and how to prevent them) / N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt & G. Leuchs // Contemporary Physics. – 2016. – Vol. 57, Issue 3. – PP. 366-387.

4. Lucamarini M. Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution / M. Lucamarini, I. Choi, M.B. Ward, J.F. Dynes, Z.L. Yuan, and A.J. Shields // Physical Review X. – 2015. – Vol. 5, Issue 3. – P. 031030.

5. Makarov V. Faked states attack on quantum cryptosystems / V. Makarov and D.R. Hjelme // Journal of Modern Optics. – 2005. – Vol. 52, Issue 5. – PP. 691-705.

6. Makarov V. Controlling passively quenched single photon detectors by bright light / V. Makarov // New Journal of Physics. – 2009. – Vol. 11. – 065003.

7. Lydersen L. Hacking commercial quantum cryptography systems by tailored bright illumination / L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar and V. Makarov // Nature Photonics. – 2010. – Vol. 4, Issue 10. – PP. 686-689.

8. Sauge S. Controlling an actively-quenched single photon detector with bright light / S. Sauge, L. Lydersen, A. Anisimov, J. Skaar and Vadim Makarov // Optics Express. – 2011. – Vol. 19, Issue 23. – PP. 23590-23600.

9. Lo H.K. Measurement-Device-Independent Quantum Key Distribution / H.K. Lo, M. Curty and B. Qi // Physical Review Letters. – 2012. – Vol. 108, Issue 13. – 130503.

УДК 004.056.5

Галенко В.В.
Національний авіаційний університет
vladkahalenko@gmail.com.ua
Гнатюк С.О.
Національний авіаційний університет
s.gnatyuk@nau.edu.ua

МЕТОД ПРОГНОЗУВАННЯ СИНЕРГЕТИЧНОГО ЕФЕКТУ В СЕГМЕНТАХ КІБЕРПРОСТОРУ

Анотація. *Світовою науковою спільнотою нині приділяється значна увага вивченню питань впливу інформаційних та кібернетичних впливів як на окремо взятого громадянина, так і суспільство й державу в цілому. Але характерною рисою останніх досліджень за визначеною тематикою є те, що вони вивчаються відокремлено одні від одних. Як наслідок, не враховується синергія взаємодії від таких дій, що у більшості випадків призводить до неможливості вироблення асиметричних заходів з протидії деструктивним впливам. Актуальність дослідження обумовлюється відсутністю методів, методик та загальноприйнятих показників оцінки синергетичного ефекту, який виникає у результаті взаємодії інформаційних та кібернетичних впливів. Отже, питання з вивчення синергії взаємодії інформаційних та кібернетичних впливів до сьогодні залишалося відкритим. Виходячи з цього, у роботі розроблено метод прогнозування синергетичного ефекту, що виникає внаслідок інформаційної та кібернетичної взаємодії у кіберпросторі.*

Синергетичний метод активно застосовується у сучасній науці, адже для кожної відкритої складної системи властивими є синергетичні процеси. Можливості практичного застосування синергетичного методу величезні і на сьогодні ще не до кінця досліджені. Синергетика займається вивченням процесів самоорганізації і виникнення, підтримки стійкості та розпаду різноманітних систем, які, хоча і мають абсолютно різну природу, але кількість математичних моделей, що використовуються для опису процесів, у них невелика. Тобто, там, де присутня впорядкованість, внутрішня складність макросистем не виявляється, вони ведуть себе подібним чином. Власне синергетика займається пошуком і вивченням моделей складних систем, питаннями виникнення порядку з хаосу та переходу від впорядкованих структур до хаотичних. Синергетика, математично описуючи необоротні

якісні зміни, які забезпечують перехід від простого до складного, виявляється теоретичним описом систем, що розвиваються. Їх вивчення має велике значення, тому що більшість відомих систем відносяться саме до такого типу [1]. В основі синергетики лежить фундаментальне явище самоорганізації у складних нелінійних динамічних системах. Однак в синергетиці ще не побудована загальна і єдина теорія самоорганізації, що є справедливою для всіх видів природних і технічних систем. Тому, в залежності від конкретних властивостей предметної області тієї чи іншої науки, синергетичний підхід набуває свої відмінні особливості і зміст. У зв'язку з цим на сьогоднішній день ми можемо говорити про синергетичний підхід як про деяку направляючу концепцію у відповідній науці. Синергетика дозволяє говорити про виникнення свого роду метамови цілісного розуміння різних природних і технічних явищ на основі єдиної наукової концепції. Ця концепція дозволяє побудувати нове відношення до процесу інтегрального пізнання різних наук [2].

Завдяки своїй міждисциплінарності синергетика веде до нового конструктивного діалогу між фахівцями в різних наукових напрямках. Синергетика робить кроки в напрямку синтезу природничих і гуманітарних наук. По Хакену, в синергетичних процесах відбувається стихійна зміна управляючих параметрів, що дає можливість вивчити властивість самоорганізації на дисипативних структурах фактично некерованої нелінійної системи. Тобто найбільш важливими властивостями є саморух і самоорганізація, а розуміння процесів полягає у вивченні причин спонтанної самоорганізації [1, 3]. Аналіз останніх досліджень і публікацій показує, що світовою науковою спільнотою нині приділяється значна увага вивченню питань впливу інформаційних та кібернетичних впливів (дій) як на окремо взятого громадянина, так і суспільство й державу в цілому. Але характерною рисою останніх досліджень за визначеною тематикою є те, що інформаційні та кібернетичні дії вивчаються відокремлено одні від одних. Як наслідок, не враховується синергія взаємодії від таких дій, що у більшості випадків призводить до неможливості вироблення асиметричних заходів з протидії деструктивним впливам [4]. Таким чином, як випливає з аналізу останніх досліджень і публікацій за цією тематикою, встановлено, що існуючий на сьогодні методичний інструментарій не забезпечує реалізацію «ефекту» завчасного регулювання. Узагальнивши передовий світовий досвід щодо ролі й місця синергетичних ефектів, які виникають внаслідок інформаційної та кібернетичної взаємодії в сегментах кіберпростору (КП), розкриємо сутність типової технології формування їх ефекту синергії. Згідно [4] синергетичний ефект матиме місце тільки тоді, коли інформаційні та кібернетичні впливи здійснюються за єдиним задумом і планом та узгоджуються за завданнями в часі та просторі. З практики відомо, що для одержання синергетичного ефекту в переважній більшості спочатку розкручуються інформаційні дії (перший ступінь розкручення процесу взаємодії), які потім доповнюються кібернетичними (другий ступінь розкручення процесу взаємодії). Тому завчасне виявлення, оцінювання і прогнозування синергетичних ефектів інформаційної та кібернетичної взаємодії слугуватиме ефективним регулятором нелінійних процесів, які суттєво впливають на процеси забезпечення міжнародної безпеки в КП. Метою цієї роботи є розробка методу прогнозування синергетичного ефекту, що виникає внаслідок інформаційної та кібернетичної взаємодії у КП.

Розроблений метод прогнозування синергетичного ефекту в сегментах КП реалізується у два етапи, останній з яких складається з чотирьох кроків [4]. На першому етапі формалізуємо задачу оцінювання синергетичного ефекту інформаційної та кібернетичної взаємодії. Нехай у результаті інформаційної та кібернетичної взаємодії формується деяка матриця взаємодії, а значення елементів матриці взаємодії визначаються як результат інформаційної та кібернетичної взаємодії. Залежно від того, яких значень набувають елементи матриці, відповідна інформаційна та кібернетична взаємодія характеризується або відсутністю ефекту, або їй властивий один з двох ефектів – синергетичний або системний. Таким чином, з урахуванням принципу наповнення елементами матриці взаємодії, потрібно оцінити синергетичних ефектів, які виникають у результаті інформаційної та кібернетичної взаємодії та знайти відповідний тренд, урахування якого забезпечить своєчасне виявлення та прогнозування проявів синергії в КП.

На другому етапі оцінюємо синергетичного ефекту графоаналітичним способом. Зважаючи на різну природу проявів інформаційних та кібернетичних дій, синергетичний ефект унаслідок їх взаємодії доцільно оцінити графоаналітичним способом. Так графоаналітична процедура визначення елементу матриці взаємодії передбачає виконання наступних чотирьох кроків. На першому кроці оцінюванню підлягає значення коефіцієнта кореляції між інформаційними та кібернетичними впливами. На другому кроці оцінюються метрики самоподібності для інформаційних та кібернетичних дій. На третьому кроці визначенню підлягає елемент матриці взаємодії. З цією метою на колі ефективності одиничного радіусу з центром у точці О по трьом осям OH_{Inf}, OC_{ij}та OH_{Cyb}, які виходять з центру кола й рознесені між собою під кутами $\alpha = \beta = \gamma = 120^{\circ}$, відкладаються значення визначених показників. Відповідно синергетичний ефект інформаційної та кібернетичної взаємодії може бути кількісно оцінений площею даного трикутника, що дорівнює:

$$e_{ij} = K^{-1} S_{\Delta C_{ij} H_{Inf} H_{Cyb}}, \quad (1)$$

де K – коефіцієнт нормування, K=1.3; $S_{\Delta C_{ij} H_{Inf} H_{Cyb}}$ – площа трикутника, $\Delta C_{ij} H_{Inf} H_{Cyb}$, $S_{\Delta C_{ij} H_{Inf} H_{Cyb}} = S_{\Delta C_{ij} H_{Inf} 0} + S_{\Delta C_{ij} H_{Cyb} 0} + S_{\Delta H_{Cyb} H_{Inf} 0}$.

Для узгодження результатів кількісного оцінювання синергії інформаційної та кібернетичної взаємодії з якісною оцінкою використовується спеціально розроблена нормована фундаментальна шкала. У випадку, коли значення показника лежить у проміжку [0,44; 1] – присутній синергетичний ефект, у разі значення показника [0,12; 0,44[– має місце системний ефект, а значення показника у проміжку [0,44; 0,12[– означає відсутність ефекту. Описана вище процедура повторюється для всіх елементів матриці взаємодії. На четвертому кроці знаходиться тренд синергетичної взаємодії. Тобто у формалізованому вигляді потрібно, знайти такий тренд синергетичної взаємодії, для якого сумарний синергетичний ефект збігається до максимуму. Інформаційна та кібернетична взаємодія в результаті комплексування узгоджених за завданнями в часі та просторі й здійснюваних за єдиним задумом і планом в КП дій, призводить до виникнення явища синергетичного ефекту.

Розроблений метод є тією теоретичною базою, яка повинна використовуватися для завчасного виявлення, оцінювання та прогнозування синергетичних ефектів, що виникають внаслідок інформаційної та кібернетичної взаємодії. Одержані у результаті оцінювання кількісні та якісні оцінки синергії сприяють виробленню ефективних заходів з протидії деструктивним інформаційним та кібернетичним впливам.

Таким чином, у цій роботі розроблено метод прогнозування синергетичного ефекту, який за рахунок формування матриці інформаційної та кібернетичної взаємодії, розрахунку коефіцієнта кореляції, метрик самоподібності (показник Херста), а також тренду синергетичної взаємодії, дозволяє прогнозувати та оцінювати (кількісно та якісно) синергетичні ефекти, які виникають внаслідок інформаційної та кібернетичної взаємодії у КП. Подальші дослідження будуть пов’язані з побудовою системи оцінювання синергетичних ефектів у КП та її експериментальним дослідження.

Література.

1. Хакен Г. Синергетика / Г. Хакен. – М.: Мир, 1980. – 406 с.
2. Колесников А.А. «Кибернетика – информатика – синергетика» как системообразующая концепция современного высшего образования / А. А. Колесников, В.Б. Яковлев // Известия Южного федерального университета. Технические науки. – 2001. – №5 – С. 26-37.
3. Колесников А.А. Синергетическая теория управления: концепции, методы, тенденции развития / А.А. Колесников. – М. : URSS, 2012.
4. Danik Yu. Synergistic effects of information and cybernetic interaction in civil aviation / Yu. Danik, R. Hryschuk, S. Gnatyuk // Aviation, 2016 – Available from: http://www.tandfonline.com/doi/abs/10.3846/16487788.2016.1237787

УДК 004.054

Гнатюк В.О.
Асистент кафедри ТКС ННІАН НАУ
viktorgnatyuk@ukr.net

МЕТОД ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ CSIRT

Анотація. *В роботі розроблено метод оцінювання ефективності функціонування CSIRT, який реалізується у такі етапи: визначення показників функціонування CSIRT, визначення KPI, побудова панелі індикаторів. Розроблений метод може використовуватись для моніторингу, управління, аналізу та підвищення ефективності функціонування CSIRT.*

Проблема інформаційної безпеки (ІБ) не втрачає своє актуальності в сучасному світі, а навпаки, починає носити глобальний характер – кіберінциденти (КІ) стають все більш складними й частими. Реагуванням на КІ, як правило, займаються спеціалізовані центри (команди) типу CSIRT, які з кожним роком отримують все більше завдань та викликів. Саме через це з'являється необхідність аналізувати та оцінювати ефективність функціонування CSIRT – даний показник, є одним з ключових для ІБ, як окремої організації, так і держави в цілому. Періодичне оцінювання функціонування CSIRT дозволить ідентифікувати сильні та слабкі сервіси, відділи, групи, окремих співробітників з метою врахування у майбутньому, а також виокремити певні тенденції на базі статистичних даних. Проведений аналіз показав, що оцінці ефективності функціонування CSIRT не відводиться достатньо уваги, що може негативно вплинути на рівень ІБ.

У сучасній науково-технічній літературі описана велика множина методів для оцінювання роботи персоналу, проте найефективнішим, згідно багатокритеріального аналізу, виявився метод управління досягненнями (Performance Management), який базується на використанні (Key Performance Indicators – KPI). Тому, для подальших досліджень, за основу обрано цей метод.

Метою роботи є розробка методу оцінювання ефективності функціонування CSIRT та інших центрів технічного обслуговування ІТС.

Основна частина роботи. Розроблений метод складається з таких етапів:

Етап 1 – Визначення показників функціонування CSIRT. При функціонуванні CSIRT здійснюється запис до бази даних інформації про КІ. Серед базових показників функціонування CSIRT, що мають кількісні значення виділяють наступні (табл. 1).

Таблиця 1

Показники функціонування CSIRT

Позначення	Назва
E	Ефективність
LRI	Рівень вирішення інциденту
INAI	Кількість некоректних призначень інциденту
DRI	Тривалість вирішення інциденту
ECS	Оцінка задоволеності клієнтів
PRI	Пріоритет інциденту
DIR	Тривалість реєстрації інциденту
CII	Повнота наданої інформації про інцидент

Для реалізації цього етапу задамо множину показників функціонування CSIRT $\boldsymbol{PI}$:

$$\boldsymbol{PI} = \{\bigcup_{q=1}^{p} PI_q\} = \{PI_1,\ PI_2, ..., PI_p\}, \quad (1)$$

де $PI_q \subseteq \boldsymbol{PI}$, $(q = \overline{1, p})$, p – кількість показників функціонування CSIRT.

Використовуючи базу даних з показниками функціонування CSIRT (за II квартал 2016 року) сформуємо табл. 2.

Таблиця 2

Значення показників діяльності CSIRT за II квартал 2016 року

№	E	LRI	INAI	DRI	ECS	PRI	DIR	CII
1	90	4	3	1539	4	3	2	40
2	115	1	0	2502	8	4	6	80
…	…	…	…	…	…	…	…	…
600	171	1	0	37	6	1	6	85

Використовуючи (1) та дані з табл. 1 при $p = 8$, отримаємо:

$$\boldsymbol{PI}_{\boldsymbol{celprov\_ua}2} = \{\bigcup_{q=1}^{8} PI_q\} = \{PI_1,\ PI_2, ..., PI_8\} =$$

$$\{PI_E,\ PI_{LRI}, PI_{INAI}, PI_{DRI}, PI_{ECS}, PI_{PRI}, PI_{DIR}, PI_{CII}\} =$$

$$\{E,\ LRI, INAI, DRI, ECS, PRI, DIR, CII\},$$

де $PI_1 = PI_E = E$, $PI_2 = PI_{LRI} = LRI$,…, $PI_8 = PI_{CII} = CII$ – показники функціонування CSIRT.

На виході цього етапу маємо матрицю з показниками функціонування CSIRT та їх значеннями які отримуємо з табл. 2.

Етап 2 – Визначення KPI. Щоб визначити з множини показників функціонування CSIRT $\boldsymbol{PI}$ ключові показники ефективності $\boldsymbol{KPI}$ використаємо процедуру множинного кореляційно-регресійного аналізу (МКРА). Множинний коефіцієнт кореляції є основною характеристикою тісноти взаємозв'язку між результативною ознакою PI_1 та сукупністю чинникових ознак $PI_2,\ PI_3, ..., PI_p$.

Отже, за допомогою розрахункової процедури МКРА ми можемо оцінити міру впливу на досліджуваний результативний показник (PI_1) кожного із введених у модель чинників ($PI_2,\ PI_3, ..., PI_p$) та визначити множину ключових показників ефективності $\boldsymbol{KPI}$:

$$\boldsymbol{KPI} = \{\bigcup_{w=1}^{v} KPI_w\} = \{KPI_1,\ KPI_2, ..., KPI_v\}, \quad (2)$$

де $KPI_w \subseteq \boldsymbol{KPI}$, $(w = \overline{1, v})$, v – кількість KPI.

Отже, на вхід подаємо матрицю з показниками функціонування CSIRT та їх значеннями (табл. 2). Далі, застосовуючи вищеописану процедуру МКРА отримуємо кореляційну матрицю (табл. 3).

Таблиця 3

Кореляційна матриця для II кварталу 2016 року

E	1							
LRI	-0,37	1						
INAI	-0,79	0,35	1					
DRI	-0,49	0,36	0,66	1				
ECS	0,82	-0,47	-0,57	-0,51	1			
PRI	-0,91	0,57	0,47	0,67	-0,63	1		
DIR	0,19	-0,52	-0,52	-0,63	0,43	-0,60	1	
CII	0,89	-0,62	-0,52	-0,45	0,72	-0,58	0,29	1
	E	LRI	INAI	DRI	ECS	PRI	DIR	CII

Проаналізувавши дані з табл. 3 можна зробити висновок, що найбільш впливають на ефективність такі чинники: PRI, INAI, ECS та CII.

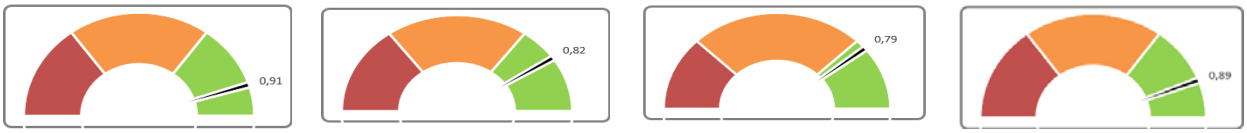
Вихідними даними цього етапу, згідно (2), при $w = 4$ є множина $\boldsymbol{KPI}$:

$$\boldsymbol{KPI}_{CSIRT\,2Q} = \{\bigcup_{w=1}^{4} KPI_w\} = \{KPI_1, KPI_2, KPI_3, KPI_4\} =$$

$$\{KPI_{PRI},\ KPI_{INAI}, KPI_{ECS}, KPI_{CII}\} = \{PRI,\ INAI, ECS, CII\},$$

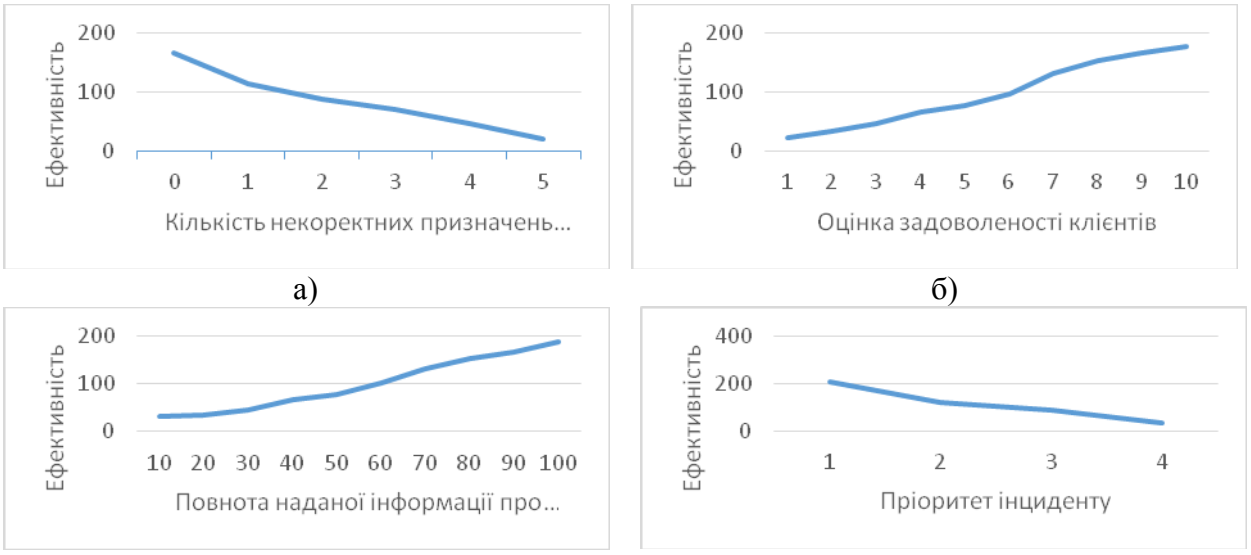
де $KPI_1 = KPI_{PRI} = PRI$, $KPI_2 = KPI_{INAI} = INAI$, $KPI_3 = KPI_{ECS} = ECS$, $KPI_4 = KPI_{CII} = CII$ – ключові показники ефективності.

Етап 3 – Побудова панелі індикаторів. На цьому етапі здійснюється побудова панелі індикаторів, за допомогою якої буде здійснено моніторинг, аналіз та управління ефективністю роботи CSIRT (рис. 1, 2).



а) б) в) г)

Рис. 1. Значення коефіцієнтів кореляції: а) PRI б) ECS в) INAI г) CII



а) б) в) г)

Рис. 2. Графік залежності ефективності від: а) INAI, б) ECS, в) CII, г) PRI

Проаналізувавши отримані результати (рис. 2), можна зробити висновок про залежість ефективності від кожного з визначених KPI та сформувати обмеження: якщо INAI > 1, то E < 100; якщо ECS < 7, то E < 100; якщо CII < 60, то E < 100; якщо PRI < 2, то E < 100.

Висновки. Отже, у роботі розроблено метод оцінювання ефективності функціонуваня CSIRT. Цей метод може бути використаний керівниками центрів реагування на КІ для моніторингу, управління, аналізу та підвищення ефективності функціонування CSIRT.

Література

1. Кінзерявий В.М. Базові показники ефективності роботи команд реагування на кіберінциденти / В.М. Кінзерявий, В.О. Гнатюк // Безпека інформації. – Том 20, №2. – 2014. – С. 193-196.

2. Мармоза А.Т. Теорія статистики / А.Т. Мармоза // Підручник для студентів вищих навчальних закладів. – К. 2013. – С. 333-397.

3. Панели индикаторов как инструмент управления: ключевые показатели эффективности, мониторинг деятельности, оценка результатов / Уэйн У. Эккерсон; Пер. с англ. – М.: Альпина Бизнес Букс, М., 2007. – 396 с.

4. Панов М. М. Оценка деятельности и система управления компанией на основе KPI / М.М. Панов. – М.: Инфра-М, 2012. – 255 с.

Сучасні методи оцінки персоналу – [Електронний ресурс]. – Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=776.

УДК 003.26:004.056.55

Гнатюк С.О.
Національний авіаційний університет
s.gnatyuk@nau.edu.ua
Кінзерявий В.М.
Національний авіаційний університет
Жмурко Т.О.
Національний авіаційний університет

КРИПТОГРАФІЧНИЙ МЕТОД ЗАХИСТУ КРИТИЧНИХ АВІАЦІЙНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Анотація. *Забезпечення конфіденційності даних є важливим етапом у процесі забезпечення кібербезпеки критичних авіаційних інформаційних систем та авіаційної галузі у цілому. Відомі методи не дозволяють у повній мірі забезпечити високу стійкість до кібератак лінійного та диференціального криптоаналізу і необхідну швидкість криптографічної обробки даних. З огляду на це, у роботі розроблено криптографічний метод захисту критичних авіаційних інформаційних систем, новий БШ Luna-2k17 і розраховано значення верхніх оцінок параметрів, що характеризують практичну стійкість до кібератак лінійного та диференціального криптоаналізу*

Цивільна авіація (ЦА) є галуззю критичної інфраструктури держави, внутрішнє середовище якої швидко і суттєво змінюється із впровадженням сучасних інформаційно-комунікаційних технологій (ІКТ). Відповідно до керівних документів у галузі ЦА найбільшого захисту потребують критичні авіаційні інформаційні системи (КАІС) [1], до яких згідно [2] відносяться, наприклад, системи управління повітряним рухом, системи дистанційного технічного обслуговування, диспетчерські системи та ін. Для мінімізації впливу кіберзагроз на ресурси КАІС необхідно вжити низку заходів [3], серед яких забезпечення конфіденційності даних (інформації). Одним із найважливіших напрямів діяльності щодо забезпечення конфіденційності даних був і залишається захист інформації криптографічними методами [4], беззаперечною перевагою яких є забезпечення захисту безпосередньо самих даних, а не доступу до них. Основним критерієм при виборі криптосистем є стійкість (криптостійкість) проте для деяких завдань ключову роль відіграє швидкість криптографічної обробки даних [4-5]. Незважаючи на різноманітність сучасних криптографічних методів та систем, далеко не всі володіють необхідним рівнем ефективності (швидкодії та стійкості) для забезпечення захисту даних, а розвиток і здешевлення ІКТ позитивно впливає на ефективність криптоаналізу, одними з найефективніших методів якого є лінійний та диференціальний криптоаналіз (ЛДК) [6]. Таким чином, розробка криптографічного методу захисту КАІС і обґрунтування його стійкості до методів ЛДК є актуальним науковим завданням. Зважаючи на це, *метою* роботи є підвищення ефективності криптографічного захисту КАІС на базі розробки нового криптографічного методу захисту даних та відповідного блокового шифру (БШ) на його основі.

Розглянемо етапи розробленого криптографічного методу захисту даних. Нехай t', p', r', q' – натуральні числа, $t=2t'$, $p=2p'$, $r=2r'+1$, $n=tp$, $q=pq'$, $w=p$, $k=2n$, $b=2^{q'}$ (параметр b визначає кількість різних таблиць підстановок, що можуть використовуватись у методі). Тоді r-раундовий метод криптографічного захисту інформації $\Im$ із множиною відкритих (шифрованих) повідомлень $V_n=\{0,1\}^n$, множиною секретних ключів V_k, множиною раундових ключів V_{n+q+w} можна описати такою послідовністю етапів:

Етап 1 – Вироблення раундових ключів. На цьому етапі із секретного ключа K, $K\in V_k$ виробляється r раундових ключів K_i, $K_i\in V_{n+q+w}$, $i=\overline{1,r}$.

Крок 1. Секретний ключ K, $K\in V_k$ розкладається на частини:

$$K=\left(B_{-4},B_{-3},B_{-2},B_{-1}\right), \tag{1}$$

$B_j\in V_{n/2}$, $j=\overline{-4,-1}$.

Крок 2. Виробляються вектори $B_j, B_j\in V_{n/2}$, $j=\overline{0,c-1}$, $c=4r\left(n+q+w\right)/n$:

$$B_j=\begin{cases}\left(S\left(B_{j-4},W_1,p'\right)\oplus\left(B_{j-2}<<<P_1\right)\oplus B_{j-1}\oplus Q_1\right)<<<B_{j-3} & ,j \bmod 4=0\\ \left(S\left(B_{j-3}\oplus B_{j-1},W_2,p'\right)\oplus\left(B_{j-2}>>>P_2\right)\oplus Q_2\right)>>>B_{j-4} & ,j \bmod 4=1\\ \left(B_{j-4}\oplus\left(S\left(B_{j-3}\right)<<<P_3,W_3,p'\right)\oplus B_{j-1}\oplus Q_3\right)>>>B_{j-2} & ,j \bmod 4=2\\ \left(S\left(B_{j-4}<<<P_4,W_4,p'\right)\oplus B_{j-3}\oplus B_{j-2}\oplus Q_4\right)<<<B_{j-1} & ,j \bmod 4=3\end{cases}, \tag{2}$$

де $\oplus$ – операція покоординатного булевого додавання двійкових векторів, $X<<<Y$ – операція динамічного циклічного зсуву вліво бітової послідовності X на Y разів, а $X>>>Y$ – операція динамічного циклічного зсуву вправо бітової послідовності X на Y разів, W_i, P_i, Q_i – деякі константи, W_i, P_i, $Q_i\in V_{n/2}$, $i=\overline{1,4}$.

Підстановка S визначаються за формулою:

$$S\left(x,y,z\right)=\left(s_{y_{z-1}}\left(x_{z-1}\right),\ldots,s_{y_0}\left(x_0\right)\right),\ x=\left(x_{z-1},\ldots,x_0\right),y=\left(y_{z-1},\ldots,y_0\right), \tag{3}$$

де $x_j\in V_t$, $y_j\in V_{q'}$, s_{y_j} – підстановка на множині V_t (за індексом y_j обирається для використання одна таблиця підстановок із b можливих), $j\in\overline{0,z-1}$.

Крок 3. Формуються вектори $C_i, C_i\in V_e$, $i=\overline{1,r}$, $e=e'n/2$, $e'=\left\lceil 2\left(n+q+w\right)/n\right\rceil$ конкатенацією векторів $B_j, B_j\in V_{n/2}$, $j=\overline{0,c-1}$, $c=4r\left(n+q+w\right)/n$ у зворотному порядку (для формування одного вектора C_i використовується e' векторів B_j):

$$C_i=\left(B_{c-1-(i-1)e'}\,\|\,B_{c-1-(i-1)e'-1}\,\|\ldots\|\,B_{c-1-(i-1)e'-e'+1}\right) \tag{4}$$

Крок 4. Розраховуються раундові ключі K_i, $K_i\in V_{n+q+w}$, $i=\overline{1,r}$:

$$K_i=\left(C_i>>>i\right)\bmod 2^{n+q+w}. \tag{5}$$

Етап 2 – Процедура шифрування. На цьому етапі відбувається шифрування секретного повідомлення $A=\left(A_1,A_2,A_3,\ldots,A_u\right)$, $A\in V_{n\cdot u}, A_j\in V_n$, $j=\overline{1,u}$, u – натуральне число.

Функція шифрування кожного $A_j\in V_n$, $j=\overline{1,u}$ буде такою:

$$F=f_{r,K_r}\circ\ldots\circ f_{1,K_1}. \tag{6}$$

Раундова функція f_{i,K_i}, для будь-яких $x\in V_n$, $K_i\in V_{n+q+w}$, $i\in\overline{1,r}$ описується таким чином:

$$f_{i,K_i}(x)=\begin{cases}\varphi\left(x\oplus k^{(1)},k^{(2)},k^{(3)}\right), & \text{якщо } i<r\\ S\left(x\oplus k^{(1)},k^{(2)},p\right), & \text{якщо } i=r\end{cases}, \tag{7}$$

де $k^{(1)}$, $k^{(2)}$, $k^{(3)}$ частини раундового ключа K_i ($k=\left(k^{(1)},k^{(2)},k^{(3)}\right)$, $k^{(1)}\in V_n$, $k^{(2)}\in V_q$, $k^{(3)}\in V_w$).

Підстановка S визначена у (3), а підстановка φ визначається за формулою:

$$\varphi(x,y,h)=S(x,y,p)M(h),\ x\in V_n,\ y\in V_q,\ z\in V_w \tag{8}$$

де $x=\left(x_{p-1},\dots,x_0\right)$, $y=\left(y_{p-1},\dots,y_0\right)$, $x_j\in V_t$, $y_j\in V_{q'}$.

$M(h)$ – оборотна $2p\times 2p$ матриця над полем $GF\left(2^{t'}\right)$, що залежить від h, а множення $S(x,y,p)=\left(s_{y_{z-1}}(x_{z-1}),\dots,s_{y_0}(x_0)\right)$ на $M(h)$ у (8) виконується над цим полем таким чином:

1. $s_{y_j}(x_j)$ ($j\in\overline{0,p-1}$) розкладається на дві t'-бітні частини

($s_{y_j}(x_j)=\left(s_{y_j}(x_j)^{(1)},s_{y_j}(x_j)^{(2)}\right)$, $s_{y_j}(x_j)^{(1)},s_{y_j}(x_j)^{(2)}\in V_{t'}$).

2. Із частин $s_{y_j}(x_j)$ ($j\in\overline{0,p}$) формується вектор B:

$B=s_{y_0}\left(x_0^{(1)}\right)||\,s_{y_0}\left(x_0^{(2)}\right)||\dots||\,s_{y_{p-1}}\left(x_{y_{p-1}}{}^{(1)}\right)||\,s_{y_{p-1}}\left(x_{y_{p-1}}{}^{(2)}\right)$.

3. Виконується множення вектора B на $M(z)$ при ототожненні двійкових векторів B_j $j\in\overline{0,2p-1}$ ($B_j\in V_{t'}$) із елементами матриці $M(z)$.

Для розробленого методу отримано аналітичні верхні оцінки параметрів, що характеризують його практичну стійкість відносно методів ЛДК:

$$EDP(\Omega)\le\tilde{\tilde{\Delta}}_{\oplus}^{\,r'\lceil B_M/2\rceil+1}\le\Delta_{\oplus}^{\,r'\lceil B_M/2\rceil+1}, \tag{9}$$

$$ELP(\Omega)\le\tilde{\tilde{\Lambda}}_{\oplus}^{\,r'\lceil B_M/2\rceil+1}\le\Lambda_{\oplus}^{\,r'\lceil B_M/2\rceil+1}, \tag{10}$$

де $EDP(\Omega)$ – середня імовірність диференціальної характеристики Ω, $ELP(\Omega)$ – середня імовірність лінійної характеристики Ω, B_M – індекс галуження матриці M, а параметри $\Delta_{\oplus}$, $\Lambda_{\oplus}$, $\tilde{\tilde{\Delta}}$, $\tilde{\tilde{\Lambda}}$ визначаються за такими формулами:

$$\Delta_{\oplus}=\max\left\{d_{\oplus}^{(s_j)}(\alpha,\beta):\alpha,\beta\in V_t\setminus\{0\},j\in\overline{0,b-1}\right\}, \tag{11}$$

$$\Lambda_{\oplus}=\max\left\{l^{(s_j)}(\alpha,\beta):\alpha\in V_t,\beta\in V_t\setminus\{0\},j\in\overline{0,b-1}\right\}, \tag{12}$$

$$\tilde{\tilde{\Delta}}_{\oplus}=\max\left\{b^{-1}\sum_{j=0}^{b-1}d_{\oplus}^{(s_j)}(\alpha,\beta):\alpha,\beta\in V_t\setminus\{0\}\right\}, \tag{13}$$

$$\tilde{\tilde{\Lambda}}_{\oplus}=\max\left\{b^{-1}\sum_{j=0}^{b-1}l^{(s_j)}(\alpha,\beta):\alpha\in V_t,\beta\in V_t\setminus\{0\}\right\}. \tag{14}$$

У (11) – (14) $d_{\oplus}^{(s_j)}$ – таблиця різниць підстановки s_j ($j\in\overline{0,b-1}$) відносно операцій побітового додавання за модулем 2, а $l^{(s_j)}(\alpha,\beta)$ – таблиці лінійної апроксимації підстановки s_j ($j\in\overline{0,b-1}$) відносно цієї самої операції.

Luna-2k17

Input: 128-бітний вхідний блок даних $state$, 160-бітні раунд. ключі $SubKey_i = \left(SubKey_i^{(1)}, SubKey_i^{(2)}, SubKey_i^{(3)}\right)$, $i = \overline{0,r}$, $SubKey_i^{(1)} \in V_{128}$, $SubKey_i^{(2)} \in V_{24}$, $SubKey_i^{(3)} \in V_8$.

Output: 128-бітний вихідний блок даних.

1. $state = AddKeyMod2\left(state, SubKey_0^{(1)}\right)$;
2. $For \quad i = 1, \quad i < r, \quad i{+}{+} \quad do$
2.1. $state = SubBytes\left(state, SubKey_i^{(2)}\right)$;
2.2. $state = ShiftRows\left(state, SubKey_i^{(3)}\right)$;
2.3. $state = MixColumns\left(state\right)$;
2.4. $state = AddKeyMod2\left(state, SubKey_i^{(1)}\right)$;
3. $state = SubBytes\left(state, SubKey_r^{(2)}\right)$;
4. $state = ShiftRows\left(state, SubKey_r^{(3)}\right)$;
5. $state = AddKeyMod2\left(state, SubKey_r^{(1)}\right)$;
6. $return \ state$.

На основі запропоновано методу розроблено й реалізовано програмно БШ Luna-2k17, псевдокод процедури зашифровування якого наведено на рис. 1. Для цього шифру прийнято такі параметри: $t' = 8$, $t = 2t' = 16$ (розрядність таблиць замін), $p' = 4$, $p = 2p' = 8$, $r' = 4$, $r = 2r' + 1 = 9$ (кількість раундів), $n = tp = 128$ (розмір блоку даних, біт), $q' = 3$, $q = pq' = 24$, $b = 2^{q'} = 8$ (використовується 8 таблиць замін на множині V_{16}), $w = 8$, $k = 2n = 256$ (розмір секретного ключа, біт).

Запропонований шифр працює із 128-бітними блоками даних з підтримкою секретного ключа довжиною 256 біт.

Рис. 1. Псевдокод процедури зашифровування БШ *Luna-2k17*

При розширенні секретного ключа виробляється необхідна кількість 160-бітного раундового ключа ($n + q + w = 128 + 24 + 8 = 160$). Блоки даних та розширені ключі представляються у вигляді 8×2 байтної матриці.

Під операцією $AddKeyMod2\left(state, SubKey^{(1)}\right)$ мається на увазі побітове додавання за модулем 2 відповідних бітів раундового ключа $SubKey^{(1)}$ та блоку данних $state$. Операція $MixColumns\left(state\right)$ є лінійним перетворенням матриці $state$. У цій операції кожна 8-байтна колонка блоку данних $state$ розглядається як поліном над полем $GF\left(2^8\right)$ з 8 термами, який перемножується за модулем $x^8 + 1$ з фіксованим поліномом $c\left(x\right)$ степені 7. В операціях $SubBytes\left(state, SubKey^{(2)}\right)$ виконується таблична заміна кожних 16 біт блоку даних $state$. У шифрі Luna-2k17 8 таблиць на множині V_{16}, при чому вибір конкретної таблиці у кожному раунді залежить від частини раундовго ключа $SubKey^{(2)}$. Таблиці замін обрані таким чином, щоб були відсутні фіксовані точки, а також щоб виконувалися рівності для параметрів: $\Delta_{\oplus} = \Lambda_{\oplus} = 2^{-14}$ – для кожної таблиці замін шифру *Luna-2k17*. В операції $ShiftRows\left(state, SubKey^{(3)}\right)$ виконується побайтовий зсув елементів у рядках матриці $state$ у залежності від частини раундового ключа $SubKey^{(3)}$.

Для експериментального дослідження БШ Luna-2k17 був програмно реалізований у вигляді консольного застосунку «Luna-2k17». Властивості послідовностей, утворених за допомогою цього застосунку (у режимі лічильника) досліджено у середовищах статистичних тестів NIST STS та Diehard. Результати показали, що БШ Luna-2k17 пройшов комплексний контроль за методиками NIST STS та Diehard і показав кращі результати ніж відомі БШ Luna-2017, ГОСТ 28147-89 та Калина. Крім того, показано, що запропонований шифр Luna-2k17 швидший за шифр ГОСТ 28147-89 приблизно у 3,5 разів, а за шифри Калина та AES у 1,41 разів (дослідження проводилися в однакових умовах на Intel (R) Core (TM) i7-2600K

CPU 3.4 GHz). Також, згідно (9) – (14), розраховано значення верхніх оцінок параметрів, що характеризують практичну стійкість БШ Luna-2k17 ($EDP(\Omega) \le 2^{-294}$, $ELP(\Omega) \le 2^{-294}$ при $r = 9$).

Таким чином, розроблено криптографічний метод захисту КАІС, який за рахунок нової послідовності операцій в процедурах вироблення раундових ключів та шифрування, а також нових процедур рандомізації вузлів заміни в алгоритмах шифрування, дозволяє забезпечити захищеність КАІС у контексті практичної стійкості до кібератак ЛДК та забезпечити вимогу ATC_2 з режимом безпеки <30:35:12> згідно мультирівневої моделі [7]. Також, створено новий БШ Luna-2k17 (і відповідне ПЗ), що дозволяє забезпечити практичну стійкість до ЛДК (при кількості раундів $r = 9$), а також підвищити швидкість криптографічної обробки даних на 27,1 % у порівнянні з відомими БШ.

Література

1. Gnatyuk S. Critical Aviation Information Systems Cybersecurity // Meeting Security Challenges Through Data Analytics and Decision Support. – NATO Science for Peace and Security Series – D: Information and Communication Security. – IOS Press Ebooks, 2016. – Vol.47. – №3. – P. 308-316.
2. Гнатюк С. Сучасні критичні авіаційні інформаційні системи / С.О. Гнатюк, Д.В. Васильєв // Безпека інформації. – 2016. – Т.22. – №1. – С. 51-57.
3. Model for Cybersecurity Requirements Definition in Civil Aviation / K. Janisz, O. Korchenko, S. Gnatyuk, R. Odarchenko // Autobusy. – 2016. – №12. – P. 630-634.
4. Гнатюк С.О. Особливості криптографічного захисту державних інформаційних ресурсів / С.О. Гнатюк, В.М. Кінзерявий, А.О. Охріменко // Безпека інформації. – 2012. – №1 (17). – С. 64-77.
5. Основні критерії та вимоги до побудови сучасних криптосистем / О.Г. Корченко, С.О. Гнатюк, Ю.Є. Хохлачова, А.О. Охріменко // Вісник Інженерної академії України. – 2011. – №3-4. – С. 77-83.
6. Математичні основи криптоаналізу: навч. пос. / С.О. Сушко, Г.В. Кузнецов, Л.Я. Фомичова, А.В. Корабльов. – Д. : Національний гірничий університет, 2010. – 465 с.
7. Харченко В.П. Мультирівнева модель даних для ідентифікації забезпеченості вимог відповідно нормативно-правовому забезпеченню кібербезпеки цивільної авіації / В.П. Харченко, О.Г. Корченко, С.О. Гнатюк // Захист інформації. – 2017. – Т.19. – №1. – С. 95-104.

УДК 004.056.5

Голев Д. В.
ст. викладач ОНАЗ ім. О. С. Попова.
denis_veteran@ukr.net
Міненко В. А.,
ОНАЗ ім. О. С. Попова.
minenko.od@gmail.com
Науковий керівник:
ст. викладач Голев Д. В.

РОЗРОБЛЕННЯ УНІВЕРСАЛЬНОЇ МОДЕЛІ ЗАГРОЗ ДЛЯ ОРГАНІЗАЦІЙ

Анотація. *Розглядається проблема захисту інформації в державних і корпоративних інформаційних мережах. Розкрито питання актуальності обраної теми. Приведена статистика загроз, що широко використовувались у світовій практиці у 2016р. Приведено поняття кіберзагрози. Розглянуті можливі джерела кібернетичних загроз. Складено перелік і класифікацію загроз, що можуть бути використані зловмисниками проти інформаційних та комп'ютерних мереж. За результатами класифікації створено модель загроз, що може використовуватися для оцінки можливих загроз для організації.*

Ключові слова: кібератака, класифікація загроз, модель загроз.

Актуальність проблеми забезпечення безпеки інформаційних мереж зростає з кожним роком. Найбільша кількість атак у 2016р. направлені проти міжнародних організацій, державних установ. За статистикою, наданою Аналітичним центром компанії InfoWatch у 2016 році було зареєстровано 1556 випадків витоку конфіденційної інформації, що перевищує дані за 2015р на 3,4% [1].

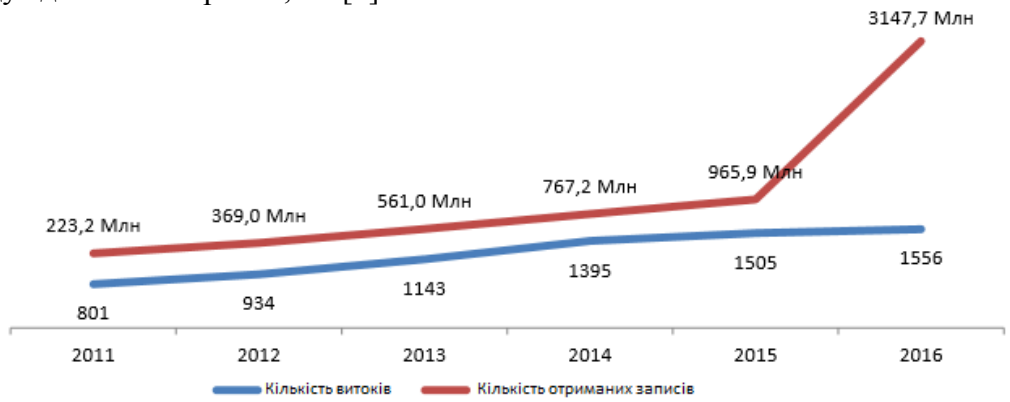


Рис. 1. Кількість витоків інформації і об'єм персональних даних, що було скомпрометовано в результаті витоків 2011 – 2016 рр.

Серед цих атак зовнішні атаки становлять 38%. 93% цих витоків – це персональні дані та платіжна інформація, а саме це 3,1 млрд персональних записів.

В роботі пропонується класифікувати загрози за їх джерелом: на зовнішні та внутрішні.

До зовнішніх загроз відносяться:

- Шкідливе програмне забезпечення, а саме:
  - Експлойти – це послідовність команд, що використовують заздалегідь відомі дефекти або вразливості програмного забезпечення для того, щоб викликати непередбачувану поведінку програми або комп'ютера.;
  - Троянські програми – шкідливе ПЗ, що не може самостійно розповсюджуватися і розповсюджується людьми, вводячи їх в оману. Як правило, трояни розповсюджуються за допомогою будь-якої із форм соціальної інженерії.
  - Комп'ютерні віруси – це шкідлива комп'ютерна програма яка, може самостійно розповсюджуватись, тобто копіювати свій шкідливий код в інші компютерні програми, файли даних, сектор завантажування жорсткого диску.
  - Комп'ютерні хробаки - самостійна шкідлива комп'ютерна програма, що може самостійно розповсюджуватися мережею, копіюючи себе на інші системи, що мають проблеми з захистом. Хробаки майже завжди шкодять мережі, наприклад, споживаючи пропускну здатність.
- Атаки на відмову в обслуговуванні:
  - Атака з одного комп'ютеру DoS-атака – це кібератака, коли злочинець прагне зробити машину або мережевий ресурс недоступним для можливих користувачів, тимчасово або на невизначений термін заблокувавши послуги хосту, підключеного до мережі Інтернет.
  - Розподілена атака на відмову в обслуговуванні DDoS-атака – DoS-атака, що здійснюється з багатьох різних джерел та робить неможливим зупинення такої атаки шляхом блокування певного джерела.;
- APT (Advanced persistent threat) – розвинена стала загроза – це вид прихованої і тривалої атаки, що часто керується особою чи особами, що націлені на конкретний об'єкт. Ціллю APT, зазвичай, є приватні або державні організації, як для бізнесу так і для політичних мотивів. APT атаки вимагають високого рівня прихованості протягом тривалого часу.;
- Соціальна інженерія:

- Претекстинг це атака по заздалегідь складеному сценарію. Результатом є отримання від жертви певної інформації чи виконання якоїсь дії. Ця техніка потребує попереднього дослідження цільового об'єкту.;
- Фішинг – техніка, спрямована на введення користувача в оману. Найчастіше зловмисник відправляє електронного листа, що має вигляд офіційного листа – від банку, платіжної системи, що потребує «перевірки» певної інформації або посилання на фальшиву веб-сторінку, що імітує офіційну сторінку і потребує введення якоїсь конфіденційної інформації.;
- «Дорожнє яблуко» - ця атака схожа на троянську програму. Зміст атаки в тому, щоб підкинути співробітнику компанії фальшивий фізичний носій інформації (флеш-накопичувач, тощо).

До внутрішніх загроз відносяться:

- Людський фактор – психічні можливості людини як потенційне і актуальне джерело інформаційних проблем та загроз при використанні людиною сучасних інформаційних технологій. Усі дії людини щодо порушення режиму безпеки можна розділити на дві категорії: навмисні та ненавмисні дії. До навмисних дій відноситься крадіжка інформації співробітниками, її модифікація або знищення. До ненавмисних можна віднести втрату носіїв інформації, знищення або спотворення інформації з необережності.
- Інсайдерська діяльність.

За такою класифікацією було створено модель загроз, яку можна використати для будь-якої організації чи державної установи:

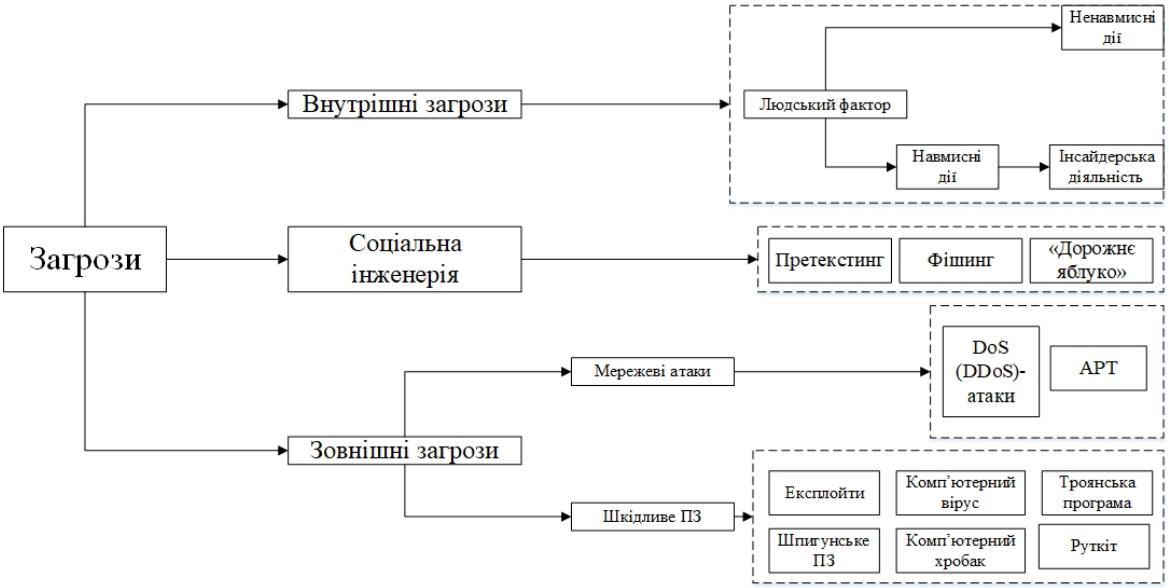


Рис. 2. Модель загроз інформаційної безпеки для організацій та державних установ

Висновки. *Було створено унікальну та універсальну модель загроз, що можна використовувати для аналізу мережі будь-якої організації чи державної установи. Після такого аналізу можна чітко виділити загрози для конкретної мережі і будувати систему захисту інформації в мережі. Беручи до уваги модель загроз пропонується використання методу ешелонованої оборони.*

Література

1. Аналітичний центр InfoWatch – Глобальное исследование утечек конфиденциальной информации в 2016 году – 2017 р.

2. ISO/IEC, "Information technology -- Security techniques-Information security risk management" ISO/IEC FIDIS 27005:2008.

УДК 004.738.5:159.923

Гріга В.С.
студент НАУ
gsmgrey1@gmail.com
Каданова В. О.
студентка НПУ ім. М. П. Драгоманова
Гізун А. І.
к.т.н., доцент кафедри БІТ НАУ

АРХІТЕКТУРА СИСТЕМИ ВИЯВЛЕННЯ ТА ІДЕНТИФІКАЦІЇ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ

Анотація. *У роботі представлено архітектуру системи виявлення та ідентифікації інформаційно-психологічного впливу, що реалізована за допомогою експертних методів та нечіткої логіки. Вона складається з таких структурних елементів: система датчиків (СД); модуль первинної обробки вхідних параметрів, що вміщує регістри ідентифікуючих параметрів (РІП), регістри ІПВ (РІПВ), блок формування зв'язки вплив-параметр (БФЗВП); модуль вторинної обробки ідентифікуючих параметрів, що складається з блоку фазифікації ідентифікуючих параметрів (БФІП) та блоку формування кортежів фазифікованих параметрів (БФКФП); модуль виконання нечітких арифметичних операцій, до якого відносяться блок формування ідентифікатора поточного стану і блок прийняття рішення; модуль формування еталонів та евристичних правил, до складу якого входять однойменні відповідні блоки; модуль представлення результату, що містить блок логічного висновку та блок візуалізації; а також модуль управління режимами (МУР), що переводить систему в режим корекції еталонів (РКЕ) або режим корекції евристичних правил (РКЕП).*

Оскільки лише виявлення інформаційного впливу, враховуючи важливість захисту соціальних груп в поєднані з стрімким розвитком сучасних засобів та способів порушення інформаційної безпеки, на сьогодні є не достатнім. Виникає необхідність в його ідентифікації, так як вибір контрзаходів є більш ефективним для конкретного і заздалегідь відомого впливу. Тому основне призначення даної системи – прогнозування або виявлення та ідентифікація ІПВ. На сьогодні аналогічних систем практично немає. Подібні системи для виявлення інформаційно-психологічного впливу засновані на теорії ймовірності [1]. Такий підхід не дозволяє виявляти невідомі методи впливу, контролювати слабоформалізований простір. Крім того для таких систем необхідний довготривалий підготовчий етап перед введенням їх в експлуатацію. В рамках такої підготовки зазвичай проходить вибірка статистичних даних, навчання системи тощо. Тому при розробці даної системи будемо використовувати підходи засновані на нечіткій логіці та експертні методи, що позбавлені таких недоліків. Призначенням СВІІПВ є виявлення та ідентифікація ІПВ. Вхідними даними системи є ідентифікатори ІПВ, контрольовані параметри та їх значення. На виході системи – інформація щодо ІПВ, його ідентифікуючі дані. Архітектура СВІІПВ представлена на рис. 1.

Прототипом розроблюваної системи є засоби управління кризовими ситуаціями, що описані в роботах [3-4].

СД розміщена в кібернетичному середовищі, що є нечітким та слабоформалізованим. Склад СД залежить від поставлених цілей. СД проводить моніторинг контексту в кібернетичному просторі.

В модулі первинної обробки вхідних параметрів задаються ІПВ, які система виявляє та ідентифікує, а також відповідні їм ідентифікуючі параметри. В РІПВ заносяться ідентифікатори основних методів інформаційно-психологічного впливу $IIS_i, i = \overline{1,n}$, а в РІП аналогічно заносяться з певною періодичністю поточні значення ідентифікуючих параметрів $P_{ij}, i = \overline{1,n}; j = \overline{1,m}$. $IIS_i \longrightarrow P_i$

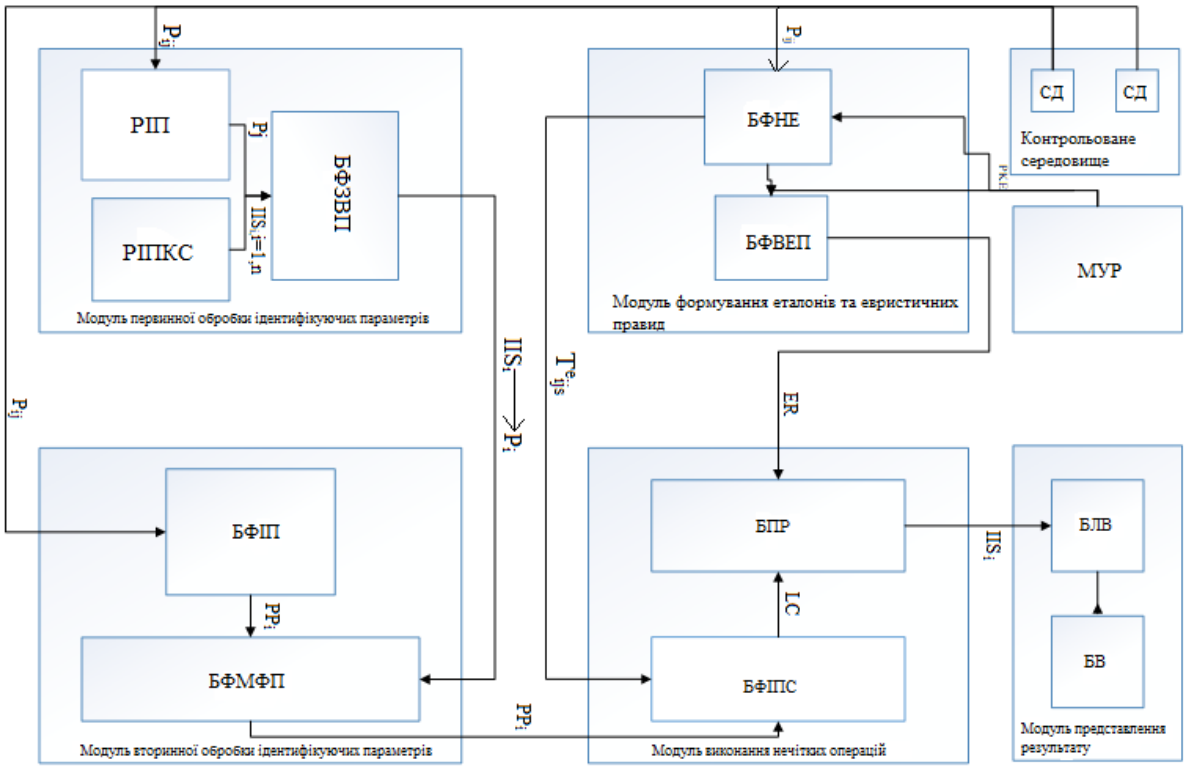


Рис. 1. Архітектура СВІІПВ

В БФЗВП формуються зв'язки $IIS_i \longrightarrow P_i$ конкретного типу ІПВ з параметрами, що необхідні для його виявлення. Так для окремих методів ІПВ створюються підмножини P_i. Модуль вторинної обробки ідентифікуючих параметрів призначений для фазифікації ідентифікуючих параметрів та подальшого їх групування відповідно до методів ІПВ, які вони визначають. В БФІП проводиться процедура фазифікації, яка полягає в перетворені виміряних поточних параметрів за певний період в нечітких термах, в результаті формуються підмножини PP_i. В БФКФП уже фазифіковані ідентифікуючі параметри групуються в підмножини у відповідністю з сформованими в БФЗІП зв'язками. В модулі формування еталонів та евристичних правил формуються еталонні величини, необхідні для виміру поточних значень контрольованих параметрів та евристичні правила для прийняття рішення. БФНЕ призначений для створення експертами множини еталонів ідентифікуючих параметрів. Еталони описуються за допомогою термів як лінгвістичні змінні.

В БФЕП у процесі зіставлення ідентифікаторів поточного стану, що визначається комбінацією значень поточних параметрів, та лінгвістичних ідентифікаторів можливості реалізації ІПВ формується набір правил для всіх заданих методів впливу. Утворені еталони та евристичні правила є основними експертними даними, що забезпечують роботу СВІІПВ. Вони задаються перед початком роботи системи з виявлення ІПВ. Існує можливість їх корекції. Для цього МУР переводить в систему в РКЕ або РКЕП, під час яких еталони та ЕП можуть бути змінені експертом чи оператором системи. Призначення модуля виконання нечітких арифметичних операцій полягає в порівнянні поточних значень параметрів з еталонними і визначені ЕП, що узгоджує поточну ситуацію, тобто прийняті рішення щодо факту існування чи можливості появи ІПВ.

В БФІПС виміряні і фазиковані ідентифікуючі параметри з використанням методу узагальненої відстані Хемінга порівнюються з еталонами, визначаючи відповідні (найбільш близькі) поточній ситуації терми, і на основі цього формується ідентифікатор поточного стану. В БПР ідентифікатор поточних станів порівнюється з наборами ЕП, в процесі чого

шукається правило, що погоджує поточний ідентифікатор. Ймовірність появи ІПВ прирівнюється значенню лінгвістичного ідентифікатора можливості реалізації ІПВ правила, що спрацювало.

Призначення модуля представлення результату полягає в відображені отриманих результатів в зрозумілій для оператора системи вигляді. Отриманий результат може бути відображений в лінгвістичній формі.

Отже, розроблена система виявлення та ідентифікації інформаційно-психологічного впливу представляє собою реалізацію раніше розробленого методу виявлення та ідентифікації інформаційно-психологічного впливу [2]. Дана система дозволяє не лише виявити, а й ідентифікувати методи інформаційно-психологічного впливу.

Література

1. Hutchinson B. Information Warfare: Using the Viable System Model as a framework to attack organizations / B. Hutchinson, M. Warren. // Australasian Journal of Information Systems. – 2002. – Vol 9. – № 2. – 10p.

2. Гріга В. Метод виявлення та ідентифікації інформаційно-психологічного впливу/ VI-та міжнародна науково-технічна конференція ITSEC 2017 р. – К. 2017. – С. 84.

3. Іванченко Є. Базова архітектура експертної системи прогнозування та попередження кризових ситуацій/ Є. В. Іванченко, О. В. Гавриленко, А.І. Гізун // Захист інформації. – 2012. – Т.14. – №3. – С. 94-98.

4. Гізун А. Обчислювальний комплекс виявлення та оцінювання кризових ситуацій в інформаційній сфері/ А.І. Гізун // Захист інформації. – 2016. – Т.18. – №1. – С. 66-73.

УДК004.056.5:378.1 (043.2)

Дика Н.В.
студентка, Національний авіаційний університет
Nadin_dyka@ukr.net
Одарченко Р. С.
доцент, Національний авіаційний університет
odarchenko.r.s@ukr.net
Шульга Б.С.
завідувач відділу телекомунікаційних досліджень,
Державний науково-дослідний
експертно-криміналістичний центр МВС України
brodka@ukr.net

МЕТОДИ ОЦІНКИ ВПЛИВУ ТА ЗАПОБІГАННЯ КІБЕРМОББІНГУ

Анотація. *Проблема кібермобінгу, як негативне соціально-психологічне явище, виникло зовсім недавно. Тим часом, кількість людей, що піддаються кібермоббінгу, зростає з кожним днем. Тому в даній роботі проаналізовані основні поняття та типи кібермоббінгу, розкрито їх сутність. Також було розроблено метод оцінки впливу різних проявів кібермоббінгу на психічне здоров'я індивідів за рахунок встановлення кореляційних зв'язків. На доданок, розроблено анкету, на основі якої було проаналізовано на скільки молодь схильна та підвержена кібермоббінгу.*

Технологічні засоби комунікації стали новітньою «зброєю» для сучасних підлітків і суспільства загалом. Іноді наслідки від кібермоббінгу можуть бути більш негативні, ніж від реального насильства, тому що віртуальний світ не має кордонів, ні просторових, ні часових.

Моббінг – психологічні утиски, переважно групові, учня з боку учнів, вчителів або вчителя з боку учнів, а так само адміністрації школи, які включають в себе постійні

негативні висловлювання, критику на адресу учня (вчителя); соціальну ізоляцію жертви моббінга всередині колективу, виключення його зі службових дій чи соціальних контактів, поширення про нього завідомо неправдивої інформації тощо, нападки ущемляють честь і гідність людини, заподіяння матеріального чи фізичної шкоди [1]. Моббінг, здійснюваний в інформаційному просторі через інформаційно-комунікаційні канали та засоби, називається Кібермоббінгом. Кібермоббінг здійснюється в інформаційному просторі через інформаційно-комунікаційні канали і засоби з застосуванням нових технологій, передусім Інтернету і мобільних телефонів за допомогою електронної пошти, програм для миттєвого обміну повідомленнями (наприклад, Viber) в соціальних мережах (Facebook, Vkontakte, LinkedIn, Twitter тощо), а також через розміщення на відеопорталах (YouTube, Vimeo та інших).

До найчастіших типів поведінки, характерних для кібермоббінгу належать [2, 3]: Flaming (образа); Harassment (домагання); Denigration (обмовлення, поширення чуток); Impersonation (використання фіктивного імені); Outing and Trickery (публічне розголошення особистої інформації); Exclusion (соціальна ізоляція); Happy Slapping (Радісне побиття); Cyberstalking (тривалі домагання і переслідування); Cyberthreats (відкрита загроза фізичної розправи). Надалі наведемо метод оцінки впливу різних видів кібермобінгу на людей.

Метод оцінки впливу кібермоббінгу на людей. Даний метод реалізується у 5 етапів.

Етап 1 – Визначення впливу кібермоббінгу. Для реалізації цього етапу введемо множину форм кібермоббінгу, які обираються із класифікації типів кібермоббінгу.

Етап 2 – Визначення показників стану психічного здоров'я. На цьому етапі обираються ключові показники стану психічного здоров'я для кожної групи кібермоббінгу *S*, Підмножини показників психічного здоров'я $\mathbf{S_{ij}} \subseteq \mathbf{S_i}$ визначимо як:

$$\mathbf{S_{ij}} = \{\bigcup_{\mathbf{p=1}}^{\mathbf{r_{ij}}} \mathbf{S_{ijp}}\} = \{S_{ij1},\ S_{ij2},\ \ldots,\ S_{ijr_j}\}, \tag{1}$$

де S_{ijp} $(p = \overline{1, r_{ij}})$ – показники стану психічного здоров'я, r_{ij} – кількість таких показників. *До основних станів психічного здоров'я відносять: агресію, стрес, настрій, афект, страх, гнів, сором, фрустрацію, радість.*

Етап 3 – Вибір показників, які впливать на психічне здоров'я. Відбувається вибір ключових показників, які впливають на показник стану психічного здоров'я, що досліджується. Для кожної факторної ознаки потрібно визначити її числові характеристики.

Вибір функції

$$\hat{Y} = f(x_1, x_2, x_3, ..., x_n), \tag{2}$$

де $\hat{Y}$ – результативна ознака-функція стану психічного здоров'я; $x_1, x_2, x_3, ..., x_n$ – факторні ознаки.

Щоб мати можливість судити про порівняльну силу впливу окремих факторів і резерви, які в них закладені, повинні бути обчислені частинні коефіцієнти еластичності E_i, а також бета-коефіцієнти β_i.

$$E_i = a_i \frac{\overline{x_i}}{\overline{y_i}}, \tag{3}$$

де a_i – коефіцієнт регресії при *i*-му факторі; $\overline{x}_i$ – середнє значення *i*-го фактору; $\overline{y}_i$ – середнє значення досліджуваного показника.

β – коефіцієнти:

$$\beta_i = a_i \frac{\sigma_{x_i}}{\sigma_y}, \tag{4}$$

де σ_{x_i} – середнє квадратичне відхилення *i*-го фактору; σ_y – середнє квадратичне відхилення показника; β – коефіцієнт показує, на яку частину середнього квадратичного відхилення змінюється стан психічного здоров'я із зміною відповідної факторної ознаки на величину його середнього квадратичного відхилення.

Коефіцієнт, який показує, яка частка внеску кожного аналізованого фактора в сумарний вплив всіх відібраних факторів:

$$\Delta_i = \frac{\beta_i r_i}{R^2}. \quad (5)$$

Етап 4 – Оцінка показників факторної ознаки. Для реалізації даного етапу використаємо підмножини показників факторної ознаки S_{ijp} (5) і відповідні формули для їх розрахунків та алгоритми проведення необхідних вимірювань, визначених у методиках, регламентованих державними та міжнародними контролюючими органами.

Етап 5 – Порівняння показників з гранично допустимими значеннями.

На даному етапі отримані значення порівнюємо з гранично допустимими, можливими для підтримання нормального стану здоров'я. Якщо ці значення перевищують допустимі, необхідно провести аналіз тих проявів кібермоббінгу, які можуть чинити найбільший вплив на психічне здоров'я людини.

Для порівняння отриманих значень в результаті розрахунків з гранично допустимими введемо логічну функцію еквівалентності:

$$E(x, y) = \begin{cases} 1, \textit{при } x > y, \\ 0, \textit{при } x \le y. \end{cases} \quad (6)$$

Анкетування. Для досягнення поставленої мети дослідження, був проведений кількісний аналіз – анонімне анкетування, яке дозволило визначити відсоткове співвідношення числа постраждалих від кібермоббінгу підлітків до числа не постраждалих. В анкетуванні брала участь молодь віком від 11 до 22 років. В основному – це підлітки віком 15 років (39%) та 16 років (25%). Всього було опитано 84 учасники.З них 63% від загального числа респондентів дівчат і 37% хлопців.

В ході проведеного досліду було виявлено, що 99% користуються Інтернетом та соціальними мережами щодня та 20% мають більше, ніж 8 аккаунтів в соціальних мережах. Це свідчить про те, що мережа Інтернет стала невід'ємним атрибутом повсякденного життя підлітків.17% мають більше, ніж 500 підписників у своїх мережах.

З усієї опитаної молоді, 32% знає що таке кібермоббінг та 46 % з опитаних підлітків вказали, що піддавалися впливу кібермоббінгу. Більше того, 12% встигли побувати в ролі кібермоббера під чужим ім'ям.

Крім цього, 52% серед опитаних вказали, що писали у мережі невтішні коментарі на адресу інших користувачів мережі. Цей результат підтверджує, що грань між кібермобберами і жертвами зовсім невелика, і мережеві агресори і їх жертви знаходяться поруч, і навіть, можливо, вчаться за однією партою.

Найбільш часто підлітки піддаються наступним типам кібермоббінгу: Найбільша кількість (17%) була під впливом Flaming (образа),яка практично в рівній мірі найбільш поширена серед молоді, де підлітки публікують неприємні і агресивні коментарі, вульгарні звернення та зауваження. Потім 5% були піддані Harassment (домагання). 65 % відповіли що не були під впливом жодного з типів кібермоббінгу.

Стикаючись з проблемою, зокрема, в Інтернеті, 59,5% підлітків схильні розповідати про це в першу чергу своїм друзям, потім 23% відповіли, що розкажуть про свої проблеми батькам та 17% залишать це при собі. Дані показники можна пояснити тим, що страх втратити доступ до соціальних мереж змушує жертв кібермоббінгу приховувати свою проблему від батьків і вчителів.

На час проходження анкети, 27% опитуючих оцінюють свій психологічний стан як « дуже добре», та лише 4 % відповіли, що відчувають «дуже погано».

Висновок. У цій роботі, було проаналізовані основні поняття кібермоббінгу. Визначено та охарактеризовано типи кібермоббінгу. Було розроблено метод оцінки впливу різних проявів кібермоббінгу на психічне здоров'я індивідів за рахунок встановлення кореляційних зв'язків кожного із можливих впливів на результуючу ознаку у виигляді психічного здоров'я, що дозволяє оцінити рівень негативного впливу проявів кіббермобінгу

на психічний стан індивідів, його прогнозування та поліпшення. Проблема кібермоббінгу зустрічається в різних вікових категоріях суспільства, проте, найбільшого впливу кібермоббінгу зазнають саме підлітки у віці від 12 до 17 років. Тому було розроблено анкету, на основі якої було проаналізовано на скільки молодь схильна до кібермоббінгу. Всього було опитано 84 людини. Аналіз опитування показує, що майже половина підлітків, які взяли участь в анкетуванні була під впливом кібермоббінгу. Також з аналізу дослідження, можна сказати, що кібермоббінг і один з його видів «Flaming» є найпоширеним в мережі Інтернет серед молоді. Користувачі Інтернет почувають себе захищеними анонімністю, що призводить до вседозволеності в мережі.

Література

1. Когутяк Н. Особливості самопрезентації підлітка в середовищі віртуального спілкування: причини кібербулінгу / Н. Когутяк // Збірник наукових праць: філософія, соціологія, психологія. – Івано-Франківськ: Вид-во ДВНЗ «Прикарпатський національний університет імені Василя Стефаника», 2014. – Вип.19. –Ч. 1. – 252 с.
2. Вавренюк Е.А., Бай Е.А. «Психологическое насилие в подростковой среде: проблема и способы решения». – Брест, БрГУ, 2012. – 305 с.
3. Кибермоббинг [Електронний ресурс] – Електронні текстові дані. – Режим доступуhttp://www.mobbingu.net/articles/section/cyber/
4. А. Бочнярц, А. Грабовіч.Кібермоббінг – виклик для сучасної освіти //Вісник ЛНУ імені Тараса Шевченка.- № 13 (272). – Ч. 2. – 2013. – С. 6-14.
5. Найдьонова Л. А. Кібербулінг або агресія в Інтернеті: способи розпізнання і захист дитини : [методичні рекомендації]/Л.А.Найдьонова. – Вип.4. – К., 2011. – 34 с.

УДК 621.321

Ковальчук Л.В.
ФТІ НТУУ «КПІ ім. Ігоря Сікорського»
lusi.kovalchuk@gmail.com
Кучинська Н.В.
ІСЗЗІ НТУУ «КПІ ім. Ігоря Сікорського»
n.kuchinska@gmail.com

МЕТОДИКИ ПЕРЕВІРКИ НЕЗАЛЕЖНОСТІ СТАТИСТИЧНИХ ТЕСТІВ

Анотація. *В роботі представлено огляд існуючих методик перевірки незалежності статистичних тестів та запропоновано нову математично обґрунтовану методику, яка має ряд переваг; представлено результати експериментального дослідження застосування нової методики до пакетів тестів.*

Необхідною умовою стійкості криптосистеми є наявність певних криптографічних властивостей у генератора, що в ній використовується. До цих властивостей відносяться: рівноймовірність та незалежність символів вихідної послідовності; непередбачуваність; великий період (більший за 2^{80} біт) та деякі інші. У зв'язку з цим, постає питання оцінки якості і генератора його окремих послідовностей.

Основним методом перевірки якості генератора є застосування до нього певних статистичних критеріїв. Існує багато наборів таких критеріїв; найбільш популярним серед них є NIST та DIEHARD. Однак слід зазначити, що на даний час більшість питань щодо формування набору тестів, визначення їх кількості, вибору значення помилки першого роду та інші питання вирішуються інтуїтивно та емпірично. У даній роботі буде представлено математично обґрунтований підхід до формування набору статистичних критеріїв.

1. Огляд попередніх результатів.

1.1. Перевірка незалежності тестів згідно NIST 800-221 та NIST 800-22 (1a).

Вперше питання необхідності перевірки незалежності статистичних тестів для усунення "надлишкових" тестів піднімається у стандарті NIST 800-221 "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications" [1]. Також про те, що потрібно позбавлятись від надлишкових тестів йдеться у однойменному оновленні цього стандарту від 2010 року NIST 800-22 (1a) [2].

Проте процедура перевірки незалежності (некорельованості) тестів в жодній версії цього стандарту не обґрунтована та не формалізована.

За результатами вивчення документу NIST 800-22 (1a) можна зробити висновки:

1) з метою виключення "надлишкових" тестів з набору, призначеного для тестування ГВП або ГПВП, необхідно перевіряти тести цього набору на незалежність;

2) автори документу NIST 800-22 (1a) не надали пояснення запропонованої методики, достатнього для розуміння принципів її роботи, а також не навели ні її обґрунтування, ні формалізації;

3) питання розробки та удосконалення відповідної методики досі залишається відкритим.

1.2. Методика перевірки незалежності тестів, що використовує центральну граничну теорему.

Дану методику вперше запропоновано та обгрунтовано у роботі [3], а потім удосконалено та узагальнено у роботах [4, 5]. Стисло наведемо та проаналізуємо її.

Нехай A і B – деякі тести. Випадкові величини ξ_A та ξ_B – індикатори проходження послідовністю тестів A та B відповідно.

Означення 1. Тести A та B назвемо незалежними (відносно деякого фіксованого генератора G), якщо індикатори ξ_A, ξ_B статистично незалежні.

Іншими словами, незалежність тестів означає, що результат застосування тесту A для послідовності не залежить від результату застосування тесту B. Дане означення більш слабке, ніж означення незалежності статистик. Зауважимо, що залежність від генератора у означенні 1 є суттєвою.

Аналогічно можна означити набір незалежних тестів.

Нехай потрібно перевірити незалежність набору з N тестів, де i-й тест має рівень значимості α_i, $i=\overline{1,N}$. Для перевірки незалежності набору використовується ГВП, який має необхідні статистичні якості. Це означає, що даний генератор повинен пройти тестування набором тестів, для якого перевіряється незалежність, та результати тестування повинні бути оцінені за методикою, вказаною в [1, 2]. За цих умов можна вважати, що цей генератор виробляє послідовності, які є реалізаціями незалежних, рівноімовірно розподілених на заданому алфавіті випадкових величин. При цьому залежність чи незалежність тестів не впливають на якість оцінки ГВЧ, а впливають лише на час проведення тестування.

Нехай отримано n послідовностей з ГВЧ (довжини послідовностей повинні бути придатними для проведення тестування).

Теорема 1 ([3])**.** Покладемо $\eta_j = 1$, якщо j-та послідовність пройшла всі тести, та $\eta_j = 0$ у протилежному випадку, тобто якщо j-тою послідовністю хоча б один тест не пройдено, $j=\overline{1,n}$. Позначимо через $\eta = \frac{1}{n}\cdot\sum_{j=1}^{n}\eta_j$ частку послідовностей, які пройшли всі тести. Покладемо

$$a=\prod_{i=1}^{N}(1-\alpha_i),\ \sigma^2=\frac{1}{n}\cdot\left(a-a^2\right). \tag{1}$$

Тоді, за умови незалежності тестів набору, випадкова величина $\eta - a \big/ \sigma$ має

асимптотично стандартний нормальний розподіл, тобто $P\left(\eta - a \big/ \sigma < x\right) \approx \Phi(x)$, де Ф – функція стандартного нормального розподілу.

Дана теорема дає можливість побудувати ефективну та математично обґрунтовану методику (надалі *Методика 1*) перевірки незалежності тестів, що застосовуються для оцінки якостей ГВП. Вказана методика спирається лише на строго доведені твердження і детально викладена в [3]. Її зручність та дієздатність у практичному використанні підтверджена застосуваннями для перевірки багатьох відомих наборів статистичних тестів, у тому числі описаних у [1-3]. Відповідний метод є:

– універсальним і може бути застосованим до будь-якої кількості тестів будь-якої природи;

– адаптивним, тобто його параметри обчислюються у залежності від певних параметрів набору (кількість тестів, рівні значимості, і т.д.);

– зручним, алгоритм його використання є чітким та простим для розуміння.

Проте запропонований підхід має і значні недоліки.

1. Методика може застосовуватись тільки до "ідеального" з точки зору криптографічних властивостей генератора. Наприклад, вона добре працює для генератора, описаного у додатку А ДСТУ 4145-2002 ([6]). Але якщо розподіл на послідовностях, що виробляє генератор, має відхилення від "ідеального", то умови теореми порушуються.

2. При формулюванні теореми припускається, що якщо рівень значимості тесту дорівнює α, то математичне сподівання пропорції послідовностей, що проходять цей тест, дорівнює $1-\alpha$. Тому методика коректно спрацьовує лише для тестів певного типу.

3. Для того, щоб наближення нормальним розподілом було коректним, кількість послідовностей повинна бути близько 10000. Тестування такої кількості послідовностей вимагає досить великого часу, особливо якщо тести є громіздкими та їх багато.

Для подолання недоліку, зазначеного у пункті 2, методику було удосконалено та узагальнено на випадок генератора з довільним розподілом та на випадок тестів довільної природи [4, 5]. Але при цьому удосконалена методика стала більш громіздкою та затратною, і вимагає ще більшу кількість послідовностей (в деяких випадках – близько 1000000).

1.3. Методика перевірки незалежності тестів, що використовує взаємну коваріацію випадкових величин.

Дану методику, запропоновано в [7, 8]. Нехай $y_1,...,y_n$ – деякі випадкові величини. Позначимо y_{ij}, $i=\overline{1,n}$, $j=\overline{1,n}$ – результат j-го спостереження (вимірювання) випадкової величини y_i, $\overline{y_i} = \frac{1}{p}\sum_{j=1}^{p} y_{ij}$. Побудуємо матрицю вибіркової коваріації цих випадкових величин: $D = \left(d_{ij}\right)_{i,j=1}^{n}$, $d_{ij} = \frac{1}{p-1}\sum_{k=1}^{p}\left(y_{ik}-\overline{y_i}\right)\left(y_{jk}-\overline{y_j}\right)$ та їх матрицю вибіркової кореляції: $R = \left(R_{ij}\right)_{i,j=1}^{n}$, $R_{ij} = \frac{D_{ij}}{\sqrt{D_{ii}D_{jj}}}$.

Теоретично для незалежних випадкових величин R - одинична матриця і її визначник повинен бути рівний 1. Але ми маємо лише оцінку R, побудовану на n вибірках обсягу p значень випадкових величин. Тому в якості критерію перевірки гіпотези H_0: $R = I$ беруть визначник: $V = \det R$.Закон розподілу V досить складний, але при досить великих значеннях p можна використовувати його асимптотичне подання:

$$P\{-m\cdot\ln V \le \nu\} = P\left\{\chi_f^2 \le \nu\right\} + \left(\gamma_2 \big/ m^2\right)\cdot\left[P\left\{\chi_{f+4}^2 \le \nu\right\} - P\left\{\chi_f^2 \le \nu\right\}\right] + O\left(m^{-3}\right), \qquad (2)$$

де $f = \frac{n(n-1)}{2}$; $m = p - \frac{2n+11}{6}$, $\gamma_2 = \frac{n(n-1)}{288}(2n^2-2n-13)$.

Зауважимо, що в «ідеалі» $\ln V = 0$. Отже, критична область для перевірки гіпотези буде $m \cdot \ln V > \nu$ при рівні значущості $\alpha = 1 - P\{-m \cdot \ln V \le \nu\}$.

Вираз (2) можна використовувати, якщо $\left(\gamma_2 / m^2\right) < 1$. Отже всі умови використання методики, яка буде наведена, визначаються цією вимогою.

Методика 2 (перевірки незалежності тестів з використанням вибіркової кореляційної матриці)

1) отримаємо значення y_{ij}, $i = \overline{1,n}$, $j = \overline{1,n}$, та обчислимо $\overline{y_i}$;

2) обчислюємо кореляційну матрицю R;

3) обчислимо визначник V кореляційної матриці;

4) задаємо рівень значущості β, знаходимо квантіль χ^2_β з f ступенями свободи;

5) Якщо $\chi^2_\beta > -m \cdot \ln V > \nu$, то гіпотеза про незалежність тестів підтверджується, інакше відхиляється.

Методика 2 не моє недоліків, притаманних Методиці 1, і може застосовуватись до довільних тестів та генераторів, при цьому не є необхідним тестувати занадто велику кількість послідовностей. Недоліком є те, що вона перевіряє лише лінійну залежність відповідних випадкових величин.

Зазначимо, що застосування Методик 1 та 2 до різних пакетів тестів, зокрема до тестів, визначених у [1-4] для ГВП з Додатку А у [6], дало приблизно однакові результати.

2. Побудова та обґрунтування методики перевірки незалежності статистичних тестів, що використовує нерівність Чебишева.

Припустимо, що ГВП, має хороші криптографічні якості, а рівень значимості кожного тесту дорівнює середній кількості послідовностей, що не проходять цей тест (проте згодом покажемо, як можна модифікувати цю методику для більш загального випадку).

Теорема 2. Покладемо $\eta_j = 1$, якщо j-та послідовність пройшла всі тести, та $\eta_j = 0$ у протилежному випадку, тобто якщо j-тою послідовністю хоча б один тест не пройдено, $j = \overline{1,n}$. Позначимо η - частку послідовностей, які пройшли всі тести: $\eta = \frac{1}{n} \cdot \sum_{j=1}^{n} \eta_j$, a, σ^2 визначено в (1). Тоді, якщо тести незалежні, то $P\{|\eta - a| > \varepsilon\} \le \frac{\sigma^2}{\varepsilon^2}$.

Використовуючи наведені результати, побудуємо методику перевірки незалежності статистичних тестів.

Методика 3 (перевірка незалежності тестів з використанням нерівності Чебишева)

1. Задати β – рівень значимості для статистичної перевірки незалежності тестів цього набору (ймовірність помилки першого роду).

2. Обчислити a, σ^2.

3. Використовуючи n послідовностей, отриманих з ГВП, обчислити η_j, $j = \overline{1,n}$.

4. Обчислити η.

5. Обчислити $\varepsilon = \sqrt{\sigma^2 \cdot \beta^{-1}}$.

6. Обчислити границі довірчого інтервалу: $I_1 = \max\{0, a - \varepsilon\}$; $I_2 = \min\{1, a + \varepsilon\}$.

7. Якщо $\eta \in [I_1, I_2]$, то гіпотеза про незалежність тестів приймається, інакше – відхиляється.

Зауваження 1. Якщо всі тести з набору мають однаковий рівень значимості α і базуються на граничних розподілах, то $a = (1 - \alpha)^N$.

Зауваження 2. Якщо ГВП має певні статистичні відхилення, або якщо у наборі є тести, в яких рівень значимості може не співпадати з імовірністю відхилення послідовності, то у п.2 Методики 3 замість величин α_i, $i = \overline{1, N}$, потрібно взяти величини A_i, $i = \overline{1, N}$, де A_i дорівнює відношенню кількості послідовностей, що *не пройшли* тест з номером i, до кількості всіх послідовностей. При цьому точність обчислень буде тим більшою, чим більша кількість послідовностей. Тому в цьому випадку рекомендується брати близько 1000 послідовностей. При цьому необхідною умовою коректної роботи методики є умова

$$\forall i = \overline{1, N}: \; A_i \neq 1. \tag{3}$$

Зазначимо, що, з урахуванням зауваження 2, Методика 3 може бути застосована до набору тестів з різними принципами побудови, а також може використовувати ГВП з різними "незначними" відхиленнями від "ідеального", де під незначними відхиленнями розуміються такі відхилення, які не порушують умову (3).

Особливою перевагою Методики 3 є те, що для її коректної роботи достатньо порівняно невеликої кількості послідовностей – вже при $n = 100$ методика дає коректні результати, тобто нетривіальні довірчі інтервали.

За результатами застосування Методики 3 до пакетів статистичних тестів, описаних у [1-4], з використанням ГПВП з Додатку А у [6], були отримані наступні результати.

1. Для пакету NIST-I, описаному у [1], за результатами 10 експериментів при $\beta = 10^{-3}$ тести завжди виявлялись залежними; при $\beta = 10^{-4}$ завжди виявлялись незалежними.

2. Для пакету NIST-II, описаному у [2], за результатами 10 експериментів при $\beta = 10^{-3}$ тести 9 разів виявлялись залежними; при $\beta = 10^{-4}$ завжди виявлялись незалежними.

3. Для пакету з шести тестів, описаному у [3, 4] (а саме: критерій χ^2 для знаків, критерій χ^2 для біграм, тест кількості серій, тест серій максимальної довжини, критерій інверсій та критерій місць знаків), за результатами 10 експериментів при $\beta = 10^{-3}$ тести завжди виявлялись незалежними; при $\beta = 10^{-2}$ 9 разів виявлялись незалежними.

Цікаво зазначити, що застосування Методики 3 навіть для ГПВП з "незначними" відхиленнями (у сенсі умови (3)) дає приблизно ті ж самі результати.

Висновки. В роботі представлено огляд всіх методик перевірки незалежності статистичних тестів, призначених для перевірки якості ГВП, ГПВП та їх послідовностей. Проведено порівняльний аналіз всіх розглянутих методик, наведено їх переваги та недоліки. За результатами порівняльного аналізу запропоновано та математично обґрунтовано вперше нову методику (Методика 3), яка має переваги як у швидкодії та простоті реалізації, так і у можливості застосування при для широкого спектра тестів та генераторів, оскільки може використовуватись для довільної кількості тестів на довільній кількості випадкових послідовностей.

Також у роботі проведено експериментальні дослідження стосовно застосування нової методики до трьох пакетів тестів. Дослідження підтвердили зручність використання та коректність запропонованої методики, яка добре працює як на хороших генераторах, так і на генераторах з слабкими статистичними властивостями.

Література

1. „A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications”, NIST 800-221.

2. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22, Rev. 1. – 131 с.

3. Ковальчук Л., Бездітний В. Перевірка незалежності статистичних тестів, призначених для оцінки криптографічних якостей ГПВ // Захист інформації 2006. – №2(29) – С. 18-23.

4. Ковальчук Л. В., Бездітний В. Т., Скрипник Л.В. Методика перевірки незалежності статистичних тестів при невідомих статистичних властивостях генератора послідовностей «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні», вип. 4 (20), 2010. – С. 66-71.

5. L.V. Skrypnik, L.V. Kovalchuk, V.T. Bezditnyi. Method of Statistical Tests Independence Checking. // Proceedings of the Ninth International Conference "Computer Data Analysis and Modeling: Complex Stochastic Data and Systems", Minsk, September 7-11, 2010. – С. 71-74.

6. ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ ДСТУ 4145 – 2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка.

7. Ковальчук Л.В., Яцук А.Г., Чуланов А.Н. Сохранение свойства независимости статистических тестов при изменении параметров тестирования // "Безопасность информации в информационно-телекоммуникационных системах", XI Международная научно-практическая конференция – Киев, май, 2008 – С.36.

8. Ковальчук Л., Чуланов А. Оценка общей ошибки 1-го рода для набора статистических тестов, статистики которых имеют нормальное или хи-квадрат распределение // Збірник тез XIV Міжнародної науково-практичної конференції «Безопасность информации в информационно-телекоммуникационных системах», 17-20 травня, 2011, Київ. –С. 28-29.

УДК 004.056

Корчинский В.В.
ОНАС им. Попова А.С.
vladkorchin@ukr.net
Кильдишев В.Й.
ОНАС им. Попова А.С.
kildishev@ukr.net,
Бердников А.М.
ОНАС им. Попова А.С.
berdnikov2000@gmail.com

СПЕКТРАЛЬНЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ТАЙМЕРНЫХ СИГНАЛОВ И ПСЕВДОСЛУЧАЙНОЙ ПЕРЕСТРОЙКИ РАБОЧЕЙ ЧАСТОТЫ

Аннотация. *В работе рассматриваются спектральные методы защиты информации на основе непозиционных таймерных сигналов и псевдослучайной перестройки рабочей частоты. Предложено использовать расширение спектра таймерных сигнальных конструкций в два этапа. На первом этапе осуществляется прямое расширение спектра псевдослучайными последовательностями, а на втором – псевдослучайная перестройка рабочей частоты. Использование прямого расширения спектра упрощает процесс выделения фронтов таймерных сигнальных конструкций при помощи корреляционного приема.*

Функционирование помехозащищённых систем связи (ПСС) в условиях преднамеренных помех можно представить как процесс радиоэлектронного конфликта (РЭК), в котором, с одной стороны, выступает ПСС, предназначенная для передачи конфиденциальной информации, а с другой – система радиоэлектронного противодействия (РЭП) противника. В задачу РЭП противника входит обнаружение сигнала ПСС и создание умышленных помех. Поэтому, в условиях РЭК актуальным является поиск методов передачи, обеспечивающих повышение защищенности существующих систем связи от средств РЭП и несанкционированного доступа (НСД).

Известно, что эффективность ПСС оценивается комплексным показателем помехозащищённости, который характеризует способность системы выполнять свои задачи с заданным качеством в условиях случайных помех, радиоэлектронного подавления и несанкционированного доступа. Важнейшим показателем помехозащищенности является скрытность. В соответствии с задачами радиотехнической разведки различают энергетическую, структурную, информационную и другие виды скрытости [1, 2]. Не менее важным показателем помехозащищенности является помехоустойчивость, которая характеризуется способностью системы связи нормально функционировать, выполняя задачи по приему информации в условиях действий помех, в том числе, умышленных.

Защищённость передачи основана на методах скрытой передачи, в которых используется расширение спектра исходного информационного узкополосного сигнала с помощью псевдослучайной перестройки рабочей частоты (ППРЧ) или псевдослучайными последовательностями [1]. Как правило, эти методы разрабатывались только для позиционных кодов. Для повышения защищённости систем связи с ППРЧ в работах [2,3] на основе предложенных алгоритмов показана возможность расширения спектра непозиционных сигналов, примером которых являются таймерные сигнальные конструкции (ТСК) [4]. В [3] показано, что использование ТСК в качестве переносчика информации в узкополосных системах связи по сравнению с разрядно-цифровым кодированием (РЦК) повышает информационную и структурную скрытность сигнальных конструкций, что объясняется способностью кодирующего устройства ТСК формировать в зависимости от задаваемых параметров построения различные ансамбли сигналов, которые отличаются структурой и числом реализаций комбинаций. К сожалению, в этих работах недостаточно исследованы вопросы по оценке взаимного влияния показателей помехоустойчивости и скрытности в зависимости от параметров построения ТСК и временных характеристик расширения спектра сигнала. Поэтому, целью данной работы является синтез сигнальных конструкций на основе ТСК и ППРЧ с учетом требований к помехоустойчивости и структурной скрытности.

Расширение спектра методом ППРЧ основано на том, что рабочая частота сигнала при передаче битов позиционного кода перестраивается в большом диапазоне частот по закону, который известен только отправителю и получателю, а, следовательно, в начале сеанса передачи недоступен средствам радиотехнической разведки (РТР) противника. В зависимости от времени передачи информации на одной несущей частоте различают быструю и медленную ППРЧ. Пусть t_0 – длительность передачи одного информационного элемента разрядно-цифрового кода, тогда при быстрой ППРЧ время передачи на одной несущей частоте $\Delta f_{\text{прч}}$ должно быть

$$t_{\text{пер}} \le t_0 . \qquad (1)$$

При медленной ППРЧ на одной несущей частоте $\Delta f_{\text{прч}}$ передается несколько бит, т.е.

$$t_{\text{пер}} > t_0 . \qquad (2)$$

Рассмотрим возможность расширения спектра ТСК с использованием быстрой и медленной ППРЧ. Для построения ТСК используется базовый временной элемент Δ и интервал $T_c = nt_0$, где n – количество элементов t_0. В пределах T_c сигнальной конструкции длительность импульсов $\tau_c = t_0 + \Delta \times l$ ($l \in 0, 1, 2, 3, \ldots$) и кратно $\Delta = t_0/s$ ($s \in 2, 3, \ldots k$). Таким образом, расстояние между значащими моментами модуляции (ЗММ) ($\tau_c \ge t_0$) меньше интервала Найквиста ($t_0 = 1/\Delta F_c$) и кратно элементу Δ. Такое условие позволяет устранить межсимвольные искажения в ТСК. Число s показывает, насколько меньше временной интервал Δ по отношению к t_0. Число переходов i в ТСК может быть различным и меняться в пределах $i = 1, 2, \ldots, n-1$. Пример формирования реализаций ТСК на интервале времени $T_c = 4t_0$ при базовом элементе Δ показан на рис. 1(а).

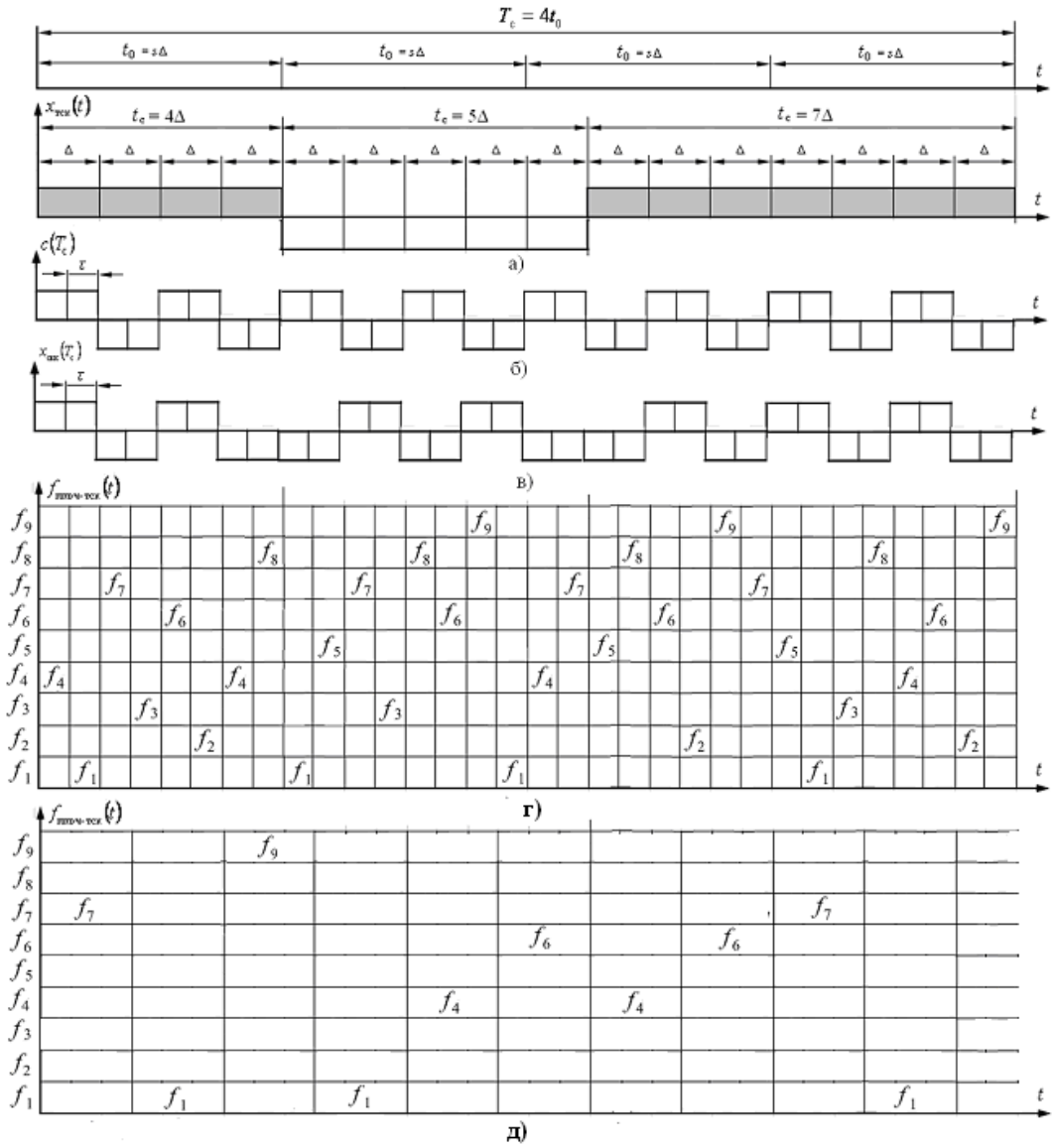


Рис. 1. Расширение спектра ТСК $x_{\text{тск}}(t_{\text{с}})$ с помощью быстрой ППРЧ (г) и медленной ППРЧ по Δ (д)

С учетом того, что $\tau_{\text{с}}$ может быть больше t_0, применить условие (1) или (2) для расширения спектра таймерных сигналов с помощью методов ППРЧ не представляется возможным из-за непозиционности ЗММ конструкции интервалам Найквиста t_0. Однако при условии $t_{\text{пер}} < t_0$ и $t_{\text{пер}} = \Delta$ возможно реализовать быструю ППРЧ, используя интервал Δ для передачи одной несущей частоты. На рис. 1 приведен пример реализации расширения спектра на интервале $T_{\text{с}} = 4t_0$ с комбинацией двух методов. Сначала спектр таймерной конструкции $x_{\text{тск}}(t_{\text{с}})$ с помощью элементов $\tau = \Delta / j$ (где j = 1, 2, 3, … – количество элементов τ на интервале Δ) псевдослучайной последовательности $c(T_{\text{с}})$ (рис. 1(б)) преобразуется в широкополосный сигнал $x_{\text{скк}}(T_{\text{с}}) = x_{\text{тск}}(t_{\text{с}}) \times c(T_{\text{с}})$ (рис. 1(в)), а затем с помощью быстрой ППРЧ формируется сигнал $u'(t) = x_{\text{тск}}(t) U_0 \cos(\omega(g(t)t))$(рис. 1(г)), где $\cos(\omega(g(t)t))$ – набор частот, который представляет собой функцию от кодового сигнала $g(t)$. Также возможно реализовать для расширения спектра ТСК медленную ППРЧ по Δ (рис. 1 (д)). В этом случае на одной поднесущей частоте передается определенное количество Δ, например, три.

Вывод. Использование ТСК совместно с методами ППРЧ повышает энергетическую и структурную скрытность сигнальных конструкций. Увеличение структурной скрытности ТСК за счет увеличения s снижает помехоустойчивость системы, что необходимо учитывать при выборе параметров сигнальной конструкции.

Литература

1. Борисов В.И. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты / В.И. Борисов, В.М. Зинчук, А.Е. Лимарев и др.; под ред. В.М. Борисова. – М.: Радио и связь, 2000. – 384 с.

2. Корчинский В.В. Конфиденциальная система связи на основе псевдослучайной перестройки рабочей частоты и таймерных сигналов / В.В. Корчинский// Вестник НТУ «ХПИ».–Харьков: ХПИ, 2013.–№ 16(989).–С.82-85.

3. Корчинский В.В. Повышение скрытности передачи на основе псевдослучайной перестройки рабочей частоты и таймерных сигналов / В.В. Корчинский // Вестник НТУ «ХПИ». Харьков: ХПИ, 2012.– № 66 (972).– С.63-67.

4. Захарченко Н.В. Оценка информационной скрытности таймерных сигнальных конструкций в системах передачи конфиденциальной информации / Н.В. Захарченко, В.В. Корчинский, Б. К. Радзимовский // Збірник наукових праць ОНАЗ ім.О.С.Попова. – 2011. – № 1. – С. 3–8.

УДК 004.056

Корчинский В.В.
ОНАС им. Попова А.С.
vladkorchin@ukr.net
Кильдишев В.Й.
ОНАС им. Попова А.С.
kildishev@ukr.net,
Осадчук Е.А.
ОНАС им. Попова А.С.
osadchuk.katya25@gmail.com
Русаловская А.А.
ОНАС им. Попова А.С.
rusalovskaya.alena@gmail.com

ПОВЫШЕНИЕ ЗАЩИЩЁННОСТИ ПЕРЕДАЧИ ИНФОРМАЦИИ НА ОСНОВЕ ТАЙМЕРНЫХ СИГНАЛЬНЫХ КОНСТРУКЦИЙИ ТЕХНОЛОГИИ OFDM

Аннотация. *В работе рассмотрен метод повышения защищённости системы связи на основе непозиционных сигналов и принципов ортогонализации передачи технологии OFDM. В качестве источников непозиционных сигналов предложено использовать таймерные сигнальные конструкции. С учетом требований основных показателей помехоустойчивости и скрытности определены граничные значения параметров мультиплексирования импульсов таймерных сигнальных конструкций для систем связи с OFDM.*

Технология OFDM (Orthogonal Frequency Division Multiplex) используется во многих стандартах передачи данных, как в проводных каналах – ассиметричная цифровая абонентская линия (ADSL), так и в беспроводных сетях – стандарты IEEE 802.11a и HiperLAN/2. Распространенность этой технологии поясняется следующими достоинствами: высокая спектральная эффективность, устойчивость к радиочастотной интерференции, низкий уровень многолучевых искажений [1, 2].

Принцип формирования сигнальных конструкций при OFDM заключается в мультиплексировании некоторого числа широкополосных сигналов с ортогональным

уплотнением и одновременной передачей их на разных поднесущих частотах с использованием модуляции КАМ. Частичное перекрытие подканалов за счет использования ортогональных поднесущих частот с достаточным их разносом позволяет обеспечить спектральную эффективность метода и минимизировать межсимвольную интерференцию. Характерно, что данный метод расширения спектра разработан для разрядно-цифровых кодов (РЦК), поэтому алгоритмически несовместим с непозиционными сигнальными конструкциями, примером которых являются ТСК [1, 2].

Теория таймерного кодирования [3] предложена в 80-е годы прошлого столетия. Применение в системах связи таймерных сигналов позволяет увеличить объем передаваемой информации в бинарном канале на ограниченном интервале найквистовых элементов. Также были разработаны алгоритмы контроля верности принимаемых сигнальных конструкций, в которых дополнительные проверочные элементы не требуются. В работах [4, 5] показано, что за счет ТСК повышается структурная и информационная скрытность передачи по сравнению с РЦК. Объясняется это большими вариационными возможностями по синтезу различных ансамблей ТСК при незначительном изменении параметров их построения. По этой причине актуально внедрение ТСК в перспективные технологии передачи данных. Целью работы является разработка алгоритма расширения спектра ТСК на основе принципов технологии OFDM.

Рассмотрим особенности построения различных ансамблей ТСК и оценим возможности таймерного кодирования по защите данных от случайных помех и несанкционированного доступа. Как правило, для построения сигнальных конструкций выбирается интервал времени $T_{\text{с}} = nt_0$, состоящий из n найквистовых элементов с длительностью t_0. В ТСК моменты модуляции в отличие от позиционных кодов кратны не t_0, а базовому временному интервалу Δ (где $\Delta = t_0/s$; $s = 1, 2, 3, ..., l$ – целые числа). Таким образом, ТСК содержит импульсы с длительностями $t_{\text{с}} = t_0 + k\Delta$ (где $k = 0, 1, 2, ..., s\cdot(n-2)$). Энергетическое расстояние между сигнальными конструкциями определяется величиной $\Delta < t_0$, поэтому число их реализаций $N_{\text{р}}$ на интервале $T_{\text{с}}$ значительно больше по сравнению с РЦК

$$N_{\text{р}} = \sum_{i=1}^{n} \frac{[(n\cdot s)-[(s-1)\cdot i]]!}{i!\cdot[[(n\cdot s)-[(s-1)\cdot i]]-i]!}, \qquad (1)$$

где i – число информационных моментов модуляции. На рис. 1 представлен пример построения трех ТСК на интервале $T_{\text{с}} = 4t_0$, $t_{\text{с}} = 4\Delta$

Для задачи обнаружения и/или исправления ошибок множество $N_{\text{р}}$ делится на подмножество разрешенных и неразрешенных сигнальных конструкций. Для этой задачи используются уравнение качества [3]:

$$\sum_{k=1}^{i} A_k x_k \equiv 0 \bmod A_0 \,. \qquad (2)$$

В уравнении (2) необходимо найти зависимость весовых коэффициентов $A_k(k = 1, i)$ и модуля A_0. Также на основе уравнения (2) реализуется декодирующее устройство. Изменение хотя бы одного значения из набора параметров n, s и i позволяет сформировать новый ансамбль сигнальных конструкций. На рис. 2. показано изменение ансамбля реализаций ТСК $N_{\text{р тск}}$ в зависимости от n, s и i. Данное свойство можно использовать в алгоритмах повышения структурной и информационной скрытности передачи в системах связи с ТСК [4].

В OFDM высокоскоростной поток позиционных элементов t_0 преобразуется в N параллельных битовых потоков с уменьшением скорости в это же число раз. Каждый из потоков передается своей отдельной поднесущей ортогональной частотой с последующей модуляцией, например, КАМ. Таким образом, общая скорость передачи данных остается неизменной.

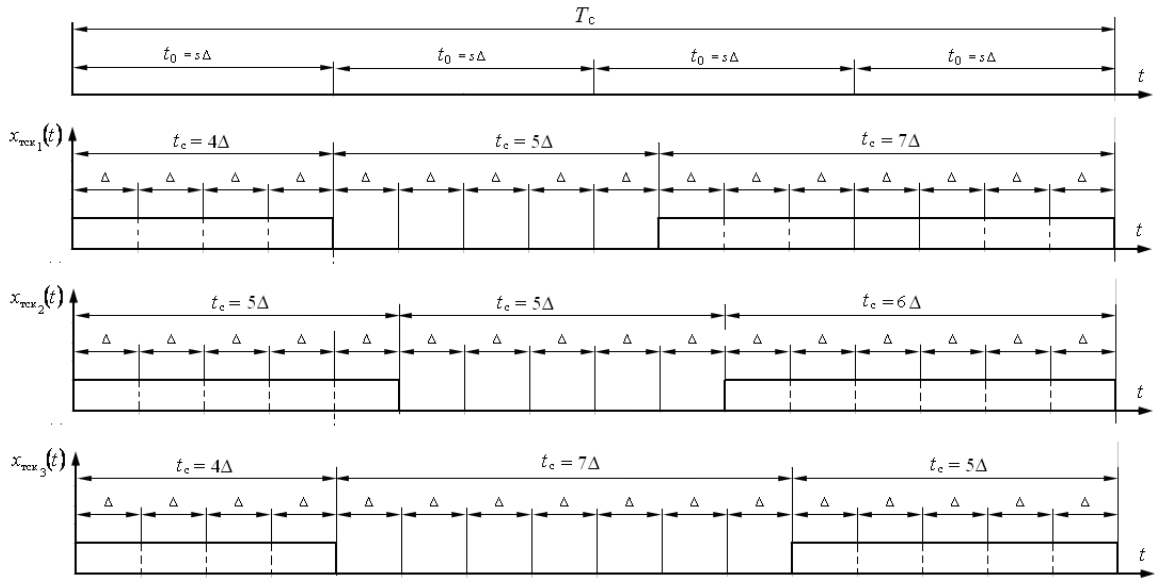


Рис. 1. Построение трех сигнальных реализаций ТСК $x_{\text{ТСК}i}$
на интервале времени $T_c = 4t_0$

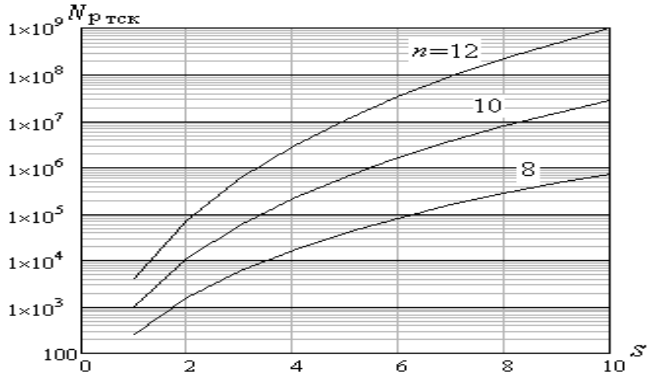


Рис. 2. Реализации ТСК в зависимости от s при значениях n=8, 10, 12

В предложенном алгоритме мультиплексирование таймерных сигналов осуществляется с учётом особенностей их построения и параметров n, s и i. На рис. 3 (а) представлены две сигнальные конструкции ТСК-1 и ТСК-2 с параметрами: $n = 4$; $s = 4$; $i = 2$. Процесс преобразования сводится в мультиплексировании импульсов t_{ci} таймерных сигналов на интервале $T_м = zT_c$ (где $z = 2$ – количество мультиплексируемых ТСК) с увеличением их длительности в $L = 2z$ раз.

На рис. 3 (б) и (в) показан процесс удлинения импульсов таймерных сигналов t_{c1}, t_{c2}, t_{c3} в $L = 4$ раз при их мультиплексировании на интервале времени $T_м = 2T_c$. В силу неэквидистантности импульсов t_{c1}^*, t_{c2}^*, t_{c3}^* получаемые защитные интервалы будут иметь различную длительность. Для импульсов ТСК-1: $T_{ЗИ1} = 16\Delta$, $T_{ЗИ2} = 12\Delta$, $T_{ЗИ3} = 4\Delta$. Очевидно, что увеличение числа мультиплексируемых каналов повышает помехоустойчивость передачи. Для $z = 2$ и $s = 4$ совместное использование ТСК с OFDM позволило уменьшить число ортогональных поднесущих частот по сравнению с РЦК. Сложная структура таймерных сигналов и особенности их мультиплексирования повышают структурную скрытность сигнальных конструкций, что усложняет несанкционированный доступ к конфиденциальной информации.

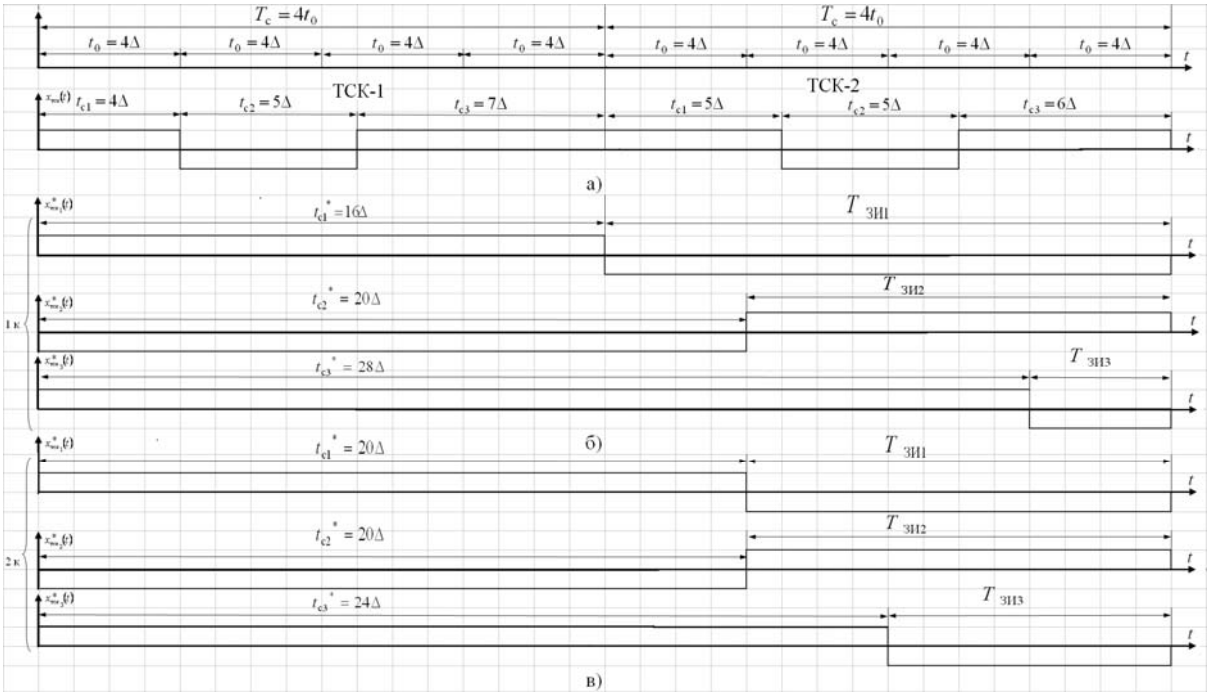


Рис. 3. Мультиплексирование импульсов двух ТСК

Вывод. Предложенный метод мультиплексирования непозиционных таймерных сигналов с последующей их ортогонализацией и модуляцией КАМ позволяет: повысить структурную скрытность сигнальных конструкций; увеличить объём передаваемых данных по сравнению с РЦК; уменьшить количество используемых поднесущих частот.

Литература

1. Тихвинский В.О. Сети мобильной связи LTE. Технологии и архитектура / В.О. Тихвинский. – М.: Эко-Трендз, 2010. – 128 с.

2. Шахнович И.В. Современные технологии беспроводной связи / И.В. Шахнович. – М.: Техносфера, 2004. – 187 с.

3. Захарченко М. В. Системи передавання даних. Том 1. Завадостійке кодування / Захарченко М. В. – Одеса: Фенікс, 2009. – 447 с.

4. Захарченко Н. В. Оценка информационной скрытности таймерных сигнальных конструкций в системах передачи конфиденциальной информации / Н. В. Захарченко, В. В. Корчинский, Б. К. Радзимовский // Збірник наукових праць ОНАЗ ім.О.С.Попова. – 2011. – № 1. – С. 3–8.

5. Корчинский В.В. Повышение скрытности передачи на основе псевдослучайной перестройки рабочей частоты и таймерных сигналов / В.В. Корчинский // Вестник НТУ «ХПИ». Харьков: ХПИ, 2012.– № 66 (972).– С.63-67.

УДК 621.396: 621.395: 007.681 (043.2)

Котелянець В.В., здобувач
Центральноукраїнський національний технічний університет, м. Кропивницький
Науковий керівник – Смірнов О.А., д.т.н., проф.
kotelyanec@ukr.net

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В СЕНСОРНИХ МЕРЕЖАХ

Анотація. *В даній роботі проаналізовані перспективи розвитку сучасних без проводових сенсорних мереж. При цьому були визначені проблемні місця систем захисту та розглянуто різні типи атак на будь-які сенсорні мережі. Основні цілі забезпечення інфор-*

маційної безпеки в безпроводових сенсорних мережах можна умовно розділити на першочергові (забезпечення конфіденційності, цілісності, аутентифікації і доступності даних) і другорядні (свіжість даних, самоорганізація, часова синхронізація, захищена локалізація). Для кожної із цілей доцільно розробити заходи із забезпечення інформаційної безпеки.

Безпроводові сенсорні мережі стають об'єктом жвавих досліджень, що включають апаратну і програмну архітектуру, мережеві технології та з'єднання, розподілені алгоритми, програмні моделі, управління даними, безпеку і т.д. В загальному розумінні сенсорна мережа – це безліч маленьких зчитувальних пристроїв (датчиків). Вони здатні реєструвати зміни різних параметрів навколишнього середовища і транслювати ці параметри іншим подібним пристроям, що знаходяться в зоні досяжності, з певною метою, наприклад: відеоспостереження, моніторинг навколишнього середовища тощо.

Серед основних цілей використання сенсорних мереж можна виділити наступні.

1) Системи безпеки – контроль периметрів, визначення вторгнення, віддалене спостереження; моніторинг персоналу, охорона цінностей та творів мистецтва, домашні системи безпеки, системи пожежної сигналізації.

2) Системи моніторингу і контролю навколишнього середовища (вологість, температура, склад повітря / ґрунту / води, тиск, магнітний фон); моніторинг забруднення навколишнього середовища, міграція тварин, комах.

3) Системи електроенергії – управління енергопостачанням; контроль кондиціонування, вентиляції, опалення, освітлення; ретранслятори для лічильників газу, води, електроенергії.

4) Надзвичайні ситуації – оповіщення про стихійні лиха: лісові пожежі, зсуви і т. п;. порятунок людей при надзвичайних ситуаціях.

Тому, як бачимо, досить часто сенсорні мережі можуть розгортатися в агресивних несприятливих середовищах, де можуть бути зроблені навмисні спроби впливу на їх роботу. Яскравим прикладом може служити їх застосування в зоні бойових дій, де таємність переданих даних і розташування, а також стійкість до спроб компрометації даних і знищення мережі мають ключове значення.

Це дозволяє сформувати мету дослідження, яка полягає в аналізі та систематизації загроз у сенсорних мережах; визначенні механізмів захисту від них.

В загальному випадку кожний пристрій оснащений мікроконтролером, прийомопередавачем, елементом живлення і набором датчиків для вимірювання деяких параметрів навколишнього середовища, наприклад, температури, освітленості, вібрації, тиску, рівня шуму та інших (рис. 1) [1].

Інтелектуальні вузли такої мережі здатні ретранслювати повідомлення один від одного по черзі, забезпечуючи значну площу покриття системи при малій потужності передавачів. За рахунок цього досягається висока енергетична ефективність системи. Нижче розглянемо протоколи, які використовуються в сучасних сенсорних мережах.

Атаки на безпроводові сенсорні мережі. Більшість загроз інформаційній безпеці в безпроводових мережах схожі з загрозами і атаками на проводові мережі, за винятком того, що безпроводові мережі важче захистити внаслідок використання відкритого середовища в якості носія даних і широкомовної природи безпроводових з'єднань. Нижче розглянемо основні мережеві атаки в БСМ.

Пасивні атаки. Аналіз трафіку і прослуховування комунікаційного каналу неавторизованими особами класифікується як пасивна атака. Атаки, націлені виключно на отримання даних, що передаються є пасивними по своїй натурі. Найбільш частими є наступні види атак, спрямовані на порушення конфіденційності даних:

Моніторинг і прослуховування. Даний вид атаки зустрічається найбільш часто. За допомогою підслуховування зловмисник може з легкістю отримати доступ до даних, що передаються. При передачі контрольної інформації про конфігурацію мережі, дана техніка може становити найбільшу небезпеку для конфіденційності даних.

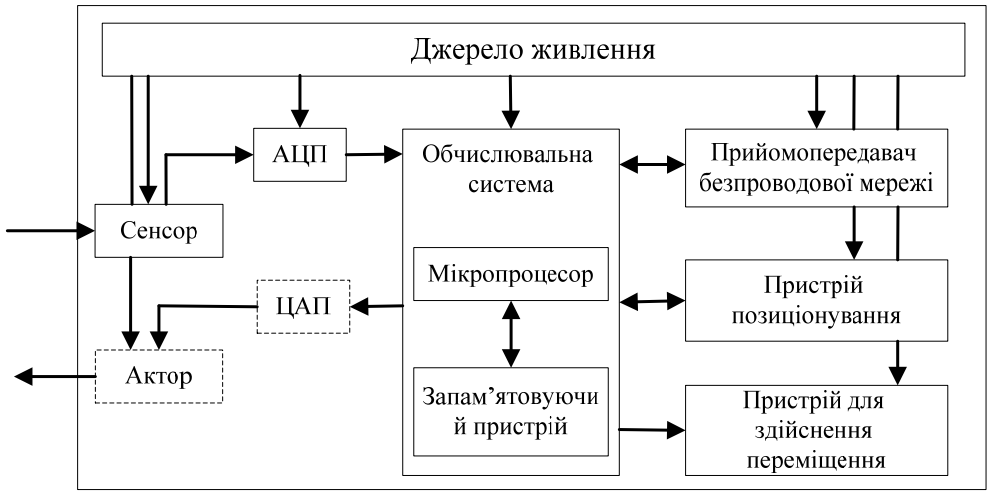


Рис. 1. Архітектура типового сенсорного вузла

Аналіз трафіку. Навіть коли інформація передається в зашифрованому вигляді, залишається ймовірність використання зловмисником техніки аналізу комунікаційних патернів. Активність сенсорів потенційно може розкрити досить інформації для нанесення зловмисником шкоди сенсорній мережі.

Активні атаки. Різні модифікації даних під час комунікації, що здійснюються авторизованими особами, класифікуються як активні атаки. Нижче надведено характеристики активних атак.

Атаки маршрутизації. Атаки, які здійснюються на мережевому рівні (network layer) моделі OSI називаються атаками маршрутизації. Наступні атаки маршрутизації зустрічаються найбільш часто:

Змінена маршрутна інформація. До впливу даної атаки найбільш схильні децентралізовані мережі, де кожен вузол є маршрутизатором і відповідно може змінювати маршрутну інформацію. Внаслідок даної атаки може відбуватися створення кільцевого маршруту, збільшуватися час доставки пакету даних до точки призначення і т. д.

Вибіркова розсилка. Скомпрометований вузол сенсорної мережі може вибірково видаляти певні пакети. Особливо ефективною дана атака може бути в комбінації з атаками, які збирають велику кількість трафіку на даному вузлі мережі. В результаті даної атаки серйозно страждає цілісність і доступність даних, що може істотно знизити рівень якості надання сервісу сенсорною мережею [2, С. 299].

Атака Воронки (Sinkhole Attack). Дана атака характерна тим, що скомпрометований вузол мережі починає діяти по типу воронки, збираючи весь трафік сенсорної мережі [3, С. 681]. Особливо в мережах з протоколом маршрутизації, заснованому на широкомовній розсилці, зловмисник прослуховує запити на маршрутну інформацію і відповідає сенсорним вузлам, що «знає» найкоротший маршрут до базової станції. Як тільки скомпрометованому вузлу вдалося стати між транслюючим сенсорним вузлом і базовою станцією, він може виконувати будь-які дії з пакетам даних, що надходили.

Атака Sybil attack. Під час даної атаки один скомпрометований вузол може використовувати кілька псевдо ідентифікаторів, видаючи себе відразу за кілька вузлів. Подібні атаки використовуються для порушення механізму розподіленого зберігання, механізмів маршрутизації, механізмів агрегації даних, механізмів голосування в мережі і т. д. По суті будь-яка мережа з рівноправними вузлами (особливо безпроводові і децентралізовані мережі) є схильними до даної атаки.

Атака Wormhole attack. Дана атака передбачає створення спеціального шляху між двома і більше скомпрометованими вузлами сенсорної мережі для передачі по ним перехоплених пакетів, доступних тільки для атакуючої системи [4, С. 1976]. Подібні атаки

представляють серйозну загрозу безпеці сенсорної мережі тому, що не вимагають компрометації вузла сенсорної мережі. Тоді, коли вузол В (базова станція або звичайний вузол) використовує трансляцію розсилки для запиту маршруту, зловмисник отримує даний запит і перенаправляє його до найближчого сусіда. Будь-який вузол, який отримав подібний перенаправлений запит розглядає себе як вузол, що знаходиться в зоні досяжності вузла В і запам'ятовує вузол В, як свого «батька». Навіть, якщо цей вузол знаходиться на великій відстані від вузла В і його відокремлюють від вузла В безліч сенсорних вузлів, він буде розглядати вузол В як найближчий від себе.

Флуд атака (HELLO flood attack). Дана атака є широкомовною атакою, яка служить для того, щоб передати в сенсорну мережу масу необов'язкових повідомлень, які повинні позбавити мережу різноманітних ресурсів – канальної ємності, обчислювальної потужності, енергетичних ресурсів і т. д. Під час подібної атаки зловмисник за допомогою високочастотного радіопередавача з достатньою обчислювальною потужністю розсилає Hello пакети безлічі вузлів сенсорної мережі. Вузли, які отримали Hello пакети, розглядають скомпрометований вузол як свого сусіда. Під час наступної передачі даних, вони будуть використовувати отриману адресу з Hello пакетів для відправки. Таким чином, зловмисник отримає доступ до даних.

Відмова в обслуговуванні. Даний вид атаки може бути результатом умисного виведення з ладу вузлів сенсорної мережі або ж результатом дій зловмисників. Найпростіша атака такого роду спрямована на витрату всіх ресурсів, доступних скомпрометованому вузлу за допомогою відправки непотрібних пакетів даних, таким чином перешкоджаючи легітимним користувачам мережі отримувати призначені їм сервіси і ресурси [5, С. 27]. Дана атака означає не тільки спроби зловмисника зруйнувати мережу або розірвати з'єднання, але і будь-яку подія, що знижує здатність мережі надавати певні послуги і ресурси. Безліч типів подібних атак може бути здійснено на різних рівнях моделі OSI, які до цього були розглянуті.

Захоплення вузла (node subversion). Захоплення вузла зловмисником може спричинити розкриття важливої інформації, наприклад, криптографічних ключів, що в свою чергу може спричинити компрометацію всієї сенсорної мережі [6, С. 6].

Несправність вузла (malfunction). Несправний в результаті атаки вузол генерує невірні дані, що може порушити цілісність сенсорної мережі, особливо, якщо несправний вузол є вузлом, який агрегує дані, наприклад, головним вузлом кластера [6, С. 6].

Простій вузла / вихід з ладу. Простій вузла або його вихід з ладу трапляється тоді, коли вузол перестає функціонувати. У разі виходу з ладу головного вузла кластера, протокол сенсорної мережі повинен бути здатним надати альтернативний маршрут для доставки пакетів даних.

Фізичні атаки. Вузли сенсорної мережі часто встановлюються в середовищах із зовнішніми впливами. В таких середовищах маленький форм-фактор вузлів сенсорної мережі в поєднанні з відсутністю постійного нагляду за ними робить їх схильними до різних фізичних атак. На відміну від інших видів атак, фізичні атаки руйнують сенсори незворотньо.

Спотворення повідомлення. Будь-яка зміна контенту повідомлення зловмисником неминуче компрометує цілісність даних, що передаються [7, С. 40].

Хибний вузол. Даний вид атак передбачає впровадження в мережу вузла, який надсилає вузлам сенсорної мережі некоректні дані. Дана атака є однією з найбільш небезпечних атак, оскільки вузол, який поширює зловмисний код, може привести до зупинки всієї сенсорної мережі [7, С. 40].

Копіювання вузла мережі. Концептуально дана атака полягає в наступному: зловмисник намагається додати заздалегідь підготовлені вузли в існуючу сенсорну мережу, використовуючи ідентифікатори вже існуючих вузлів в ній. Для цього зловмисник фізично захоплює один вузол мережі з метою отримання його унікальних даних. Отримані дані згодом використовуються для конфігурації заздалегідь підготовлених вузлів, які згодом

стають клонами захопленого вузла. За допомогою впровадження реплікованих вузлів в певні точки мережевої топології зловмисник може з легкістю управляти сегментом мережі.

Висновки. У даній роботі було проаналізовано протоколи, які використовуються в сенсорних мережах та визначено їх недоліки з точки зору забезпечення інформаційної безпеки; систематизовано можливі типи атак на сенсорні мережі та запропоновані механізми забезпечення безпеки в сенсорних мережах, що дозволяють значно мінімізувати загрози інформаційній безпеці в БСМ.

Майбутні дослідження мають на меті встановлення недоліків БСМ з точки зору забезпечення конфіденційності цілісності та доступності в концепції e-Health.

Література

1. Dunkels, A. Distributed TCP caching for wireless sensor networks / A. Dunkels, J.Alonso , T.Voigt , and H.Ritter // In Proceedings of the 3rd AnnualMediterranean Ad Hoc Networking Workshop (MedHoc-Net). - 2004.

2. Chris Karlof, David Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures”, AdHoc Networks (elsevier), Page: 299–302, year 2003.

3. Culpepper B.J., Tseng H.C. Sinkhole intrusion indicators in DSR MANETs // Proc. First International Conference on Broad band Networks. 2004. – Pp. 681–688.

4. Hu Y., C. Perrig, Johnson D.B. Packet leashes: a defense against wormhole attacks in wireless networks // Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies, – Volume 3. – 3 April 2003. – Pp. 1976–1986.

5. Blackert W.J., Gregg D.M., Castner A.K., Kyle E.M., Hom R.L., and Jokerst R.M. Analyzing interaction between distributed denial of service attacks and mitigation technologies // Proc. DARPA Information Survivability Conference and Exposition, – Volume 1. – 24 April, – 2003. – Pp. 26–36.

6. Pathan A.S.K., Hyung-Woo Lee Choong Seon Hong, “Security in wireless sensor networks: issues and challenges” Advanced Communication echnology (ICACT), Page(s):6, year 2006.

7. Zia T., Zomaya A., “Security Issues in Wireless Sensor Networks”, Systems and Networks Communications (ICSNC) Page(s):40–40, year 2006.

УДК 004.056:621.37

Котенко В.М.,
Житомирський військовий інститут ім. С. П. Корольова.
amyr-777@ukr.net

РОЗПІЗНАВАННЯ СИГНАЛІВ ЕЛЕКТРОМАГНІТНОГО ВИПРОМІНЮВАННЯ З PSK МАНІПУЛЯЦІЄЮ

Анотація. *Проведено аналіз існуючих методів та пристроїв розпізнавання виду модуляції фазоманіпульованих радіосигналів з багатократною фазовою маніпуляцією. На основі отриманого виразу для спектра комплексної обвідної фазоманіпульованого сигналу на виході фазового модулятора проведено аналіз його складових залежно від параметрів аналізованого електромагнітного випромінювання. Показана потенційна можливість реалізації одноканального пристрою розпізнавання кратності маніпуляції фазоманіпульованих сигналів.*

Постановка проблеми. Одним з найбільш небезпечних типів загроз є радіотехнічний канал витоку інформації, в основі якого лежить електромагнітне поширення небезпечного сигналу за межі контрольованої зони. Крім того, радіотехнічний канал можуть утворювати навмисно за допомогою закладних пристроїв підслуховування. У ході моніторингу з метою

виявлення сигналів засобів знімання інформації зазвичай вирішують завдання розпізнавання образів. При цьому процес розпізнавання типу сигналу, а за ним і пристрою знімання інформації полягає в порівнянні його ознак з ознаками заздалегідь визначених груп (еталонів) і віднесенні цього сигналу до відповідної групи. В основі розпізнавання типу виявлених сигналів лежить інформація визначення виду модуляції сигналу і вимірювання параметрів його внутрішньої частотно-часової структури.

Найбільш ефективним методом протидії радіотехнічному каналу витоку, а також пристроям підслуховування є постійний радіоконтроль з використанням програмно-апаратних комплексів чи інших засобів виявлення. Для його організації в спеціально обладнаному приміщенні на об'єкті створюють пункт радіоконтролю, до складу якого, як правило, включають один чи кілька програмно-апаратних комплексів, що дозволяє перевіряти усі необхідні приміщення.

У даний час для розпізнавання сигналів розроблені апаратні та програмні методи, які достатньо широко розглянуті в наукових друкованих джерелах, наприклад [1, 3–4]. В основі апаратних методів розпізнавання лежить операція перетворення вхідних ознак модуляції спеціальними пристроями-демодуляторами. При цьому базовим є кореляційний метод.

На теперішній час для передачі повідомлень використовують сигнали з багатократною фазовою маніпуляцією, що дозволяє значною мірою збільшити ефективність використання таких систем передачі інформації, покращити перепускну здатність каналів зв'язку. До недавнього часу найбільш широко використовували дво- та чотирикратну маніпуляцію, але швидкий розвиток цифрових ліній зв'язку дозволив збільшити кратність маніпуляцій до восьми, шістнадцяти і навіть тридцяти двох. Знаючи, з якою кратністю фазової модуляції передають інформацію в системах зв'язку, можна розробляти апаратні та програмні комплекси для демодуляції каналів зв'язку, що спостерігають, для їх моніторингу.

Огляд останніх досліджень і публікацій. Сигнали з фазовою маніпуляцією є коливаннями, які складаються із N елементарних радіоімпульсів однакової амплітуди U_c, довжини τ_c і частоти ω_c, примикаючи один до одного, причому фаза радіоімпульсів може приймати одне із можливих значень $\varphi_1,...,\varphi_N$ відносно фази першого імпульсу або деякої опорної гармоніки тієї ж частоти.

Якщо на одній несучій частоті дискретну інформацію передають від одного джерела інформації, то використовують однократну фазову маніпуляцію ($\varphi_k = 0,\ \pi$).

У загальному випадку на одній несучій частоті одночасно можна передати повідомлення від n джерел, використовуючи для цього n-кратну фазову маніпуляцію.

Для визначення виду модуляції сигналів, а також для розпізнавання кратності фазової маніпуляції сигналів з багатократною фазовою маніпуляцією запропоновані методи та пристрої, в роботу яких покладений принцип подвоєння несучої частоти з подальшим порівнянням ширини спектра прийнятого сигналу та перетвореного сигналу на подвоєній частоті [1,3]. Як правило, одноканальні пристрої дають можливість розпізнавати фазоманіпульовані сигнали з однократною фазовою маніпуляцією. Для розпізнавання фазоманіпульованих сигналів з багатократною фазовою маніпуляцією пропонується використовувати багатоканальні пристрої, у яких у першому каналі частота прийнятого сигналу помножується на два, у другому – на чотири, а в третьому – на вісім і т. д. [1].

До недоліків відомих пристроїв слід віднести багатоканальність та складність у технічній реалізації помножувачів частоти. Пропонується застосувати як помножувач частоти одноканальний фазовий модулятор, робота якого ґрунтується на теорії фазової модуляції гармонічного коливання високої частоти фазоманіпульованим сигналом проміжної частоти [2].

Формулювання завдання дослідження. Провести дослідження частотного спектра комплексної обвідної вихідного сигналу фазового модулятора при модуляції вхідного гармонічного коливання високої частоти фазоманіпульованим сигналом проміжної частоти

та розробити пропозиції щодо побудови одноканального пристрою розпізнавання кратності фазової маніпуляції.

Спектр комплексної обвідної вихідного сигналу фазового модулятора. На вхід фазового модулятора подамо гармонічне коливання надвисокої частоти одиничної амплітуди вигляду

$$U_{вх}(t) = \exp\, j(2\pi f_0 t + \varphi_0), \tag{1}$$

де f_0, φ_0 – відповідно частота і початкова фаза високочастотного сигналу, а на модулюючий вхід подамо фазоманіпульований сигнал одиничної амплітуди

$$U_M(t) = U_M \sum_{n=1}^{N} \sin(2\pi f_M (t - t_n) + \theta_n + \varphi_M), \tag{2}$$

де U_M, f_M, θ_n, φ_M – амплітуда, частота, початкова фаза дискрети фазоманіпульованого сигналу та початкова фаза фазоманіпульованого сигналу відповідно;

$t_n = (n-1)\tau_0$ – затримка в часі фазоманіпульованого сигналу на тривалість дискрети τ_0;

N – кількість дискрет фазоманіпульованого сигналу.

При взаємодії вхідного і модулюючого коливання у фазовому модуляторі (рис. 1) на його виході сформується фазоманіпульований сигнал:

$$U_{вих}(t) = \exp\, j(2\pi f_0 t + \varphi_0) \sum_{n=1}^{N} \exp\, j(M_\varphi \sin(2\pi f_M (t - t_n) + \theta_n + \varphi_M), \tag{3}$$

де $M_\varphi = S_\varphi U_M$ – індекс фазової модуляції; $S_\varphi = \Delta u / \Delta\varphi$ – крутизна фазової модуляційної характеристики.

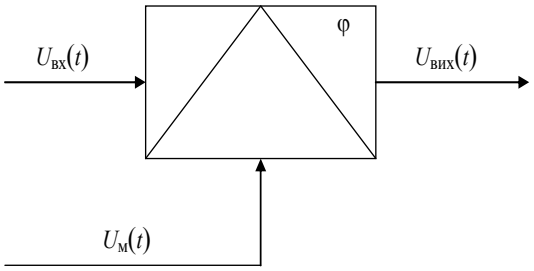


Рис. 1. Структурна схема фазового модулятора

В [3] показано, що спектр комплексної обвідної фазоманіпульованого сигналу можна записати у вигляді:

$$\begin{aligned} \dot{G}(f) &= \tau_i I_0(M_\varphi)\sin c(\pi f \tau_i) + \\ &+ \tau_i \sum_{m=1}^{M} I_m(M_\varphi)\sin c(\pi(mf_M - f)\tau_i)\times \\ &\times \sum_{n=1}^{N} \exp - j(2\pi m f_M (n-1)\tau_0 - m\theta_n) + \\ &+ \tau_i \sum_{m=1}^{M} (-1)^m I_m(M_\varphi)\sin c(\pi(mf_M - f)\tau_i)\times \\ &\times \sum_{n=1}^{N} \exp - j(2\pi m f_M (n-1)\tau_0 - m\theta_n). \end{aligned} \tag{4}$$

Аналіз виразу (4) показує:

амплітудно-частотний спектр (АЧС) симетричний;

центральна складова АЧС розташована на частоті f_0 і являє собою функцію $\sin c(x)$;

бокові спектральні складові розташовані на відстані від центральної на величину $N\ f_M$;

ширина спектра парних складових визначається величиною τ_i і обернено пропорційна тривалості імпульсу, оскільки $2*0=2*\pi=0$;

ширина спектра непарних складових визначається величиною τ_0 і обернено пропорційна їй.

Аналіз спектра комплексної обвідної вихідного сигналу фазового модулятора. На рис. 2 наведено графіки розрахунків модуля спектра комплексної обвідної фазоманіпульованого сигналу з однократною фазовою маніпуляцією для параметрів: $\theta_n \in [\pi,\pi,\pi,0,0,\pi,0]$.

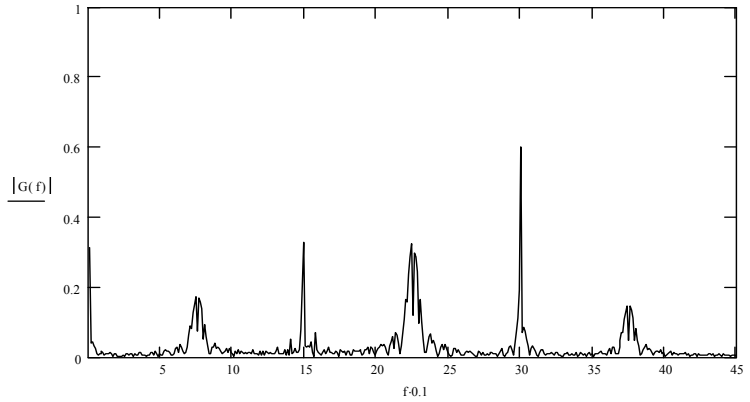


Рис. 2. Модуль спектра комплексної обвідної фазоманіпульованого сигналу з однократною фазовою маніпуляцією

На рис. 3 наведено графіки розрахунків модуля спектра комплексної обвідної багаточастотного фазоманіпульованого сигналу з двократною фазовою маніпуляцією при законні зміни початкової фази дискрет фазоманіпульованого сигналу $\theta_n \in [\pi/2,\pi,\pi/2,\pi,\pi/2,\pi,3\pi/2,0,3\pi/2,0,\pi/2,\pi,3\pi/2,0]$.

Аналіз спектра комплексної обвідної фазоманіпульованого сигналу, наведеного на рис. 2, показує, що фазова маніпуляція при законі маніпуляції $0,\pi$ зникає в другій, четвертій та шостій складових спектра фазоманіпульованого сигналу на виході фазового модулятора, тобто в кожній парній складовій спектра.

Аналіз спектра комплексної обвідної фазоманіпульованого сигналу з двократною фазовою маніпуляцією, наведеного на рис. 3, показує, що нульова та четверта складові спектра багаточастотного фазоманіпульованого сигналу прндставляють функцію виду *sinc x.*

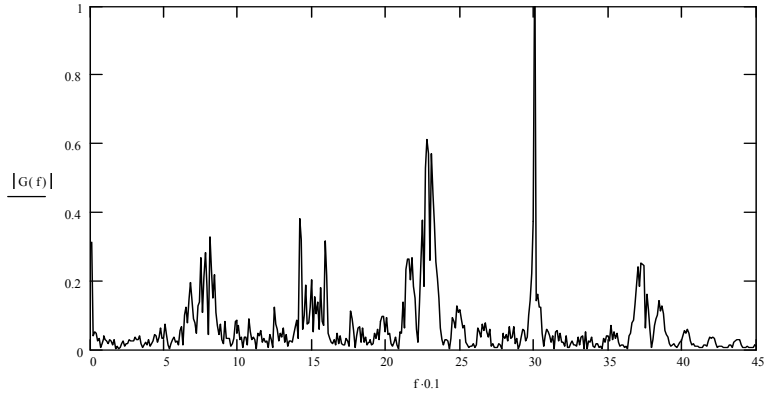


Рис. 3. Модуль спектра комплексної обвідної фазоманіпульованого сигналу з двократною фазовою маніпуляцією

Нескладно математично показати, що якщо для передачі буде застосовуватись восьмикратна фазова маніпуляція, то згортка спектра проводитиметься у восьмій боковій складовій спектра комплексної обвідної фазоманіпульованого сигналу.

Висновки. Проведений аналіз розрахованих спектрів комплексних обвідних фазоманіпульованих сигналів показав, що для різних законів фазової маніпуляції є суттєві відмінності в спектральній структурі сигналів, які можна використати для розпізнавання кратності фазової маніпуляції PSK маніпульованих сигналів. При цьму для технічної реалізації процесу розпізнавання використовується одноканальний пристрій.

Література

1. Пошук та локалізація радіо закладних пристроїв : навч. посіб. / В. О. Хорошко, О. Д. Азаров, Г. О. Максименко, Ю. Є. Яремчук. – Вінниця : ВНТУ, 2007. – 333 с.

2. Теория и техника генерирования, излучения и приема радиолокационных сигналов : учеб. для слушателей академии / Н. Г. Батурин, В. И. Гомозов, В. Ф. Екимов и др. ; под ред. Ю. Н. Седышева. – Х.: ВИРТА, 1986. – 650 с.

3. Розпізнавання сигналів електромагнітного випромінювання з багатократною фазовою маніпуляцією / В. М. Котенко, В. Д. Меленський // Збірник наукових праць ЖВІНАУ. – 2010. – Випуск 4. – С. 197 – 204.

4. Обнаружение и анализ сигналов сложной структуры : ученик под ред. А. И. Замарина. – М. : МО РФ, 1996. – 522 с.

УДК 004.773.5

Криштафор З. З.,
ОНАЗ ім. О. С. Попова.
zurab929@gmail.com
Науковий керівник:
к. т. н. Басов В. Є.
ОНАЗ ім. О. С. Попова.
basvic@bigmir.net

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ ОРГАНІЗАЦІЇ ЗАХИЩЕНОГО КАНАЛУ ПЕРЕДАЧІ ДАНИХ

***Анотація**. Розглядається проблема захисту інформації при передачі повідомлень каналами передачі даних з використання програмного забезпечення типу «месенджер». Приведено поняття захисту інформації при передачі каналами передачі даних. Розкрито питання актуальності обраної теми. Приведена розроблена теоретична схема взаємодії користувачів програмного забезпечення. Приведені та обрані методи та технології захисту інформації. Розроблено програмне забезпечення із використанням розробленої теоретичної схеми взаємодії користувачів та реалізацією обраних технологій захисту інформації.*

Ключові слова: програмне забезпечення, схема взаємодії, захист інформації, шифрування, хешування, канал передачі даних.

Все більше людей використовують для спілкування програмні забезпечення, які реалізують передачу повідомлень інтернет каналом передачі даних. В наш час актуальним питанням є захист особистої інформації при спілкуванні. З усіх більш популярних програм типу «месенджер», які ще називають «Програми миттєвого обміну повідомленнями», 30% не надають захист інформації методом шифрування повідомлень.

Передача даних – фізичне перенесення даних від точки до точки або від точки до кількох точок засобами електрозв'язку по каналу передачі даних.

Зазвичай під каналом передачі даних розуміються комплекси технічних засобів, задіяних в передачі даних від джерела до приймача, а також середовище між ними.

Мною була розроблена схема взаємодії користувачів програмного забезпечення із посередником у вигляді серверу, який має свій функціонал та базу даних. Також для реалізації захисту інформації я використав хешування та шифрування. Мною був обраних алгоритм хешування MD5 та взаємодія двох алгоритмів шифрування: симетричний алгоритм шифрування ГОСТ 28147-89 із 256-бітним ключем та асиметричний алгоритм шифрування RSA із 1024-бітним ключем.

Нижче представлена розроблена мною схема реалізації взаємодії користувачів при використанні програмного забезпечення із реалізацією захисту інформації.

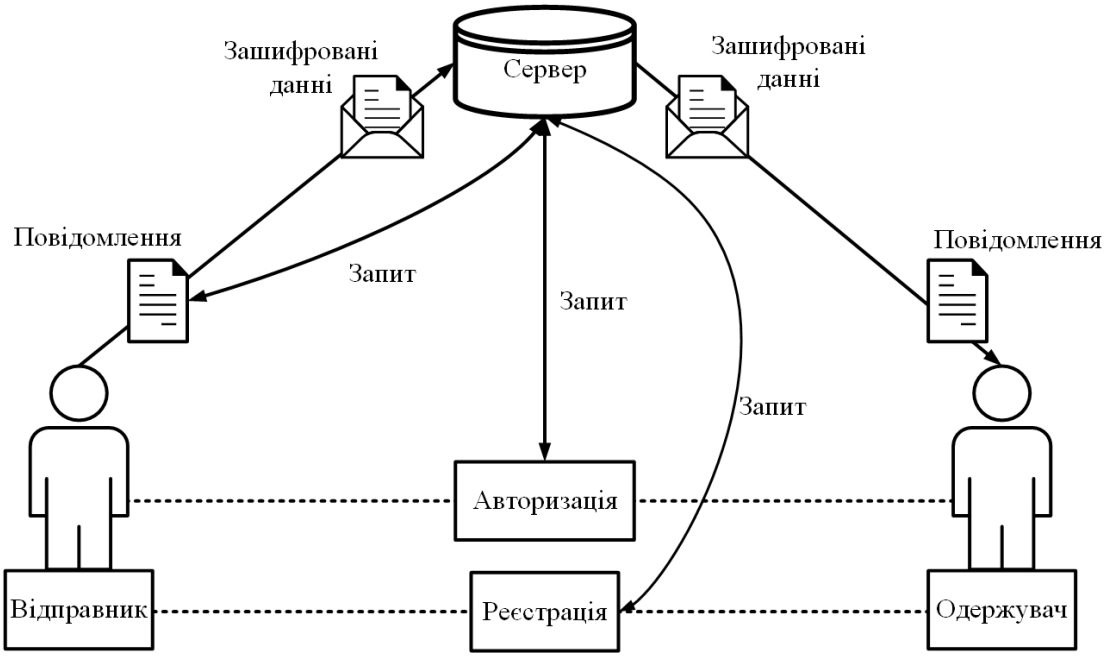


Рис. 1. Схема реалізації взаємодії користувачів із сервером-посередником

Кроки взаємодії:

- Відправник та одержувач реєструються
- Відправник авторизується та обирає співбесідника
- Відправник пише повідомлення та при відправці воно зашифровується на стороні відправника
- Відправлені зашифровані дані зберігаються на сервері
- Одержувач авторизується та вибирає співбесідника
- При виборі сервер надсилає користувачу зашифровані дані
- Зашифровані дані на стороні одержувача розшифровуються

При реєстрації користувач повинен ввести обов’язкові дані, при тому, що логін повинен бути унікальним. При відправці запиту на реєстрацію генерується відкритий та закритий ключі шифрування алгоритму RSA, генерується унікальний ідентифікатор користувача та введений пароль піддається розрахунку його хеш-функції. Усі ці данні зберігаються на сервері. При авторизації користувач вводить логін та пароль. При відправці запиту на авторизацію також розраховується хеш-функція паролю. Логін із розрахованою хеш-функцією передаються на сервер для зрівняння з даними, які знаходяться на сервері. Якщо на сервері є такий обліковий запис з веденим логіном та ідентичною хеш-функцією, то сервер поверне відповідь з дозволом на вхід в обліковий запис.

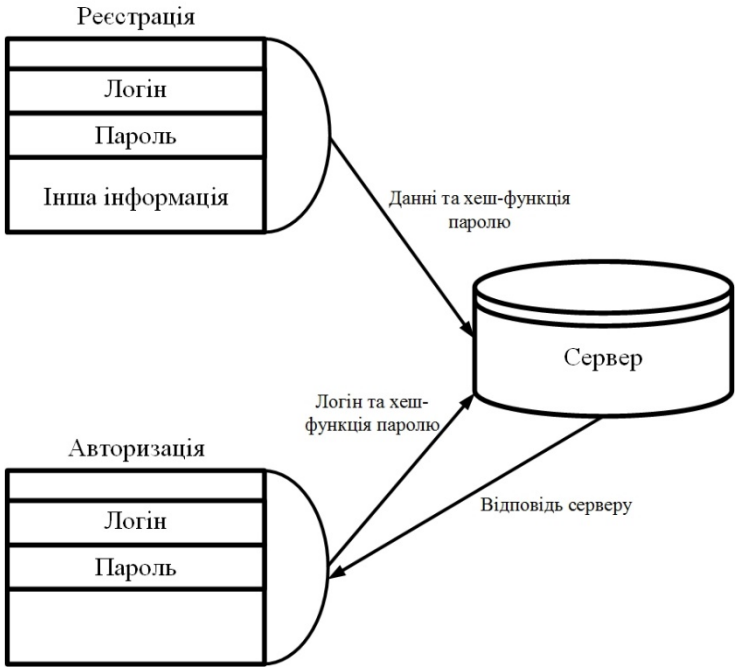


Рис. 2. Схема реалізації реєстрації та авторизації

Після входу в обліковий запис можна обрати співбесідника та написати йому повідомлення. Написане повідомлення, при відправці, піддається шифруванню. Нижче приведена схема реалізаціє алгоритмів шифрування із взаємодією користувачів.

Рис. 3. Схема реалізації алгоритмів шифрування в розробленій схемі взаємодії

При відправці генерується 256-бітний ключ. Повідомлення піддається шифруванню алгоритмом шифрування ГОСТ за допомогою генерованого ключа. При виборі співбесідника ми отримали його відкритий ключ алгоритму RSA. Тепер маючи зашифроване повідомлення та ключ від повідомлення, зашифруємо ключ від повідомлення алгоритмом RSA за допомогою відкритого ключа співбесідника. Таким чином ми маємо зашифроване повідомлення та зашифрований ключ від зашифрованого повідомлення. Повідомлення передається на сервер. Коли одержувач авторизується він отримає зашифровані дані з серверу, але він і тільки він має свій секретний ключ від алгоритму RSA, тому він може

розшифрувати ключ від зашифрованого повідомлення. Розшифрувавши ключ він може розшифрувати повідомлення. Розшифроване повідомлення показується в формі повідомлень.

Взаємодія двох алгоритмів шифрування була використана бо якщо використовувати тільки симетричне шифрування, то перехопивши зашифроване повідомлення за відкритий ключ їх можна використати для зчитування інформації. Якщо ж використовувати тільки асиметричний алгоритм шифрування, то для великих обсягів даних шифрування та розшифрування може зайняти більше часу, ніж якщо шифрувати інформацію симетричним алгоритмом, та зашифровувати ключ від симетричного алгоритму.

Висновки. Було розроблено схему взаємодії користувачів програмного забезпечення та реалізовано захист інформації від несанкціонованого ознайомлення. Було запропоновано та розроблено взаємодію алгоритмів шифрування для кращого захисту інформації. Було розроблене програмне забезпечення, яке реалізує захист інформації, яка циркулює між співбесідниками.

Література

1. Передача інформації. Канали передачі інформації: http://poradi.ru/tehnika-ta-tehnologii/31224-peredacha-informacii-kanali-peredachi-informacii.html

2. Криптография в C#: https://studlearn.com/works/details/primery-kriptografii-na-c-rsa-des-sha1-575.

3. Электронные расчёты:
http://www.e-biblio.ru/book/bib/09_ekonomika/el_raschet_v_kom_deajt/posob/index.htm .,
Авторы: Гамов И.А., Дик В.В., Касаткина С., Михайлов А.С., Павлековская И.В., Печенкин А.Е., Суспицын П.Ю., Уринцов А.И., Устинов И.Г.

УДК 004.056.53::510.254

Мохор В.В.,
ІПМЕ ім. Г.Є. Пухова НАН України.
v.mokhor@gmail.com
Кравцов Г.О.,
ІПМЕ ім. Г.Є. Пухова НАН України.
hryhoriy.kravtsov@gmail.com
Цуркан В.В.,
ІСЗЗІ КПІ ім. Ігоря Сікорського,
v.v.tsurkan@gmail.com

УДОСКОНАЛЕНА МІРА СХОЖОСТІ ДВОХ КЛАСІВ РИЗИКІВ БЕЗПЕКИ ІНФОРМАЦІЇ

Анотація. *Розглянуто обмеження процесу оцінювання ризиків безпеки інформації. Для подолання означеного обмеження запропоновано використання теорії класифікації. Класифікацію ризиків безпеки інформації відображено орієнтованим деревом. Показано, що місце та ранг класу визначається шляхом уточнення. Для двох довільних шляхів уточнення введено відносну відстань між двома класами ризиків безпеки інформації. Встановлено, що використання цієї міри ускладнюється відсутнітю можливості визначення схожості/відмінності двох класів. Тому їх схожість/відмінність визначається як міра Жокара. Використання цієї міри не задовольняє умовам нерівності трикутника. Тому для запобігання цьому запропоновано удосконалену міру схожості/відмінності двох класів ризиків безпеки інформації.*

Інтелектуальність, слабка формалізованість процесу оцінювання ризиків безпеки інформації призводить до його ускладнення [1-3]. Для подолання означеного обмеження запропоновано використання теорії класифікації [4, 5]. Класифікація формально

представляється математичною структурою орієнтованого дерева. Його вершинами відображаються класи ризиків безпеки інформації

$$F_Y^i =< F, i, Y >,$$

де F – плоска класифікація; i – площина поділу класифікації F; Y – шлях уточнення плоскої класифікації F^i.

Місце та ранг класу окремої площини поділу плоскої класифікації F^i ризиків безпеки інформації однозначно визначається шляхом уточнення Y як послідовністю виду, наприклад [4],

$$Y = [a, b, c, ...].$$

Це означає, що для $F_{[a]}$ ранг класу дорівнює одиниці, а $F_{[a,b]}$ – двом.

Нехай $F^i_{[a]}$, $F^i_{[b]}$, $F^i_{[a,b]}$ – класи плоскої класифікації F ризиків безпеки інформації. Тоді відносна відстань R між двома класами $F^i_{[a]}$ і $F^i_{[b]}$ дорівнюватиме числу унікальних операцій уточнення від найближчого спільного узагальнюючого класу F [4]. Наприклад [5], якщо виконуються дві операції уточнення стосовно F

$$F + F^i_{[a]} = F^i_{[a]},$$
$$F + F^i_{[b]} = F^i_{[b]},$$

то

$$R(F^i_{[a]}, F^i_{[b]}) = 2.$$

З огляду на тлумачення відносної відстані R виконуються такі рівності для двох довільних шляхів уточнення Y та I класифікації F ризиків безпеки інформації у площині поділу i

$$\begin{aligned} R(F_Y^i, F_I^i) &= R(F_I^i, F_Y^i), \\ R(F_I^i, F_I^i) &= 0. \end{aligned} \tag{1}$$

При цьому не враховується положення класів $F^i_{[a]}$ і $F^i_{[b]}$ у плоскій класифікації F. Воно єдине та кінцеве завдяки її відображенню орієнтованим деревом. Відносна відстань $R(F_I^i, F_Y^i)$ інваріантна, якщо клас F, що уточнюється класами F_I^i і F_Y^i ризиків безпеки інформації, стає уточнюючою класифікацією. Оскільки структура між двома класами F_I^i і F_Y^i незмінна, то й шлях між ними незмінний [4, 5].

Зв'язок відносної відстані між класами F_I^i і F_Y^i та абсолютними відстанями до цих класів від вершини класифікації F, а також відносної відстані від вершини класифікації F до спільного узагальнюючого класу $F_I^i \cdot F_Y^i$ описується рівністю [4]

$$R(F_I^i, F_Y^i) = R(F, F_I^i) + R(F, F_Y^i) - 2R(F, F_I^i \cdot F_Y^i). \tag{2}$$

Якщо $R(F, F_I^i \cdot F_Y^i) \geq 0$, то (2) може бути узагальнена до такого виду

$$R(F_I^i, F_Y^i) \leq R(F, F_I^i) + R(F, F_Y^i). \tag{3}$$

Завдяки виконанню властивостей симетричності, рефлексивності для рівностей (1) та нерівності трикутника (3), відносна відстань $R(F_I^i, F_Y^i)$ розглядається як міра на класифікації F ризиків безпеки інформації. Однак, використання цієї міри ускладнюється відсутнітю можливості визначення схожості/відмінності двох класів F_I^i і F_Y^i. Тому їх схожість/відмінність визначається як міра Жокара за умови [4-7]

$$O(F_I^i, F_Y^i) = \frac{R(F, F_I^i \cdot F_Y^i) + 1}{R(F, F_I^i \cdot F_Y^i) + R(F_I^i, F_I^i \cdot F_Y^i) + R(F_Y^i, F_I^i \cdot F_Y^i) + 1}.$$

Для зручності ця рівність позначається як $O(F^i)$ і називається мірою схожості на площині поділу класифікації F^i. Однак, ця міра не задовольняє умовам нерівності трикутника (3). Подолання цього обмеження здійснюється використанням рівності

$$\overline{O}(F_I^i, F_Y^i) = 1 - O(F_I^i, F_Y^i).$$

якій властиві симетричність і рефлексивність

$$\overline{O}(F_I^i,\ F_Y^i) = \overline{O}(F_Y^i,\ F_I^i),$$
$$\overline{O}(F_I^i,\ F_I^i) = 0. \tag{4}$$

Тоді

$$\overline{O}(F_I^i,\ F) + \overline{O}(F_Y^i,\ F) \geq \overline{O}(F_I^i,\ F_Y^i). \tag{5}$$

Оскільки (5) є нерівністю трикутника, то з урахуванням (4) $\overline{O}(F_I^i,\ F_I^i)$ є мірою відмінності на класифікації F ризиків безпеки інформації. Якщо обрати два довільних класи, відносна відстань між якими постійна та кінцева, то міра відмінності (5) спадає зі збільшенням відносної відстані від найбільш загальної класифікації до найближчого узагальнюючого класу обраних класів

$$\overline{O}(F_I^i,\ F_Y^i) = 1 - \frac{R(F, F_I^i \cdot F_Y^i) + 1}{R(F, F_I^i \cdot F_Y^i) + C + 1},$$
$$C = R(F_I^i, F_I^i \cdot F_Y^i) + R(F_Y^i, F_I^i \cdot F_Y^i),$$
$$C \geq 0.$$

Як наслідок,

$$\overline{O}(F_I^i,\ F_Y^i) = 1 - \lim_{R(F, F_I^i \cdot F_Y^i) \to \infty} \frac{R(F, F_I^i \cdot F_Y^i) + 1}{R(F, F_I^i \cdot F_Y^i) + C + 1} = 0.$$

Тоді як

$$\overline{O}(F_I^i,\ F_Y^i) = 1 - \lim_{R(F, F_I^i \cdot F_Y^i) \to 0} \lim_{C \to 1} \frac{R(F, F_I^i \cdot F_Y^i) + 1}{R(F, F_I^i \cdot F_Y^i) + C + 1} = \frac{1}{2}.$$

Уточнення класифікації за однією ознакою класифікації на кожному рівні приводить до такої міри відмінності

$$\overline{O}(F_I^i,\ F_Y^i) = 1 - \lim_{R(F, F_I^i \cdot F_Y^i) \to 0} \frac{R(F, F_I^i \cdot F_Y^i) + 1}{R(F, F_I^i \cdot F_Y^i) + C + 1} = \frac{C}{C+1}.$$

Якщо визначені плоскі класифікації $F^1, .., F^i, .., F^N;\ i = \overline{1, N},$ сукупність яких представляє собою класифікацію $F = F^1 \times ... \times F^i \times ... \times F^N$ з мірою відмінності $\overline{O}(F)$, то

$$\overline{O}(F) = \frac{1}{N} \sum_{i=1}^{N} \overline{O}(F^i). \tag{6}$$

Для врахування ваги або ступеня впливу i площини поділу класифікації F^i на міру відмінності (6) отримаємо

$$\overline{O}_K(F) = \frac{1}{NK} \sum_{i=1}^{N} \overline{O}(F^i) p(F^i),$$
$$K = \sum_{i=1}^{N} p(F^i),$$

де $\overline{O}_K(F)$ – нормована міра відмінності на класифікації F ризиків безпеки інформації з визначеним ступенем довіри [4], $p(F^i)$ – вага або ступінь впливу F^i на $\overline{O}_K(F)$.

Таким чином, завдяки використанню теорії класифікації можливе подолання обмежень при оцінюванні ризиків безпеки інформації. Їх класи відображаються вершинами орієнтованого дерева. Місце та ранг кожного з них однозначно визначається шляхом уточнення. Тому відносна відстань між двома класами дорівнює числу унікальних операцій уточнення від найближчого спільного узагальнюючого класу. Завдяки виконанню властивостей симетричності, рефлексивності та нерівності трикутника, відносна відстань розглядається як міра на класифікації ризиків безпеки інформації. Використання цієї міри ускладнюється відсутнітю можливості визначення схожості/відмінності двох класів. Тому для запобігання цьому запропоновано удосконалену міру відмінності двох класів ризиків безпеки інформації.

Література

1. Мохор В.В. Спроба локалізації ISO GUIDE 73:2009 «Risk management – Vocabulary» / В.В. Мохор, О.М. Богданов, О.М. Крук, В.В. Цуркан, // Безпека інформації. – 2012. – Том 18, № 2. – С.12-22.

2. Information technology. Security techniques. Information security risk management : ISO/IEC 27005:2011. – Second edition 2011-06-10. – Geneva, 2011. – 68 p.

3. Керування ризиком. Методи загального оцінювання ризику (IEC 31010:2009, IDT) : ДСТУ IEC 31010:2013. – [Чинний від 2014-07-01]. – К. : Мінекономрозвитку України, 2015. – 73 с. – (Національний стандарт України).

4. Кравцов Г.А. Модель вычислений на классификациях / Г.А. Кравцов // Электронное моделирование. – 2016. – Т. 38, № 1. – С. 73-85.

5. Мохор В.В. Використання теорії класифікації для оцінювання ризику безпеки інформації / В.В. Мохор, Г.О. Кравцов, В.В. Цуркан // Захист інформації і безпека інформаційних систем: матеріали V міжнародної науково-практичної конференції (01-02 червня 2017 року). – Львів : Видавництво Львівської політехніки, 2017. – С. 21-22.

6. Загоруйко Н.Г. Меры сходства, компактности, информативности и однородности обучающей выборки / Н.Г. Загоруйко, И.А. Борисова, В.В. Дюбанов, О.А. Кунтенко // Тр. Всероссийской конф. «Знания – Онтологии – Теории» (ЗОНТ-09). Том 1. – Новосибирск, 2009. – С. 93-102.

7. Елисеева И.И. Группировка, корреляция, распознавание образов. Статистические методы классификации и измерения связей / И.И. Елисеева, В.О. Рукавишников. – М.: Статистика, 1977. – 144 с.

УДК 621.396: 621.395: 007.681 (043.2)

Одарченко Р.С., к.т.н., доцент
Національний авіаційний університет, м. Київ
odarchenko.r.s@ukr.net

ПІДВИЩЕННЯ РІВНЯ КІБЕРБЕЗПЕКИ СУЧАСНИХ СТІЛЬНИКОВИХ МЕРЕЖ В УКРАЇНІ

Анотація.*У даній роботі проаналізовано хронологію розвитку стільникових мереж зв'язку в Україні Також були проаналізовані системи безпеки цих мереж, визначені їх проблемні місця. Зокрема, були розглянуті можливі атаки в мережах LTE, що можуть створити потенційні проблеми в майбутньому. В результаті проведених досліджень стало зрозумілим, що ці мережі відіграватимуть в майбутньому найбільш значущу роль в формуванні електронного суспільства, критичної інфраструктури в Україні тощо. Були сформульовані ключові напрямки удосконалення систем кібербезпеки стільникових мереж, що дозволило обґрунтувати необхідність проведення подальших досліджень, пов'язаних із оптимізацією захисту стільникових мереж в Україні. Це дозволить створити нову більш гнучку масштабовану архітектуру системи безпеки стільникових мереж, що буде в змозі забезпечити всі вимоги різноманітних різнорідних систем, що входять до сфери застосування стільникових мереж 4-го покоління.*

16 червня 1993 року офіційно вважається датою, коли в Україні було запроваджено стільниковий зв'язок [1, 2]. З того часу за період майже в 23 роки інформаційно-комунікаційна інфраструктура в Україні кардинально трансформувалась, дійшовши до сучасного вигляду.Проте в більш розвинутих країнах, зокрема, в США, Європі та країнах Азії вже є доволі багато операторів, які надають послуги за допомогою мереж LTE [3], а вже до 2020 року планується запуск перших мереж 5G у комерційну експлуатацію[4-5].

При цьому кожен користувач будь-якої мережі прагне забезпечити конфіденційність передаваних даних та унеможливити спроби мережевих атак на мобільні пристрої. До того ж набирає популярності концепція Інтернету речей IoT [6], що висуває ще більші вимоги до захисту інформаційної інфраструктури.

Безпека є одним з основних проблемних місць комунікаційної мережі в даний час. Розгортання жодної мережі не може відбутися без забезпечення гарантованої безпеки для всіх зацікавлених сторін, наприклад, кінцевих користувачів, постачальників послуг, віртуальних операторів, провайдерів інфраструктури. Таким чином, метою даної роботи є виявлення недоліків систем захисту мереж попередніх поколінь та формування рекомендацій щодо забезпечення та підвищення рівня кібербезпеки сучасних стільникових мереж в Україні.

В Україні вже анонсовано продаж ліцензій на запровадження мереж четвертого покоління LTE. Орієнтовно з наступного 2018 року вже почнеться будівництво (модернізація існуючих) мереж нового покоління. Тому рівень забезпечення кібербезпеки будемо розглядати саме крізь призму розгортання мереж LTE.

Основні аспекти архітектури безпеки мережі LTE описані в TS 33.401. Відповідно до цієї специфікації, для безпечного обміну даними в мережі LTE необхідне створення надійного з'єднання між призначеним для користувача пристроєм і мережею оператора – PublicLandMobileNetwork. Так само безпечні з'єднання повинні бути створені між призначеним для користувача пристроєм і безпосередньо опорною мережею – IMS CoreNetworkSubsystem, перш ніж користувачеві можуть бути надані будь-які послуги.

Стандарт виділяє п'ять основних груп безпеки [7]:

– Архітектура безпеки мережі повинна забезпечити користувачів надійним доступом до сервісів і забезпечити захист від атак на інтерфейси

– Мережевий рівень дозволяє вузлам мережі безпечно обмінюватися даними, як для користувача, так і керуючими, і забезпечує захист від атак на провідні лінії.

– Користувацький рівень забезпечує безпечний доступ до мобільного пристрою.

– Прикладний рівень дозволяє додаткам безпечно обмінюватися повідомленнями.

– Видимість і можливість змінювати налаштування безпеки дозволяє користувачеві дізнатися, чи забезпечується безпека і включати різні режими.

Модель безпеки (trustmodel) мережі LTE дуже схожа на модель, запропоновану в рамках мереж UMTS. Її можна грубо описати як мережу, що складається з надійної опорної мережі (corenetwork), а також сукупності інтерфейсів між базовими станціями, користувацькими пристроями та опорною мережею, які є вразливими для атак.

Взаємодія базових станцій і опорної мережі ґрунтується на протоколах IPsec і IKE. Сильні криптографічні методи забезпечують захист типу «точка-точка» для з'єднання між опорною мережею і призначеним для користувача пристроєм.

В архітектурі мережі LTE для створення плоскої структури мережі було прийнято рішення відмовитися від контролерів радіомережі – RNC. Проте, оскільки в технології LTE деякий функціонал контролерів інтегрований в базові станції, то рішення, що застосовуються в рамках мереж третього покоління, не можуть бути прямо перекладені на мережі LTE.

Основні рушійні сили розвитку стільникових мереж можуть бути згруповані в чотири основні характеристики,кожна з яких має вплив на формування вимог для забезпечення безпеки і недоторканності приватного життя. Ці характеристики наступні: нові моделі довіри, нові моделі служби доставки, розширений перелік загроз, і збільшення рівня конфіденційності.

Отже, ці характеристики впливають на те, як ми повинні підходити до формування вимог до систем безпеки та конфіденційності в сучасних мережах, в тому числі й в Україні.

Нові моделі довіри.Для сучасних мобільних систем, модель довіри досить проста, і вона включає абонента(і його термінал) і два оператора (домашню і гостьову мережі). Натомість мережі 4G спрямовані на підтримку нових бізнес-моделей і включають в себе нові ролі, а тому моделі довіри мають змінитися, породжуючи розширення вимог у таких областях, як аутентифікація між різними суб'єктами, підзвітність і безвідмовність.

Безпека для нових моделей надання послуг. Використання хмарних сервісів і віртуалізації підкреслює залежність від використання безпечного програмного забезпечення, і призводить до появи нового впливу на вимоги до систем безпеки.

Розширенийперелік загроз.Мережі 4G відіграватимуть ще більш центральну роль в якості критичної інфраструктури. Багато людей вже випробували випадки, коли всі види зв'язку переставали надаватися одночасно, наприклад, внаслідок дії природних катаклізмів. І суспільство точно не хоче втрачати подачу електроенергії, мобільну телефонію тощо в в один і той самий час. Крім того, великі проблеми, такі як збільшення загроз кібертероризму, тіньової економіки, електронного шахрайства, також створюються за рахунок нових можливостей мереж 4G.

Збільшення недоторканності приватного життя. Захист персональних даних було обговорено в рамках програм ЄС. В даний час ця проблема розглядається в органах стандартизації, таких як 3GPP і IETF (Internet EngineeringTaskForce), обговорюються на багатьох інших форумах.

Забезпечення безпеки. Як вже було відзначено, цілком імовірно, що мережі 4G відіграватимуть найбільш центральну роль в якості критичної інфраструктури в порівнянні з попередніми поколіннями, і тому забезпечення безпеки буде дуже критичним.

Управління ідентифікацією. Стандарт 4G LTE вимагає наявність USIM (Універсальний модуль ідентифікації абонента), щоб отримати доступ до мережі.

При цьому загроза перехоплення IMSI залишається достатньо високою, тому робота в даному напряму для посилення захисту IMSI заслуговує уваги для 4G в майбутньому.

Безпека радіомережі 4G. У зв'язку із розширеноюкількістю загроз і нових технологій, що забезпечує користувачам альтернативне програмувати своїх власних пристроїв (навіть на рівні радіодоступу), захист від атак на радіо мережі повинен бути більш чітко вираженим в новій архітектурі мереж4G, що має враховувати захист від загроз таких як DoS (відмова в обслуговуванні) через потенційно некоректнопрацюючі пристрої і додаючи заходіви з пом'якшення наслідків нового дизайну радіопротокола.

Гнучка і масштабована архітектура безпеки. У зв'язку із можливістю віртуалізації і більш динамічної конфігурацій, що входять до бачення4G, здається логічним, розглянути більш динамічну і гнучку архітектуру безпеки для неї.

Енергоефективна безпека. У той час, як сервіси забезпечення безпеки пов'язані із витратами, це не являється більше проблемою для мобільних телефонів і аналогічних пристроїв. Витрати енергії на шифрування одного бітув один або два рази менше величини витрат на передачу одного біта [8]. Тим не менш, для найбільш енергонезалежних пристроїв з необхідним тривалим часом роботи, може виникнути необхідність розглянути ще більш легші рішення.

Хмарна безпека. Забезпеченняхмарної безпеки вже надзвичайно гаряча тема, і вонабезперечно буде додана до списку проблем 4G.

Висновки. Технологія LTE цілком підходить під характеристику "технологій завтрашнього дня". У LTE зберігаються і методи аутентифікації користувачів по прив'язці до карти USIM, як в традиційній мобільного зв'язку: користувач може заблокувати доступ до телефону по PIN-коду. В LTE від GSM і UMTS успадковуються схеми протоколу аутентіфікаіції EAP, в які додані нові алгоритми, довші ключі і розширена ієрархія PKI. Передбачено й нові функціональні можливості для нових сценаріїв, що включають міжмашинну взаємодію (M2M) і одноразову аутентифікацію (SSO). Крім того, передбачений захист від несанкціонованих з'єднань поверх мультимедійної IP-мережі IMS. Цілком можливо, що використовувана в мобільному зв'язку більш жорстка система аутентифікації дозволить забезпечити необхідний рівень кібербезпеки. Проте все одно дуже актуальними і важливими є питання, пов'язані із забезпеченням інформаційної безпеки в майбутніх мережах 4G. Тому були сформульовані ключові напрямки удосконалення систем безпеки стільникових мереж (управління ідентифікацією, безпека радіомережі, підвищення енергоефективності, гнучка і масштабована архітектура, безпека хмарних сервісів тощо), що дозволило обґрунтувати необхідність проведення подальших досліджень, пов'язаних із оптимізацією захисту мереж LTE під час їх розгортання в Україні.

Література

1. Мобільний зв'язок в Україні [електронний ресурс] – електронні текстові дані – режим доступу: http://uateka.com/uk/article/society/1227/

2. Одарченко Р.С. Стратегії розвитку операторів стільникового зв'язку в Україні // Наукоємні технології Том 26, № 2 (2015). – С. 141-148.

3. http://www.gsacom.com/downloads/pdf/GSA_Evolution_to_LTE_report_060514.php4

4. 4G America's recommendation on 5G Requirements and Solutions, October 2014, p. 40;

5. Understanding 5G [електронний ресурс]– електронні текстові дані – режим доступу: http://www.arnitsu.com

6. Белоцерковский А.Е. Интернет вещей – это будущее, которое уже наступило [електронний ресурс] – електроннітекстовідані – режим доступу: http://www.therunet.com/interviews/5015-internet-veschey-eto-buduschee-kotoroe-uzhe-nastupilo

7. Скорость и безопасность в LTE [електронний ресурс]– електроннітекстовідані – режим доступу: http://www.osp.ru/nets/2012/06/13032673/

8. C. Margi, B. Trevizan, G. de Sousa, M. Simplicio, P. Barreto, T. Carvalho, M. Nдslund, R. Gold, "Impact of Operating Systems on Wireless Sensor Networks (Security) Applications and Testbeds", Proceedings of ICCCN 2010, pp. 1-6, 2010.

УДК 621.396 (043.02)

Поліщук Ю.Я.
Національний авіаційний університет
liya7954@gmail.com
Гнатюк С.О.
Національний авіаційний університет
s.gnatyuk@nau.edu.ua
Лукашенко В.В.
Національний авіаційний університет
v.v.lukashenko@gmail.com

МЕРЕЖЕВО-ЦЕНТРИЧНИЙ МЕТОД ОЦІНЮВАННЯ МАНІПУЛЯТИВНОГО ВПЛИВУ МАС МЕДІА НА ГРОМАДСЬКУ ДУМКУ

Анотація. *Бурхливий розвиток інформаційно-комунікаційних технологій,мас медіа, поява інформаційної зброї, створення спеціальних технологій впливу, відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства та надмірний вплив мас медіа є критичними для сучасного суспільства. Проте, попри велику кількість досліджень і робіт, на сьогодні не існує жодного методу оцінювання маніпулятивного впливу, який використовує мас медіа як канал впливу.Саме тому було розроблено метод маніпулятивного впливу мас медіа на громадську думку. Отримані результати є важливими для забезпечення кібербезпеки суспільства в умовах інформаційної війни.*

Використання засобів маніпулювання громадською думкою виникли ще вкінці XVII сторіччя – вже тоді стало зрозумілим, що будь-яка боротьба супроводжується маніпулюванням.

У кінці XX сторіччя маніпулювання громадською думкою вийшло на новий рівень – виник феномен інформаційної війни, який є реалізацією політики, що проводиться засобами мас медіа і передбачає доступність великих масивів інформації, які впливають на громадську думку різних категорій людей. Яскравим прикладом такої доступності до закритих даних є феномен Wikileaks, нові методи маніпулювання думкою, менталітетом, сприйняттям, емоціями, інтересами, вибором і т.п.

Дослідженнями методів і моделей маніпулятивного впливу займалися Шиян А., Сінюгін В., Яремчук Ю., Хатян А., Пелещишин А., Гумінський Р. [1-4]. Проте попри велику

кількість досліджень і робіт на сьогодні не існує жодного методу оцінювання маніпулятивного впливу саме мас медіаяк каналу впливу, адже усі методи розглядають маніпуляції без врахування широко спектру моделей і засобів, що використовують сучасні мас медіа.**Метою роботи** є створення методу оцінювання маніпулятивного впливу мас медіа на громадську думку.

Запропонований***мережево-центричний метод оцінювання маніпулятивного впливу мас медіа на громадську думку*** реалізується у 8 етапів: 1) Оцінювання фінансових витрат; 2) Ранжування причин за ступенем їх небезпеки; 3) Визначення цілей проведення кампанії маніпулювання; 4) Визначення задач проведення кампанії маніпулювання; 5) Вибір стратегій реалізації кампанії маніпулювання; 6) Вибір мас медіа для маніпулювання; 7) Вибір методу за допомогою якого буде проведена кампанія; 8) Оцінювання маніпулятивних впливів.

Оскільки мережево-центрична концепція [5] передбачає підготовку до проведення маніпулятивного впливу операції задовго до початку, то природною складовою цієї підготовки повинен бути безперервний моніторинг положення. Моніторинг веде спрямований збір інформації і її аналіз, що стосується можливого об'єкта атаки і фокус-груп (аудиторії), які його цікавлять. Мережево-центрична система моніторингу об'єднує засоби моніторингу всіх рівнів і напрямків управління в єдине ціле. Вона повинна забезпечувати доведення всієї необхідної інформації до адресатів в реальному часі або близькому до нього в міру її отримання та, що дуже важливо, використовуючи інформацію, отриману на всіх місцях дислокації [5-6].

Реалізація цього методу дозволить оцінити величину маніпулятивного впливу мас медіа на громадську думку.Підготовчим етапом для проведення методу є оцінювання ефективності маніпулятивних дій. Цей етап є лише додатковим і необхідним лише для замовника. На цьому етапі необхідно із бази даних інформації про мас медіа вибрати ті мас медіа, які на думку експерта підходять для реалізації маніпулятивного впливу, визначити економічний ефект рекламування в обраних мас медіа та, якщо необхідно, оцінити ефективність реклами у відношенні прибутку підприємства, отриманого від реклами до прибутку до початку рекламування.

Розглянемо більш детально етапи методу:

Етап 1 – Оцінювання фінансових витрат. Причини, що вимагають проведення кампанії маніпуляції громадською думкою, повинні бути оцінені, і в разі необхідності, проведе ранжування. Оцінювання причин може бути проведене в кожному регіоні за своїми критеріями. Частина цих критеріїв, або навіть всі, можуть не збігатися, наприклад, фінансові витрати, ризики проведення кампанії, викликані різними причинами. Для кожної можливої причини на період підготовки та проведення кампанії в певному районі необхідноо цінити ресурси для маніпулятивної атаки (крок 1). Слід також вказати обмеження на ресурси, пов'язані з фінансовими можливостями проведення кампанії (крок 2).

Етап 2 – Ранжування причин за ступенем їх небезпеки.Проведення кампанії маніпулювання громадською думкою може викликати заходи протидії, боротьбу з організацією, яка ініціювала та фінансувала кампанію. Оцінювання небезпеки причин маніпулювання визначити важко, тому необхідно залучити експертів, які проведуть попарне порівняння причин з виставленням відповідних балів. Далі бали додаються за кожною причиною – найнебезпечнішою є та причина, яка набрала найбільше балів.

Етап 3 – Визначення цілей проведення кампанії маніпулювання. На цьому етапі експерти відбирають із бази даних множину цілей, що відносяться до причин проведення кампанії маніпулювання і є можливим їх наслідком (крок 1), вибирають фокус-групи (аудиторію),на якібуде націлено вплив (крок 2), та критерії,за якими будуть вибиратися цілі, завдання та стратегії кампанії маніпулювання (крок 3).

Етап 4 – Визначення завдання проведення кампанії маніпулювання. Кожен агент формує множину задач (крок 1) та критеріїв для оцінювання задач кампанії маніпулювання громадською думкою. Підраховується частка узгоджених позитивних оцінок за критеріями кожного завдання кожного агента (крок 2). У кінцевому варіанті вибирається завдання з

найбільшим балом від агента і, при подальшому оцінюванні стратегій кожним агентом потрібно враховувати відповідність стратегії цій задачі.

Етап 5 – Вибір стратегій реалізації кампанії маніпулювання. Цілі маніпулювання різними групами виробляються в різний час і мають різні перевагами. Відповідно до сформульованих цілей (див. крок 1 етапу 3) вибираються і реалізуються їх стратегії. Агент формує множину стратегій (крок 1), а далі із списку стратегій в базі даних кожен агент вибирає стратегію на кожен період і проводить їх ранжування. Далі визначається бал і місце стратегії при ранжуванні, заснованих на порядкових оцінках (крок 2).

Етап 6 – Вибір мас медіа для маніпулювання.Оскільки основним засобом маніпулювання громадською думкою є мас медіа, необхідно визначити ті мас медіа, які буде використовувати кожен агент у районі своєї активності. Впливовість окремих мас медіа сильно залежить від багатьох причин і, звичайно, від характеру фокус-групи та місця її розташування. Для оцінювання ефективності маніпулятивних впливів кожного мас медіа може бути використаний так званий індекс відповідності, який розраховується за співвідношенням рейтингу мас медіа в фокус-групі або її сегменті до рейтингу мас медіа у населення міста (області) (крок 1).Зауважимо, що такі співвідношення повинні бути розраховані для кожної фокус-групи в кожному районі дислокації. Значення індексу співвідношення значно менше 1 говорить про те, що інформаційний вплив через цей засіб мас медіа сягатиме випадкових людей частіше, ніж у фокус-групи, тому що рівень інтересу в фокус-групі до розглянутого засобу мас медіа нижче, ніж населенняв цілому. Отримати такі дані можна тільки за допомогою соціологічних досліджень.Спочатку визначається ефективність інформаційного впливу. Далі у базі даних системи маніпулювання мас медіа зберігається матриця цін і розраховуються «витрати на тисячу» читачів і «питома ефективність інформаційних витрат» (крок 2). На кроці 3 вибираються пара альтернативних засобів мас медіа і відбувається їх попарне порівняння. У кінцевому випадку буде отримано кращі альтернативи засобів мас медіа, за допомогою яких буде реалізовано маніпулятивний вплив.

Етап 7 – Вибір методу за допомогою якого буде проведена кампанія.Кожен агент із бази даних вибирає ті методи[7-8], які на його думку будуть ефективними для використання. Далі формується список критеріїв за яким проводиться відбір методів.

Етап 8 – Оцінювання маніпулятивних впливів.Змістовно завдання оперативного маніпулятивного впливу полягає у зміні поглядів і уподобань фокус-груп. Завдання маніпулювання полягає у зміні думки групи. У результаті реалізації послідовності оперативних маніпулятивних впливів формується кінцева думка фокус-груп. Спочатку необхідно розрахувати цільову функцію модифікації громадської думки. Завдання управління полягає у виборі прийнятного методу управління, який максимізує ефективність маніпулятивного впливу. Далі визначається величинаманіпулятивного впливу і його ефективність.

Отже, в роботі було розроблено мережево-центричниий метод оцінювання маніпулятивного впливу мас медіа на громадську думку. Цей метод, на відміну від відомих, дає можливість оцінити маніпулятивний вплив, що реалізується через сучасні мас медіа і використовує методи маніпулятивного впливу на громадську думку. Отримані результати можуть використовуватися у галузі інформаційної безпеки, зокрема для оцінювання маніпулятивного впливу мас медіа на громадську думку. Подальші дослідження будуть пов’язані з формалізацією усіх процесів, що описані в етапах реалізації методу, а також з проведенням експериментального дослідження для його верифікації.

Література

1. Шиян А.А. Модель та методи захисту структурованої соціальної групи від негативного інформаційно-психологічного впливу/ Шиян А.А., Яремчук Ю.Є. // Захист інформації. – 2014. – Т.16, №4.– С. 311-317.

2. Шиян А.А. Модель процесу просторового розповсюдження суспільної думки в задачах управління інформаційною безпекою / Шиян А.А., Яремчук Ю.Є., Нікіфорова Л.О., Сінюгін В.В. // Сучасний захист інформації. – 2015. – №2. – С. 34-39.

3. Хатян О.А. Інформаційно-комунікативна модель суспільної комунікації як основа дослідження соціально-економічних явищ. / О.А. Хатян // Сучасні інформаційні технології у сфері безпеки та оборони. – 2011. – № 3(12). – С. 66-71.

4. Пелещишин А.М. Модель інформаційного середовища віртуальної спільноти / А.М. Пелещишин, Р.В. Гумінський // Східно-Європейський журнал передових технологій. – Х. 2014. – № 2/2 (68). – С. 10-16.

5. Гнатюк В.О. Метод мережево-центричного моніторингу кіберінцидентів в сучасних інформаційно-телекомунікаційних системах / О.Г. Корченко, В.О. Гнатюк, Є.В. Іванченко, С.О. Гнатюк, Н.А. Сєйлова // Захист інформації. – №3. – 2016. – С. 229-247.

6. Сетецентрические особенности управленческих решений манипулирования общественным мнением. [Электронный ресурс]. – Режим доступа: http://ubs.mtas.ru/bitrix/components/bitrix/forum.interface/show_file.php?fid=8736.

7. PolishchukYu., Gnatyuk S., Seilova N. Massmediaas a channelofmanipulativ einfluenceonsociety // UkrainianScientificJournalofInformationSecurity. – 2015. –Vol. 21, Issue 3. – P. 301-308.

8. PolishchukYu. Information-psychologicalsecurityofsocietyinthecontextofinformationwarfare: monograph / Yu. Polishchuk, T. Zhmurko; AkademiaTechniczno-Humanistyczna. – Bielsko-Biała: 2016. – P. 321-342.

УДК 004.056.053:004.421.5(043.2)

Сапожнік Т.М.
Національний авіаційний університет
tanya.sapojnik@gmail.com
Кінзерявий В.М.
Національний авіаційний університет
v.kinzeryavyy@gmail.com

МЕТОД ГАРАНТОВАНОГО ВИДАЛЕННЯ ДАНИХ

Анотація.*У роботі досліджено міжнародні стандарти та методи гарантованого видалення даних, які існують у різних країнах, наведена порівняльна характеристика програмних засобів для знищення інформації, запропоновано новий метод гарантованого видалення даних за рахунок розробленого генератора псевдовипадкових послідовностей, розроблено алгоритмічне та програмне забезпеченнярозробленого методу гарантованого видалення даних, проведено експериментальні дослідження розроблених рішень для підтвердження їх ефективності. Розроблений метод гарантованого видалення даних відноситься до галузі захисту інформації від НСД та може використовуватися для розширення можливостей систем обробки та зберігання інформації.*

Із розвитком сучасних технологій питання щодо забезпечення інформаційної безпеки набувають все більшої актуальності. При цьому основна увага приділяється програмним, апаратним та комунікаційним загрозам, коли є можливість фізичного доступу до пристроїв збереження даних. Виникають ситуації при яких приватна та секретна інформація потребує видалення без можливості їх відновлення. Просте видалення чи форматування носія не гарантує повного знищення інформації. На сьогодні існує досить велика кількість програмних засобів для видалення даних без можливості їх відновлення, які побудовані на основі міжнародних стандартів.Проте дані методи (стандарти) являються дещо застарілими для сучасних засобів і технологій. Тому, на сьогодні актуальним єрозробканових та удосконалення існуючихметодівгарантованого видалення даних, що дозволить швидко та надійно знищувати всю інформацію без можливості її відновлення.

Метою роботи є підвищення ефективності гарантованого знищення інформації за допомогою використання запропонованого методу гарантованого видалення даних.

На сьогодні найбільш відомими є такі міжнародні методи гарантованого видалення даних: національний стандарт Міністерства оборони США DoD 5220.22M, американський національний стандарт NAVSO P-5239-26, німецький національний стандарт VSITR, Канадський RCMP TSSIT OPS-II, російський державний стандарт ГОСТ Р 50739-95, алгоритм Брюса Шнейєра та метод Пітера Гутмана.

Аналіз даних методівдозволив виділити перевагиі недоліки кожного з них (табл. 1).

Таблиця 1

Порівняльна характеристика міжнародних методів видалення даних

Назва методу	Дата створення	Раунди	Переваги	Недоліки
Російський стандарт ГОСТ Р50739-95	1995	1	Найшвидший метод	Надійність видалення дуже низька, оскільки перезапис даних виконується тільки 1 раз
Німецький стандарт VSITR	1999	7	У порівнянні з DoD він більш надійний	Не гарантує неможливість відновлення даних, вимагає багато часу
Метод Брюса Шнайера	1996	7	Метод більш надійний, порівняно з німецьким, при тій же кількості циклів	Надійність знищення інформації низька. Перезапис може займати тривалий час
Метод Пітера Гутмана	1996	35	Вважається абсолютно надійним – по закінченні процесу не можна відновити ні одного байта	Швидкість видалення дуже маленька
Американський стандарт DoD 5220.22-M	1993	3	Є досить вдалим компромісом між надійністю і швидкістю	Стандарт не сильно надійний, армія США не використовує його для видалення секретної інформації
Канадський RCMP TSSIT OPS-II	1993	7	Використовує 7 циклів, що гарантує більшу надійність видалення даних	Не до кінця досліджений, не існує як самостійне ПЗ, а використовується для розробки утиліт-шредерів
Американський стандарт NAVSO P-5239- 26	1995	3	Використовується для MFM-кодованих пристроїв	Мала кількість циклів, не завжди надійний, деякі файли вдається відновити

Найнадійнішим методом серед переглянутих вважається Метод Пітера Гутмана, проте швидкість його роботи дуже мала, найшвидшим – Російський стандартГОСТ Р50739-95, проте дані видалені ним можна відновити. Проаналізувавши дані методи гарантованого видалення даних можна зробити висновок, що ефективність знищення інформації (надійність та швидкість видалення) залежить,як від кількості раундів та і від кількості операцій у кожному раунді.

Далі були проаналізовані наступні програмні застосунки гарантованого видалення даних – Ashampoo UnInstaller**,** Hardwipe, FreeraserSetup, Files Terminator Free, File Shredder, PrivacyEraser Free. Для проведення аналізу на флеш–носію створювалися file_1, file_2 та file_3 різних форматів та розмірів. Потім проводилося видалення кожного файлу за допомогою вказаних програм. Для перевірки надійності видалення використовувалося різне

програмне забезпечення для відновлення файлів. Результати проведення експерименту наведені в табл. 2.

Таблиця 2

Порівняльна характеристика ПЗ для гарантованого видалення даних

Програма для видалення файлу	Назва та розмір файлу	Час видалення	ОС	Можливість відновлення	Кількість циклів
1	2	3	4	5	6
Secure-Delete	file_1.pdf – 365 КБ	3с	Windows Linux	Неможливо	Від 1 до 35
	file_2.mp3 – 9010 КБ	7 с		Неможливо	
	file_3.mkv – 9506801 КБ	1год 23хв		Неможливо	
Hardwipe	file_1.pdf – 365 КБ	2с	Windows	Неможливо	1, 2, 3, 7, 35 циклів
	file_2.mp3 – 9010 КБ	11с		Неможливо	
	file_3.mkv – 9506801 КБ	1год 57хв		Неможливо	
FreeraserSetup	file_1.pdf – 365 КБ	2с	Windows	Відновлено назву та розмір файлу	1, 3, 35 циклів
	file_2.mp3 – 9010 КБ	9 с		Відновлено назву та розмір файлу	
	file_3.mkv – 9506801 КБ	1год 35хв		Відновлено назву файлу	
Files Terminator Free	file_1.pdf – 365 КБ	3с	Windows	Неможливо	1, 3, 7, 35 циклів
	file_2.mp3 – 9010 КБ	11с		Неможливо	
	file_3.mkv – 9506801 КБ	1год 31хв		Відновлено	
File Shredder	file_1.pdf – 365 КБ	2с	Windows Linux	Неможливо	1, 2, 3, 7, 35 циклів
	file_2.mp3 – 9010 КБ	6с		Неможливо	
	file_3.mkv – 9506801 КБ	1год 48хв		Неможливо	
PrivacyEraser Free	file_1.pdf – 365 КБ	1 с	Windows	Відновлено назву та розмір файлу	3, 7, 35, можливість самостійного налаштування
	file_2.mp3 – 9010 КБ	5с		Відновлено назву та розмір файлу	
	file_3.mkv – 9506801 КБ	1год 3хв		Відновлено лише назву файлу	
Shred	file_1.pdf – 365 КБ	1 с	*Linux*	Неможливо	25 циклів та можливість самостійного налаштування
	file_2.mp3 – 9010 КБ	6 с		Неможливо	
	file_3.mkv – 9506801 КБ	1 год17с		Неможливо	

У табл. 3. наведено переваги та недолікидосліджених програмних модулів.

Таблиця 3

Переваги та недоліки ПЗ для гарантованого видалення даних

Програма для видалення файлу	Переваги	Недоліки
1	2	3
Secure-Delete	Швидка і зручна у використанні утиліта	На SSD і флеш-носіях не завжди файли видаляються, деякі видаленні файли в ОС Windows можна відновити
Hardwipe	Утиліта містить декілька варіантів перезапису, невеликий час видалення порівняно з іншими	У безкоштовній версії доступні лише найслабші алгоритми, які не завжди ефективні
FreeraserSetup	Утиліта пропонує три режими видалення даних швидкий, надійний і безкомпромісний	Безкомпромісний режим недоступний у безкоштовній версії, даних використовуючи швидкий і надійний режими файли можна відновити
Files Terminator Free	Безкоштовна програма, використовує різні методи для видалення файлів, які можна вибрати виходячи з потреб. За допомогою програми можна надійно видаляти як окремі папки так і файли	Процес видалення, може зайняти багато часу
File Shredder	Видаляє файли без можливості відновлення, підходить як для жорстких дисків так і флеш накопичувана, маленький розмір програми і зручний інтерфейс, містить 5 алгоритмів видалення	Очищення в File Shredder залишає після виконання операції тимчасові файли з беззмістовною інформацією, дещо повільним при очищенні від непотрібних і застарілих файлів
PrivacyEraser Free	Видає докладну інформацію по кожному робочому процесі, підтримує три відомі алгоритми затирання даних, а також дає можливість користувачеві самому налаштувати кількість циклів для знищення даних	Безкоштовна версія підтримує лише один із методів затирання даних, всі інші платні
Shred	Простий і структурований спосіб видалення даних, можливість задавати кількість необхідних циклів	Не всі типи файлів можна видалити з першого разу. Не видаляє каталоги

Проаналізувавши програмні засоби та методи гарантованого знищення даних, можна виділити деякі недоліки. По перше методи з малою кількістю циклів не є достатньо надійними. По друге методи з більшою кількістю циклів працюють дуже повільно і не завжди мають бажаний результат.

Тому, розроблено новий програмний модуль гарантованого знищення даних – STM Shredder, який дозволяє ефективно видаляти дані та базується на запропонованому методі гарантованого видалення даних.

В основі запропонованого методу гарантованого знищення інформації лежить декілька варіантів перезапису: заміна даних нулями, заміна даних псевдовипадковими числами (використовуєтьсярозроблений генератор PVP-Security) та заміна даних числами, значення яких беруться зі спеціальних таблиць.

Етапи роботи методу наведені на рис. 1.

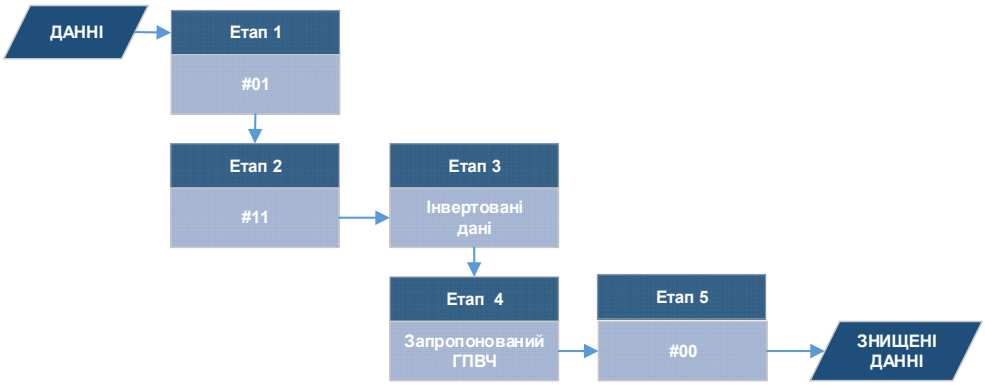


Рис. 1. Метод гарантованого видалення даних

Розроблений метод складається із п’яти етапів, що дозволяє підвищити швидкість видалення порівняно таких методів гарантованого знищення інформації, як німецький стандарт VSITR, метод Брюса Шнайера таканадського RCMPTSSITOPS-II, що виконуються у 7 етапів. Використання розробленого генератора ПВП , який застосовується на четвертому етапі дозволило підвищити надійність видалення даних, без можливості їх відновлення порівняно із американськими стандартамиDoD 5220.22-M, NAVSOP-5239- 26 та російськимГОСТ Р50739-95, які виконуються у 3 етапа.

Запропонований генератор PVP-Security побудований із чотирьох регістрів зсуву з лінійно-зворотнім зв’язком A, B, C і D, кожен з яких генерує 32 біти, має свою довжину, свій порядок та кількість операцій.

На рис. 2 зображено структурну схему роботи генератора PVP-Security.

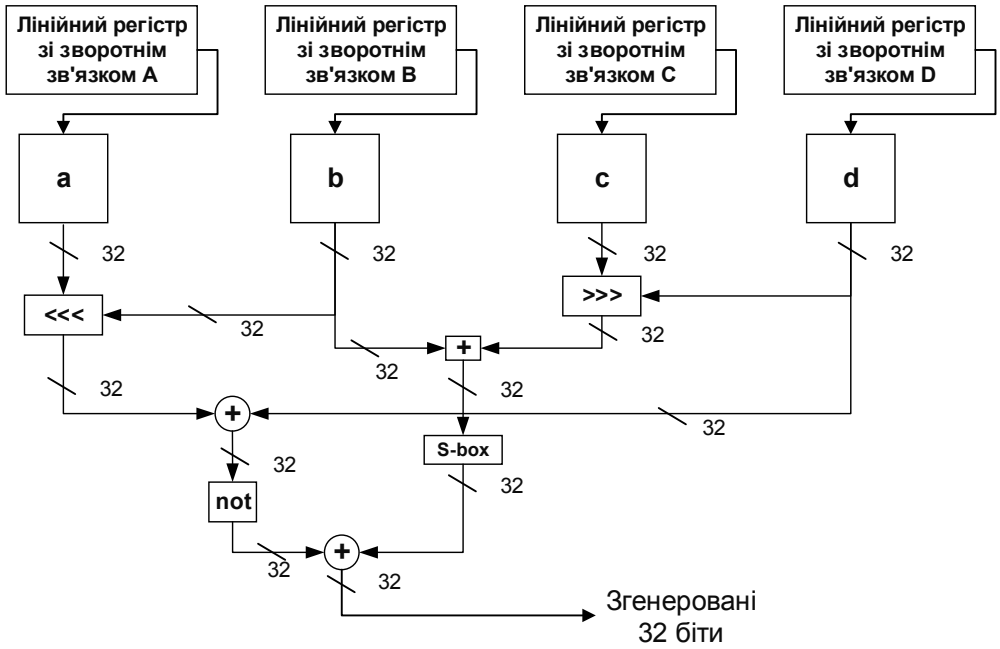


Рис. 2. Схема роботи генератора PVP-Security

Для підтвердження досягнення поставленої мети було проведено експериментальне дослідження – визначалась швидкість та надійність гарантованого видалення інформації програмного модуля Shredder STM, результати порівнювались із відомими програмними модулями. Експеримент проводився на п’ятьох різних ПК на кожному з яких за допомогою програмного модуля Shredder STM видалялися три файлів розміром 36,5КБ, 9,1МБ, 7,96ГБ. При цьому визначався середній час та швидкість видалення інформації. Для перевірки надійності видалення використовувалися програмні засоби Foremost та FinalDatадля відновлення файлів.

Отримані результати наведені в табл. 4.

Таблиця 4

Результати дослідження ефективності програмного модуля Shredder STM

Назва програми	Розмір файлу	Тип файлу	Час видалення	Швидкодія, КБ/с	Відновлення	
					Foremost	FinalData
1	2	3	4	5	6	7
Secure-Delete	36,5 КБ	.pdf	3 с	12,17	Не відновлено	Не відновлено
	9,1 МБ	.mp3	7 с	1300	Не відновлено	Не відновлено
	7,96 ГБ	.mkv	1год23хв	1598,39	Не відновлено	Не відновлено
Hardwipe	36,5 КБ	.pdf	2 с	18,25	Не відновлено	Не відновлено
	9,1 МБ	.mp3	11 с	827,27	Не відновлено	Не відновлено
	7,96 ГБ	mkv	1год 57хв	1133,9	З помилками	Не відновлено
FreeraserSetup	36,5 КБ	.pdf	2 с	18,25	Не відновлено	Не відновлено
	9,1 МБ	.mp3	9 с	1011,11	Не відновлено	Не відновлено
	7,96 ГБ	.mkv	1год35хв	1396,49	Не відновлено	Не відновлено
File Shredder	36,5 КБ	.pdf	2 с	18,25	Не відновлено	Не відновлено
	9,1 МБ	.mp3	6 с	1516,67	Не відновлено	Не відновлено
	7,96 ГБ	.mkv	1год 48хв	1228,4	Не відновлено	Не відновлено
PrivacyEraser Free	36,5 КБ	.pdf	1 с	36,5	Відновлено	Не відновлено
	9,1 МБ	.mp3	5 с	1820	Відновлено	З помилками
	7,96 ГБ	.mkv	1год 3хв	2105,82	Відновлено	З помилками
Shred	36,5 КБ	.pdf	1 с	36,5	Не відновлено	Не відновлено
	9,1 МБ	.mp3	6 с	1516,67	Не відновлено	Не відновлено
	7,96 ГБ	.mkv	1год 17хв	1722,94	З помилками	З помилками
Shreder STM	36,5 КБ	.pdf	3 с	12,2	Не відновлено	Не відновлено
	9,1 МБ	.mp3	6 с	1517	Не відновлено	Не відновлено
	7,96 ГБ	.mkv	53хв	2503	Не відновлено	Не відновлено

Результати експериментального дослідження показало, що розроблений програмний модуль Shredder STM для файлів менших розмірів показавгірший результат ніж відомі програмні засоби. Проте для файлів, що мають великий розмір запропонований програмний модуль мінімум на 18% швидше видаляє дані ніж відомі програмні засоби.

Таким чином, у роботі був проведений аналіз міжнародних стандартів та програмних засобів для гарантованого видалення даних, який показав основні переваги та недоліки кожного з них. Для підвищення ефективності гарантованого знищення інформації запропоновано використання розробленого методу гарантованого видалення даних. Також у

роботі було проведено експериментальні дослідження даного методу та розробленого на його основі програмного модуля STM Shredder, яке показало, що використання STM Shredder дає змогу підвищити,як надійність так і швидкість видалення даних.

Література

1. Бабаш А. В. Криптографические и теоретико-автоматные аспекты современной защиты информации / А. В. Бабаш. ТОМ 1– М: Изд. центр ЕАОИ, 2009. – 414 с.

2. Бем М. В. Захист персональних даних/ М. В. Бем, І. М. Городиський, Г. А. Саттон, О. М Родіоненко// Правове регулювання та практичні аспекти: науково-практичний посібник. – К.: К.І.С., 2015. – 220 с. – ISBN 978-617-684-129-6.

3. Гапак О. М. Визначення довжини періоду генераторів псевдовипадкових послідовностей на основі регістрів зсуву зі зворотним зв'язком та перенесення / О. М. Гапак // Моделювання та інформаційні технології. – 2014. – № 73. – С. 92– 97.

4. Гультяев О. К. Відновлення даних / О. К. Гультяев. – пітер: СПб, 2006. – 379 с.

5. Коженевский С.Р., Методы гарантированного уничтожения данных на жестких магнитных дисках/С. Р. Коженевский// [Электронный ресурс]: Режим доступа: World Wide Web. – URL: http://www.epos.ua/

6. Шреддінг, або Як видалити інформацію без можливості відновлення? [Електронний ресурс] // Архів статей. – 2011. – Режим доступу до ресурсу: http://arhiv-statey.pp.ua/index.php?newsid=5934.

УДК 006.03:330.131.7

Стайкуца С.В.,к.ф.н., доц. каф. ІБ та ПД
Одеська національна академія зв'язку ім. О.С.Попова,
s.staikuca@gmail.com
Дігол С.О., директор ТОВ «Гофер Корпорейшн»,
Бердніков О.М., директор ПП «Ардо»,
Верстаков В.І.,
Одеська національна академія зв'язку ім. О.С.Попова
vers1977@gmail.com
Науковий керівник - к.ф.н., Стайкуца С.В.

АНАЛІЗ РИЗИКІВ КОРПОРАТИВНОГО СЕРЕДОВИЩА З ПОЗИЦІЇ МІЖНАРОДНИХ СТАНДАРТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. *В роботі розглянуті етапи організації побудови режиму ІБ на підприємстві. З позиції моделей Cartner Group і Carnegie Mellon University розглянуто моделі зрілості компаній. Детально розглянуто напрямок аналізу ризиків - технології, кількісні та якісні методи оцінювання ризиків, активні і пасивні контрзаходи. Представлений аналіз основних міжнародно-правових документів, а також відомчих і корпоративних стандартів управління ІБ.*

Бізнес-середовище сучасного підприємства характеризується великими обсягами інформації, динамікою і малим часом прийняття управлінських рішень. Процеси і алгоритми, які описують питання організації режиму ІБ на підприємстві, для підвищення ефективності повинні знаходитись в практичній області. Саме такий формат став основою для ряду міжнародних та національних стандартів оцінки та управління інформаційною безпекою. До таких відносяться ISO 15408, ISO / IEC 27002: 2005 (BS7799), BSI. Також до відзначених вище стандартів варто віднести стандарти аудиту, які передають бачення питань інформаційної безпеки з позиції COBIT, SAC, COSO, SAS 55/78 тощо [1]. У відповідність з

цими стандартами процедура забезпечення режиму ІБ в компанії передбачає виконання ряду пунктів, а саме:

1. Аналіз інформаційного середовища та формування цілей забезпечення інформаційної безпеки компанії.

2. Побудова ефективної СУІБ.

3. Розрахунок сукупності деталізованих показників для оцінки відповідності ІБ заявленим цілям.

4. Застосування інструментарію забезпечення ІБ та оцінки її поточного стану.

5. Використання ефективних методик процесі аналізу та управління ризиками[2].

Покоління стандартів ІБ, яке зараз використовується, характеризується “офіціалізацією” технологій забезпечення режиму ІБ та більш детальним комплексним урахуванням показників безпеки компанії. Консолідований облік показників передбачає, що при формуванні режиму ІБ використовується перевірка на відповідність певним правилам. При цьому контролюється і підтримується не тільки програмно-технічна складова ІБ, але і організаційно-адміністративні заходи щодо її забезпечення.

Наявність СУІБ (Information Security Management) в сукупності із напрямом управління інформаційними ризиками (Risk Management) - обов'язковий компонент організації режиму ІБ на підприємстві. Основним фактором, що визначає ставлення організації до питань інформаційної безпеки, є ступінь її зрілості. У класичному варіанті часто оцінюють зрілість компанії з позиції життєвого циклу організації за методикою, запропонованою І.Адізесом [3].

Проте дана модель не враховує відповідність різних потреб компаній в області інформаційної безпеки. Для цього існують кілька моделей, що дозволяють в повній мірі оцінити рівень зрілості компанії з позиції ІБ.

Так, модель Cartner Group виділяє чотири рівні зрілості компанії, починаючи з нульового рівня і закінчуючи третім. Тут максимальний рівень виділяє той факт, що проблематика забезпечення ІБ управлінням компанії усвідомлена повною мірою. Більш розширену модель визначення рівня зрілості компанії з точки зору інформаційної безпеки пропонує університет Carnegie Mellon University [4]. Відповідно до цієї моделі виділяється 5 рівнів зрілості компанії, яким можна поставити у відповідність різне розуміння проблем ІБ організації, починаючи від рівня "анархії" і закінчуючи рівнем "оптимізації". Організації, починаючи з 3-го рівня зрілості, застосовують будь-який варіант системи управління ризиками. На даному етапі (рівень 3 - стандарти) керівництво компанії усвідомлює завдання в області ІБ. В організації є документація (можливо неповна), що відноситься до політики інформаційної безпеки. Керівництво зацікавлене у використанні стандартів в області інформаційної безпеки, оформленні документації відповідно до них. Усвідомлюється завдання управління режимом ІБ на всіх стадіях життєвого циклу інформаційної технології. На даному етапі в організації вважається за доцільне слідувати в тій чи іншій мірі стандартам і рекомендаціям, які забезпечують базовий рівень інформаційної безпеки (наприклад, ISO 17799) [5].

Завдання аналізу ризиків досить актуальне. Аналіз ризиків розглядається як один з елементів технології управління режимом інформаційної безпеки на всіх стадіях життєвого циклу. Поняття ризику включає ланку аспектів, таких, як ймовірність, загрозу, вразливість, інколи вартість.

Один з варіантів визначення ризику (певного класу) в цьому випадку: ймовірність виникнення інциденту в результаті того, що наявна вразливість (певного класу) буде сприяти реалізації загрози (певного класу).

Сучасні технології аналізу ризиків дозволяють визначити рівень інформаційних ризиків в компаніях. Це особливо важливо в тому разі, коли до інформаційної системи підприємства пред'являються підвищені вимоги в області ІБ.

Тут під оцінкою ризику розуміється, як правило, міра ймовірності і збитку. Згадана міра може бути виражена як якісно, так і кількісно, а збитки в грошовому еквіваленті.

Оцінювання ризиків може здійснюватися за допомогою:

– експертних оцінок (безпосередньо або побічно - з використанням автоматичних програмних засобів);

– історичних відомостей про ймовірність реалізації вразливості і збитку від її реалізації (недоліками методу є потреба в досить великому обсязі історичних даних (а для деяких загроз їх може просто не існувати) і неможливість точного оцінювання тренда в разі мінливої обстановки, що ми спостерігаємо практично у всіх сферах ІБ);

– аналітичних підходів, наприклад, з побудовою графів зважених переходів для визначення величини збитку від реалізації уразливості.

Заходи, спрямовані на парирування ризиків, можуть включати в себе пасивні і активні дії. До пасивних дій відносяться:

– прийняття ризику (рішення про прийнятність спостережуваного рівня даного ризику без будь-яких контрзаходів);

– ухилення від ризику (рішення про трансформацію діяльності, яка спричинить за собою даний рівень ризику);

До активних дій слід віднести:

– обмеження або зниження конкретного ризику (складається з набору організаційних і технічних заходів);

– передача ризику (страхування);

Технологія управління режимом інформаційної безпеки в повному варіанті включає наступні елементи:

– документування інформаційної системи організації з позиції інформаційної безпеки;

– розподіл на категорії інформаційних ресурсів з позиції керівництва організації;

– визначення можливого впливу різного роду подій в сфері безпеки на інформаційну технологію;

– аналіз ризиків;

– технологію управління ризиками на повній ділянці т з урахуванням всіх етапів життєвого циклу;

– аудит в області ІБ.

Рис. 1. Методи оцінки та зниження ризиків

Как видно из представленного выше рисунка, при работе с рисками принято использовать классические меры – принятие, ограничение, передача и уклонение. Эти принципы стали основой при формировании комплексных систем информационной безопасности при их разработке национальными институтами стандартов и отраслевыми организациями. К основным стандартам относятся:

– ISO / IEC 27002: 2005 (Великобританія)
– BSI (Німеччина)
– NIST 800-30 (США)

Наприклад, поточна версія стандарту ISO / IEC 27002: 2005 (BS 7799-1: 2005) розглядає такі актуальні питання забезпечення інформаційної безпеки організацій та підприємств:

– необхідність забезпечення ІБ;
– основні поняття і визначення ІБ;
– політика інформаційної безпеки компанії;
– організація інформаційної безпеки на підприємстві;
– управління корпоративними інформаційними активами;
– кадровий менеджмент та інформаційна безпека;
– методи та засоби фізичної безпеки, застосування інженерно-технічних та технічних засобів охорони об'єктів;
– адміністрування безпеки корпоративних ІС;
– управління доступом;
– вимоги з безпеки до корпоративних інформаційних систем в ході їх розробки, експлуатації і супроводу;
– управління інцидентами ІБ;
– управління безперервністю бізнесу;
– відповідність вимогам законодавства.

Крім міжнародних стандартів, існують відомчі та корпоративні стандарти управління ІБ. До найбільш поширених з них відносяться:

– XBSS - специфікації сервісів безпеки X / Open;
– стандарт NASA «Безпека інформаційних технологій»;
– концепція управління ризиками MITRE.

Концепція MITRE близька до рекомендацій, що представлені в стандарті США NIST 800-30 [6]. Організація MITRE в "некомерційному" форматі розповсюджує базовий інструментарій на основі електронної таблиці, призначений для використання на етапі ідентифікації та оцінки ризиків, вибору можливих контрзаходів відповідно до цієї концепції - «Risk Matrix» [7]. При використанні представленої моделі ризик не поділяється загрози і вразливості. В деяких випадках такий підхід може виявитися більш зручним та ефективним з позиції власників інформаційних ресурсів.

Литература

1 Петренко С. А. Анализ рисков в области защиты информации / Сергей Анатольевич Петренко, 2009. – 153 с. – (Информационно-методическое пособие по курсу повышения квалификации «Управление информационными рисками»).

2 Базові поняття у сфері оцінки ризиків стану захищеності систем [Електронний ресурс] // Студопедия. – 2015. – Режим доступу до ресурсу: http://studopedia.su/20_7592_bazovi-ponyattya-u-sferi-otsinki-rizikiv-stanu-zahishchenosti-sistem.html

3 Адизес И. Управление жизненным циклом корпораций / Ицхак Калдерон Адизес. – М.: Манн, Иванов и Фербер, 2014. – 512 с.: ил.

4 Корпоративный сайт компании MethodWare - http://www.methodware.com

5 Information technology - Code of practice for Information security management. International Standard ISO/IEC 17799:2000(E).

6 Risk Management Guide for Information Technology Systems, NIST, Special Publication 800-30

7 Корпоративный сайт компании Risk Matrix - http://www.mitre.org

УДК 004.78: 621.391:654.9:681.327

Стайкуца С.В.,к.ф.н., доц. каф. ІБ та ПД
Одеська національна академія зв'язку ім. О.С.Попова,
s.staikuca@gmail.com
Дігол С.О., директор ООО «Гофер Корпорейшн»,
Седов К.С.,
Одеська національна академія зв'язку ім. О.С.Попова
sedovmail2@gmail.com
Науковий керівник - к.ф.н., Стайкуца С.В.

АНАЛИЗ И ОБОСНОВАНИЕ ВЫБОРА ПЕРИМЕТРАЛЬНЫХ СИСТЕМ ОХРАНЫ

Аннотация. *В работе рассмотрены основные задачи систем охраны периметра и их компонентный состав. Представлены критерии выбора СОП на раннем этапе "жизненного" цикла системы - этапе проектирования, а также расширенная классификация систем охраны периметра. Детально рассмотрены критерии выбора оптимальных решений при выборе СОП, основой которых выступают параметры эффективности - вероятность обнаружения нарушителя и вероятность ложных срабатываний. При анализе СОП на основе оптимальных решений представлена зависимость потенциала выявления нарушителя от принципа действия СОП, в результате чего сейсмические системы охраны периметра показали максимальный результат.*

Технические средства охраны (ТСО) играют немалую роль при формировании систем безопасности объектов информационной деятельности. В базовой версии ТСО обычно включает в себя системы охранно-пожарной сигнализации, СКУД, системы видеонаблюдения и системы охраны периметра. При этом на СОП полагается первоочередное задание по выявлению нарушителя.

Охрана периметра – это совокупность механизмов, оборудования и средств защиты, которые обеспечивают целостность и сохранность определенных участков или территорий, а также предупреждают факты незаконного проникновения третьих лиц на территорию, которая подлежит охране. При этом, как отмечается в [1, с.93], любая система охраны периметра (СОП) решает четыре основные задачи, представленные в табл. 1.

Таблица 1

Основные задачи СОП

№	Задача	Описание
1	Запугивание	Оказание максимального уровня сдерживания в направлении потенциального нарушителя
2	Засечка	Обнаружение нарушителя
3	Задержка	Создание таких условий, при которых нарушитель будет расходовать время на преодоление пространства от границы объекта до самого объекта после срабатывания сигнализации
4	Задержание	Произведение физического захвата нарушителя

СОП обычно включают в себя механические заграждения (заборы, сборные сетчатые конструкции и т.д.) и технические средства защиты. Кроме того, включение в состав СОП внешних систем охраны (например, систем видеонаблюдения) позволяет существенно повысить эффективность охранной системы и повысить вероятность выявления нарушителя [2]. С позиции компонентного состава технические средства систем охраны периметра включают:

- извещатели (датчики);

– анализаторы и контроллеры;
– приемно-контрольные приборы;
– панели управления;
– средства мониторинга и наблюдения.

Как отмечается автором в [2], СОП имеют ряд качественных особенностей, которые отличают их от других систем охраны. Так, СОП отличаются по принципам действия, конструктивным исполнениям и вариантам конфигурации. При этом большинство периметральных систем используются для охраны открытых территорий в условиях непрерывного воздействия неблагоприятных природных факторов.

На этапе выбора СОП крайне необходимо получить наиболее детальную информацию по условиям применения и эксплуатации, ограничений по применению СОП и остальных критериев. Такая информация может быть отображена в техническом задании на проектирование и использована при подготовке эскизного проекта. Стоит понимать, что выбор любого технического средства охраны, в том числе, и систем охраны периметра, предполагает последовательное выполнения ряда пунктов ”жизненного” цикла ТСО. Согласование требований и внесение изменений на ранних этапах ”жизненного” цикла позволяет в дальнейшем эксплуатировать СОП с наиболее эффективными параметрами. Основные критерии выбора систем охраны периметра на этапе проектирования представлены на рис.1

Рис. 1. Критерии выбора систем охраны периметра на стадии проектирования

Классификация СОП достаточно обширна. Исходя из задач, представленных в техническом задании на проектирование СБ, могут выбираться проводные или беспроводные решения. Также следует понимать, что не все решения в сфере СОП требуют наличия физических барьеров и ограждений. Так, например, применение сейсмических СОП обусловливается установкой сейсмических датчиков в грунт, на глубину 0,5 метра. Такой тип монтажа позволяет скрытно эксплуатировать систему и делает ее остаточно эффективной для обнаружения нарушителя, при этом не требуя физического крепления на элементы ограждений. Также физические заграждения необязательны для применения радиолучевых и инфракрасных систем. В то же время, технология применения вибрационных, емкостных или электрошоковых систем охраны периметра подразумевает монтаж элементов СОП на конструкции ограждений.

Как отмечается в [3,4], общая классификация СОП может включать в себя следующие типы систем:

- радиолучевые
- радиоволновые (ЛВВ)
- инфракрасные (активные и пассивные)
- емкостные
- оптоволоконные
- оптико-электронные
- вибрационные
- сейсмические
- магнитометрические
- электрошоковые

Основой любой СОП является датчик, основная задача которого - улавливать изменение ”нормированного” сигнала. Как отмечается в [5, с.41], принято применять классификацию датчиков с разделением на следующие типы:

- пассивные и активные датчики;
- датчики скрытой и открытой установки;
- объемные и линейные датчики;
- стационарные и быстроразвертываемые датчики

При таком многообразии технологий, способов реализации, особенностей проектирования, монтажа и обслуживания систем охраны периметра обоснование выбора должно базироваться на критериях выбора оптимальных решений. Как отмечает в своей работе Ю.Тарасов, «выбор оптимального варианта построения СОП осуществляется на основе сравнительного анализа их основных характеристик, в первую очередь, таких, как эффективность и стоимость» [6]. Кроме указанных выше базовых параметров, при выборе оптимального варианта следует также рассматривать характеристики, при помощи которых можно оценить конкретные свойства (функциональные требования) системы охраны периметра. К таким могут относиться адаптивность, сбалансированность, гарантированность, унифицированность и устойчивость.

Рассмотрим более детально критерий эффективности СОП. Говоря об эффективности, принимается, что вероятность обнаружения нарушителя системой охраны должна быть максимальной, а вероятность ложных срабатываний – минимальной. Удобно использовать качественные оценки (баллы) показателей надежности обнаружения и устойчивости к ложным тревогам, которые принято называть потенциалом обнаружения и потенциалом ложных тревог [7]. Так, согласно данной методике, вероятность обнаружения нарушителя оценивается в диапазоне от низкой (ниже 0,7) до очень высокой (0,98 и выше). Всего в данной модели применяется 5 этапов оценки вероятности. Похожий принцип используется для измерения частоты ложных тревог, где 5 этапов распределены от очень низкой частоты ложных тревог до очень высокой. При оценке показателей выявления нарушителя рассматриваются различные способы преодоления нарушителем периметра. Так, кроме стандартной ходьбы и бега, в оценке задействованы такие способы передвижения нарушителя, как подкоп, перелезание через заграждение, разрезание заграждения, прыжки, перекаты и т.д. Применяя такой подход, появляется возможность оценить любую систему охраны периметра по показателю суммарного потенциала выявления нарушителя. На рис. 2 представлена зависимость потенциала выявления нарушителя от типа используемой СОП.

Как видно из графика, максимальным потенциалом выявления нарушителя при использовании различных способов преодоления периметра обладают сейсмические СОП. Для потенциала ложных тревог наоборот, лучшими являются наименьшие, а не наибольшие значения.

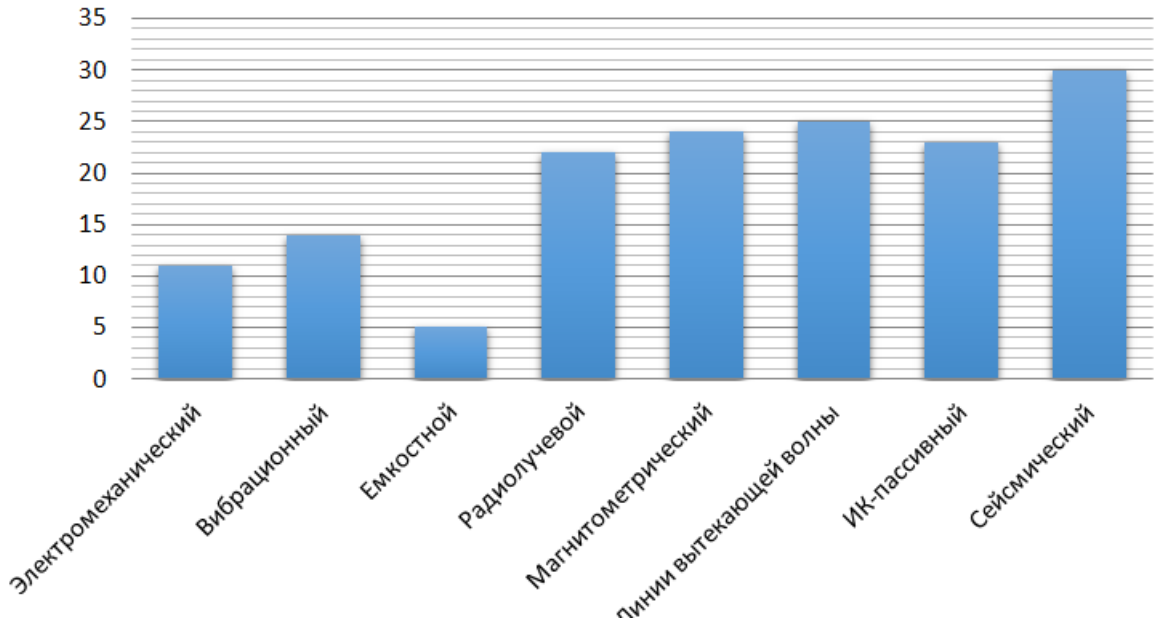


Рис. 2. Зависимость потенциала выявления нарушителя от принципа действия СОП

Выводы. Подводя итоги, хочется отметить, что выбор СОП для объекта информационной деятельности является достаточно сложной и масштабной задачей. Использование алгоритмов вычисления потенциалов обнаружения и ложных тревог для различных типов ТСО выступает одним из методов решения такой задачи. При этом, конечно, немаловажным фактором, помимо технической эффективности, будет выступать стоимость СОП. Здесь показатель ТСО (совокупная стоимость владения) должен учитывать проектные работы, стоимость оборудования и материалов (систем ограждений, технических средств охраны, систем наблюдения и оповещения), монтажные и пусконаладочные работы, а также сервисное обслуживание.

Литература

1. Дворський М.М., Палатченко С.М. Технічна безпека об’єктів підприємництва, І том. - Київ: Видавництво "А-ДЕПТ", 2006. – 302 с.
2. Кукушкин В. Первый рубеж охраны объекта - защита периметра [Електронний ресурс] / Виталий Кукушкин // Медиапортал о безопасности "Хранитель". – 2007. – Режим доступу до ресурсу: http://www.psj.ru/saver_people/detail.php?ID=7760.
3. Классификация технических средств охраны периметра [Електронний ресурс] // Портал "ОхранПроект - Системы безопасности" – Режим доступу до ресурсу: http://www.ohranproekt.ru/fireguard/2/see5.html.
4. Рувинова Э. Охрана периметров. Средства обнаружения и сигнализации / Э. Рувинова. // Электроника: Наука, технология, бизнес. – 2001. – С. 48–51.
5. Варнеев Н. Системы охраны периметра – задачи и проблема выбора / Н. Варнеев, В. Никитин. // БДИ. – 2006. – С. 40–47.
6. Тарасов Ю. Моделирование систем охраны периметра / Ю. Тарасов. // Алгоритм безопасности. – 2012. – С. 60–62.
7. Петровский Н. П. Периметровые ТСО: особенности выбора / Н. П. Петровский. // Системы безопасности. – 2000.

УДК 004.056.5;057.2

Стайкуца С.В.,к.ф.н., доц. каф. ІБ та ПД
Одеська національна академія зв'язку ім. О.С.Попова,
s.staikuca@gmail.com
Кільдішев В.Й., к.т.н., доц. каф. ІБ та ПД
Одеська національна академія зв'язку ім. О.С.Попова,
vit.kildishev@gmail.com
Дергач В.Г.,
Одеська національна академія зв'язку ім. О.С.Попова
dergach.viktor@gmail.com
Науковий керівник - к.т.н., Кільдішев В.Й.

АНАЛІЗ ОСНОВНИХ РИЗИКІВ ІТ-ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА

Анотація. *В роботі показано актуальність використання ІТ-інфраструктури в роботі підприємств. Розглянуто базові відомості щодо напряму інформаційної інфраструктури сучасного підприємства – ключові ознаки, компонентний склад, типи систем за критерієм безперервності роботи. Проведено аналіз ІТ-інфраструктури з позиції життєвого циклу. Детально розглянуто основні загрози ти ризики інформаційної інфраструктури, в рамках чого представлено класифікацію загроз ІТ-інфраструктури з позиції реалізації. Запропоновано базові методи захисту інформаційної інфраструктури.*

ІТ-інфраструктура - це досить складна і неоднорідна система, яка об'єднує всі інформаційні технології та ресурси, що використовуються конкретною організацією або компанією. ІТ-інфраструктура включає в себе сукупність інформаційних центрів, підсистем, банків даних і знань, систем зв'язку, центрів управління, апаратно-програмних засобів і технологій забезпечення збору, зберігання, обробки і передачі інформації, а також забезпечує доступ споживачів до інформаційних ресурсів. Якісний та кількісний склад інформаційної інфраструктури підприємства залежить від ряду критеріїв, наприклад, масштабу, обраної бізнес-моделі, стратегічних планів керівництва, виду господарської діяльності, кількості та кваліфікації персоналу, загального рівня автоматизації тощо.

Слід відзначити,що інформаційна інфраструктура (ІТ) - це не просто набір окремих рішень, які об'єднані в рамках одного підприємства, а багаторівнева комплексна система, що підтримує життєдіяльність всієї організації. Ефективно побудовану інформаційну інфраструктуру підприємства відрізняють три ключові ознаки:

- комплексне функціонування всіх частин інформаційної системи;
- промислова і функціональна сумісність;
- максимальний комфорт у використанні.

До основних складових інформаційної інфраструктури відносяться обладнання, комунікаційне середовище та програмне забезпечення. Компонентний склад інформаційної інфраструктури може поділятися на базовий і додатковий. Так, базовий склад інфраструктури задовольняє основні потреби організації в сервісах, необхідних для роботи та є платформою для підтримки і розгортання служб і додатків, критичних для бізнесу компанії. У зв'язку з цим надійність інфраструктурного ядра повинна знаходитися на високому рівні. Декілька слів щодо надійності та безперервності роботи інформаційної інфраструктури. В міжнародній практиці прийнята класифікація, яка характеризує ІТ-системи з позиції втрат для бізнесу, де основним критерієм оцінки виступає час аварійного відновлення. Так, наприклад, вихід з ладу систем типу Business Critical (системи, що критично важливі для бізнесу, з режимом роботи 24×7×365) тягне за собою серйозні втрати для бізнесу. Рекомендований час аварійного відновлення подібних систем - не більше 2-х годин. Для таких систем повинні використовуватися кластерні рішення і інфраструктурні рішення з частковим резервуванням компонентів. Класифікація ІТ-систем за рівнем безперервності представлена на рис. 1.

Рис. 1. Класифікація ІТ-систем за рівнем безперервності

На різних етапах життєвого циклу в площині ІТ-інфраструктури підприємства можлива реалізація різних загроз і ризиків. Під "життєвим циклом" розуміється час, який починає свій відлік з моменту прийняття рішення про необхідність створення ІТ-інфраструктури і закінчується в момент її повної зупинки. В цілому спільне бачення життєвого циклу ІТ як системи в цілому, так і кожного з її компонентів, дозволяє більш ефективно використовувати ресурси підприємства, оптимізувати економічні показники, виявляти загрози та використовувати найбільш ефективні методи і засобів захисту. Структуру "життєвого" циклу визначає міжнародний стандарт ISO/IEC 12207. Відповідно до даного стандарту, структура "життєвого" циклу базується на трьох основних групах процесів:

1. Основні процеси (придбання, поставка, впровадження, експлуатація, супровід, обслуговування);

2. Допоміжні процеси, спрямовані на забезпечення основних процесів (документування, управління конфігурацією, забезпечення якості, безпеки, верифікація, атестація, оцінка, аудит, дозвіл проблем);

3. Організаційні процеси (управління проектами, створення інфраструктури проекту, визначення, оцінка та поліпшення самого життєвого циклу інфраструктури, навчання) [1];

Варто відзначити, що знання основних етапів “життєвого циклу” ІТ-інфраструктури дозволяє виявити приховані раніше інформаційні потужності, збільшити час використання апаратних та програмних засобів, провести документування та опис ІТ-процесів, скласти моделі загроз, провести картографування існуючих ризиків, обрати методи та засоби захисту тощо. Як результат, оптимізація показнику сукупної вартості володіння TCO (Total Cost of Ownership) та більше ефективне використання матеріальних коштів на етапах експлуатації та обслуговування.

Так, інвентаризація, як рішення для збільшення "життєвого" циклу ІТ-інфраструктури, дозволяє виявити ПЗ з вичерпаним терміном підтримки, морально-застаріле обладнання, несанкціоновані програмні і апаратні засоби тощо. Завдяки інвентаризації ІТ-служба підприємства отримує можливість оперативно реагувати на поточні події. Правильно проведена інвентаризація дозволяє досить ефективно управляти апаратними та програмними ресурсами, які присутні на балансі підприємства. З точки зору управління обладнанням, тут можна говорити про можливість виявлення виходу з ладу або розкрадання врахованого обладнання, а так само про виявлення стороннього (шкідливого) обладнання [2].

Як підкреслювалося раніше, на ІТ-інфраструктуру підприємства може бути направлено ряд загроз і ризиків як антропогенного, так і технологічного характеру. Варто відзначити, що роль антропогенного чинника в інформаційній безпеці досить висока. Не є винятком і моделювання загроз для інформаційної інфраструктури підприємств. Так, з такої позиції основними загрозами інфраструктур підприємств, в залежності від роду господарської діяльності, масштабів, тощо можуть виступати уряди недружніх держав, терористи, промислові шпигуни та організовані злочинні угруповання, а також хактивісти та хакери. Варто відзначити, що перераховані вище загрози можна віднести до зовнішніх загроз антропогенного характеру.

При цьому, незважаючи на загальноприйнятну думку про те, то основні загрози несуть зовнішні порушники, реальна загроза часто виходить саме з внутрішнього інформаційного поля компаній. Так, загальновідомо, що 70-80% всіх порушень в корпоративному середовищі доводиться на долю інсайдерів. Досить інформаційно потенційні дії інсайдера представлено в рамках моделі шкідливих дій в [3]. Отже, інсайдер – це людина, допущена до роботи з інформацією, яка призначена для строго обмеженого кола осіб. "Психологічний" портрет інсайдера може різнитися в залежності від його мотивації, рівня підготовки, посади, рівня лояльності до керівництва і компанії в цілому, звичок та хобі, зв'язків з конкурентами, криміналітетом тощо.

Небезпека інсайдерської загрози полягає в тому, що співробітник підприємства, на відміну від зовнішнього порушника, володіє наступними характеристиками:

– знання та посадові повноваження;
– зв'язки і можливість отримання інформації від інших співробітників;
– можливість очікування найбільш «зручного» (відомого і очікуваного) моменту вчинення: профілактичні роботи, тимчасове делегування більших повноважень та ін.;
– велика можливість вступу в змову з іншими співробітниками з «відсутніми» для створення інциденту посадовими повноваженнями.

При цьому завжди є багато груп співробітників, які можуть вчинити будь-який злочин виходячи із сукупності їх посадових повноважень.

Проте варто зазначити, що вчинення злочину може відбутися тільки при наявності трьох умов:

– нагальна потреба;
– психологічна готовність;
– можливість бездоказового вчинення.

При цьому відсутність хоча б одного з цих умов призводить до неможливості здійснення злочину.

На рис. 2 представлена загальна класифікація загроз, спрямованих на інформаційну інфраструктуру підприємства. Так, наприклад, в якості загроз безпеки для технічних засобів виступають як антропогенний фактор (зовнішні и внутрішні порушники), так і природні явища.

Рис. 2. Класифікація загроз IT-інфраструктури з позиції реалізації

Як зазначається в [4], «втрата або знищення важливої інформації часто стає критичною проблемою, приводячи до фінансово - репутаційних втрат або повного знищення бізнесу». Експоненціальне зростання обсягів інформації та формування нових вимог до бізнесу, виявлення загроз і ризиків робить формування системи захисту IT-інфраструктури основним завданням керівництва компаній.

Аналіз методів і засобів захисту IT-інфраструктури базується на твердженні, що фундаментально існують 3 складових безпеки IT, які включають в себе:

– засоби фізичного захисту (засоби захисту кабельної системи, систем електроживлення, засоби архівації, дискові масиви, ТЗО тощо)

– програмні засоби захисту (антивірусні програми, системи розмежування повноважень, програмні засоби контролю доступу.

– адміністративні (організаційні) заходи захисту, що включають контроль доступу в приміщення, розробку стратегії безпеки фірми, плани дій в надзвичайних ситуаціях, елементи безперервності бізнес-процесів, навчання персоналу тощо.

Як відзначають автори в [5], тільки за рахунок впровадження організаційно-технічних методів контролю кількість потенційних порушників суттєво зменшується (з 85% до 12%).

Литература

1. Стайкуца С. В. Анализ IT-инфраструктуры современного предприятия с позиции "жизненного" цикла / С. В. Стайкуца, В. А. Аверьянов // 71-ша науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів та студентів. – 2016. – С. 95–98

2. Инвентаризация ИТ-ресурсов как шаг к информационной безопасности предприятий. // Защита информации. INSIDE. – 2015. – №2. – С. 73–75.

3. Стайкуца С. В. Ідентичність об'єктів інформаційної мережі як елемент моделі кібербезпеки / С. В. Стайкуца, В. Й. Кільдішев. // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2016. – С. 185–190.

4. Стайкуца С. В. Стратегия выживания / Сергей Владимирович Стайкуца. // Бизнес и безопасность. - 2016. - С. 32-33.

5. Кононович В.Г. Визначення ідентичності об’єктів у системі соціальної та інформаційної безпеки / В. Г.Кононович, І. В. Кононович, С. В. Стайкуца, О. О. Цвілій. // Сучасний захист інформації. – 2015. – С. 19–28.

УДК 004.056.53 (083.73)

Степаненко І.В.
Національний авіаційний університет
stepanenko.iryna.v@gmail.com
Лозінський І.Л.
Національний авіаційний університет
i.l.lozinsky@gmail.com
Кінзерявий В.М.
Національний авіаційний університет
v.kinzeryavyy@gmail.com

ПРОГРАМНИЙ ЗАСТОСУНОК ОБФУСКАЦІЙНОГО ЗАХИСТУ

Анотація.*У даній роботі був проведений аналіз існуючих обфускаційних застосунків, визначені основні переваги та недоліки їх роботи. Аналіз існуючого програмного забезпечення показав, що програмні застосунки не є досконалим, реалізована недостатня кількість обфускаційних перетворень для унеможливлювання проведення процесу реверс-інжинірингу. На основі отриманих даних був представлений обфускаційний додаток, який*

базується на обфускаційному методі захисту «StiK». Для даного програмного застосунку розроблені вимоги роботи та представлений псевдокод програми.

Аналіз захищеності програмного забезпечення є однією з першочергових задач для безперервності роботи компанії. Розроблені та встановленні програмні продукти повинні бути захищені від проведення несанкціонованого аналізу виконуючих файлів програми, відновлення алгоритму роботи, знаходження незахищених місць у коді та проведення процесу модифікації.

Основною проблемою для забезпечення захисту програмного забезпечення на території України є відсутність необхідного правового регулювання з боку держави та відсутність розробленого механізму захисту від процесу реверс-інжинірингу. Компанія повинна самостійно впроваджувати системи для захисту програмного забезпечення. Одним із видів даного захисту є використання обфускаційних застосунків, які за допомогою певних обфускаційних перетворень ускладнюють процес аналізу та модифікації початкового коду програми. Був проведений аналіз сучасних обфускаційних програм, встановлені основні переваги та недоліки у їх роботі.

Для забезпечення захисту програмного забезпечення був проаналізований програмний додаток StarForce C++ Obfuscator розроблений російською компанією «ПротекшенТехнолоджи». Даний обфускатор проводить трансформацію коду написаних на мові C/C++ та направлений на зміну логіки роботи програми. StarForce C++ Obfuscator використовує декілька достатньо ефективних обфускаційних перетворень: введення помилкових зв'язків, об'єднання ділянок коду. Використовувати дану програму можна на операційних системах Windows, Mac, Linux, iOS, Android. Однак основними недоліками даного додатку є необхідність покупки ліцензованого програмного забезпечення, відсутність пробної демонстраційної версії та не достатня кількість реалізованих обфускаційних перетворень для забезпечення захисту від процесу реверс-інжинірингу.

Програмний застосунок C/C++ Obfuscator розроблений компанією Stunnix. Даний продукт може бути встановлений на Windows (з WinXP до Win10), Mac OS (починаючі з версії 10.4) та Linux. Однак трансформація програмного коду відбувається лише за рахунок зміни назви файлів, каталогів та змінних, також проводить видалення коментарів та з’єднання рядків коду. Даний програмний застосунок можна безкоштовно використовувати протягом трьох місяців, проте з облежаним діапазоном функцій.

C++ SourceCodeObfuscator – це програмний застосунок для протидії реверс-інжинірингу, розроблений компанією SemanticDesigns. Обфускаційний метод захисту даної програми базуються на технології SD DMS SoftwareReengineeringToolkit – надзвичайно узагальненому аналізі програмного забезпечення та зміні масиву коду. C++ SourceCodeObfuscator трансформує початковий код за допомогою видалення коментарів, відступів пробілів; проводить перейменування ідентифікаторів програми (змінних, функцій). Однак даний продукт не підтримує операційні системи вище Windows 8, не має розробленої пробної версіє та реалізує не достатню кількість обфускаційних перетворень.

Відповідно до проведеного аналізу існуючих програмних додатків для обфускаційного захисту програмного забезпечення, які використовуються для мовах програмування C/C++, були встановленні наступні недоліки: відсутність демонстраційної пробної версіїроботи обфускатора; не достатня кількість реалізованих обфускаційних перетвореньдля забезпечення захисту початкового коду від процесу реверс-інжинірингу; велика вартість за ліцензовану версію обфускатора.

Тому *актуальним завданням* є розробка надійного обфускаційного застосунку для захисту програмного забезпечення від процесу реверс-інжинірингу.

Метою роботи є розробка надійного обфускаційного застосунку, який за рахунок достатньої кількості обфускаційних перетворень, дозволить забезпечити захист програмного коду від процесу реверс-інжинірингу.

Для досягнення поставленої мети був розроблений обфускаційний метод захисту «StiK». До цього методу висувалися наступні вимоги:

1. Трансформований код програми повинен суттєво відрізнятися від його початкового коду, проте залишатися дієздатним і виконуватиме ті самі функції.

2. Алгоритм роботи початкового коду та трансформованого коду повинен буди різним.

3. Проведення процесу аналізу трансформованого коду повинен займати більше часу та буди більш складним, ніж аналіз початкового коду.

Запропонований програмний застосунок для захисту програмного забезпечення був розроблений на основі обфускаційного методу захисту «StiK». Далі представлений псевдокод запропонованого програмного застосунку.

Input: $NameFile$ − ім'я файлу із початковим кодом, перетворення S, P, V.

Output: $NameFileNew$ − ім'я файлу із трансформованим кодом D.

1. $A = OpenFile(NameFile)$;

2. $\{A_x\} = DivFunction(A)$, $A = (A_1,...,A_n)$, A_x – логічна частина A, $n \in N$, $x = \overline{1,n}$;

3. $for(x = 1; x \le n; x++)$

3.1. $\{A_x\} = FunGoTo(\{A_x\})$

3.2. $for(x_1 = 1; x_1 \le 3; x_1++)$

3.2.1. $\{i\} = FunRand(S)$;

3.2.2. $A_x = CodeStructure(A_x, S, i)$, $i \in \overline{1,6}$;

3.3. $\{A_x\} = FunGoTo(\{A_x\})$

3.4. $B = AssociationF(\{A_x\})$;

4. $\{B_y\} = DivFunction(B)$, $B = (B_1,...,B_m)$, B_y – логічна частина B, $m \in N$, $y = \overline{1,m}$;

5. $for(y = 1; y \le m; y++)$

5.1. $\{B_y\} = FunGoTo(\{B_y\})$

5.2. $for(y_1 = 1; y_1 \le 2; y_1++)$

5.2.1. $\{j\} = FunRand(V)$;

5.2.2. $B_y = VariableFun(B_y, V, j)$, $j \in \overline{1,4}$;

5.3. $\{B_y\} = FunGoTo(\{B_y\})$

5.4. $C = AssociationF(\{B_y\})$;

6. $\{C_z\} = DivFunction(C)$, $C = (C_1,...,C_g)$, C_g – логічна частина C, $g \in N$, $z = \overline{1,g}$;

7. $for(z = 1; z \le g; z++)$

7.1. $\{C_g\} = FunGoTo(\{C_g\})$

7.2. $for(z_1 = 1; z_1 \le 1; z_1++)$

7.2.1. $C_z = PunctionFun(C_z, P, z)$;

7.3. $\{C_g\} = FunGoTo(\{C_g\})$

7.4. $D = AssociationF(\{C_z\})$;

8. $Cheking(D)$

9. $WriteFile(D, NameFileNew)$

Відповідно до представленого псевдокоду програма виконує послідовно три категорій обфускаційних перетворень: перетворення структури коду, змінних та пунктуаційні перетворення. У кожному з блоків трансформації реалізовано більше двох обфускаційних перетворень. Також після кожного етапу трансформаціїпроводиться додаткове обфускаційне перетворення з використанням міток безумовних переходів (функція goto).

Висновки. У даній роботі розглянута проблема забезпечення захисту програмного забезпечення від проведення процесу реверс-інжинірингу. Проаналізувавши сучасне обфускаційне забезпечення, що використовується для заплутування початкового коду, було встановлено, що механізм захисту є недосконалим: у програмах використовуються лише декілька обфускаційних перетворень (видалення токенів, перейменування ідентифікаторів введення помилкових зв'язків, об'єднання ділянок коду); дані програмні застосунки потребують оплати за ліцензію, а демонстраційна версія обфускатора або відсутня, або має обмежений перелік функцій. На основі отриманих даних був представлений обфускатор, який використовує обфускаційний метод захисту «StiK». Для даного обфускатора розроблені основні вимоги роботи та описаний псевдокод із загальним описом функцій, що будуть використовуватися у ньому. В подальшому планується проведення експериментальних досліджень та порівняннятриманихрезультатівіз вже існуючими обфускаційними програми.

Література

1. Каплун В.А. Захист програмного забезпечення: навч. пос. / В.А. Каплун, О.В. Дмитришин, Ю.В. Баришев – Вінниця : ВНТУ, 2014. – 105 с.

2. Кінзерявий В.М. Обфускаційний метод захисту програмного коду / В.М. Кінзерявий, І.В. Степаненко, І.Л. Лозінський // Вісник інженерної академії України : науковий журнал. – Київ, 2016. – Вип. 2. – С. 81-85.

3. Степаненко І.В. Обфускаційний алгоритм захисту / І.В. Степаненко, І.Л. Лозінський // Пятаміжнар. наук.-техн. конф. «ITSEC» / Кафедра безпеки інформаційних технологій Національного авіаційного університету. – Київ : НАУ, 2016. – С. 81.

4. Сучасні обфускаційні методи захисту програмного коду / І.В. Степаненко, В.М. Кінзерявий, А.А. Наджі, І.Л. Лізінський // Безпека інформації. Ukrainian ScientificJournalofInformationSecurity. – 2016. – №1– С. 32-37.

5. A genericapproachtoautomaticdeobfuscationofexecutablecode / B. Yadegari, B. Johannesmeyer, B. Whitely, S. Debray. – IEEE SymposiumSecurityandPrivacy (S&P), 2014. – 18 p.

УДК 681.3.06

Теліженко О.Б.
Інститут СЗРУ
tel63@ukr.net

РОЗБИТТЯ ГРУПИ ТОЧОК КРИВОЇ ЕДВАРДСА В ПРЯМУ СУМУ ЦИКЛІЧНИХ ПІДГРУП

Анотація. *У даній роботі розглядаються криві Едвардса, що не містять точок восьмого порядку. Аналізується структура групи точок кривих Едвардса, що мають порядок 4N, де N – велике просте число. Наведений опис розбиття групи точок кривої Едварда на множини, що не перетинаються, згідно її розбиття на пряму суму циклічних підгруп четвертого порядку та максимального простого порядку N.*

Розробники криптографічних систем все більше звертають увагу на еліптичні криві в формі Едвардса (криві Едвардса) [1] як на перспективні для побудови сучасних асиметричних криптографічних систем.

Ці криві є більш привабливі ніж відомі еліптичні криві у канонічній формі [1] за рахунок швидкодії, універсальності закону додавання та наявності афінних координат нейтрального елемента (нуля) абелевої групи точок кривої Едвардса.

Криптографами світу активно вивчається можливість розробки нових стандартів цифрового підпису, що базуються на кривих Едвардса [2]. Знання структури групи точок кривих Едвардса може бути використане для проведення криптографічного аналізу асиметричних систем, що побудовані на основі цих кривих.

Найбільш перспективними з практичної точки зору є криві Едвардса, у яких порядок дорівнює $4N$, де N – велике просте число. Надалі будемо розглядати саме такі криві.

Для доведення криптографічної стійкості систем, що побудовані на основі кривих Едвардса важливе значення має будь-яка інформація про структуру групи точок кривої Едвардса [2].

Крива Едвардса над простим полем F_p, де $p \neq 2$ [1] задається рівністю

$$E: x^2 + y^2 = 1 + dx^2y^2,\ d \in F_p^*,\ d \neq Q_p\ . \tag{1}$$

Для множини точок кривої Едвардса задається операція додавання, відносно якої зазначена множина буде циклічною абелевою групою, що породжується деякою точкою $G = (x, y) \in E$, $x \in F_p$, $y \in F_p$: $E =< G >$.

Точка G називається генератором групи E.

Генератор G будь-якої циклічної групи можна знайти, наприклад, згідно алгоритму, що описаний у [4].

Правила додавання точок кривої Едвардса задаються формулою (2)

$$\forall R, S \in E,\ R = (x_1, y_1),\ S = (x_2, y_2):$$

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right), \tag{2}$$

де $1 - dx_1x_2y_1y_2 \neq 0$, $1 + dx_1x_2y_1y_2 \neq 0$, $\forall x_1, x_2, y_1, y_2 \in F_p^*$.

На відміну від еліптичних кривих у канонічній формі нейтральним елементом групи точок кривої Едвардса буде точка $O = (0,1)$.

Група точок кривої Едвардса має всі властивості, що має будь-яка циклічна і будь-яка абелева група.

Для будь-якої абелевої групи справедлива наступна теорема [4].

Теорема. Будь-яка скінченновизначена абелева група E або є примарною циклічною групою, або нескінченно циклічною, або розкладається у пряму суму скінченної кількості примарних циклічних і нескінченно циклічних груп, і такий розклад єдиний з точністю до ізоморфізму доданків і порядку їх розкладу в сумі.

Доведення теореми в [4].

Група E має порядок $4N$, тому нескінченних підгруп у неї нема.

Згідно зазначеної теореми маємо:

$$E \cong Z\!\!\!/_{2^2} \oplus Z\!\!\!/_{N}\,.$$

У групі E існує єдина підгрупа порядку N [1], яку позначимо H_N та єдина підгрупа порядку 4 [1], яку позначимо M.

Таким чином група E розкладається у пряму суму підгруп H_N і $M =< F >$, де F – точка четвертого порядку:

$$E = M \oplus H_N\,. \tag{3}$$

Згідно (3) будь-яка точка $P = (x, y)$ з групи E може бути представлена в єдиний спосіб в одному з наступних чотирьох варіантів:

$$P = O + R_1,\ P = D + R_2,\ P = F + R_3,\ P = (-F) + R_4,$$

де $R_1, R_2, R_3, R_4 \in H_N$, $D = (0,-1)$, $F = (1,0)$, $-F = (-1,0)$.

Маємо взаємно-однозначне відображення:

$$f: M \times H_N \leftrightarrow E\,. \tag{4}$$

Згідно відображення (4) можна отримати чотири варіанти взаємно-однозначних відображень у відповідності з тим до якого суміжного класу групи точок кривої Едвардса буде належити точка $P=(x,y)\in E$.

1. Якщо $P=(x,y)$ належить суміжному класу $O+H_N$: $P=O+R_1$, де $R_1=(x_1,y_1)$, то згідно (2):

$$P=(x,y)=(x_1,y_1):\ ((0,1),(x_1,y_1))\leftrightarrow(x_1,y_1).$$

2. Якщо $P=(x,y)$ належить суміжному класу $D+H_N$: $P=D+R_2$, де $R_2=(x_2,y_2)$, то згідно (2):

$$P=(x,y)=(-x_2,-y_2):\ ((0,-1),(x_2,y_2))\leftrightarrow(-x_2,-y_2).$$

3. Якщо $P=(x,y)$ належить суміжному класу $F+H_N$: $P=F+R_3$, де $R_3=(x_3,y_3)$, то згідно (2):

$$P=(x,y)=(y_3,-x_3):\ ((1,0),(x_3,y_3))\leftrightarrow(y_3,-x_3).$$

4. Якщо $P=(x,y)$ належить суміжному класу $(-F)+H_N$: $P=(-F)+R_4$, де $R_4=(x_4,y_4)$, то згідно (2):

$$P=(x,y)=(-y_4,x_4):\ ((-1,0),(x_4,y_4))\leftrightarrow(-y_4,x_4).$$

Таким чином ми отримали розбиття групи *E* за множинами точок підгрупи H_N, що не перетинаються:

$$E=\bigcup_{(x,y)\in H_N}\{(x,y),(-x,-y),(y,-x),(-y,x)\}. \qquad (5)$$

Згідно розбиття (5) можливо для кожної точки *kG* кривої Едвардса однозначно визначити множину, де вона буде знаходитися. Цю властивість, а також розбиття групи точок кривої Едвардса за суміжними класами за різними її підгрупами можна використати при проведенні криптографічного аналізу та вирішення задачі *DLP*.

Література

1. Edwards H.M. A normal form for elliptic curves. Bulletin of the American Mathematical Society, Volume 44, Number 3, july 2007, Pages 393-422.

2. Бессалов А.В., Дихтенко А.А. Криптостойкие кривые Эдвардса над конечными полями // Прикладная радиоэлектроника. – 2013. – 12, №2. – С. 285-291.

3. Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривих: Учебное пособие. – Киев: ІВЦ “Политехника”, 2004, – 224 с.

4. Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра: В 2-х т. М.: Гелиос-АРВ, 2003.

УДК 621.391.7

Тихонов В.И..
ОНАС им. А. С. Попова
victor.tykhonov@onat.edu.ual
Тихонова Е. В.
ОНАС им. А. С. Попова
elena.tykhonova@onat.edu.ua
Березовский В.В.
Аспирантура ОНАС им. А. С. Попова
vasiliy.berezovsky@gmail.com

АЛГОРИТМ ШИФРОВАНИЕ ДАННЫХ В КАНАЛЕ СВЯЗИ НА ОСНОВЕ КВАНТОВЫХ РЕГИСТРОВ С ТРОИЧНЫМИ РАЗРЯДАМИ

Аннотация. *В работе предложен алгоритм кодирования и шифрования данных в цифровом канале на основе квантовых регистров переменной длины с троичными разрядами. Особенность предложенного алгоритма шифрования заключается в*

использовании метаязыка управления процессом обмена данными, алфавит которого образуют избыточные состояния квантового регистра. Данный способ позволяет изменять степень защищенности канала связи путем вариации длины передаваемых символов и размеров соответствующих таблиц шифрования.

Защита каналов связи занимает важное место в общей системе обеспечения информационной безопасности. Само понятие «канал информационной связи» может иметь различные уровни интерпретации. В данной работе мы будем рассматривать понятие «канал связи» в достаточно узком смысле как телекоммуникационную подсистему, образованную двумя цифровыми приемо-передатчиками, соединенными физической линией связи, на которую могут воздействовать различного рода естественные (непреднамеренные) и искусственные (преднамеренные) помехи, а также может иметь место пассивный и/или активный несанкционированный доступ (НСД). В канале связи существует множество различных типов угроз, и в зависимости от каждого из них разрабатываются специфические методы борьбы с ними [1]. Основной единицей приема-передачи данных на канальном уровне являются символы или блоки символов. Простейшим символом передачи данных является бит. Современные телекоммуникационные системы используют более крупные символы, содержащие от 2 до 64 бит и более. Главная цель борьбы с естественными помехами в канале связи – это повышение достоверности передаваемой информации, формализуемой по выбранному критерию, например ограничением вероятности приема ложного символа.

По отношению к каналу связи будем различать два понятия: «физическая скорость передачи» (ФСП) символов независимо от их семантического содержания, и «содержательная скорость передачи» (ССП), которая определяется объемом полезной информации, передаваемой в единицу времени. При заданном способе кодирования символов, ФСП можно изменять путем вариации тактовой частоты. Существует определенная закономерность в канале связи – при прочих равных условиях, увеличение ФСП приводит к увеличению вероятности ложного приема символов. Для компенсации этого явления применяют т.н. избыточное кодирование, при котором на передающей стороне содержательные блоки символов отображаются в расширенные блоки передачи, анализ которых на приемной стороне канала позволяет обнаружить либо исправить ошибки определенных типов. При одинаковой ФСП, увеличение избыточности передаваемых блоков символов приводит к снижению ССП, но при этом уменьшает вероятность ошибок; это, в свою очередь, позволяет увеличить тактовую частоту передачи.

В результате совместного влияния двух факторов (увеличения избыточности и одновременного опережающего увеличения ФСП) может быть достигнуто общее увеличение ССП. Однако кривая роста ССП при этом имеет асимптотический характер и переходит в насыщение, т.е. при определенной физической скорости передачи символов ее дальнейшее увеличение практически полностью компенсируется необходимым увеличением избыточности. Рис. 1 иллюстрирует качественный характер зависимости между ФСП и ССП. Значения ФСП и ССП показаны в условных относительных безразмерных единицах. Предельное значение ССП может рассматриваться как теоретически возможная пропускная способность канала (ПСК). Приближение к ПСК за счет увеличения избыточности и физической скорости передачи приводит к увеличению аппаратно-программных ресурсов, необходимых для кодирования и декодирование информации, передаваемой по каналу связи.

Для защиты информации от несанкционированного доступа типа «прослушивание» используют различные методы криптографии: замена (подстановка) символов, перестановка, аналитические преобразования шифруемых данных, гаммирование (сложение случайных чисел т.н. гамма-последовательности с числовыми кодами шифруемых символов в каком-либо конечном поле, например, в поле Галуа).

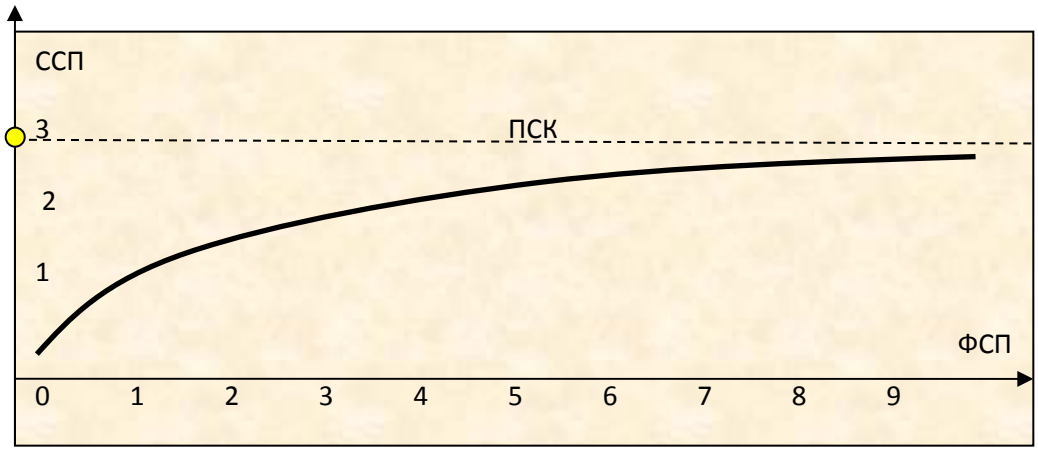


Рис. 1. Качественный характер зависимости между физической скоростью передачи данных (ФСП) в канале связи и содержательной скоростью передачи (ССП); ПСК – теоретически возможная пропускная способность канала.

Простой и очевидный по реализации метод шифрования – это замена передаваемых символов на символы из того же самого алфавита, осуществляемая по секретным таблицам шифрования. На основе этого метода можно построить теоретически идеальный алгоритм, который в принципе не поддается дешифровке при отсутствии таблицы шифрования. Для этого достаточно, чтобы множество символов подстановки образовывало «чисто случайную последовательность» длиной не менее передаваемого сообщения (с равной вероятностью всех символов подстановки и нулевой корреляцией между любой парой символов подстановки). Ограничения такого метода шифрования обусловлены техническими возможностями создания, обмена и хранения таблиц шифрования больших размеров. В условиях дальнейшего повышения скоростей передачи и уменьшения количества энергии для переноса единицы информации в современных оптических каналах связи начинают проявляться квантовые эффекты, связанные с неопределенностью идентификации принимаемых символов. С точки зрения детектора принимаемого сигнала, один и тот символ (например, один бит), генерируемый на передающей стороне канала, может находиться в двух состояниях (ноль и единица). Например, если передатчик генерирует достаточно длинную последовательность единиц, то приемник детектирует некоторую последовательность из нулей и единиц. При этом относительные частоты появления нулей и единиц приближаются к вероятностям их появления; обозначим их как $p(1,0)$ − вероятность детектирования состояния «0» при передаче «1»; и $p(1,1))$ − вероятность детектирования состояния «1» при передаче «1».

Аналогичным образом если передатчик генерирует достаточно длинную последовательность нулей, то вероятности детектирования нуля и единицы обозначим $p(0,0)$ и $p(0,1)$соответственно. Таким образом, свойства симплексного канала связи как телекоммуникационной системы (ТКС) «генератор − линия связи − детектор» определяются матрицей вероятностей $\vec{P} = p(i,k)$, где i – значение передаваемого символа, k − значение принимаемого символа. Матрица $\vec{P}$ характеризует телекоммуникационный канал как целостную систему и является чувствительной к изменениям ее физических свойств. Например, при несанкционированном доступе к каналу путем любого вида энергетического взаимодействия с линией связи, матрица $\vec{P}$ изменится в той или иной мере. Свойства канала связи в прямом и обратном направлениях не обязательно совпадают. В общем случае, дуплексный канал связи характеризуется комплексной матрицей вероятностей $\vec{P} = (\vec{P}, \vec{P})$.

Матрица $\vec{P}$ является своеобразным квантовым портретом канала связи, который может быть исследован и зафиксирован на этапе создания ТКС, а затем использован для детектирования принимаемых сигналов, а также для выявления фактов НСД. Если число

возможных квантовых состояний сигнала на принимаемой стороне равно двум, то по аналогии с детерминированными системами, вместо понятия «бит» вводят понятие «кубит» (q-бит, кьюбит, − от quantum bit). Для символов с тремя возможными состояниями эквивалентным понятием является «кутрит». В общем случае для произвольного количества возможных квантовых состояний введено понятие «кунит» или «квантовый регистр» [2].

В работе [3] предложен способ троичного кодирования отдельных разрядов символа передачи данных по когерентному оптическому или радиоканалу с помощью кусочно-линейных функций фазовой модуляции. В данном методе количество разрядов символа может динамически изменяться от минимального значения 1 до 256 в зависимости от текущего состояния канала связи, условий распространения электромагнитных волн, наличия помех, дальности передачи и других факторов, которые в совокупности определяют пропускную способность канала. Используя данный способ кодирования символов, в данной работе предлагается следующий алгоритм шифрования данных.

Передаваемое сообщение, представленное в виде последовательности нулей и единиц, разбивается на блоки. Длина блока выбирается таким образом, чтобы число квантовых состояний блока двоичных цифр не превышало числа квантовых состояний текущего символа передачи данных с троичными разрядами, таб.1. Рассмотрим случай $n = 4$; при этом размер блока двоичной последовательности равен 6 бит, а множество из 64 состояний блока двоичных данных отображается во множество из 81 состояний квантового регистра из четырех троичных разрядов. Избыточность такого шифрования составляет 81−64=17 состояний.

Таблица 1.

Зависимость размера блока шифруемых двоичных данных от размера символа с троичными разрядами

Количество троичных разрядов в символе передачи данных n	Количество состояний символа передачи данных 3^n	Количество состояний блока двоичных данных 2^m	Длина блока шифруемых двоичных данных m	Избыточность кода шифрования $3^n - 2^m$
1	3	2	1	1
2	9	8	3	1
4	81	64	6	17
8	6561	4096	12	2465
…	…	…	…	

Принцип шифрования данных заключается в следующем. Взаимодействующие стороны заранее обмениваются некоторым набором таблиц шифрования; каждая таблица T имеет размер $L \times 64$, где L – длина таблицы шифрования (количество строк). Каждая строка таблицы шифрования формируется следующим образом. Первый элемент строки является случайным числом из множества 81 чисел в диапазоне от 0 до 80. Второй элемент является случайным числом из множества 80 чисел в диапазоне от 0 до 80, при этом исключено появление первого числа. Третий элемент – это случайное число из множества 79 чисел в диапазоне от 0 до 80, при этом исключено появление первых двух чисел строки, и т.д. В результате такого кодирования, в каждой строке таблицы T окажутся 64 различных случайных чисел. Первая строка кодирует первый символ сообщения, вторая – следующий символ и т.д.

В общем случае, длина L таблицы T предполагается меньшей, чем длина сообщения или последовательности сообщений. Поэтому периодически одни и те же строки таблицы используются для шифрования более чем одного символа в сообщениях, что создает потенциальные возможности для дешифровки в НСД. Для усложнения шифра используется избыточность шифрования. А именно, в каждой строке таблицы T остаются

неиспользованными 17 случайных чисел из диапазона от 0 до 80. Упорядоченные наборы таких чисел в виде таблицы размером $L \times 17$ определяют таблицу шифрования алфавита для специального метаязыка управления процессом шифрования. Этот язык является засекреченным, и может быть использован для вставки специальных скриптов типа «пароль − ответ» в передаваемый текст, для аутентификации сообщений, для переключения таблиц шифрования путем случайного перехода на различные строки таблицы и т.п. Выбирая различную длину символов троичного регистра и длины ответствующих таблиц шифрования, можно варьировать в достаточно широком диапазоне степень защищенности канала связи от НСД. При этом анализ матриц корреляции состояний квантовых регистров с троичными разрядами дает дополнительную возможность обнаруживать факт НСД на физическом уровне лини связи.

Выводы. Защита каналов связи занимает важное место в общей системе обеспечения информационной безопасности. В данной работе рассмотрены некоторые аспекты информационной безопасности канала связи как телекоммуникационной подсистемы из двух приемо-передатчиков, соединенных физической линией связи. Предложен алгоритм кодирования и шифрования данных в цифровом канале на основе квантовых регистров переменной длины с троичными разрядами. Особенность предложенного метода шифрования заключается в использовании метаязыка управления процессом обмена данными, алфавит которого образуют избыточные состояния квантового регистра. Данный метод позволяет изменять степень защищенности канала связи путем вариации длины передаваемых символов и размеров соответствующих таблиц шифрования.

Література

1. Защита каналов связи. Режим доступа: http://www.bezpeka.com/files/lib_ru/book-domarev03/ch_14.pdf .

2. Квантовый регистр и сплетенные состояния. Режим доступа: http://www.intuit.ru/ studies/courses/12176/1169/lecture/24929?page=3.

3. Tikhonov V.I. Piecewise linear phase modulation for ternary data coding in coherent wireless channel. − Вісник національного технічного університету "ХПІ", Серія: Інформатика та моделювання, № 44 (1216), 2016, с.162−169.

УДК 004.056.5:57.087.1

Фесенко А.О. к.т.н.
Асистент кафедри кібербезпеки та захисту інформації
Київський національний університет імені Тараса Шевченка
e-mail:a.fesenko@meta.ua
Рябий М.О. к.т.н.
Начальник відділу забезпечення технічних засобів безпеки
Компанія «Миронівський хлібопродукт»
e-mail:smayluk@ukr.net
Фесенко В.О.
Студент кафедри безпеки інформаційних технологій
Національний авіаційний університет
e-mail:fes_vlad@ukr.net

ВИБІР РОЗРЯДНОСТІ КОДУ В БІОМЕТРИЧНИХ СИСТЕМАХ ІДЕНТИФІКАЦІЇ ПО РАЙДУЖНІЙ ОБОЛОНЦІ ОКА

Анотація. *Автентифікація людини поза всяких сумнівів є актуальним завданням, практичним вирішенням якої зайняті тисячі і мільйони людей по всьому світу. Автоматизація цього процесу важлива складова розвитку сучасного суспільства. Завдання автентифікації і ідентифікації людини тепер вирішуються за допомогою автоматичних*

біометричних систем, складаючи одну з нових областей прикладної математики, біометричну ідентифікацію. Біометрична автентифікація по райдужці, на сьогоднішній день, визнаний лідер по точності і надійності серед біометричних ознак. На даний час іде активне впровадження біометричних технологій на пунктах прикордонного контролю в аеропортах, що в свою чергу викликає значне збільшення об'єму бази даних і вимагають здатність алгоритмів розпізнавання райдужної оболонки працювати в ідентифікаційному режимі пошуку "один до багатьох".

Сучасне суспільство майже не можливо уявити без систем контролю та управління доступом (СКУД). Особливе місце при використанні СКУД, займають біометричні системи ідентифікації, зазначимо, що біометрична система ідентифікації – це система розпізнавання, яка встановлює автентичність специфічних біологічних або поведінкових характеристик властивих користувачеві. Як правило, біометрична система розділена на дві підсистеми: модуль реєстрації та модуль ідентифікації.

Всі біометричні методи мають відповідні переваги та недоліки. Однак, деякі біометричні методи більш зручні, ніж інші, в певних своєрідних аспектах їх застосування. Одним з найбільш універсальних, є метод ідентифікації по райдужній оболонці ока. Даний факт зумовлений тим, що кожна біометрична модельність характеризується за 7 критеріями[1]:

1. Універсальність – кожна людина повинна мати цю характеристику.
2. Унікальність – не повинно бути двох осіб, що мають однакову характеристику. Структура райдужної оболонки людини абсолютно випадкова, а чим більша степінь випадковості, тим більша ймовірність того, що в кожної людини структура райдужної оболонки ока (РОО) буде унікальна. Досліди показали, що текстура РОО має ступінь свободи рівною 250, що наприклад, набагато більше ступеню свободи відбитків пальців, який дорівнює 35 [2].
3. Сталість – характеристика не повинна змінюватися. Структура РОО може змінюватись на протязі життя, тільки внаслідок захворювання ока, таких як катаракта, або механічних пошкодженнях.
4. Вимірність – характеристика повинна мати кількісну міру і вимірюватися досить просто. Текстура РОО цілком відповідає даному критерію
5. Ефективність – можливість ідентифікації , гнучкість методу застосування.
6. Доступність – готовність людей використовувати біометричний метод в повсякденному житті. Зауважимо, що зображення ока людини можливо достатньо легко отримати навіть звичайним цифровим фотоапаратом.
7. Захищеність від підробки – відображає захищеність системи від обману. Структуру РОО людини практично не можливо скопіювати.

Провівши аналіз біометричних характеристик людини, можна зробити висновок, що метод ідентифікації по райдужній оболонці ока має всі перераховані характеристики.

Однак, на даний час біометричні системи ідентифікації працюють в режимі один до одного (Рис1.). Тобто, крім біометричної характеристики, користувач кожного разу при користуванні СКУД додатково надає ще якийсь ідентифікатор (вводить ПІН-код, підносить магнітну карту до зчитувача та інше). Даний факт, звичайно, завдає незручності у використанні таких систем, а саме: користувач витрачає значно більше часу на ідентифікацію, а також установа яка використовує біометричну СКУД витрачає більше коштів на додаткові зчитувачі магнітних карт чи на панелі для вводу ПІН-коду. Дані незручності в більшій своїй мірі викликані не тільки підвищенням рівня безпеки за рахунок багатофакторної ідентифікації (біометричний ідентифікатор і електронна карта чи введення ПІН-коду), а і невирішеними проблемами унікальності запису в базу даних бінарного ідентифікатора для досить великої кількості користувачів (10000 і більше).

Рис. 1. Загальна схема роботи біометричних систем ідентифікації

Провівши аналіз найбільш поширених систем ідентифікації та автентифікації по райдужній оболонці ока (табл.1), неможливо не звернути увагу на те, що у них всіх без виключення, обмежена кількість записів в базі даних. Отже, постає актуальна наукова і практична задача, а саме робота систем біометричної ідентифікації по райдужній оболонці ока в режимі роботи один до багатьох, а це в свою чергу ставить питання вибору розрядності коду, щоб він був ідентичний для бази даних яка могла б охопити все населення землі.

Таблиця 1

Системи найбільш поширені на ринку систем контролю і управлінням доступом з використанням райдужки

Система	Параметри					
	Фокусна відстань, м	Час на зйомку, с	Максимальна кількість записів в БД	Пропускна можливість системи користувачів за хв.	FAR	FRR
LG -3000	0.1	0.04	1000	10	0,00066	0,00078
OKI IRISPASS-WG	0.45	30	1000	1-2	0,00066	0,00078
Panasonic BM-ET300	0.35	0.5	10000	10	0,00066	0,00078
Securimetrics Pier 2.3	0.12	0.008	2000	30	0,00066	0,00078
Sarnoff IOM	3	8	50000	30	0,00066	0,00078
Циркон 4	0.4	2	2000	12-30	0,00066	0,00078

Сучасні вимоги до СКУД заснованих на біометричній ідентифікації по РОО такі, що необхідна здатність алгоритмів розпізнавання райдужної оболонки працювати в ідентифікаційному режимі пошуку "один до багатьох", в якому користувач попередньо не декларуються за допомогою магнітних карт або інших ідентифікаторів (документів), і алгоритми повинні самостійно визначити особистість, здійснивши повний інтенсивний пошук в базі зареєстрованих даних. Таким чином, більшість біометричних технологій спроможні тільки на роботу в верифікаційному режимі порівняння "один до одного". У такому режимі особа спочатку декларується, і програмою для прийняття рішення "так / ні" досить виконати зіставлення з одним зареєстрованим шаблоном, що як вже зазначалось раніше завдає незручностей у використанні.

В світі є приклади використання біометричних СКУД заснованих на особливостях РОО в аеропортах, а саме для пасажирів міжнародних рейсів які використовують свою біометричну характеристик (РОО) замість пред'явлення паспорта. Такі системи запроваджуються в міжнародному аеропорті Heathrow (Лондон) в 2001 р було перше широке застосування даної технології, а також в аеропорту Schiphol (Амстердам, Нідерланди).

Пасажири, які досить часто здійснюють авіаподорожі, змогли взяти участь в програмі Privium і отримати свій Iris-код, занесений в базу даних. Мандрівники які користуються Privium сплачують щорічну абонентську плату і в аеропорті Schiphol мають змогу не стояти в довгих чергах і чекати імміграційної перевірки. Натомість учасники програми автоматично отримують дозвіл на в'їзд до Нідерландів, для цього їм достатньо зафіксувати на декілька секунд погляд прямо перед камерою. Використання новітніх технологій в камері дозволяють : активуватися при наближенні особи, автофокус, автоматичне наближення, позиціонування за допомогою допоміжного дзеркала і голосових підказок, що в свою чергу створює користувацький інтерфейс. Як правило ідентифікація відбувається за декілька секунди, а високий дозвіл і якість одержуваних зображень знижує рівень помилок "відмова в реєстрації" і "відмова в розпізнаванні". Схожий проект "Iris-код як паспорт" - впроваджується в аеропорту Frankfurt / Main, в ньому приймають участь 10000 часто літаючих клієнтів німецької авіаліній. Вже після першого року використання програми, нею щодня користувалось близько 140 пасажирів, а їх число постійно збільшується. Аналогічні програми "Iris-код як паспорт" в рамках проекту IRIS (Імміграційна система розпізнавання райдужної оболонки) були спроектовані і для інших аеропортів, зокрема це - вісім великих канадських аеропортів і 10 терміналів аеропортів Великобританії.

Об’єм баз даних СКУД на базі РОО залежить від розрядності коду. Якщо розрядність коду райдужки 8x256 біт, то ймовірність його повторення ≈1:10000. Звідси, об’єм бази даних має бути менший 10000 записів, тому актуальною є задача отримання стійкого коду райдужної оболонки ока, який не буде повторюватись 2^{33} раз[3].

Так як зараз населення землі $7.3x10^{9}$ людей, то ймовірність співпадіння РОО буде $1.369x10^{-10}$. Для того, щоб код райдужки не повторювався його розрядність повинна бути більше 33 розрядів. Тоді використовуючи, те що сучасні процесори мають 64 розряди і для виключення помилки переповнення розрядної сітки будем використовувати 56 розрядів в одному стовпчику коду РОО, кількість стовпців буде відповідати кутовому дозволу 1^{0}, тобто 360 стовпців. Загальна вірогідність повторення коду РОО буде визначатися як умовна ймовірність 56-ти розрядного коду з можливістю повторення в одному із 360 стовпчиків. Отже, ймовірність має дорівнювати $P(2^{-56}|360)=4,996x10^{-15}$.

Література

1. Фесенко А.О. Основні біометричні характеристики, сучасні системи та технології біометричної аутентифікації/ А.О.Фесенко, В.А.Швець//Безпека інформації. – 2013. – №2, Том 19. – С. 99 – 111.

2. Resources Related to Biometrics and People with Disabilities, international center for disability resources on the internet [Электронный ресурс]. – Режим доступу: http://www.icdri.org/biometrics/biometrics.htm

3. Фесенко А.О. Методи обробки даних для систем ідентифікації та аутентифікації на основі біометричних характеристик ока: Автореф… дис. канд. техн. наук. – Київ: «НВФ «Славутич-Дельфін», 2017. – 20 с.

4. Болл Р.М. Руководство по биометрии: пер. с англ. Н.Е. Агаповой. – М.: Техносфера, 2007. – 368 с.

5. Лебеденко Ю.И. Биометрические системы безопасности. Тула: Изд-во ТулГУ, 2012, 160 с. ISBN 978-5-7679-2377-9

6. Лакни Г. Ф. Биометрия: Учеб. пособие для биол. спец. вузов-4-е ИЗД., перераб. и Доп.-М.: Бысш. шк., 1990. 352 С.

7. Daugman J. High confidence visual recognition of persons by a test of statistical independence [Электронный ресурс] // IEEE Transaction on Pattern Analysis and Machine Intelligence, Vol. 15, NO 11, NOVEMBER 1993. P. 1148 – 1160. Режим доступа: World Wide Web. – URL: http:// www.cl.cam.ac.uk/~jgd1000/ PAMI93.pdf.

УДК 621.391.052

Харлай Л.О.
викладач,
Державний заклад «Київський коледж зв'язку»
Lharlay@i.ua

МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ В ОПТИЧНИХ МЕРЕЖАХ

Анотація *Розглянуто методи захисту від несанкціонованого доступу в оптичних мережах, серед яких принципи додаткового кодування оптичного лінійного коду, що використовується на оптичних мережах, шляхом збільшення кількості одиниць, які входять до складу кодових комбінацій та принципи захисту від несанкціонованого доступу до лінійних споруд мереж зв'язку шляхом рефлектометричного моніторингу імпровізованого коаксіального кабелю, який утворено за рахунок металевих елементів оптичного кабелю.*

Ключові слова: *волоконно-оптична лінія, лінія затримки, кодування, декодування, оптичний кабель, броньовий покров, центральний силовий елемент.*

Збільшення ролі інформації та знань у житті спільноти, збільшення частки інформаційних комунікацій, продуктів та послуг, створення глобального інформаційного простору, який забезпечує ефективну, інформаційну взаємодію людей, їх доступ до світових інформаційних ресурсів та задоволення їх потреб в інформаційних продуктах та послугах призводить до збільшення навантаження на інформаційні мережі та підвищення вимог до безпеки передачі інформації.

Волоконно-оптична мережа забезпечує найбільш надійний захист від несанкціонованого доступу та перехоплення конфеденційної інформації. Така здатність оптики пояснюється відсутністю випромінювань в радіодіапазоні, а також високою чуттєвістю до коливань. У разі спроб прослуховування вбудована система контролю може відключати канал та попереджувати про перехоплення. Існують різні методи захисту інформації на інфокомунікаційних оптичних мережах.

Одним з них є моніторинг ліній для фіксації моменту несанкціонованого доступу до лінії [1]. Іншим методом протидії може бути зміна оптичних лінійних кодів безпосередньо в точці підключення оптичного лінійного тракту. З цією метою запропоновано застосування додаткового кодування оптичних лінійних кодів за допомогою пасивних оптичних пристроїв.

На цей час на оптичних мережах зв'язку має місце використання лінійного коду типу RZ (з поверненням до нуля) [4]. Як показують результати досліджень, при використанні оптичною системою передавання лінійного коду RZ-0,25 існує можливість, використовуючи

виключно такі пасивні оптичні елементи, як оптичні лінії затримки та оптичні розгалужувачі, провести додаткове кодування (маскування) сигналу на вході в лінію з метою захисту інформації, що передається по лінійному тракту.

На рис. 1 наведено метод додаткового кодування лінійного оптичного сигналу з метою захисту його від несанкціонованого доступу до лінійного тракту та подальшого його декодування на приймальному кінці. На рис.2 показано побудову лінійного тракту, що використовує цей принцип.

Як видно з рисунку, вихідний сигнал системи передавання, який водночас є вхідним сигналом для лінійного тракту, на базі коду RZ-0,25, позначений як $I_{вх}$, подається на оптичний розгалужувач (РО). Оптичний розгалужувач працює, як дільник оптичної потужності навпіл. Після чого, на входи другого дільника, що працює в режимі суматора, подається та частина сигналу, що пройшла через оптичну лінію затримки (ОЛЗ) з часом затримки Т/2 ($I_{вих\ (T/2)}$) та незатримана частина сигналу. В результаті цього, на виході другого дільника формуються кодові комбінації, що відрізняються від вихідних подвійною кількістю одиниць (I_{Σ}), які і передаються по лінійному тракту. На виході лінійного тракту включено дільник оптичної потужності навпіл. При цьому на другий дільник, що працює в режимі суматора, подається незатримана частина сигналу, та частина сигналу, що пройшла через оптичну лінію затримки (ОЛЗ) з часом затримки Т/4 ($I_{вих\ (T/4)}$).

Після складання цих частин формується оптичний сигнал, відповідний початковому, тільки в коді NRZ ($I_{\Sigma вихNRZ}$). Подвійна кількість одиниць в оптичному лінійному тракті під час передавання робить неможливим адекватне відновлення сигналу при спробах несанкціонованого доступу до інформації. Таким чином забезпечується захист інформації, що передається.[2]

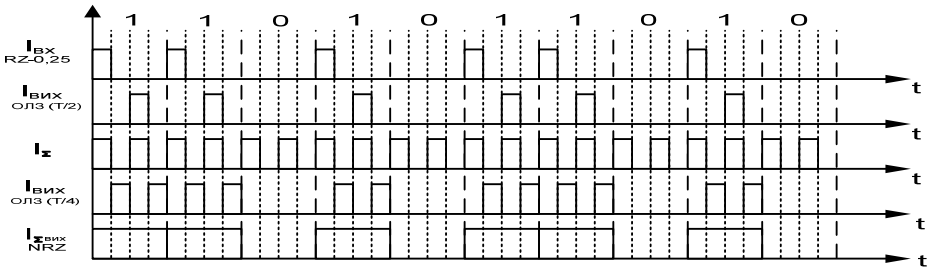


Рис. 1. Метод кодування та декодування оптичного сигналу
в коді RZ-0,25 при передачі його по лінійному тракту

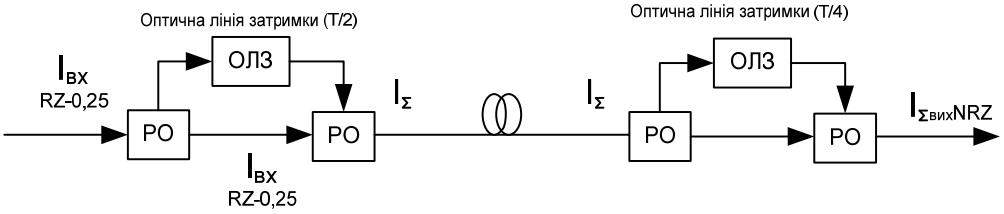


Рис. 2. Побудова лінійного тракту, що використовує кодування
та декодування оптичного сигналу в коді RZ-0,25 за допомогою пасивних елементів

Усе більшого значення набуває проблема захисту від несанкціонованого доступу на рівні лінійно-кабельних споруд.

Завжди існує принципова можливість зняття інформації, що передається по оптичному кабелю (ОК) [3]. Перехоплення інформації можливе лише у випадку порушення цілісності зовнішньої оболонки й інших захисних покровів кабелю з метою безпосереднього доступу апаратури перехоплення до оптичних волокон (ОВ).

Для забезпечення випромінювання за межі ВС в цьому випадку формується вигин оптичного волокна. В місці вигину порушується закон повного внутрішнього відбиття і має

місце випромінювання світлової енергії за межі ВС. Завдяки цьому процесу в точці перехоплення інформації волокно характеризується підвищеним рівнем втрат, і це можна визначити методом оптичної рефлектометрії [4], або за рахунок збільшення коефіцієнту помилок в лінії [5]. В певних випадках визначення факту та місця підключення за допомогою апаратури контролю лінії є проблематичним. Таким чином, існує проблема попередження несанкціонованого доступу ще на початковому етапі демонтажу захисних покровів ОК.

З метою забезпечення неможливості доступу до оптичних волокон ОК та локалізації місця доступу запропонованj метод визначення моменту порушення броньових покривів кабелю. Зазначений метод базується на тому, що в багатьох ОК модульного типу присутні такі елементи конструкції, що у комплексі являють собою імпровізований коаксіальний кабель (КК) [6]. Вони в більшості випадків виготовляються зі сталі й у складі ОК являють собою коаксіальний кабель. Модулі з волокном розташовані навколо центрального силового елементу та захищені броньовим покриттям. Тобто, для одержання вільного доступу до ОВ необхідно повністю зняти броньовий покрив на конкретній ділянці, і це порушує однорідність хвильового опору імпровізованого КК. З цього випливає, що, якщо по імпровізованій коаксіальній парі надходить імпульсний сигнал, то, у випадку усунення броньового покриву у певному місці утвориться обрив провідника коаксіальної пари, і сигнал відбивається в зворотному напрямку від місця обриву. Відбиття імпульсного сигналу має місце навіть при відсутності обриву, але наявності пошкодження броньового покрову, оскільки в лінії з'являється неоднорідність щодо хвильового опору. Зафіксувавши час між поданням сигналу в лінію та надходженням відбитого сигналу можна визначити як факт порушення елементів ОК (поява відбитого сигналу) так і локалізувати місце порушення за часом затримки та швидкістю розповсюдження сигналу.

Для оцінки характеристик методу були проведені розрахунки параметрів імпровізованого КК для конкретного типу конструкції ОК. Як зразок, для розрахунків використовувався типовий ОК модульної конструкції. Результати розрахунку залежності хвильового опору та швидкості розповсюдження сигналу в кабелі від частоти наведено на рис. 3, 4.

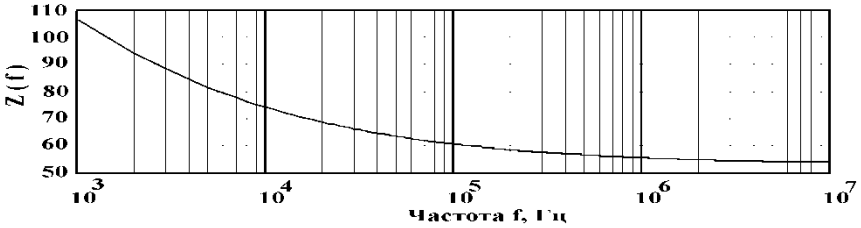


Рис. 3. Залежність хвильового опору Z(f) [Ом]коаксіального кабелю від частоти

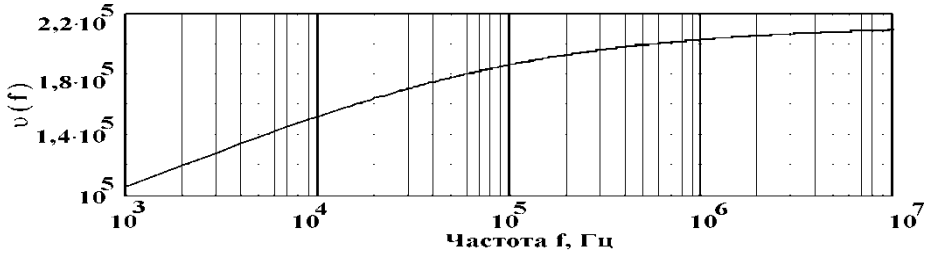


Рис. 4. Залежність швидкості розповсюдження сигналу v(f) [км/с] в коаксіальному кабелі від частоти

Запропонований метод може застосовуватися для безперервного моніторингу ділянок волоконно-оптичної лінії зв'язку з метою запобігання несанкціонованого доступу до ОВ.

Зокрема, він може використовуватися в локальних мережах, що охоплюють ряд будинків, і застосовують ВОЛЗ на магістральних ділянках. Приєднання вимірювального приладу до лінійного ОК і його функціонування при цьому провадиться без переривання режиму передачі.

Література

1. Гордієнко С.С., Манько О.О., Гордієнко С.Б. Моніторинг лінійних споруд ВОЛЗ із метою захисту інформації від несанкціонованого доступу // Зв'язок. – 2012. – №1(97). – С. 32 – 34.

2. Коновалов О.Ю., Манько О.О., Нікіфоренко К.Б., Харлай Л.О. Метод захисту інформації на оптичних ІТ – мережах Шістнадцята міжнародна науково-технічна конференція ОНАЗ ім. О.С. Попова (ВОТТП-16-2017)

3. Каток В. Б. Волоконно-оптичні системи зв'язку. – Київ: „Велар", 1999.

4. Листвин А.В., Листвин В.Н. Рефлектометрия оптических волокон. – М.: ЛЕСАР, 2005. – 208 С.

5. Яковлев А. В. Волоконно-оптическая система передачи конфиденциальной информации // Электросвязь. – 1994. – № 10. – С.11-13.

6. Коновалов О.Ю., Манько О.О., Нікіфоренко К.Б., Харлай Л.О. Принцип захисту інформації на лінійних спорудах ІТ – мереж, Шістнадцята міжнародна науково-технічна конференція ОНАЗ ім. О.С. Попова (ВОТТП-16-2017)

УДК 004.056

д.т.н., с.н.с. Хлапонін Ю.І.
завідувач кафедри
кібербезпеки та комп'ютерної інженерії
Київський національний університет будівництва і архітектури.
y.khlaponin@gmail.com
Рудніцька О.В., аспірант КНУБА
Пальчик С.П., аспірант КНУБА

ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація *Інтенсивний розвиток та впровадження інтелектуальних систем у галузь безпеки об'єктів критичної інфраструктури відзначається збільшенням складності та масштабу відповідних систем. У роботі розглядаються основні принципи побудови складних інтелектуальних систем безпеки, а також деякі рекомендації щодо рівня захисту таких систем***.**

Останнім часом, зважаючи на події в нашій країні та загалом у світі постає питання актуальності розробки інтелектуальної системи безпеки об'єктів критичної інфраструктури або нових сучасних підходів до неї.

Система безпеки – комплекс організаційних заходів та інженерно-технічних засобів, що направлені на захист життєво важливих ресурсів об'єктів від різноманітних загроз.

Типові технічні засоби безпеки:

- Системи охоронної сигналізації;
- Системи протипожежного захисту;
- Системи охоронного відеоспостереження;
- Системи контролю доступу;
- Системи моніторингу та оповіщення про загрозу.

Їх взаємодія для вирішення конкретних задач є найбільш важливою у сфері забезпечення безпеки.

Загальна структура роботи системи контролювання доступу. Система контролювання доступу складається з засобів ідентифікації (різноманітні зчитувачі ідентифікаторів), виконуючих пристроїв (тих, що перегороджують прохід – замків, турнікетів, шлагбаумів, тощо), контролюючих пристроїв та логіки управління (набору реєстрів та правил доступу, що реалізуються у вигляді програмного забезпечення системи).

Типова схема роботи СКД – ідентифікація, перевірка прав доступу, рішення (надання доступу чи відмова у доступі), відстеження переміщення через точку контролю.

Код, отриманий від ідентифікатора користувача системи, надходить до контролера доступу, в якому виконується перевірка права даного користувача отримати доступ через точку, що контролюється цим контролером, в цей момент часу. Правила надання доступу контролером встановлюються програмним забезпеченням, що веде реєстр користувачів та керує мережею контролерів доступу.

Спрощено, СКД працює за алгоритмом «подія – дія», в якому:

- первинна подія – зчитування ідентифікатору користувача;
- дія – перевірка прав користувача;
- подія – дозвіл на прохід;
- дія – відкриття виконуючого пристрою;
- подія – очікування факту проходу;
- дія – реєстрація факту проходу, закриття виконуючого пристрою.

При відхиленні у виконанні даного алгоритму система повинна сформувати тривожну подію, наприклад, невідомий ідентифікатор, заборонена проходу для даного ідентифікатора, не закриття проходу, тощо.

Взаємодія з іншими системами. При реалізації систем безпеки на об’єктах завдання систем ускладнюється. Ефективна робота комплекту систем потребує складних організаційних заходів, частину яких можна автоматизувати шляхом організації взаємодії систем.

Об’єднання систем в комплекс, який взаємодіє між системами на рівні первинних подій та надає оператору інформацію в об’єднаному інтерфейсі, систематизуючи та поєднуючи інформацію про події, надає значні переваги в швидкості реагування та ефективності локалізації загрози. Дозволяє автоматизувати рутинний набір дій оператора, розвантажуючи його для спостереження за розвитком загрози, координування реагуванням та зменшуючи вірогідність прийняття помилкового рішення.

Негативні фактори використання автономних засобів безпеки

- Збільшується навантаження на операторів спостереження;
- Ускладнюються алгоритми підтвердження факту виникнення загрози;
- Збільшується час на реагування;
- Збільшується вплив людського фактору на результативність роботи системи безпеки.

Інтеграція систем – взаємодія систем для запобігання впливу негативних факторів, підвищення ефективності використання окремих типових систем, автоматизації прийняття рішення при виникненні загрози.

Типові системи поєднуються для забезпечення оптимального використання ресурсів об'єкту, для протидії виникненню загроз та оптимізації їх впливу

Щодо інтелектуальної складової, то до типових технічних засобів системи безпеки додаються аналітичні підсистеми:

- Єдина система управління та моніторингу;
- Відеоаналітичні модулі;
- Аудіо аналітика;
- Аналітика відвідувань та часу перебування осіб на окремих територіях;

тощо

Переваги інтелектуальних систем

- Використання інтелектуальних методів обробки відео зображень та розпізнавання образів;
- Відеоаналітика дозволяє вести моніторинг відео без прямої участі людини;
- Використання інтелектуальних алгоритмів реагування на події;
- Можливість реалізувати різноманітні сценарії подій та реагування;
- Інтелектуальні алгоритми дозволяють підвищити ймовірність та оперативність реагування та критичні події.

«Підводні камені» інтеграції:

- Проблема «чорної скриньки»;
- Версійність протоколу обміну;
- Зміни структур даних з оновленням версій систем.

«Підводні камені» інтелектуалізації систем безпеки:

- Необхідність централізованого зберігання великих об’ємів даних перетворює задачу зберігання архівів багатьох користувачів в проблему Big Data;
- Алгоритми інтелектуальних підсистем потребують великої експертизи в налагодженні, якої, найчастіше, спеціалісти на об’єкті не мають та не можуть легко отримати;
- Використання інтелектуальних підсистем потребує знань граничних умов та обмежень у використанні, про які спеціалісти на об’єкті не мають уяви;
- Значна вартість впровадження та налагодження таких підсистем.

З усього вище наведеного постає три основних питання:

1. Яку стратегію обрати при побудові інтелектуальних систем безпеки об’єктів критичної інфраструктури?
   - Рішення на одному бренді.
   - Гетерогенний комплекс.
2. Якою повинна бути архітектура комплексу?
   - Рівень відмовостійкості системи, методи резервування системи та інформації та методи відновлення після катастрофи.
   - Модульність (автономність, автоматичний контроль цілісності, дублювання).
3. Як побудувати роботу з інформацією?
   - Вимоги до рівнів обробки інформації (наприклад: центральний офіс, територіальне відділення, локальний об’єкт).
   - Вимоги до рівнів збереження інформації.
   - Обмежений обсяг даних для кожного рівня та правила обміну даними між рівнями системи.

Безпека систем безпеки

- Проектування систем на базі аналізу загроз.
- Безпечна архітектура системи контролю доступу.
- Ризики маніпуляції з даними, що циркулюють в системі.
- Захист даних в системі контролю доступу: захист ідентифікаторів, достовірність ідентифікації, захист виконуючих елементів, захист каналів зв'язку, захист сховищ даних.
- Розмежування прав доступу.

Висновки. Побудова інтелектуальних інтегрованих систем безпеки об’єктів критичної інфраструктури з урахуванням сучасних вимог дозволить не тільки значно покращити захист об’єкту в цілому та матеріальних і нематеріальних цінностей, але й підвищити безпеку життєдіяльності співробітників. Також такі системи, як "побічний ефект" роблять можливим комплексний аналіз проблем та їх передбачення на об’єкті, що охороняється. Таким чином використання інтелектуальних інтегрованих системи безпеки дозволяє отримати значні переваги не тільки в галузі безпеки, але й в інших напрямках діяльності і процесах суб’єкта господарювання

Література

1. Барсуков, В.С. Сучасні технології безпеки / В.С. Барсуков, В.В. Водолазський. – М.: Нолидж, 2009. – 496 с., Іл.

2. Зегжда, Д.П. Основи безпеки інформаційних систем / Д.П. Зегжда, А.М. Івашко. – М.: Гаряча лінія-Телеком, 2008. –452 с.

http://www.secfocus.ru/shop/books/15708.htm#ixzz4pu8JLeLw.

УДК 004.056.5

Юдін О.Ю.
ДержНДІ Спецзв'язку
alex@ukrdeftech.com.ua
Гнатюк С.Є.
ДержНДІ Спецзв'язку
dndi@dsszzi.gov.ua

АНАЛІЗ ВИМОГ ДО ЕЛЕМЕНТІВ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ УПРАВЛІННЯ ЕНЕРГЕТИЧНОЮ ІНФРАСТРУКТУРОЮ, ЯКІ ЗАБЕЗПЕЧУЮТЬ КІБЕРЗАХИСТ

Анотація. *З урахуванням законодавства України, запропонована структура основних систем електроенергетичних доменів та взаємодії між ними. Також, проведений аналіз нормативно-правових актів Сполучених Штатів Америки та України стосовно вимог до елементів інформаційно-телекомунікаційних систем. Результати аналізу викладені у вигляді вимог (профілів захищеності).*

Актуальність дослідження

Сучасна світова енергетична спільнота визнає існування і актуальність проблеми кібербезпеки новітніх і перспективних електроенергетичних систем. Дослідженню і розв'язанню цієї проблеми приділяється все більше уваги в багатьох передових країнах світу.

В підтвердження цієї тези можемо послатися на ініціативу Міністерства енергетики США, викладену в документі «Модель зрілості стану кібербезпеки в галузі електроенергетики» [1], в якому, поряд з викладенням основних принципів організації зрілої системи кібербезпеки електроенергетики, пропонується, зокрема, і створити відповідну раду з кіберзахисту, наділивши її функціями координації діяльності Міністерства енергетики США і енергетичних компаній з попередження кіберзагроз і подолання інцидентів.

В цьому ж контексті слід назвати ряд інших документів Міністерства енергетики США, зокрема, це «Настанови щодо процесу поводження з ризиками з кібербезпеки в галузі електроенергетики» [2], «Кібербезпека постачання електроенергії» [3].

В той же час, в Україні відсутні нормативні документи які б визначали політику щодо забезпечення кібербезпеки електроенергетичних систем.

Предмет дослідження

Предметом дослідження та аналізу стали нормативні документи США та України, які регламентують вимоги до елементів інформаційно-телекомунікаційних систем (далі ІТС) управління енергетичною інфраструктурою, що забезпечують кіберзахист. При цьому під енергетичною інфраструктурою розглядається лише електроенергетична система.

В ході дослідження:

- визначено перелік ІТС управління енергетичною інфраструктурою;
- сформовано перелік елементів ІТС управління енергетичною інфраструктурою;
- визначено перелік елементів, що забезпечують кіберзахист ІТС систем управління енергетичною інфраструктурою, до яких будуть висуватись вимоги;

- на основі норм українського та американського права здійснено аналіз вимог до елементів ІТС управління енергетичною інфраструктурою, що забезпечують кіберзахист.

Результати дослідження

В результаті досліджень виділені основні домени, їх системи та взаємозв'язки між ними (рис. 1).

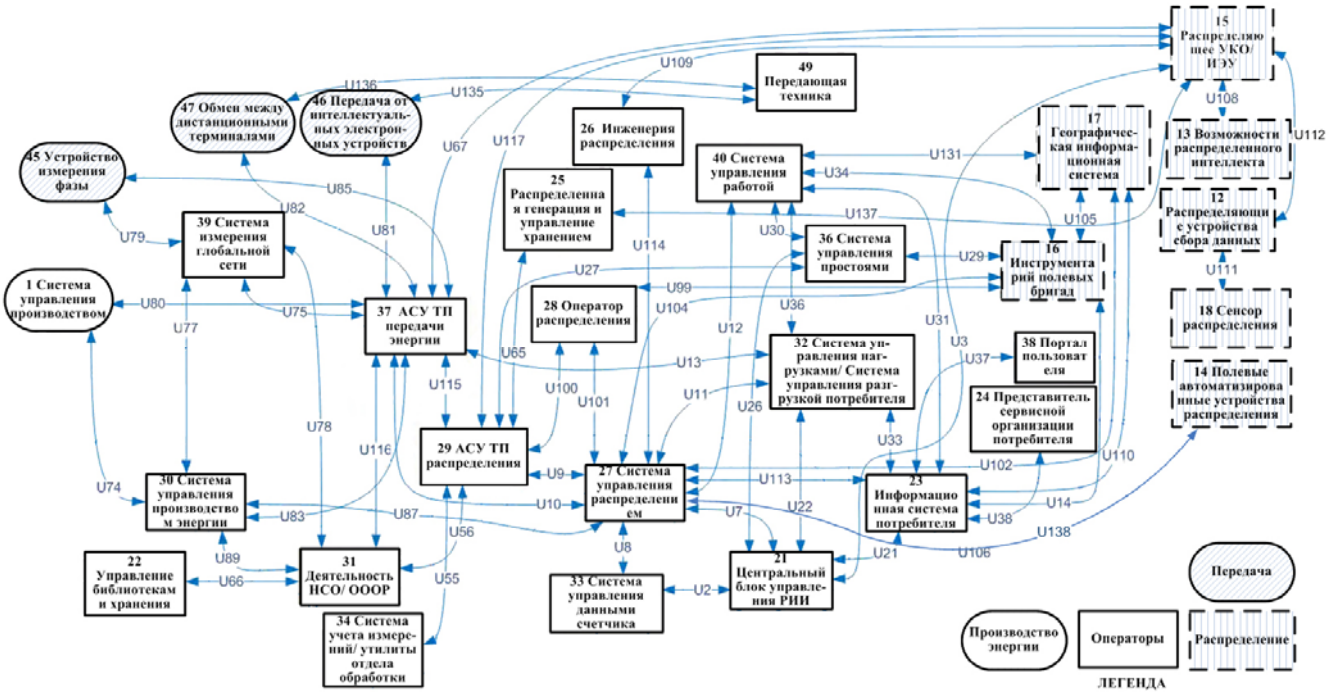


Рис. 1. Схематична структура основних систем доменів та їх взаємодії: оператори, енергогенеруючий, енергорозподілюючий, енергопередавальний

З використанням схематичної структури систем доменів зроблений:

1. Опис категорій логічних інтерфейсів взаємодії основних систем доменів - оператори, енергогенеруючий, енергорозподілюючий, енергопередавальний;
2. Сформульований перелік ІТС;
3. Сформульований перелік елементів ІТС управління енергетичною інфраструктурою;
4. Визначений перелік елементів, що забезпечують кіберзахист ІТС систем управління енергетичною інфраструктурою, до яких будуть висуватись вимоги;
5. Висунуто вимоги з безпеки інформації за категоріями логічних інтерфейсів об'єктів доменів;
6. Зроблена компіляція вимог до безпеки за номерами елементів, логічних інтерфейсів та категоріями інтерфейсів. При цьому, вимоги щодо конфіденційності, цілісності і доступності визначені за найвищим ступенем, який зустрічається в групі категорій;
7. Зроблено зіставлення вимог визначених нормативними документами [4, 5].

З урахуванням компіляції вимог до безпеки, зіставленням вимог визначених нормативними документами, а також даних наведених в:

- рекомендаціях [6] щодо стандартних функціональних профілів захищеності, що входять до складу автоматизованих систем, які призначені для керування технологічними процесами;
- рекомендаціях [6] щодо стандартних функціональних профілів захищеності;
- рис. 2 – 3 «Logical Reference Model» [4], щодо зв'язаності елементів,

викладено вимоги до кожного елементу ІТС управління енергетичною інфраструктурою у вигляді табл. 1.

Таблиця 1

Вимоги до найбільш критичних елементів ІТС управління енергетичною інфраструктурою

№ ел.	Додаткові функціональні критерії	Стандартний функціональний профіль захищеності	Остаточний функціональний профіль захищеності
15	КД-2, КД-3, КД-4, КО-1, КК-2, КВ-1, ЦД-3, ЦА-2, ДР-2, ДР-3, ДС-2, ДС-3, ДВ-3, НР-1, НР-2, НР-3, НР-4, НР-5, НИ-1, НИ-2, НИ-3, НК-1, НК-2, НО-1, НО-3, НЦ-1, НТ-3, НВ-2, НВ-3	2.КЦД.5 = { КД-4, КА-4, КО-1, КК-2, ЦД-4, ЦА-4, ЦО-2, ДР-3, ДС-3, ДЗ-3, ДВ-3, НР-5, НИ-2, НК-2, НО-3, НЦ-3, НТ-2 }	КД-2, КД-3, КД-4, КА-4, КО-1, КК-2, КВ-1, ЦД-3, ЦА-2, ЦО-2, ДР-2, ДР-3, ДС-2, ДС-3, ДЗ-3, ДВ-3, НР-1, НР-2, НР-3, НР-4, НР-5, НИ-1, НИ-2, НИ-3, НК-1, НК-2, НО-1, НО-3, НЦ-1, НТ-3, НВ-2, НВ-3
21	КД-2, КД-4, КО-1, КК-2, КВ-1, ЦД-3, ЦА-2, ДР-3, ДС-2, ДС-3, ДВ-3, НР-1, НР-2, НР-4, НИ-1, НИ-2, НИ-3, НК-1, НК-2, НО-1, НО-3, НЦ-1, НТ-3, НВ-2, НВ-3	2.КЦД.5 = { КД-4, КА-4, КО-1, КК-2, ЦД-4, ЦА-4, ЦО-2, ДР-3, ДС-3, ДЗ-3, ДВ-3, НР-5, НИ-2, НК-2, НО-3, НЦ-3, НТ-2 }	КД-2, КД-4, КА-4, КО-1, КК-2, КВ-1, ЦД-3, ЦА-2, ЦО-2, ДР-3, ДС-2, ДС-3, ДЗ-3, ДВ-3, НР-1, НР-2, НР-4, НИ-1, НИ-2, НИ-3, НК-1, НК-2, НО-1, НО-3, НЦ-1, НТ-3, НВ-2, НВ-3
23	КД-2, КД-4, КО-1, КК-2, КВ-1, ЦД-3, ЦА-2, ДР-2, ДР-3, ДС-2, ДС-3, ДВ-3, НР-1, НР-2, НР-4, НИ-1, НИ-2, НИ-3, НК-1, НК-2, НО-1, НО-3, НЦ-1, НТ-3, НВ-2, НВ-3	3.КЦД.4 = { КД-3, КА-3, КО-1, КК-1, КВ-3, ЦД-1, ЦА-3, ЦО-2, ЦВ-2, ДР-3, ДС-2, ДЗ-2, ДВ-2, НР-4, НИ-2, НК-1, НО-3, НЦ-3, НТ-2, НВ-2, НА-1, НП-1 }	КД-2, КД-4, КА-3, КО-1, КК-2, КВ-1, ЦД-3, ЦА-2, ЦО-2, ДР-2, ДР-3, ДС-2, ДС-3, ДЗ-2, ДВ-3, НР-1, НР-2, НР-4, НИ-1, НИ-2, НИ-3, НК-1, НК-2, НО-1, НО-3, НЦ-1, НТ-3, НВ-2, НВ-3, НА-1, НП-1
27	КД-2, КД-4, КО-1, КК-2, КВ-1, ЦД-3, ЦА-2, ДР-2, ДР-3, ДС-2, ДС-3, ДВ-3, НР-1, НР-2, НР-4, НИ-1, НИ-2, НИ-3, НК-1, НК-2, НО-1, НО-3, НЦ-1, НТ-3, НВ-2, НВ-3	2.КЦД.5 = { КД-4, КА-4, КО-1, КК-2, ЦД-4, ЦА-4, ЦО-2, ДР-3, ДС-3, ДЗ-3, ДВ-3, НР-5, НИ-2, НК-2, НО-3, НЦ-3, НТ-2 }	КД-2, КД-4, КА-4, КО-1, КК-2, КВ-1, ЦД-3, ЦА-2, ЦО-2, ДР-2, ДР-3, ДС-2, ДС-3, ДЗ-3, ДВ-3, НР-1, НР-2, НР-4, НИ-1, НИ-2, НИ-3, НК-1, НК-2, НО-1, НО-3, НЦ-1, НТ-3, НВ-2, НВ-3
29	КД-2, КД-4, КО-1, КВ-1, ЦД-3, ЦА-2, ДР-3, ДС-2, ДС-3, ДВ-3, НР-1, НР-2, НР-4, НИ-1, НИ-2, НК-1, НК-2, НО-1, НО-3, НЦ-1, НТ-3, НВ-2, НВ-3	2.КЦД.5 = { КД-4, КА-4, КО-1, КК-2, ЦД-4, ЦА-4, ЦО-2, ДР-3, ДС-3, ДЗ-3, ДВ-3, НР-5, НИ-2, НК-2, НО-3, НЦ-3, НТ-2 }	КД-2, КД-4, КА-4, КО-1, КК-2, КВ-1, ЦД-3, ЦА-2, ЦО-2, ДР-3, ДС-2, ДС-3, ДЗ-3, ДВ-3, НР-1, НР-2, НР-4, НИ-1, НИ-2, НК-1, НК-2, НО-1, НО-3, НЦ-1, НТ-3, НВ-2, НВ-3
37	КД-2, КД-4, КО-1, КК-2, КВ-1, ЦД-3, ЦА-2, ДР-3, ДС-2, ДС-3, ДВ-3, НР-1, НР-2, НР-4, НИ-1, НИ-2, НИ-3, НК-1, НК-2, НО-1, НО-3, НЦ-1, НТ-3, НВ-2, НВ-3	2.ЦД.3 = { КО-1, ЦД-1, ЦА-3, ЦО-2, ДР-3, ДС-2, ДЗ-2, ДВ-2, НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2 }	КД-2, КД-4, КО-1, КК-2, КВ-1, ЦД-3, ЦА-2, ЦО-2, ДР-3, ДС-2, ДС-3, ДЗ-2, ДВ-3, НР-1, НР-2, НР-4, НИ-1, НИ-2, НИ-3, НК-1, НК-2, НО-1, НО-3, НЦ-1, НТ-3, НВ-2, НВ-3

Література

1 Elecrticity Subsector Cybersecurity Capability Maturity Model Version 1.1 – DoE/February 2014. http://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf.

2 Elecrticity Subsector Cybersecurity Risk Management Process Guideline. –DoE/ May 2012. http://energy.gov/sites/prod/files/Cybersecurity Risk Management Process Guideline –Final – May 2012.pdf.

3 Roadmap to Achieve Energy Delivery Systems Cybersecurity. –DoE/ September 2011. http://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf.

4 NISTIR 7628. Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements // National Institute of Standards and Technology. – 2010.

5 НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28 квітня 1999 р. №22.

6 НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28 квітня 1999 р. №22.

ЗМІСТ