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

Друга всеукраїнська науково-практична конференція

"ПЕРСПЕКТИВНІ НАПРЯМИ ЗАХИСТУ ІНФОРМАЦІЇ"

03-07 вересня 2016 року

Збірник тез

Одеса
ОНАЗ
2016

УДК 004.056.5

Перспективні няпрями захисту інформації: матеріали другої всеукраїнської наук.-пр. конф. – м. Одеса, 03-07 вересня 2016 р. – Одеса: ОНАЗ, 2016. – 87 с.

Даний збірник містить тези матеріалів, що представлені на другу всеукраїнську науково-практичну конференцію “**Перспективні няпрями захисту інформації**”, що проводиться 03-07 вересня 2016 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 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;
Корченко О.Г.	д.т.н., проф., зав. каф. безпеки інформаційних технологій, Національний авіаційний університет
Оксіюк О.Г.	д.т.н., проф., зав. каф. кібербезпеки та захисту інформації, КНУ ім. Тараса Шевченка;
Рудницький В.М.	д.т.н., проф., зав. каф. системного програмування, Черкаський державний технологічний університет;
Захарченко М.В.	д.т.н., проф., зав. каф. інформаційної безпеки та передачі даних, ОНАЗ ім. О.С. Попова;
Корчинський В.В.	д.т.н., проф. каф. інформаційної безпеки та передачі даних, ОНАЗ ім. О.С. Попова;
Гнатюк С.О.	к.т.н., доц. каф. безпеки інформаційних технологій, Національний авіаційний університет;
Ніколаєнко С.В.	к.т.н., доц. каф. інформаційних технологій, ОНАЗ ім. О.С. Попова;
Стайкуца С.В.	к.филос.н., доц. каф. інформаційної безпеки та передачі даних, ОНАЗ ім. О.С. Попова;
Онацький О.В.	к.т.н., доц. 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

Організаційний комітет

Васіліу Є.В.	д.т.н., проф., директор навчально-наукового інституту радіо, телебачення та інформаційної безпеки, ОНАЗ ім. О.С. Попова;
Ніколаєнко С.В.	к.т.н., доц. каф. інформаційних технологій, 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;
Михайлова Л.В.	викл. каф. інформаційної безпеки та передачі даних, ОНАЗ ім. О.С. Попова;
Кишмар І.Б.	пров. фахівець каф. інформаційної безпеки та передачі даних, ОНАЗ ім. О.С. Попова
Лімарь І.В.	аспірант каф. інформаційної безпеки та передачі даних, ОНАЗ ім. О.С. Попова

УДК 681.3.06

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

НОВІ ЙМОВІРНІСНІ МЕТОДИ ПЕРЕВІРКИ НЕЗВІДНОСТІ ТА ФАКТОРИЗАЦІЇ ПОЛІНОМІВ

Анотація. *У роботі було узагальнено метод Полларда, його еліптичний аналог та теорему Ленстри для використання в кільці поліномів. З використанням цих теорем отримано три ймовірнісні алгоритми факторизації поліномів над полем довільної характеристики відмінної від 3.*

Більшість сучасних криптосистем, як симетричних, так і асиметричних використовує незвідні поліноми. На сьогоднішній день існують як класичні алгоритми перевірки незвідності поліному, так і нові ймовірнісні. У цій роботі продовжується тема побудови імовірнісних алгоритмів перевірки незвідності поліномів, але, на відміну від попередніх результатів – з використанням еліптичних кривих.

Далі наведено алгоритми отримані у роботі.

Узагальнення еліптичного аналогу тесту (S.Goldwasser, J. Kilian, A.O.L. Atkin) для поліномів.

Вхід:

- $f(x) \in F_p[x],\ \deg f = n$

Алгоритм:

1. Обрати довільні поліноми $\mathrm{a}(\mathrm{x}) \in \mathrm{F_p}[\mathrm{x}],\ \mathrm{u}(\mathrm{x}) \in \mathrm{F_p}[\mathrm{x}],\ \mathrm{y}(\mathrm{x}) \in \mathrm{F_p}[\mathrm{x}]$, де $\deg \mathrm{a} < \mathrm{n},\ \deg \mathrm{u} < \mathrm{n},\ \deg \mathrm{y} < \mathrm{n}$.
2. Обчислити $\mathrm{b}(\mathrm{x}) = \left[\mathrm{y}(\mathrm{x})^2 - \mathrm{u}(\mathrm{x})^3 - \mathrm{a}(\mathrm{x})\mathrm{u}(\mathrm{x})\right] \bmod \mathrm{f}(\mathrm{x})$. Пара (u, y) – точка кривої E, заданої рівнянням $\mathrm{y}^2 = \mathrm{u}^3 + \mathrm{au} + \mathrm{b}\left(\bmod \mathrm{f}(\mathrm{x})\right)$.
3. Якщо E – сингулярна, то повертаємось до кроку 1.
4. Використовуючи один з відомих алгоритмів обчислити $m = |E|$. Якщо в процесі отримано вираз, що неможливо обчислити, то $f(x)$ – звідний. Якщо m не може бути представлено як $m = kq$, де k – невелике ціле, а q – просте, $q > \left(p^{\frac{n}{4}} + 1\right)^2$ то повертаємось до кроку 1.
5. Обчислити $Q_1 = mP$ и $Q_2 = kP$. Якщо в процесі отримано вираз, що неможливо обчислити, то $f(x)$ – звідний. Якщо $Q_1 \neq \Theta$, то $f(x)$ – звідний. Якщо $Q_2 = \Theta$, то повертаємось до кроку 1. Інакше $f(x)$ – незвідний.

Узагальнення $(p-1)$-алгоритму Полларда для факторизації поліномів

Вхід:

- $f(x) \in F_p[x],\ \deg f = n$

$B \in Z$

Алгоритм:

1. Обчислити $k = HOK(1,2,\ldots,B)$.
2. Обрати $a(x) \in F_p[x], \deg a < n$.
3. Обчислити $d(x) = (a(x),\ f(x))$. Якщо $\deg d(x) > 1$, то $d(x)$ – нетривіальний дільник $f(x)$.
4. Обчислити $g(x) = a(x)^k \ mod\ f(x)$. Якщо $g(x) = 1$, то повертаємось до кроку 2.
5. Обчислити $u(x) = (g(x) - 1, f(x))$. Якщо $\deg u(x) \geq 1$, то $u(x)$ – нетривіальний дільник $f(x)$. Інакше $f(x)$ – незвідний

Серед наведених алгоритмів найбільш перспективними є наведені нижче. На сьогоднішній день алгоритм Ленстри для чисел входить до трійки найшвидших алгоритмів факторизації. Він належить до класу суб-експоненціальних алгоритмів. У роботі алгоритм та відповідна теорема були узагальнені для поліномів над полями як характеристик 2 так і $p > 3$.

Алгоритм Ленстри для факторизації поліномів ($p > 3$)

Вхід:

- $f(x) \in F_p[x]$ – звідний поліном, $p > 3$ – просте, $\deg f = n$

Алгоритм:

1. Генеруємо пару (E,P), де E – еліптична крива задана формулою $y^2 = x^3 + ax + b,\ a,b \in F_p[x],\ P \in E$.
2. Якщо $(4a^3 + 27b^2, f) = f$, то повертаємось до кроку 1. Інакше, якщо $(4a^3 + 27b^2, f) \neq 1$, ми отримуємо нетривіальний дільник f.
3. Обираємо межі $B, C \in N$, $k = \prod_{l \leq B} l^{a_l}$, де всі l – прості, $a_l = [\log C / \log l]$
4. Обчислюємо kP. Якщо в процесі обчислення отримуємо знаменник $d(x) : (d,f) \neq 1$ і $(d,f) \neq f$, то d – нетривіальний дільник f. Інакше, якщо $(d,f) = f$, повертаємось до кроку 1. Якщо вдалося обчислити kP, повертаємось до кроку 1.

Алгоритм Ленстри для факторизації поліномів ($p = 2$)

Вхід:

- $f(x) \in F_p[x]$ – звідний поліном, $p = 2$, $\deg f = n$

Алгоритм:

1. Генеруємо пару (E,P), де E – еліптична крива задана формулою $y^2 + xy = x^3 + ax^2 + b,\ a,b \in F_p[x],\ P \in E$.

2. Якщо $(b,f)=f$, то повертаємось до кроку 1. Інакше, якщо $(b,f)\neq 1$, ми отримуємо нетривіальний дільник f.
3. Обираємо межі $B,C\in N$, $k=\prod_{l\le B} l^{a_l}$, де всі l – прості, $a_l=\left[\log C/\log l\right]$
4. Обчислюємо kP. Якщо в процесі обчислення отримуємо знаменник $d(x):(d,f)\neq 1$ і $(d,f)\neq f$, то d – нетривіальний дільник f. Інакше, якщо $(d,f)=f$, повертаємось до кроку 1. Якщо вдалося обчислити kP, повертаємось до кроку 1.

Висновки. *Алгоритми факторизації поліномів за допомогою еліптичних кривих запропоновано вперше і поки ще важко оцінити однозначний виграш при їх застосуванні при побудові криптосистем. Проте, щонайменше, вони є красивими та оригінальними з точки зору математики.*

Література

1. Коблиц Н. Курс теории чисел и криптографии. – М.: Научное изд-во ТВП, 2001. – 260 с.
2. Silverman J. The Arithmetic of Elliptic Curves. – Heidelberg etc.: Springer, 1986. – 513 p.
3. Washington L. Elliptic Curves Number Theory and Cryptography. – Series Discrete Mathematics and Its Applications, Chapman & Hall/CRC, second ed, 2008. –524 p.
4. Schoof R. Elliptic Curves over finite fields and the computation of square roots mod p. – Math. Corp., 1985. – 490 p.
5. Gupta R., Murty M.R. Primitive points on elliptic curves. – Compositio Math., 1986. – 13-14 p.

УДК 004.056.53

Блідар А.І., Гізун А.І.
Національний авіаційний університет.
anya.liider@gmail.com

БАНКІВСЬКІ ПЛАТІЖНІ КАРТКИ: УРАЗЛИВОСТІ ТА МЕТОДИ ЇХ МІНІМІЗАЦІЇ

Анотація. *Представлено основні уразливості банківських карт. Наведено головні особливості магнітних та smart-карток. Виявлено, що захист банківських платіжних карт – це система, що складається із технічного, соціального та механічного захисту. Зазначено, що банківський клієнт задля власної безпеки повинен мати хоча б дві SIM-карти. Також представлені основні способи шахрайства. Наведено рекомендації для мінімізації загроз викрадення коштів у власників банківських карт.*

Останнім часом стрімко збільшилась кількість власників банківських платіжних карток (БПК), за допомогою яких можна здійснити покупки в Інтернет-магазині, розрахуватись у ресторані, отримати стипендію або заробітну платню. У 2015 р. кількість населення України становила близько 43 млн, а кількість активних БПК, за даними Мінфіну, – 30 млн, що становить 70% кількості всіх жителів країни. Тому актуальною є проблема захисту БПК від несанкціонованого доступу.

Власники БПК створюють загрозу своїм фінансам, розміщуючи мобільний номер, що прив'язаний до банківських рахунків, на сайтах продажу та соціальних мережах; публічно повідомляючи реквізити карток та телефонів для отримання матеріальної допомоги; вводячи дані на фальшивих веб-ресурсах. Шахраям зазвичай достатньо знати перші шість цифр, щоб

визначити банк-емітент картки своєї жертви та номер мобільного телефону. Вони періодично здійснюють дзвінки на стільниковий з трьох різних номерів, щоб знати, які три номера телефонували найчастіше та поповнюють рахунок на 1-2 гривні, щоб знати коли поповнювався рахунок. Ця інформація допоможе зловмисникам розблокувати чужу SIM-карту та отримати доступ до КД.

Метою цієї роботи є аналіз особливостей функціонування БПК найкрупніших банків, послугами яких користуються більшість українців, та наданих ними сервісів, а також виявлення уразливостей при користуванні БПК та формування рекомендацій щодо їх усунення або уникнення.

Першу трійку лідерів за обсягом користувачів банківськими картками станом на 01.01.2016 р. становлять: «ПриватБанк», який випустив найбільшу кількість БПК в Україні, «Ощадбанк» та «Райффайзен Банк Аваль».

БПК поділяються на картки з магнітною смугою та з чіп-модулем (smart-картки). Особливістю першої є магнітна стрічка на зворотній стороні картки, яка зберігає інформацію об'ємом близько 100 байт: термін закінчення дії картки, PIN-код, прізвище та ім'я власника. Такі карти працюють з банком в режимі on-line, на відміну від карти з мікропроцесором. Картка з чіпом (smart-карта) – це карта з вбудованою мікросхемою, можливості якої залежать від банка-емітента [1].

Технічна небезпека

Поширеним видом банківського шахрайства є скімінг – використання технічного пристрою, який зчитує інформацію з магнітної картки (наприклад, з дебетної карти «Ощадбанку»). Його можна побачити неозброєним оком, якщо уважно придивитись до термінального обладнання, оскільки він порівняно габаритний. Різновидом скімінгу є шимінг, який полягає у застосуванні шиммера – гнучкої плати товщиною з людську волосину, яка вставляються в кардрідер банкомату і не помітна для людського ока. Цей пристрій з легкістю «зчитує» магнітну карту, тому БПК з чіпом більш надійніші.

Ще однією суттєвою технічною загрозою є встановлення вірусного ПЗ. Банківські трояни «крадуть» конфіденційні дані (КД), при користуванні мобільним та Інтернет-банкінгом (ІБ). Найпоширенішими серед шкідливих ПЗ є ZeuS та його різновид – Citadel [2]. Головною метою зловмисників, що використовують ZeuS, є крадіжка аутентифікаційних даних користувачів від різних сервісів, включаючи ІБ. Викрадена таким чином інформація використовується для переказу грошових коштів на підставні рахунки, з яких знімаються гроші «мулами» – особами, готовими знімати кошти сумнівного походження за невеликий відсоток. Після того як вірус потрапляв в систему, троянська програма перехоплювала реєстраційні дані, отримавши які, зловмисник робив перекази на рахунки спільників невелику суму грошей, тим самим унеможливлюючи знаходження рахунку зломщика. Деякі версії ZeuS маскувалися під цифровим підписом лабораторії Касперського. Citadel – модифікована версія трояна ZeuS, що заразила більше 10 тис ПК і за даними спецслужб США стала інструментом крадіжки понад 500 млн дол..

Соціальна небезпека

Соціальний інжиніринг (СІ) – безкоштовний та дієвий спосіб дізнатись CVV/CVV2 коди або інші КД. Серед засобів СІ – фальшиві емоційні повідомлення, які викликають почуття жалю та просять про допомогу бійцям АТО, хворим дітям тощо. Також іноді сповіщають про виграш великої суми грошей, яку можливо отримати, ввівши свої КД. Соціальні хакери можуть створювати фальшиві веб-ресурси Інтернет-магазинів та ІБ.

Декілька років тому розповсюджувались фішинг-атаки на користувачів послугою «Приват 24». Шахраї діяли за наступною схемою:

1) Купівля веб-адреси, схожої на адресу сторінки служби «Приват24».
http://www.privat24-ua.com/logins – підроблений;
https://www.privat24.ua/#login – справжній.
2) Копіювання та перенесення вмісту справжнього сайту на фальшивий.
3) Відправлення листів на всі електронні адреси спамерської бази даних.

Останній крок є помилковим, адже ті користувачі Інтернету, які не користуються послугами ІБ, після отримання цих повідомлень, повідомлять адміністрації справжнього банку про фальшивий сайт. Але певний час, за який вони отримують доступ до банківських рахунків певного відсотку користувачів «Приват-24», у фішерів є,. Щоб уникнути швидкого знищення підробленого сайту, фішери у своїх листах надсилають потенційним жертвам посилання на Приват-24, яке переводить користувача на зовсім інший сайт з абсолютно іншою назвою. Цей веб-ресурс автоматично направляє користувача на фальшивий сайт ІБ [3].

Інший випадок СІ – клієнту банка телефонує нібито банківський співробітник, що диктує дані картки власника і просить сказати свої дані внаслідок втрати банком клієнтських баз даних. Слід зазначити, що в даному випадку поле для діяльності шахраїв практично не обмежене і можна навести багато інших прикладів таких атак на КД.

Механічна небезпека

Користувач БПК може створити загрозу власному банківському рахунку своєю необачністю. Розраховуючись у закладі харчування, клієнт віддає свою картку офіціанту, не підозрюючи, що той може бути потенційним шахраєм.

Також картка може зазнати фізичних пошкоджень: погнутись, зламатись тощо.

Рекомендації

- Щоб забезпечити себе від банківських троянів, варто завантажувати Java-застосунки з перевірених веб-ресурсів, про що свідчить https протокол в адресі сайту та зображення замку зеленого кольору. Варто зробити закладку, щоб завжди потрапляти лише на перевірений веб-ресурс.
- Користування послугою OTP (one time password), різновидом якого є SMS-оповіщення дозволить швидко дізнатись про всі операції з карткою.
- Послуга 3D-secure (можна підключити, наприклад у Райффайзен Банк Аваль) покращить безпеку користувачів БПК.
- Якщо клієнту не потрібно переводити одну валюту в іншу, потрібно вимкнути послугу конвертації коштів.
- Мати мінімум 2 телефонних номера, один з яких не буде прив’язаний до банківських рахунків. Саме його можна розповсюджувати.
- Не дозволяти обслуговуючому персоналу користуватись карткою для оплати продуктів і послуг за межами видимості власника карти.
- Бути стійким до психологічних впливів та не реагувати на провокаційні повідомлення, не повідомляти КД по телефону, а зателефонувати до банку за офіційним номером.
- Встановити грошовий ліміт.

Висновок. Захист власної банківської карти не є одноразовою процедурою. Це складний процес, що вимагає постійної пильності та уважності. Надані рекомендації допоможуть мінімізувати випадки крадіжки коштів за допомогою БПК. Представлено методи захисту власної картки для того, щоб зловмисники не могли за допомогою технічних засобів (троянів та технічних пристроїв) викрасти кошти; засоби захисту, якщо дані вже відомі стороннім особам. Також наведений приклад реальної фішингової атаки задля уникнення повторного інциденту. Крім того важливою в цьому питані є психологічна стійкість особи, до соціотехнічних атак, процедура визначення якої була описана у попередніх роботах [4].

Список літератури

1. Пиріг СО. Платіжні системи: навч. посіб. – К: Центр учбової літератури, 2008. – 40 с.

2. Українська антивірусна лабораторія Zillya. –[Електронний ресурс]. – Режим доступу: http://zillya.ua/qr-fishing-novii-trend-v-mobilnikh-zagrozakh

3. Інформаційні технології в економіці: навч. посіб. для студ. кооп. Вузів / А. Я. Страхарчук, В. П. Страхарчук; Навч.-метод. центр "Укоопосвіта". – К., 1999. – 355 с. – Бібліогр.: – С. 354-355. – укр.

4. Блідар А.І., Гізун А.І. / Захист інформації і безпека інформаційних систем: матеріали V Міжнар. наук.-техн. конф. – 3-22 Львів : Видавництво Львівської політехніки, 2016. – 172 с.

УДК 004.5

Бурячок В.Л., Мякухін Ю.В.,
Наконечний В.С., Розорінов Г.М.,
Державний університет телекомунікацій, м. Київ.
yurivitit@gmail.com

ОЦІНКА ЖИВУЧОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ ПРИ ВПЛИВІ КІБЕРАТАК НА ОСНОВІ КОЕФІЦІЄНТА ЗБЕРЕЖЕННЯ ЕФЕКТИВНОСТІ ТЕХНІКИ

***Анотація**. Пропонується новий спосіб оцінки живучості інформаційних систем, який будується на основі класичного математичного методу, що дозволяє обчислювати коефіцієнт збереження ефективності техніки. Представлений метод є універсальним і може застосовуватися, зокрема, для радіоелектронних систем різного призначення та технічних засобів охорони.*

Розвиток і удосконалення систем обчислювальної техніки, її елементної бази, нових технологій побудови комп'ютерних локальних мереж й програмного забезпечення призводить до збільшення переліку нових програмно-апаратних уразливостей в створених пристроях та спеціалізованих програмних продуктах. Наявність таких уразливостей, як "відкрите вікно", сприяє успішній реалізації кібератак на відповідні інформаційні системи (ІС) [1].

Зважаючи на це, завдання забезпечення надійності та безвідмовності ІС є надзвичайно актуальним й таким, що потребує найшвидшого вирішення. Одним із показників, оцінки стану працездатності інформаційних систем – є показник оцінки рівня їх живучості. В роботі [2] для визначення живучості ІС пропонується таке тлумачення: «… Под живучестью системы понимают ее способность адаптироваться к новым не предусматриваемым условиям функционирования, противостояния нежелательным влияниям при одновременной реализации основной функции. Живучесть в традиционном понимании – это фундаментальное свойство сложных систем. Биологические, социальные и многие другие системы изначально обладают свойством живучести, что позволяет им сохранять целостность, выполнять свои функции и развиваться вопреки деградации, независимо от наличия неблагоприятных (деструктивных) воздействий со стороны внешней среды …».

Оскілки саме тлумачення живучості ще є не сталим, ми даємо інше тлумачення. Таке трактування відображає суть математичного методу визначення живучості, що наводиться нижче.

Пропонується для визначення живучості ІС таке тлумачення - здатність ІС виконувати свої основні завдання з допустимими відхиленнями в працездатності при впливі передбачених для неї переліку кібератак (загроз) із заданою тривалістю дії.

Для чисельного оцінювання рівня живучості ІС пропонується використовувати функцію, яка дозволяє обчислювати коефіцієнт збереження ефективності техніки (тлумачення терміну «коефіцієнт збереження ефективності техніки» та вигляд відповідної функції наведено в [3,4]). З цією метою в роботі були проведені перетворення відомого класичного трактування, що дозволило інтерпретувати значення функції, яка відображає рівень живучості ІС при впливі кібератак. Як результат, функція, що відображає живучість ІС в умовах впливу кібератак матиме такий вигляд:

$$K_G = \frac{E(\overline{X_N} - \overline{TR_{N,k}})}{E_0(\overline{X_N})}, \qquad (1)$$

де E – функція, що відображає показник технічної ефективності ІС при впливі зазначених загроз;

E_0 – функція, що виражає показник технічної ефективності ІС без впливу загроз;

N – кількість даних технічних характеристик (ТХ) ІС;

k – порядковий номер розглянутої загрози ($k = \overline{1, K}$);

K – кількість врахованих загроз;

$\overline{X}_N$ – вектор розмірності $\boldsymbol{N}$, елементами (x_n) якого є нормовані значення вхідних ТХ ІС, які входять до функції;

x_n – значення n-ої ТХ;

$\overline{TR_{N,k}}$ – вектор розмірності $\boldsymbol{N}$, елементи якого є нормованими значеннями впливу розглянутої k-ої загрози зі своїми атрибутами, на відповідні значення ТХ.

Зв'язок елементів вектору $\overline{TR_{N,k}}$ $\left(\overline{TR_{N,k}} = \left(tr_{1,k}, tr_{2,k}, ..., tr_{n,k}, ..., tr_{N,k}\right)\right)$ з відповідними значеннями атрибутів для k-ої загрози пропонується здійснювати наступною залежністю:

$$\overline{\overline{TR_{N,M_k}}} = \left(\overline{tr_{1,M_k\ k}}, \overline{tr_{2,M_k}}, ..., \overline{tr_{n,M_k}}, ..., \overline{tr_{N,M_k}}\right) = \overline{TR_{M_k}} * A_{N M_k}(x_{n\ \mathrm{m}_k}), \qquad (2)$$

де $\overline{\overline{TR_{N,M_k}}}$ - вектор з не нормованими значеннями, що відповідають нормованому вектору $\overline{TR_{N,k}}$;

M_k – кількість розглянутих атрибутів для k-ої загрози;

$\overline{TR_{M_k}}$ – нормований вектор, елементи якого є значення m-го атрибуту k-ої загрози, що зараз впливає на ІС.

$A_{N\,\mathrm{M_k}}(x_{n\ \mathrm{M_k}})$ – матриця значень, що відображає взаємозв'язок m-го атрибуту k-ої загрози с n-ою ТХ.

У математичному виразі (2) наводиться випадок, коли M_k=N. Було також розроблено модифікований математичний вираз (2), у випадку коли $M_k \neq N$. Передбачається, що усі значення (вхідні та вихідні) наведених в (1) та (2) є нормованими значеннями.

Розроблений математичний метод визначення живучості ІС буде адекватним і коректним при використанні, якщо адекватно і коректне буде задана функція ефективності (E_0), яка має відображати структуру функціонування (топологію) даної ІС. Інакше, при не дотриманні цієї вимоги, отриманий результат буде невірним. Треба зауважити, що вигляд функції E такий самий, як і для E_0, без врахування $\overline{TR_{N,k}}$.

Запропонований математичній метод є універсальним. Він може застосовуватися при визначені живучості як радіотехнічних систем різного призначення так і технічних засобів охорони.

Література

1. Мякухин Ю.В. Расчет вероятности защищенности информационных систем от кибератак /Ю.В. Мякухин, Г.Н. Розоринов // Проблеми кібербезпеки інформаційно-телекомунікаційних систем. Зб. матеріалів доповідей та тез науково-технічної конференції м. Київ, 10-11 березня 2016 р., Київський національний університет ім. Тараса Шевченка, 2016. –С 58-59.

2. Додонов А.Г. Живучесть информационных систем. /А.Г. Додонов, Д.В. Ландэ. – К.: Наук. думка, 2011. –256 с.

3. Под ред. д-ра техн. наук. Рембезы А.И. Надежность и эффективность в технике: Справ очник: в 10 т. Т.1. Методология. Организация. Терминология. М.: Машиностроение, 1986. -224 с.

4. Аполлонский С. М. Надежность и эффективность электрических аппаратов: Учебное пособие / С.М. Аполлонский, Ю.В. Куклев. –СПб.: Изд. «Лань», 2011. - 448 с.

УДК 004.056.53+530.145

Василіу Л.М.[1], Василіу Є.В.[2]
[1]Одеський національний політехнічний університет
[2]Одеська національна академія звязку ім О.С. Попова
lada.vasiliu@gmail.com

АТАКА РОЗДІЛЕННЯ ЧИСЛА ФОТОНІВ НА КВАНТОВИЙ ПРОТОКОЛ РОЗПОДІЛЕННЯ КЛЮЧІВ ІЗ ШІСТЬОМА СТАНАМИ

Анотація. *Проаналізовано найбільш потужну атаку розділення числа фотонів – атаку із заміною квантового каналу зі втратами на ідеальний – на протокол квантового розподілення ключів із шістьома станами. Показано, що стійкість протоколу із шістьома станами до атаки розділення числа фотонів вище на декілька процентів, ніж стійкість протоколу BB84. Показано, що як і для протоколу BB84, стійкість протоколу із шістьома станами зменшується як при збільшенні середнього числа фотонів в імпульсі, так і при зменшенні коефіцієнту передачі каналу*

Одними із найважливіших завдань симетричної криптографії із секретним ключем є розроблення та удосконалення процедур розподілення ключа між користувачами (суб'єктами *A* и *B*). На сьогодні для розподілення секретного ключа широко використовують схеми з відкритим ключем, наприклад, схему цифрового конверта або алгоритм Діфі-Хелмана, які мають тільки обчислювальну стійкість, тобто використовують обмеженість обчислювальних потужностей зловмисника (суб'єкта *E*). Альтернативою таким схемам розподілення ключів на основі асиметричної криптографії є системи квантового розподілення ключів, стійкість яких ґрунтується на законах квантової фізики й за певних умов досягає теоретико-інформаційної [1]. Для досягнення теоретико-інформаційної стійкості квантових протоколів розподілення ключів (КПРК) необхідні оцінки кількості інформації, що могла потрапити до зловмисника при реалізації протоколу [1]. Як наближену оцінку, як правило, розглядають інформацію $I_{AE}(D)$, що могла утекти до суб'єкта *E* при виконанні протоколу квантової передачі [1].

Атака розділення числа фотонів (РЧФ) на сьогодні детально досліджена для протоколу BB84 [2,3], який використовується в більшості систем квантового розподілення ключів, що пропонуються на ринку рядом компаній. Але для протоколу із шістьома станами, якій є узагальненням BB84 на максимально можливе для кубітів число взаємно незміщених базисів (три базиси), атака РЧФ раніше не досліджувалась. Протокол з шістьома станами має меншу інформаційну місткість, ніж BB84, але більшу стійкість до некогерентної атаки. Тому дослідження його стійкості до атаки РЧФ є актуальною задачею.

Відомо, що взаємна інформація між суб'єктами *A* і *B* для всіх квантових протоколів розподілення ключів з кубітами дається виразом [3]:

$$I_{AB}(D) = \frac{1}{2}\varphi(1-2D), \tag{1}$$

де *D* – рівень помилок у легітимних користувачів, а функція φ визначається виразом:

$$\varphi(x) = (1-x)\log_2(1-x) + (1+x)\log_2(1+x). \tag{2}$$

У роботі [3] було показано, що при оптимальній некогерентній атаці на протокол BB84 ймовірність для суб'єкта *E* правильно вгадати стан, що був переданий суб'єктом *A*, а відповідно й правильно вгадати переданий біт, дорівнює

$$P_{correct}^{nc}(D) = 1/2 + \sqrt{D(1-D)}. \tag{3}$$

При атаці РЧФ ця ймовірність дається виразом [3]:

$$P_{correct}^{pns} = \frac{1 - e^{-\mu}(1+\mu) + (1-k)\mu e^{-\mu} \cdot P_{correct}^{nc}(D)}{1 - e^{-\mu}(1+\mu k)}, \tag{4}$$

де k – частка однофотонних імпульсів, які блокує суб'єкт E у відповідності до стратегії своєї РЧФ-атаки з заміною квантового каналу зі втратами на ідеальний [1]:

$$k = \frac{1}{\mu}\left(e^{\mu(1-\eta)} - 1\right); \tag{5}$$

μ – середнє число фотонів в імпульсі; η – коефіцієнт передачі каналу.

Остаточно, оскільки ймовірність для суб'єкта E невірно вгадати стан, переданий суб'єктом A, дорівнює $\left(1 - P_{correct}^{pns}(D)\right)$, то $I_{AE}(D)$ для атаки РЧФ на протокол BB84, за аналогією з (1) для $I_{AB}(D)$, просто дорівнює

$$I_{AE}(D) = \frac{1}{2}\varphi\left[1 - 2\left(1 - P_{correct}^{pns}(D)\right)\right], \tag{6}$$

де $\varphi(x)$ означено в (2).

Одержимо тепер вираз для взаємної інформації між легітимним користувачем і зловмисником при атаці РЧФ на протокол із шістьома станами. Ймовірність для зловмисника правильно вгадати переданий стан буде визначатись тим же виразом (4), в який необхідно підставити ймовірність правильно вгадати переданий стан при некогерентній атаці на протокол із шістьома станами.

Відповідна ймовірність була одержана в роботі [4]:

$$P_{correct}^{nc\,(6st)}(D) = \frac{1}{2}\left(1 + D + \sqrt{D(2 - 3D)}\right). \tag{7}$$

Тоді взаємна інформація $I_{AE}(D)$ між суб'єктами A и E при атаці РЧФ на протокол із шістьома станами буде описуватися тим же виразом (6), де $P_{correct}^{pns\,(6st)}(D)$ визначається наступною формулою:

$$P_{correct}^{pns(6st)}(D) = \frac{1 - e^{-\mu}(1 + \mu) + (1 - k)\mu e^{-\mu}\left(1/2\left(1 + D + \sqrt{D(2 - 3D)}\right)\right)}{1 - e^{-\mu}(1 + \mu k)}. \tag{8}$$

На рис. 1 показані криві $I_{AE}(D)$ при атаці РЧФ на протоколи BB84 та з шістьома станами для каналу з невеликими втратами η= 0,9. На рис. 2 показані відповідні криві для каналу з набагато більшими втратами η= 0,5. Як видно з рис. 1, 2, протокол із шістьома станами є більш стійким до атаки РЧФ, ніж протокол BB84, але перевага в стійкості протоколу з шістьома станами невелика.

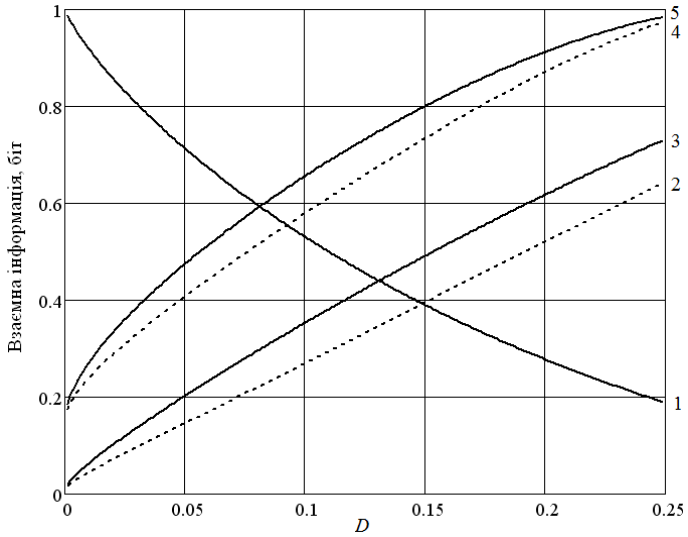

Рисунок 1 – Взаємна інформація при атаці РЧФ на протоколи BB84 і з 6-ма станами при η= 0,9: 1 – взаємна інформація між легітимними користувачами $I_{AB}(D)$; 2 – взаємна інформація $I_{AE}(D)$ при атаці РЧФ на протокол з 6-ма станами при μ = 0,2; 3 – взаємна інформація $I_{AE}(D)$ при атаці РЧФ на протокол BB84 при μ = 0,2; 4 – взаємна інформація $I_{AE}(D)$ при атаці РЧФ на протокол з 6-ма станами при μ = 1; 5 – взаємна інформація $I_{AE}(D)$ при атаці РЧФ на протокол BB84 при μ = 1

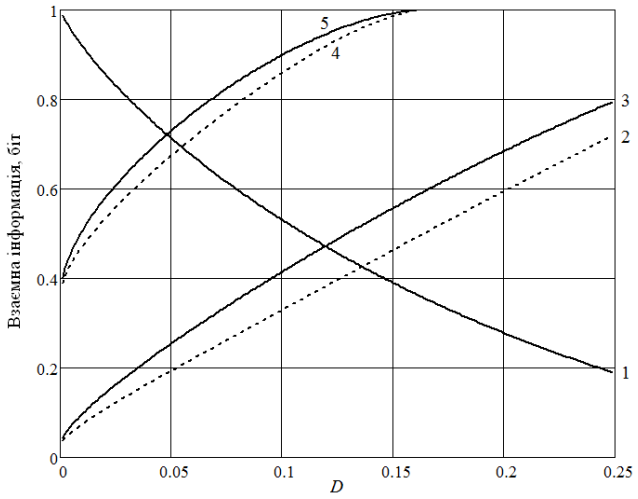

Рисунок 2 – Взаємна інформація при РЧФ-атаці на протоколи BB84 і з 6-ма станами при $\eta = 0{,}5$

Згідно з теоремою Цізара – Кернера [5], легітимні користувачі можуть одержати повністю секретний ключ, виконавши так звану процедуру підсилення секретності, якщо взаємна інформація між ними більше за взаємну інформації між легітимним користувачем та зловмисником $I_{AB}(D) > I_{AE}(D)$. Таким чином, величина рівня помилок $D_{\max}$, яка відповідає точці перетину кривих $I_{AB}(D)$ і $I_{AE}(D)$, є гранично допустимим рівнем помилок, при якому легітимні користувачі можуть встановити секретний ключ.

У табл. 1 наведені одержані чисельним розв'язуванням рівняння $I_{AB}(D_{\max}) = I_{AE}(D_{\max})$ значення $D_{\max}$ для оптимальної некогерентної та когерентної атак на однофотонні імпульси та для атаки РЧФ при тих же значеннях μ і η, що на рис. 1, 2.

Таблиця 1

Максимальні рівні помилок $D_{\max}$ для протоколів BB84 та з шістьома станами, при яких легітимні користувачі можуть встановити секретний ключ

Вид атаки	Параметри		Максимальний рівень помилок для протоколу BB84, %	Максимальний рівень помилок для протоколу із шістьома станами, %
	μ	η		
Оптимальна некогерентна	–	–	14,6	15,6
Розділення числа фотонів	0,2	0,9	13,1	14,9
	1	0,9	8,1	9,2
	0,2	0,5	12,0	13,6
	1	0,5	4,8	5,5
Когерентна	–	–	11,0	11,8

Таким чином, протокол із шістьома станами є дещо більш стійким – на декілька відсотків, як до атак на однофотонні імпульси (некогерентної та когерентної), що було відомо раніше, так і до атаки РЧФ, що є основним результатом цієї роботи. Але платою за цю невелику додаткову стійкість є більш низька інформаційна місткість протоколу із шістьома станами (1/3 для цього протоколу і 1/2 для BB84), і відповідно більш низька швидкість передавання ключа.

Література

1. Gisin, N. Quantum cryptography / N. Gisin, G. Ribordy, W. Tittel, H. Zbinden // Reviews of Modern Physics. – 2002. – V. 74, №1. – P. 145 – 195.
2. Niederberger, A. Photon-number-splitting versus cloning attacks in practical implementations of the Bennett-Brassard 1984 protocol for quantum cryptography /

A. Niederberger, V. Scarani, N. Gisin // Physical Review A. – 2005. – V. 71, №4. – 042316.
3. Williamson, M. Eavesdropping on practical quantum cryptography / M. Williamson, V. Vedral // Journal of Modern Optics. – 2003. – V. 50, issue 13. – P. 1989–2011.
4. Bruss, D. Optimal Eavesdropping in Quantum Cryptography with Six States / D. Bruss // Physical Review Letters. – 1998. – V. 81, issue 14. – P. 3018–3021.
5. Csiszar I. Broadcast channels with confidential messages / I. Csiszar, J. Korner // IEEE Trans. on Inform. Theory. – 1978. – V. IT-24, № 3. – P. 339 – 348.

УДК 351.007

Варда Т.В., Єрьоменко А.І., Бохонько М.В.
ОНПУ.
lyalko_erema@mail.ru
Науковий керівник – к.т.н., Зорило В.В.

РОЗРОБКА ДИНАМІЧНОЇ МОДЕЛІ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ НА ПРИКЛАДІ ГРУПИ КІБЕРБЕЗПЕКИ

Анотація. *Розглянуто проблеми розробки імітаційної моделі процесу інформаційно-психологічного впливу на цільову групу на прикладі групи, що складає типову службу кібербезпеки підприємства або установи. Формулюються принципи та алгоритм моделювання. Запропоновані параметри математичної моделі як динамічної системи. Визначаються план моделювання та область застосування математичної моделі. Розроблена модель дозволить удосконалити та підвищити ефективність формування й професійної виучки членів служби кібербезпеки.*

Вступ. «Інформаційно-психологічний вплив (ІПсВ) – це вплив на свідомість окремої людини, групу осіб та/або населення держави з метою змінення (корекції) їх поведінки [1, с. 6]». Серед об'єктів ІПсВ є системи розробки й прийняття рішень, система формування громадської думки, світогляду, політичних поглядів, загальноприйнятих правил поведінки, інформаційна інфраструктура та її персонал, зокрема професійні групи служби кібернетичної та інформаційної безпеки.

Метою даної роботи є вирішення проблем розробки імітаційної моделі процесу інформаційно-психологічного впливу на цільову групу на прикладі групи, що складає типову службу кібербезпеки підприємства або установи.

Теоретичні положення моделювання.

Теоретична частина моделювання систем інформаційно-психологічної безпеки та сучасних моделей управління масовою свідомістю викладено у [1; 2] та інших. «Імітаційне моделювання є процес конструювання моделі реальної системи та постановки експериментів на цій моделі з метою або зрозуміти поведінку системи, або оцінити різні стратегії, які забезпечують функціонування даної системи [1, с. 272]». Проте, математичних моделей поведінки цих систем є порівняно мало, що зумовлює актуальність таких задач.

Взаємодії людей у групі можна описати за допомогою теорії «збуджуваних середовищ». Основні положення цієї теорії такі [1, с. 277]. Функціонування системи пов'язане з проведенням хвилі збудження або із синхронізацією станів елементів спільноти, яка вивчається. Хвиля розповсюджується за рахунок того, що вона заново генерується кожною точкою дискретного середовища. Тобто хвиля генерується в процесі спілкування кожного члена групи із сусідніми членами. Такі хвилі можуть виникати у різних тематичних групах, наприклад, у студентських групах, групах, які виконують спільну роботу, зокрема у службах кібербезпеки тощо.

Формалізована математична модель збуджуваного середовища у авторів теорії (Н. Вінера та А. Розенблюта) мала такі властивості. Кожен елемент має певний поріг збудження. Хвиля збудження розповсюджується в усі сторони з однаковою швидкістю – на

один сусідній елемент за один модельний такт. Кожен елемент середовища може знаходитись послідовно в одному з трьох станів: *спокою*, в якому елемент характеризується сприйнятливістю до зовнішніх збуджуючих імпульсів, тобто впливів; *активному*, у якому буває лише на миттєвому фронті хвилі; *рефрактерному*, у якому не сприймає збуджуючі сигнали. Рефрактерний стан має постійну тривалість – τ_r. Тому за кожним фронтом активності слідує хвиля рефрактерного стану фіксованої ширини.

Модель середовища доповнюється властивістю спонтанної активності. Спокійний елемент може збуджуватись періодично через певні проміжки часу. Це відповідає випадку, коли в групі є настільки перезбуджені люди, що вони можуть спонтанно активізувати найближчих сусідів. В групі завжди формується один або декілька лідерів, які ведуть інших за собою.

Найпростіший алгоритм.

У розробленій моделі розповсюдження хвилі моделює не переміщення людей у просторі, а передачу думок, характеру поведінки в процесі їх взаємодії між собою. «Нехай кожна людина має вісім сусідів, які безпосередньо можуть взаємодіяти з ним. Активуючі впливи від далі розташованих людей можуть розповсюджуватись на значні відстані. Чим далі розташована конкретна людина від іншого, тим слабше стає сигнал, який він передає. У моделі передбачене сумування збуджуючих сигналів [1, с. 280]». Це є певним аналогом ефекту «думки більшості». Чим більше людей притримуються однієї думки, тим сильніший сигнал отримують сусідні люди.

Даний алгоритм легко модифікувати для більш складних випадків. Можна регулювати поріг збудження. Можна змінювати кількість сусідів, наприклад – 6 або 4. Для створення направлених хвиль не обов'язково мати синхронізатора цієї діяльності або лідера. Таким синхронізатором може бути деяка подія, що привернула увагу людей.

Цікаво, що модель може описувати процес того, «як деяка ідея заволодіває умами, розповсюджується, розвивається і помирає. Якщо традиційні засоби передавання інформації передбачали розповсюдження по ланцюгу від людини, то тепер інформація може бути одночасно доведена до мільйонів членів суспільства через ЗМІ, мобільний зв'язок та Інтернет. Важливим випадком являється розповсюдження певної ідеї всередині віртуальної сфери – соціальної мережі, блогосфери. Пробують моделювати, як, наприклад, певна нова наукова ідея або новий науковий напрям розповсюджується у науковій спільноті [3]».

Формальний опис моделі.

Зразком формального опису моделі являється робота [3]. У випадку, коли люди в групі взаємодіють за принципом «кожен з кожним» модель реалізується за допомогою апарату клітинних автоматів або за допомогою двомірної матриці станів учасників групи. Якщо взаємодія в групі здійснюється за мережним принципом, то модель можна реалізувати як задачу на графах.

У нашому випадку маємо наступне формальне описання моделі. «В моделі Вінера-Розенблюта двомірна сітка складається із елементів, які перенумеровані парою індексів i та j. Стан елементів визначається двома змінними Φ_{ij}^n – фазою та n_{ij}^n – концентрацією активатора. Тут верхній індекс n означає помер модельного часового такту. Елемент переходить із стану спокою у стан збудження, якщо, якщо концентрація активатора перевищує поріг величиною h [3]».

Потім елемент, знаходячись у рефрактерному стані, на кожному такті змінює свою фазу на одиницю. Коли фаза стає рівною $\tau_e + \tau_r$, елемент повертається у стан спокою. Активатор виробляється елементами, які заходяться у збудженому стані. Активатор розпадається на протязі часу $u_{ij}^{n+1} = gu_{ij}^n$. Елементи соціальних систем не являються еквівалентними. Кожен елемент має власний поріг збудження h_{ij}, швидкість розпаду активатора g_{ij}, проміжок часу життя збудженого стану τ_{ij}^e і проміжок часу перебування у рефрактерному стані τ_{ij}^r. Переходи із одного стану в інший здійснюються у відповідності з наступними правилами [3]:

$$\Phi_{ij}^{n+1} = \begin{cases} \Phi_{ij}^{n} & \text{якщо} \quad 0 < \Phi_{ij}^{n} < \tau_{ij}^{e} + \tau_{ij}^{n}, \\ 0 & \text{якщо} \quad \Phi_{ij}^{n} = \tau_{ij}^{e} + \tau_{ij}^{r}, \\ 0 & \text{якщо } \Phi_{ij}^{n} = 0 \text{ й } u_{ij}^{n+1} < h_{ij}, \\ 0 & \text{якщо } \Phi_{ij}^{n} = 0 \text{ й } u_{ij}^{n+1} \geq h_{ij}. \end{cases} \quad (1)$$

Можна вважати, що вплив кожного члена групи на будь-якого іншого є однакові. Тоді кожен елемент отримує активатор від усіх збуджених елементів.

$$u_{ij}^{n+1} = g_{ij} u_{ij}^{n} + \sum_{k,l} C_{kl} I_{i+k,j+l}\,, \quad (2)$$

де матриця C_{kl} описує величину взаємного впливу елементів один на одного. У нашому випадку $C_{kl} = 1$;

$$I_{ij}^{n} = \begin{cases} 1, & \text{якщо} \quad 0 < \Phi_{ij}^{n} \leq \tau_{ij}^{e}, \\ 0, & \text{якщо} \quad \tau_{ij}^{e} < \Phi_{ij}^{n} \leq \tau_{ij}^{e} + \tau_{ij}^{r} \quad \text{або } \Phi_{ij}^{n} = 0. \end{cases}$$

У рівнянні (1) перший доданок описує розпад активатора поточного елемента. Другий доданок – це активатор, який поступає від інших елементів групи.

Висновки.

На слайдах презентації доповіді показані деякі результати моделювання. Застосування математичної моделі процесу інформаційно-психологічного впливу на цільову групу дає потужний інструмент для вивчення складних механізмів синхронізації поведінки людей у групі, перевіряти заходи по захисту від деструктивного впливу. Розроблена модель дозволить удосконалити та підвищити ефективність формування та професійної виучки членів служби кібербезпеки.

Література

1. Петрик В.М. Информационно-психологическая безопасность в эпоху глобализации: учебное пособие / В.М. Петрик, В.В. Остроухов, А.А. Штоквиш // Под ред. В.В. Остроухова. – К., 2008. – 544 с.

2. Минаев В.А. Как управлять массовым сознанием: современные модели : монография [Текст] / В.А. Минаев, А.С. Овчинский, С.В. Скрыль, С.Н. Тростянский Т.В – М., 2012. – 213 с.

3. Тарасевич Ю.Ю. Академическая сеть как возбудимая середа [Текст] / Ю.Ю. Тарасевич, В.А. Зеленухина // Компьютерные исследования и моделирование. Модели экономических и социальных систем. Т. 7 № 1. – Астрахань: АГУ, – 2015. – С. 177-183.

УДК 621.395.7

Ганшин Д.Г.
Харьковский национальный университет радиоэлектроники.
d.hanshyn@gmail.com
Научный руководитель – д.т.н., проф. Цопа О.І.

ОЦЕНКА ЗАЩИЩЕННОСТИ СИСТЕМЫ СВЯЗИ С ПСЕВДОСЛУЧАЙНЫМ СКАЧКООБРАЗНЫМ ИЗМЕНЕНИЕМ ЧАСТОТЫ *OFDM* СИГНАЛА

Аннотация. *Предложен один из вариантов построения системы связи с использованием псевдослучайной перестройки частот OFDM сигнала. На основе концепции отводного канала получены данные скрытности беспроводных широкополосных систем связи с использованием OFDM модуляции, а так же проведена оценка скрытности предложенной системы связи с использованием псевдослучайной перестройкой частоты.*

Для построения производительных ведомственных систем связи, работающих в каналах с частотно-селективными замираниями, приняты целый ряд стандартов передачи мультимедийной информации *ADSL, WLAN, WiMAX, LTE, DAB, DVB-T* на основе технологии с ортогональным частотным разделением каналов *OFDM* (*Orthogonal Frequency-Division Multiplexing*), которая может успешно противостоять межсимвольной интерференции [1].

В тоже время псевдослучайная перестройка рабочей частоты (ППРЧ) является одним из двух основных распространенных методов расширения спектра сигналов, которые также позволяют повысить эффективность работы в частотно-селективных каналах, и имеет низкую вероятность перехвата (*LPI - low probability of interception*). Этот метод широко применяется в системах военной связи для работы в условиях сильных преднамеренных помех, а также используется в некоторых беспроводных стандартах передачи информации, таких как *GSM*, *Bluetooth* и др. [2].

Сочетание технологии *OFDM* и ППРЧ, позволяет существенно увеличить спектральную эффективность, повысить защищенность системы связи от перехвата, снизить влияние многолучевости, а также существенно уменьшить влияние помех.

В докладе рассматривается один из вариантов построения системы связи с псевдослучайным скачкообразным изменением частоты *OFDM* сигнала (рис. 1).

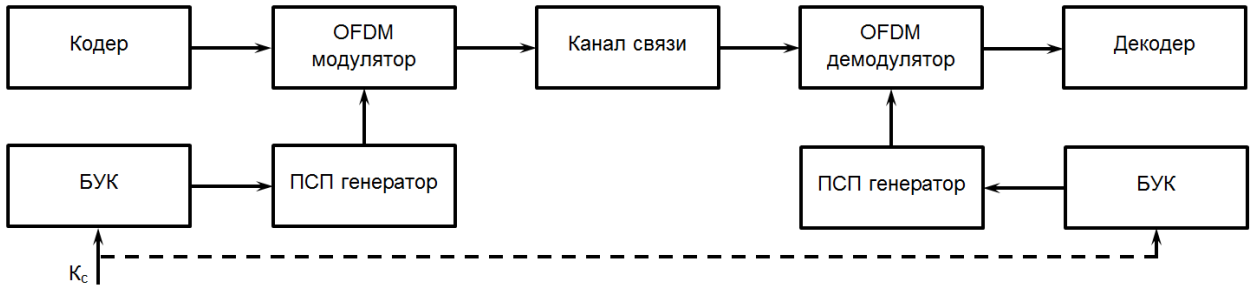

Рисунок 1 – Упрощенная стуркурная схема системы связи с псевдослучайной перестройки частоты *OFDM* сигнала

В данном примере формирования псевдослучайной перестройки частоты происходит после цифроаналогового преобразователя, который подключен к смесителю (рис. 2).

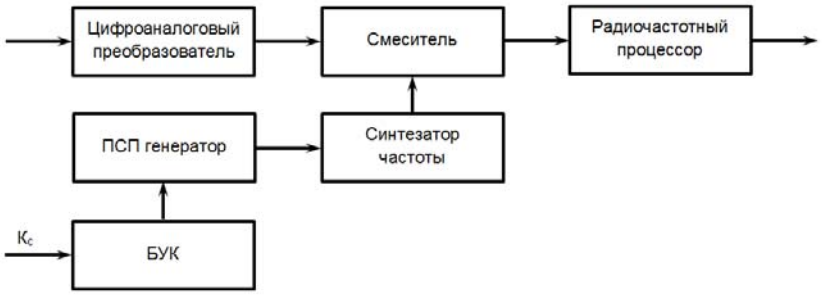

Рисунок 2 – Формирование псевдослучайной перестройки частоты *OFDM* сигнала

На выходе смесителя формируеться *OFDM* сигнал с псевдослучайной перестойкой частоты (рис. 3). Синтезатор частоты управляется генератором псевдослучайной последовательности, который в свою очередь управляеться блоком управления ключем (БУК).

Ключ K_C поступает в блок управления ключем в котором формируеться новый ключ. Для формировании нового ключа в данном блоке может использоваться М-последовательность. Ново сформированный ключ поступает в генератор псевдослучайной последовательности. В ПСП генераторе используеться М-последовательность.

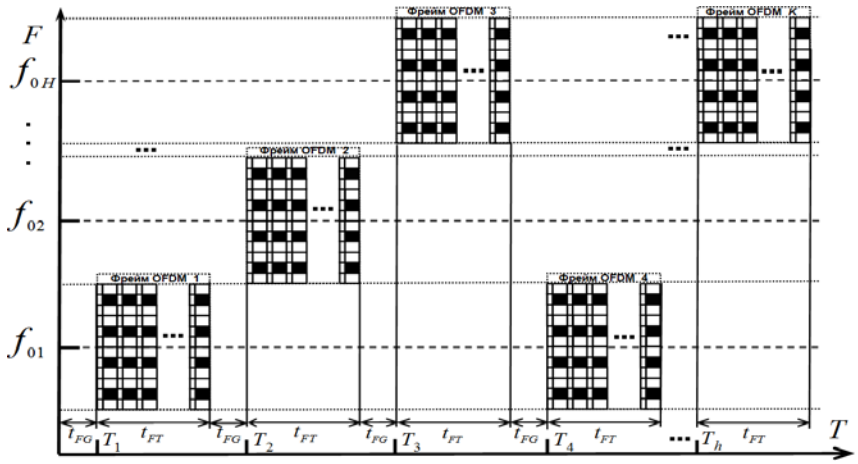

Рисунок 3 – Частотно временная диаграмма сформированного OFDM сигнала с псевдослучайной перестройкой по частоте

Оценка потенциальной структурной скрытности системы связи, является одним из важнейших параметров систем связи. Противостояние системы против радиотехнической разведки, которая предполагает выполнения трех основных задач таких как: выявления факта работы системы связи (обнаружения сигнала); определение структуры обнаруженного сигнала и его основных параметров; раскрытие передаваемой информации.

При оценке скрытности сигналов используются два основных подхода. В первом скрытность определяется как вероятность успешного выявления сигнала в заданное время. Во втором оценивают скрытность сигнала через затраты на выявления его состояния с заданной достоверностью (вероятность правильного решения).

Потенциальная скрытность является характеристикой собственно объекта исследования (в нашем случае сигнала), его выраженным в числовой форме качеством, способностью противостоять выявлению текущего состояния. Потенциальная скрытность сигнала не зависит от действий системы выявления его состояний, так как предполагает использование оптимального алгоритма поиска. Фактически она является наиболее «*осторожной*» оценкой скрытности.

Потенциальная структурная скрытность зависит от ансамбля (арсенала) A реализаций сигнала и определяется числом двоичных измерений (диз), которые необходимо осуществить для раскрытия структуры широкополосного сигнала. Общее выражение для потенциальной структурной скрытности имеет вид [1]:

$$S_P = \log_2 A \ \ [\text{диз}], \tag{1}$$

где A – ансамбль (арсенал) реализаций, определяемый количеством всех возможных значений каких-либо параметров сигнала.

Такими параметрами сигнала могут быть несущая частота, амплитуда, вид модуляции, структура линейного кода, параметры формы и временные характеристики сигнала, а также другие специфические параметры, зависящие от физического уровня конкретной технологии передачи сигналов. В общем случае скрытность зависит от способа построения конкретного вида сигнала, используемого для переноса информации.

Оценка структурной скрытности *OFDM* сигналов с учетом возможных ансамблей значений параметров данного сигнала можно провести, используя формулу (2):

$$S_P = S_{OFDM} + S_{QAM} \tag{2}$$

На основе этого подхода можно дать оценку потенциальной скрытности предложенной нами системы связи с псевдослучайной перестройки частоты *OFDM* сигнала.

$$S_P = S_{OFDM} + S_{QAM} + S_{ППРЧ} \tag{3}$$

В табл. 1 приведены данные о потенциальной структурной скрытности сигналов современных беспроводных систем связи: *Wi-Fi, WiMAX, LTE, DBV*.

Таблица 1

Данные о структурной скрытности сигналов *OFDM* для различных систем связи

Вид технологии	Тип сигнала	Количество поднесущих частот *N*	Уровень модуляции *M-QAM*	Длина *L* фрейма *OFDM*	ППРЧ *B*	Скрытность S, диз
Wi-Fi IEEE.802.11	*OFDM*	64	16	80	-	10
WiMAX IEEE.802.16d	*OFDM*	256	256	40	-	16
WiMAX IEEE.802.16e	*OFDM*	512	256	40	-	17
LTE	*OFDM*	1024	256	120	-	18
DBV-T	*OFDM*	6800	64	40	-	18
DBV-T2	*OFDM*	32000	256	40	-	23
Система FH-OFDM	*OFDM*	2048	256	120	100	482

С табл.1 видно, что в системах с использованием псевдослучайной перестройки частоты *OFDM* сигнала существенно повышается скрытность системы связи.

Література

1. Методы прогнозирования защищенности ведомственных систем связи, основанные на концепции отводного канала. / Под редакцией А. И. Цопы и В. М. Шокало. – Харьков: КП «Городская типография», 2011. – 502 с.

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

3. Ганшин Д. Г. Исследование защищенности системы связи с многочастотными сигналами. / Д. Г. Ганшин, В. В. Маслий, А. И. Цопа // Радиотехника. Всеукраинский межведомственный научно-технический сборник. – 2013. – Выпуск № 173. – С. 195-203.

УДК 004.056.53:004.492.3

Гізун А.І.
Національний авіаційний університет.
andriy.gizun@gmail.com

СИСТЕМИ УПРАВЛІННЯ КРИЗОВИМИ СИТУАЦІЯМИ ЯК СКЛАДОВА СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. *Концепція управління безперервністю бізнесу як перспективний напрям оперативного та стратегічного менеджменту визначає важливість захисту інформаційних ресурсів в умовах впливу кризових ситуацій. У цій роботі проведений аналіз систем управління кризовими ситуаціями і обґрунтоване їх віднесення до окремого класу в структурі системи менеджменту інформаційної безпеки, визначені їх функціональні взаємозв'язки з іншими захисними системами, такими як системи виявлення та попередження вторгнень, системи аналізу та оцінки ризиків, системи антивірусного захисту, системи управління інцидентами інформаційної безпеки.*

Внаслідок розвитку можливостей ІТ у сучасному світі пріоритетним напрямом є автоматизація управлінських, технологічних, виробничих та інших процесів. Інформаційні системи займають провідні ролі в системі функціонування бізнесу та держави, причому взаємозв'язок ІТ та бізнес-процесів стає настільки тісним, що життєздатність підприємств

повністю залежить від надійності технологій, що забезпечують підтримку найбільш важливих критичних підприємницьких процесів. Так, невпинно зростає роль систем реагування на кризові явища в процесі управління та підтримання життєздатності підприємств та організацій усіх форм власності. Тому великі корпорації почали цілеспрямовано впроваджувати технології забезпечення безперервності бізнесу в непередбачених ситуаціях [1,2]. У розвинених країнах ринок технологій і послуг, що забезпечують безперервність бізнесу, динамічно розвивається. Рівень його зростання становить близько 25% на рік і обумовлений, головним чином, тим, що середні компанії слідом за лідерами індустрії активно впроваджують у своїй діяльності технології управління кризовими ситуаціями (КС) [2].

Однак, залишається досить багато проблем. Зокрема, слід відзначити, наявність багатьох різних трактувань основних моментів концепції управління безперервністю бізнесу та недостатній рівень реалізації технічних систем управління КС (СУКС), в першу чергу, в інформаційній сфері. Тому основною метою даної статті є аналіз та визначення місця і ролі систем управління КС в системі менеджменту інформаційної безпеки (СМІБ).

В роботі [3] запропонований прототип системи виявлення КС і ліквідації їх наслідків, заснованої на застосуванні методів нечіткої логіки, та її базова архітектура, а в [4,5] описані відповідні методи, на яких вона реалізуються. Крім того, відомі роботи щодо розробки і створення подібних методів [6] та систем [7] для виявлення порушника інформаційної безпеки в комп'ютерних системах та мережах. Тому, для ефективного забезпечення стану інформаційної безпеки та безперервності бізнесу необхідною вбачається розробка системи виявлення інцидентів/потенційних кризових ситуацій (СВІПКС) та системи оцінки критичності ситуації, спричиненої виявленим інцидентом (СОКС). Покажемо місце і роль цих систем в менеджменті інформаційної безпеки.

Серія міжнародних стандартів ISO 27k регламентує і визначає основні процеси управління інформаційною безпекою, в тому числі, охоплює питання управління ризиками, інформаційними ресурсами, комунікаціями, інцидентами інформаційної безпеки тощо. Згідно стандартів, створення систем менеджменту інформаційної безпеки (СМІБ) здійснюється в чотири етапи: планування та створення ІС; впровадження та використання; моніторинг та аудит; підтримка та вдосконалення ІС, що повністю відповідають циклу Шухарта-Демінга (цикл PDCA). Таким чином, захист інформації реалізується завдяки використанню сукупності різноманітних систем проектування, моніторингу, аудиту, керування інформаційною безпекою і іншими сферами обслуговування та управління ІС. Серед таких систем доцільно виділити системи антивірусного захисту (САЗ), системи виявлення/попередження вторгнень (IDS/IPS), системи аналізу та оцінки ризиків (САОР), системи управління інцидентами інформаційної безпеки (СУІБ, що включають в себе програмне та апаратне забезпечення для команд реагування на комп'ютерні інциденти (CERT) щодо фіксації, ідентифікації, обробки, реагування, ліквідації інцидентів, збирання статистичних даних тощо). Визначені системні засоби функціонують на кожному з етапів циклу PDCA і інтегруються в системах менеджменту (управління) інформаційної безпеки.

Отже, виходячи з функціоналу і взаємодії між собою зазначених захисних систем, проектовані СВІПКС та СОКС разом з САЗ і IDS/IPS утворюють особливий клас СМІБ – СУКС. Серед основних функцій СУКС слід виділити виявлення, ідентифікацію КС, проведення їх оцінки, забезпечення прийняття рішень в умовах КС та автоматизація цього процесу, підбір засобів реагування, ліквідація КС і т.п. На сьогодні в світі даний клас реалізований у вигляді вузькоспеціалізованих засобів, які, в основному, не застосовуються в сфері інформаційної безпеки, а також не можуть бути використані в умовах нечіткості. Детальний аналіз відомих СУКС наведено в [8]. Місце СУКС в менеджменті інформаційної безпеки та взаємозв'язки даного класу систем з іншими системами захисту інформації представлено на рис. 1.

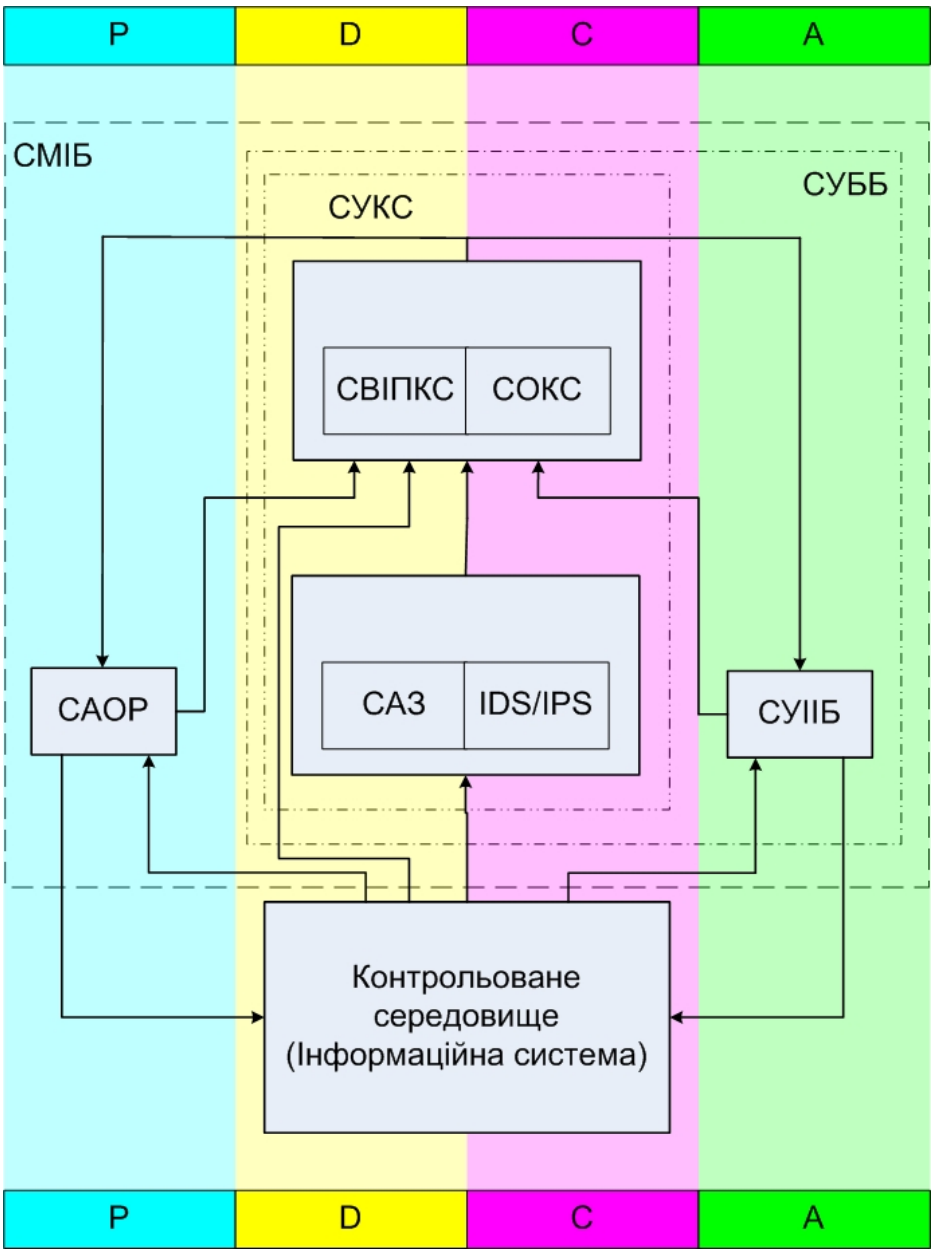

Рисунок 1 – Взаємозв’язки СУКС з компонентами СМІБ

Як видно з рисунку, САОР переважно використовуються на етапі планування і створення ІС, САЗ та IDS/IPS в основному взаємодіють з ІС, що захищається, на стадіях впровадження та моніторингу, а СУІІБ – на етапі підтримки та вдосконалення. Слід зазначити, що СВІПКС і СОКС на етапах впровадження та моніторингу взаємодіють з інформаційними системами безпосередньо або через САЗ та IDS/IPS і є основою класу СУКС. В поєднанні з СУІІБ СУКС утворюють клас систем управління безперервності бізнесу (СУББ), який разом з САОР формують загальний клас СМІБ. Розроблені системи СВІПКС та СОКС в якості вхідних даних використовують параметри, зняті давачами в контрольованому середовищі (тобто в інформаційних системах або мережевих пристроях), а також інформацію з САОР, САЗ, IDS/IPS, СУІІБ і крім того мають зворотний зв'язок з САОР та СУІІБ, що забезпечує можливість корегування їх роботи, оновлення даних та формування статистики.

Таким чином, запропоновані системні засоби є невід’ємною складовою СМІБ і разом з тим утворюють окремий клас СУКС, що може функціонувати для вирішення задач захисту інформації в поєднанні з відомими захисними системами, розширяючи їх функціональні можливості, або автономно, замінюючи більшість з них.

Висновки. Розглянуті сучасні системи управління кризовими ситуаціями, а також їх основні характеристики, що надало можливість виділення даних систем в окремий клас. Визначено місце та взаємозв'язки систем управління кризовими ситуаціями з компонентами системи менеджменту інформаційної безпеки, а саме, встановлено особливості взаємодії з іншими системами менеджменту та захисту інформації.

Список літератури

1. Гізун А.І. Сучасні підходи до захисту інформаційних ресурсів для забезпечення безперервності бізнесу / А.І. Гізун, В.О. Гнатюк, О.П. Дуксенко, А.О. Корченко // Матеріали X Міжнародної наук–техн. конференції «АВІА–2011». – К.: НАУ, 2011. – Т1 – С. 2.5-2.9.
2. Петренко С.А. Управление непрерывностью бизнеса. Ваш бизнес будет продолжаться / С.А. Петренко, А.В. Беляєв – М.: ДМК–Пресс, Компания АйТи, 2011. – 400 с.
3. Harris S. CISSP Certification All–in–One Exam Guide / S. Harris. – McGraw–Hill Osborne Media, 2010. – 5th edition. – 1216 p.
4. Іванченко Є.В. Базова архітектура експертної системи прогнозування та попередження кризових ситуацій / Є.В. Іванченко, О.В. Гавриленко, А.І. Гізун // Захист інформації. – 2012. – № 3. – С. 94-104.
5. Карпінський М.П. Метод виявлення інцидентів/потенційних кризових ситуацій / М.П. Карпінський, А.О. Корченко, А.І. Гізун // Захист інформації. – 2015. – Т.17. – №2. – С. 124-130.
6. Корченко А.О. Метод оцінки рівня критичності для систем управління кризовими ситуаціями / А.О. Корченко, В.А. Козачок, А.І. Гізун // Захист інформації. – 2015.– Т.17. – №1. – С. 86-98.
7. Корченко А.О. Метод виявлення та ідентифікації порушника в інформаційно-комунікаційних системах / А.О. Корченко, А.І. Гізун, В.В. Волянська, С.О. Гнатюк // Захист інформації. – 2013. – Т.15. – №4. – С. 387-393.
8. Корченко А.О. Система виявлення та ідентифікації порушника в інформаційно-комунікаційних мережах / А.О. Корченко, В.В. Волянська, А.І. Гізун // Безпека інформації. – 2013. – Т.19. – №3. – С. 158-162.
9. Гізун А.І. Аналіз сучасних систем управління кризовими ситуаціями / А.І. Гізун, А.О. Корченко, С.О. Скворцов // Безпека інформації. – 2015. – Т.21. – №1. – С. 87-101.

УДК 32.019.51:94

Гріга В.С., Гізун А.І., Іванченко І.С.
Національний авіаційний університет.
gsmgrey1@gmail.com

ХАРАКТЕРИСТИКА БАЗОВИХ СКЛАДОВИХ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА

Анотація. *Досліджено наявні теорії інформаційного протиборства. Представлено характеристики його базових складових – інформаційної війни, спеціальної інформаційної операції та акції інформаційного впливу. Проведено порівняння вищенаведених компонентів. Під час дослідження виявилося, що інформаційна війна є найбільш складним і затратним компонентом інформаційного протиборства, на відміну від акції інформаційного впливу, яка може здійснюватися суб'єктами навіть несвідомо.*

Керування інформаційними потоками внаслідок інформатизації та технічного розвитку суспільства має у наші дні досить велике значення. Важливість інформаційного протиборства доводив китайський воєначальник Сунь-Цзи у своєму Трактаті «Мистецтво війни» ще у IV ст. до н. е., але повністю світова спільнота усвідомила це в 2010-их рр., коли

воно почало вноситися у військові доктрини багатьох держав світу. Першим документально засвідченим дослідженням з теорії інформаційного протиборства є робота М. Лібікі «Що таке інформаційна війна?», (серпень 1995 року, Національний інститут оборони США). У ній автор намагався розкрити суть інформаційного протиборства та війни, а також визначив її форми. Однак ще раніше термін «інформаційна війна» увів в обіг китайський теоретик Шень Веньгуань [5]. Значних успіхів досягли американські дослідники Дж. Стейн і Р. Шафранскі, російський С. Расторгуєв, українські Я. Жарков, В. Петрик, М. Присяжнюк.

Метою роботи є визначення та дослідження базових складових інформаційного протиборства, їх порівняння та розкриття основних ознак та особливостей для формування концептуального поняття теорії інформаційних воєн.

В теорії інформаційних протиборств основне місце займає інформаційний вплив – організований та цілеспрямований вплив за допомогою інформаційних технологій на свідомість особистості, соціальних груп, суспільства та народу, інформаційну інфраструктуру, що поділяється на інформаційно-психологічний та інформаційно-технічний вплив. Інформаційно-психологічний вплив – це вплив на свідомість та підсвідомість людини та суспільства з метою внесення змін в їх поведінку [1]. Інформаційно-технічний вплив – це вплив на інформаційну інфраструктуру з метою внесення змін в її роботу. Реалізація названих впливів породжує інформаційне протиборство Формами інформаційного протиборства є інформаційні війни, спеціальні інформаційні операції (СІО) та акції інформаційного впливу (АІВ). Інформаційна війна – це форма ведення інформаційного протиборства між різними суб'єктами, що передбачає здійснення комплексу заходів із завдання шкоди інформаційній сфері конфронтуючої сторони й захисту власної інформаційної безпеки. Інформаційні війни складаються з СІО та АІВ.

Акція інформаційного впливу – це одноразова акція інформаційно-психологічного та інформаційно-технічного впливу, яка передбачає спланований впливу на свідомість і поведінку людей [3]. Основними ознаками їх є сенсаційність, лавино подібність розгортання подій, короткостроковість. АІВ тривають один-три дні. Основними суб'єктами АІВ виступають ЗМІ, неурядові організації, Інтернет-ресурси. Об'єктами АІВ є свідомість і підсвідомість суспільства, певної групи людей. Головним інструментом АІВ є «інформаційний вкид», який надалі різними методами використовується задля досягнення певних цілей. «Інформаційний вкид» - це інформаційна новина, здебільшого не правдивого характеру, яка з'являється в інформаційному просторі та за достовірність і джерело якої ніхто не несе відповідальність. Основними методами проведення АІВ є дезінформування та поширення чуток.

Дезінформування – це метод, який передбачає обман чи уведення об'єкта впливу в оману щодо справжності намірів для спонукання його до запрограмованих дій [4]. Найчастіше у світовій практиці застосовуються такі форми дезінформування: тенденційне викладення фактів; дезінформування "від зворотного"; термінологічне "мінування"; "сіре" та "чорне" дезінформування. У загальному вигляді акції дезінформування можуть проводитися шляхом створення видимості випадкового витоку закритої інформації, успіхів розвідки іноземних партнерів, використання засобів масової інформації (власні інформаційні агентства, теле-, радіокомпанії, друковані видання, "кишенькові" журналісти й т. ін.) [2].

Поширення чуток – це діяльність щодо поширення переважно неправдивої інформації серед широких верств населення здебільшого неофіційними каналами з метою дезорганізації суспільства та держави або їхніх установ чи організацій [2]. За одним із визначень, чутки – це циркулююча форма комунікації, за допомогою якої люди, котрі перебувають у неоднозначній ситуації, об'єднуються, утворюючи зрозумілу їм інтерпретацію цієї ситуації, спільно використовуючи власні інтелектуальні можливості. Чутки можна класифікувати за експресивною характеристикою на чутки-бажання, чутки-залякування й роз'єднувальні агресивні чутки, за інформаційною характеристикою – на абсолютно недостовірні, недостовірні, недостовірні з елементами правдоподібності та правдоподібні [2,4]. Чутки самопоширювані. Позитивний чинник використання цієї форми АІВ полягає ще й у тому, що

практично немає ефективних засобів протидії чуткам. На офіційному рівні зупинити їх неможливо: офіційні заходи протидії викликають прямо протилежний ефект: для людей, яких безпосередньо цікавлять чутки, це є підтвердженням правдивості останніх [3].

Середня вартість проведення однієї АІВ складає порядку 1 тис. Євро. Цілями проведення АІВ є порушення стабільного стану інформаційного простору держави, «розігрів» аудиторії різноплановою інформацією задля підтримки нестабільності інформаційного простору та створення певної аудиторії. Основним результатом проведення АІВ є створення інформаційного приводу для можливого подальшого проведення СІО та зацікавлення певною аудиторією новиною, «інформаційним вкидом» [4]. Прикладом АІВ є випуск новин на телеканалі «Россия24», згідно яких українські бійці у зоні АТО катували хлопчика у м. Слов'янськ Донецької області.

Спеціальна інформаційна операція – це сплановані дії, спрямовані на аудиторію з метою схилення до прийняття певних рішень або (та) вчинення певних дій, вигідних для суб'єкта інформаційного впливу. Перед здійсненням операції може відбутися кілька АІВ. Існує класичний алгоритм проведення СІО: 1) Інформаційний етап; 2) «Розкручування» інформаційного приводу; 3) Загострення напруження; 4) Вихід із операції або етап закріплення. Основними ознаками проведення СІО є збільшення повідомлень негативного змісту з певної тематики, зростання емоційності, зростання тенденційності, збільшення сенсаційності, лавиноподібність розгортання подій, взаємоузгодження дій суб'єктами операції. СІО проводяться за час від одного тижня до двох місяців. Основними суб'єктами СІО виступають керівництва іноземних держав, ЗМІ, неурядові організації, спецслужби іноземних держав, Інтернет ресурси, агентура впливу іноземних держав. Об'єктами СІО є свідомість і підсвідомість «людини, що приймає рішення», населення країни.

СІО передбачає досягнення різних цілей залежно від стадії інформаційного протиборства (див. таблицю 1) [2]. Основними методами проведення СІО є пропаганда, диверсифікація громадської думки, психологічний тиск. Пропаганда – поширення політичних, філософських, наукових, художніх, інших мистецьких ідей із метою їх упровадження в громадську думку та активізації використання цих ідей у масовій практичній діяльності населення. Водночас до пропаганди належать повідомлення, які поширюються для здійснення вигідного впливу на громадську думку, провокування запрограмованих емоцій та зміни ставлення чи поводження певної групи людей у напрямі, безпосередньо чи опосередковано вигідному організаторам. Диверсифікація громадської думки – це розпорошення уваги панівної еліти держави на різні штучно акцентовані проблеми й відволікання цим від вирішення нагальних завдань суспільно-політичного та економічного розвитку для нормального функціонування суспільства й країни. Форми диверсифікації громадської думки: дестабілізація обстановки в державі чи окремих її регіонах; активізація кампаній проти політичного курсу панівної еліти та окремих її лідерів різними міжнародними установами; ініціювання антидемпінгових кампаній й іншого роду скандальних судових процесів, застосування міжнародних санкцій з інших причин. Психологічний тиск – це вплив на психіку людини шляхом залякування, погроз із метою її спонукання до запланованої моделі поведінки. Форми психологічного тиску: доведення до об'єкта впливу відомостей про реальні чи неіснуючі загрози та небезпеки; прогнози щодо репресій, переслідувань, убивств тощо; шантажування; здійснення вибухів, підпалів, масових отруєнь, захоплень заручників, інших терористичних акцій.

Середня вартість однієї СІО складає порядку 100 тис. Євро. Результатом проведення СІО є зміни в поведінці та (або) світогляді певної групи людей або суспільства. Прикладом проведення СІО є підготовка Росією до анексії Автономної республіки Крим, згідно якої населення півострова переконували у їхній приналежності до російського народу та т. з. «історичну помилку» передачі у 1954 р. республіки Україні.

Отже, представимо узагальнену таблицю порівняння АІВ та СІО (табл. 1).

Таблиця 1

Порівняння СІО та АІВ як складових інформаційного протиборства

Параметри	АІВ	СІО
Об'єкти	Свідомість і підсвідомість суспільства, певна група людей.	Свідомість і підсвідомість «людини, що приймає рішення», суспільство.
Суб'єкти	ЗМІ, неурядові організації, Інтернет-ресурси.	Керівництва іноземних держав, ЗМІ, неурядові організації, спецслужби іноземних держав, Інтернет-ресурси, агентура впливу іноземних держав
Ціль	Порушення стабільного стану інформаційного простору, «розігрів» аудиторії, створення певної аудиторії суспільства.	Домінування в інформаційному просторі, вплив на соціально-політичну ситуацію в регіоні,; інформаційно-психологічне забезпечення діяльності вищого військово-політичного керівництва; забезпечення процесу формування лояльної влади, сприяння соціально-економічному розвитку в регіоні.
Час на проведення	1-3 доби	Від 1 тижня до 2 місяців
Вартість проведення	1 тис. Євро	100 тис. Євро
Результати	Створення інформаційного приводу, «зацікавлення» певною інформацією	Зміни в поведінці та (або) світогляді людей або суспільства

Висновок. Базовими характеристиками інформаційного протиборства є інформаційна війна, спеціальні інформаційні операції, акції інформаційного впливу. Причому, інформаційна війна є симбіозом двох інших компонентів. В роботі виокремленні та розглянуті основні характеристики цих компонент, зокрема їх об'єкти, суб'єкти, ціль, час на проведення, вартість проведення та результати.

Список літератури

1. В. Грига. Информационно-психологическая безопасность общества, как средство сохранения народа / В. Грига, С. Гнатюк, А. Гизун // Безпека інформації. – 2015. – Том 21 #2. – С. 179-191.

2. Жарков Я. М. Інформаційно-психологічне протиборство (еволюція та сучасність) : монографія / Я. М. Жарков, В. М. Петрик, М. М. Присяжнюк [та ін.]. – К. : ПАТ «Віпол», – 2013. – 248 с.

3. Почепцов Г. Г. Информационные войны / Г. Г. Почепцов. – Москва-Киев :Ваклер-Рефлбук, 2000. – 576 с.

4. Гриняев С. Н. Война в четвертой сфере / С. Н. Гриняев // Независимое военное обозрение. – 2000. – № 42.

5. Бєльська Т. В. Інформаційно-психологічна війна як спосіб впливу на громадянське суспільство та державну політику держави / Т. В. Бєльська. – Технології та механізми державного управління. – 2014. – №3. – С. 49-56.

УДК 004.451.056.53

Зерко А. Л.
КНУ імені Т. Шевченка
a.l.zerko@ukr.net
Науковий керівник – д. т. н., Оксіюк О. Г.

ДОСЛІДЖЕННЯ ВАЖЛИВОСТІ ПОБУДОВИ МАТЕМАТИЧНИХ МОДЕЛЕЙ ДОВЕДЕННЯ ЗАХИЩЕНОСТІ ОПЕРАЦІЙНИХ СИСТЕМ

Анотація. *Проведено аналіз сучасного стану забезпечення захисту інформації та цілісності інформації в середовищі операційних систем. Проведено дослідження наявності та рівня механізмів захисту інформації в операційних системах, системі захисту інформації та антивірусного програмного забезпечення, основуючись на експертні висновки Державної Служби Спеціального Зв'язку та Захисту Інформації України і документи системи Технічного Захисту Інформації. Розгляд проблеми визначення загальної оцінки захищеності ОС з додатковим програмним забезпеченням. Обґрунтування необхідності побудови математичної моделі оцінки захисту інформації.*

З появою інформаційних цифрових технологій та початком їх використання загострилось питання захисту інформації. На сьогоднішній день питання та проблеми захисту інформації є зростаючою в важливості темою. І поки будуть існувати й розвиватись цифрові технології – актуальним буде питання забезпечення захисту інформації.

Зазначимо, що одну з найважливіших ролей в захисті інформації грає забезпечення безпеки та надійності операційної системи (надалі ОС). Дуже багато факторів можуть впливати на забезпечення захищеності ОС. У сучасних ОС розробниками реалізовано певний перелік механізмів забезпечення безпеки – алгоритми шифрування інформації, автентифікації при доступі до інформації, захисту від несанкціонованого доступу тощо. Проте наявність механізмів захисту не дає гарантій захищеності інформації в ОС, адже захист інформації також має забезпечувати й програмне забезпечення встановлене в середовищі ОС.

Питання забезпечення надійності та безпеки інформації і самої ОС в процесі життєвого циклу системи в цілому є одним з найменш досліджуваних. З часом компоненти програмного забезпечення можуть втрачати свій рівень захисту, можуть з'являтися прогалини в механізмах захисту, можуть накопичуватися помилки, які не видно для звичайних користувачів, а іноді і для адміністраторів безпеки. Також завжди залишається питання надійності апаратного забезпечення.

В Україні існує своя законодавча база оцінки рівнів захисту програмного забезпечення, яка основується на стандартах оцінювання нормативного документа Системи Технічного Захисту Інформації. Проведено дослідження забезпечення захисту інформації деякого програмного забезпечення.

Без відповідей залишається питання забезпечення надійності та безпеки функціонування системи захисту інформації в середовищі ОС – кожен з компонент має власні механізми захисту інформації, які використовують пріоритетні механізми захисту інформації в середовищі ОС.

Висновки

Розглянуто дві основні проблеми забезпечення надійності та безпеки сучасних ОС:

1. Строге доведення захищеності та надійності ОС, як єдиного комплексу;
2. Виконання математичних оцінок захищеності та надійності роботи ОС під час життєвого циклу, з урахуванням програмного забезпечення, що використовується в середовищі ОС.

Вирішення таких питань без побудови математичних моделей оцінки забезпечення захищеності інформації в ОС – не уявляється можливим.

Література

1. Державна служба спеціального зв'язку та захисту інформації України. http://www.dstszi.gov.ua/dstszi/control/uk/index.
2. Компанія «АТМНІС», https://atmnis.com/files/user_files/BBOS.pdf.
3. Компанія «Майлинукс», http://mylinux.ua/press-release5.

УДК 003.26:004.056.55

Золотарьова Д.О.,
ОНПУ.
allacia.gilbert@gmail.com
Науковий керівник – к.т.н., доц. Кононович В.Г.

МОДЕЛЮВАННЯ ПРОЦЕСУ УПРАВЛІННЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОЮ БЕЗПЕКОЮ ІНДИВІДУАЛЬНОЇ СВІДОМОСТІ ТА ОБРАЗУ МАЙБУТНЬОГО

Анотація. *Розглянуто проблему моделювання процесу управління інформаційною та психологічною безпекою колективної та індивідуальної свідомості, і, зокрема, її складової – колективного образу майбутнього. Представлена словесна модель суб'єкта-агресора. Запропонована спрощена математична модель багатоетапного кібернетичного циклу управління. Математична модель будується як відкрита динамічна система із вхідним і вихідними потоками інформації та взаємодією між етапами циклу. Модель дозволяє проводити дослідження динаміки циклічних процесів із зворотними зв'язками в термінах системи формування індивідуальної та масової свідомості в умовах деструктивного впливу. Отримані результати дозволять удосконалити та підвищити ефективність системи формування позитивного образу майбутнього у громадян України.*

Науково-практичними дослідженнями відмічається «дуже важлива залежність національної безпеки держави від забезпечення інформаційної безпеки, яка постійно буде зростати за мірою розвитку інформаційних технологій [1, с. 6]». Одною з важливих проблем, яка вимагає свого вдосконалення, є управління інформаційною безпекою колективної та індивідуальної свідомості. «Прийдешня інформаційна епоха характеризується специфічною формою соціальної організації, в якій нові технології генерування, обробки й передачі інформації стали фундаментальним джерелом продуктивності і влади [2, с. 5]». Інформаційна складова управлінської, виробничої, суспільної, політичної, освітньої, культурної, і навіть побутової діяльності набуває небувалої ваги і проходить в умовах як законної конкурентної розвідки, так і жорсткого ворожого інформаційного протистояння й інформаційної війни. Численні публікації містять словесні структурні моделі управління системами інформаційної безпеки колективної та індивідуальної свідомості й формування позитивного образу майбутнього. Теоретичний аналіз соціально-психологічних факторів прогнозування колективного образу майбутнього пропонується в [3]. Проте, математичних моделей поведінки цих систем є порівняно мало, що зумовлює актуальність таких задач.

Метою даної роботи є використання апарату дискретних відображень для розробки математичної моделі процесу управління інформаційною безпекою колективної та індивідуальної свідомості й системи формування позитивного образу майбутнього у громадян України, а також саме моделювання. Для здійснення цієї мети вирішуються задачі: аналізу основних теоретичних підходів до методів забезпечення інформаційної безпеки колективної та індивідуальної свідомості й формування колективного образу майбутнього;

аналізу існуючих структурних і математичних моделей та сфер їх застосування; вибору та адаптації математичної моделі згідно визначеної мети роботи.

Основна термінологія та особливості об'єкта моделювання. Приймемо, що «*інформаційна безпека* – це стан захищеності об'єкта (особи, суспільства, держави, інформаційно-технічної інфраструктури), за якого досягається його нормальне функціонування незалежно від наявності внутрішніх та зовнішніх впливів [1, с. 45]». Конкретно, «*інформаційна безпека особистості* – це стан захищеності психіки людини від негативного впливу, який здійснюється шляхом впровадження деструктивної інформації у свідомість та (або) підсвідомість людини, що приводить до неадекватного сприймання ним дійсності [1, с. 46]» А «*інформаційна безпека суспільства* – це можливість безперешкодної реалізації суспільством та окремими його членами своїх конституційних прав, пов'язаною з можливістю вільного отримання створення й поширення інформації, а також степінь їх захисту від деструктивного інформаційного впливу. Основні положення формування образу майбутнього наведені в роботі Нестик. «Без розуміння соціально-психологічних аспектів групового відношення до майбутнього дуже важко розширити горизонт передбачення в сучасних організаціях і суспільстві в цілому, забезпечити не тільки своєчасний аналіз майбутнього, але й спільні дії з попередження довгострокових ризиків [3]». «*Інформаційне управління* – це процес вироблення та реалізації управлінських рішень в ситуації, коли управляючий вплив носить неявний характер і об'єкту управління дається (така, що визначається суб'єктом управління) інформація відносно ситуації (інформаційна картина), орієнтуючись на яку цей об'єкт начебто сам обирає лінію своєї поведінки [4, с. 142]».

Колективний образ – це образ, який має сформувати увесь колектив (група людей, країна). *Соціальне уявлення про майбутнє* – це сукупність уявлень про майбутні процеси й явища, які поділяються членами соціальної групи й створюються ними в міжособистісному дискурсі [див 3]. «Цей образ виробляє все суспільство, політичні партії, суспільні організації на основі досліджень, які окреслюють коридор можливостей, простір цілей, які можуть бути досягнуті у перспективі, ризики, які пов'язані з різними варіантами розвитку, і ціну, яку суспільству доведеться заплатити за вирішення поставлених задач [5, с. 27]».

Основні загрози шкідливого інформаційного впливу на груповий образ майбутнього. «Соціальні процеси з'єднують воєдино соціальні об'єкти і створені структури, здійснюючи перехід соціальної системи із одного стану в інший. Кожен з них забезпечується складним інформаційним процесом, який вимагає створення, перетворення та споживання певних інформаційних сукупностей [див. 4, с. 239]». Разом з цими процесами функціонують процеси захисту інформації від несанкціонованого доступу та вбудовані у кожен із інформаційних процесів засоби кібербезпеки. Вивченню типових загроз присвячено величезна кількість робіт. *Загрози спотворень інформації.* Навмисні спотворення інформації можуть призводити до свідомої дезінформації та обману людей або суспільства. Неправда і наклеп на побутовому рівні, спотворення даних у фінансових документах з метою обману ділових партнерів є розповсюдженим явищем у суспільстві. У тоталітарних державах неправда може бути основою політики. За останні роки сформувалась *злободенна загроза перетворення стратегії формування позитивного колективного образу майбутнього на вимушено раціональний колективний образ майбутнього*.

Розглянемо коротко *модель суб'єкта-агресора*. Суб'єкт-агресор, як і система управління свідомістю, представляє собою мережеву інформаційну систему в умовах загального ресурсу. Він має свої цілі в інформаційному просторі й веде цілеспрямований вплив на захищену систему, з метою нанесення їй збитку й отримання переваги. Суб'єкт-агресор здійснює свою діяльність такими етапами: підготовчий етап (розвідка), визначення економічної й іншої доцільності впливу, інформації щодо стану свідомості об'єкта; етап аналіз інформації (відбір потрібної інформації, редукція, консолідація, переробка); етап прийняття рішень (формування управлінського рішення); виконання самого акту інформаційного впливу на об'єкт. На підготовчому етапі суб'єкт-агресор проводить атаки, які орієновані на збирання інформації про роботу системи і стратегії управління. Атаки

здійснюються за допомогою перехоплення та аналізу інформаційних потоків, а також іншими технічними й організаційними методами. На етапі реалізації інформаційного впливу на об'єкт можна виділити: дезінформування, маніпулювання, пропаганду.

Таким чином, модель деструктивного впливу можна представити як кібернетичний цикл управління. Прототипом математичної моделі кібернетичного циклу управління може бути трьох-рівнева динамічна модель із зворотними зв'язками Гереги, або чотирьох-рівнева динамічна система, що моделює системи обробки інцидентів інформаційної безпеки [6].

Математична модель. Розглянемо найпростіший випадок, коли атакований об'єкт піддається циклічно етапам конструктивного та деструктивного впливу інтенсивністю x_{ai} та x_{bi}, відповідно. Об'єкт споживає вхідний потік із свого навколишнього середовища – x_{in} і видає в навколишнє середовище вихідний інформаційний потік – x_{out}. Тоді математична модель динамічної системи буде мати такий вигляд:

$$\Phi\left(x^{(a)}, x^{(b)}\right) = \begin{cases} x_{n+1}^{(a)} = x_n^{(a)} - k_{ab} p_a \left(x_n^{(a)}\right)^2 + k_{ba} p_b \left(x_n^{(b)}\right)^2 + x_{in} \\ x_{n+1}^{(b)} = x_n^{(b)} + k_{ab} p_a \left(x_n^{(a)}\right)^2 - \left(k_{ba} + k_{out}\right) p_b \left(x_n^{b}\right)^2 \end{cases} \quad (1)$$

де $x^{(a)}$, $x^{(b)}$ – динамічні змінні, які визначають інтенсивність інформаційно-психологічного впливу на об'єкт, відповідно конструктивного – a і деструктивного – b; динамічні змінні x_n^a, x_n^b описують відповідні поточні значення; k_{ij} – перехідні коефіцієнти, що характеризують динамічну взаємодію етапів обробки інформації, у даному випадку взаємодію конструктивного і деструктивного впливу; p_a, p_b – розподільчі коефіцієнти, x_{in} – інтенсивність інформаційних елементів потоку, що поступають із навколишнього середовища на перший етап обробки; причому, $\{k_{ij}\}$ и $\{p_a, p_b\} \in (0,1)$, $\{x_a, x_b\} \in R$, $x_{in} = const \in R^+$. Змінна n характеризує модельний час.

Інформація обробляється дискретним способом. Порціями інформації являються повідомлення, документи, меми (одиниці вимірювання смислів) тощо. Наявність двох груп коефіцієнтів (k_{ij} та p_a, p_b) має конкретне пояснення: коефіцієнти k_{ij} описують відносну величину редукції і консолідації інформації за синтаксичними ознаками, наприклад, форматами відомостей і повідомлень, та задають долю результуючого впливу, який переходить з одного етапу на сусідній. Частина інформаційного впливу переходить на попередній етап обробки. Коефіцієнти p_a, p_b описують розподіл елементів інформаційного впливу за їх видами по семантичним ознакам, наприклад, по змісту. Перехід між етапами обробки визначається добутком коефіцієнтів обох груп. Така модель дає якісне наближене описання багатьох інших інформаційно-аналітичних або управляючих систем, де обробка інформації виконується двох-етапними циклами.

Висновки. На слайдах презентації доповіді показані результати дослідження: виникаючі стаціонарні та квазіперіодичні коливання, хаос, а в перехідний період можливі турбулентність і сингулярність. Застосування математичної моделі циклічного впливу може допомогти в удосконаленні методів забезпечення і контролю поетапного процесу формування позитивного образу майбутнього у громадян України.

Література

1. Петрик В.М. Информационно-психологическая безопасность в эпоху глобализации: учебное пособие / В.М. Петрик, В.В. Остроухов, А.А. Штоквиш // Под ред. В.В. Остроухова. – К., 2008. – 544 с.

2. Владимирова, Т.В. Социальная природа информационной безопасности [Текст] : монография / Т.В. Владимирова ; АНО содействия развитию соврем. отечеств. науки. Изд. дом «Научн. обозрение». – М.: Изд. Дом «Научн. обозрение», 2014. – 239 с.

3. Нестик Т.А. Коллективный образ будущего: социально-психологические факторы прогнозирования [Электронный ресурс] / Т.А. Нестик // Вопросы психологии, 2014, № 1. –

10 с. – Режим доступа: http://spkurdyumov.ru/forecasting/kollektivnyj-obraz-budushhego-socialno-psixologicheskie-aspekty-prognozirovaniya.

4. Информационная безопасность системы организационного управления. Теоретические основы : в 2 т. / Н.А. Кузнецов, В.В. Кульба, Е.А. Микрин и др.; [отв. ред. Н.А. Кузнецов, В.В. Кульба] ; Ин-т пробл. передачи инф. РАН. – М.: Наука, 2006. Т.1 – 495 с.

5. Иванов В.В. Наука XXI века и формат войн будущего [Электронный ресурс] / В.В. Иванов, Г.Г.Малинецкий // REGNUM. – М.: 2015. – 7 с. – Режим доступа: http://www.centrasia.ru/newsA.php?st=1446498780 [Название с экрана].

6. Герега О.М. Гіпотеза і формальна модель сингулярної динаміки інцидентів кібернетичної безпеки [Текст] / О.М. Герега, С.О. Гнатюк, В.Г. Кононович, І.В. Кононович // Інформатика та математичні методи моделювання. – 2016. – Т.6. – №1. – С. 26 – 37.

УДК 004.056.52:621.391

Каптур В.А., Князєв О.А.
Одеська національна академія зв'язку ім. О.С. Попова,
vadim.kaptur@onat.edu.ua

ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ РОБОТИ АДАПТИВНОЇ КОМПЛЕКСНОЇ СИСТЕМИ ФІЛЬТРАЦІЇ КОНТЕНТУ

Анотація. *Розроблено імітаційну модель адаптивної комплексної системи фільтрації контенту (АКСФК), що базується на використанні апарату мереж Петрі та програмної оболонки CPN Tools. Проведені розрахунки поведінки АКСФК шляхом зміни характеристик імітаційної моделі, побудовані графіки залежності часу затримки при обробці запиту від параметрів АКСФК., На основі проведених досліджень було зроблено висновок, що використання АКСФК підвищує ефективність фільтрації у порівнянні із стаціонарними системами.*

Як відомо [1], основним технічним методом протидії розповсюдженню небажаної інформації, шкідливих ресурсів та шкідливого програмного забезпечення в мережі Інтернет є використання так званих систем фільтрації контенту (СФК). Проведений на попередніх стадіях дослідження аналіз переваг та недоліків різних систем фільтрації контенту [2] показав, що найбільш перспективною на сьогодні є ідея створення так званих комплексних систем фільтрації контенту (КСФК), тобто систем, що складаються з двох чи більше засобів фільтрації, кожен з яких може використовувати різні види, методи та підходи до фільтрації контенту. В подальших дослідженнях авторів [3] було запропоновано метод адаптивної оцінки універсальних ідентифікаторів ресурсів (Universal Resource Identifier, URI) в КСФК, а також концепцію так званих адаптивних КСФК (АКСФК), тобто КСФК, робота якої адаптується до характеристик зовнішнього (користувацького) середовища.

Слід однак зазначити, що оцінка ефективності пропонованого підходу можлива лише при розробці відповідних імітаційних та математичних моделей. З цією метою було створено імітаційну модель АКСФК (рис. 1), що базується на використанні апарату мереж Петрі [4]. Програмну реалізацію моделі виконано в середовищі CPN Tools [4]. За допомогою створеної моделі було проведено чотири дослідження.

Під час першого дослідження було розглянуто поведінку системи при зміні ймовірності спрацьовування однієї СФК в межах КСФК та було визначено середній час обробки одного запиту в межах КСФК. Результати дослідження представлені на рис. 1.

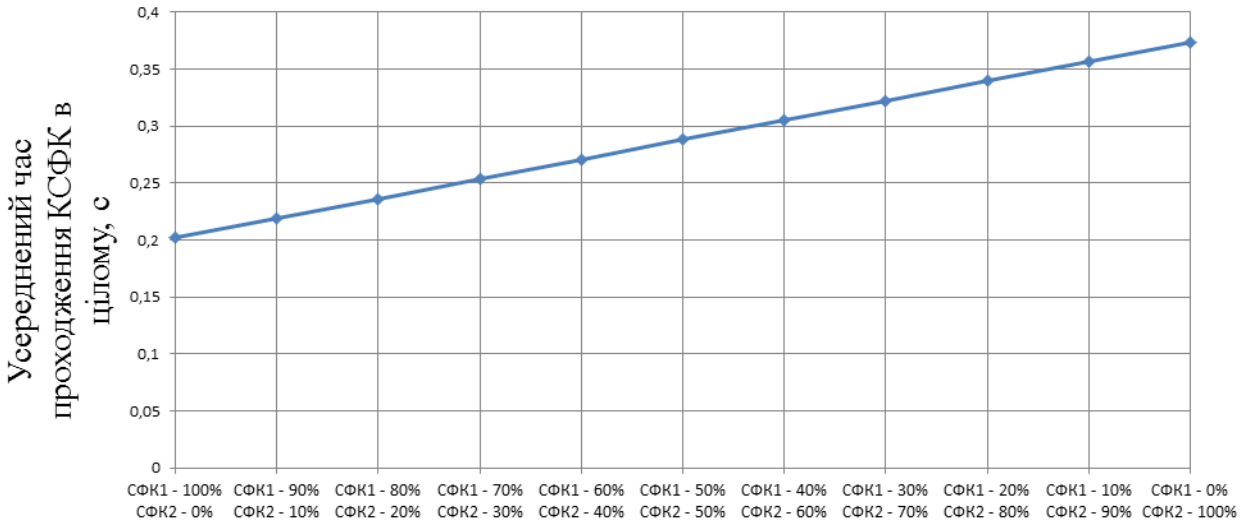

Рис. 1. Залежність часу обробки одного запиту в межах КСФК від розподілу ймовірностей спрацьовування СФК в межах КСФК

З рис. 1 видно, що при зміні ймовірностей спрацьовування процедур СФК всередині КСФК, змінюється і час обробки одного запиту в межах КСФК. При цьому при максимальній ймовірності спрацьовування першої СФК (СФК1 – 100%, СФК2 – 0%), час обробки запиту мінімальний.

В процесі другого дослідження (рис. 2) був проведений аналіз поведінки загального часу затримки в межах СФК1 та СФК2.

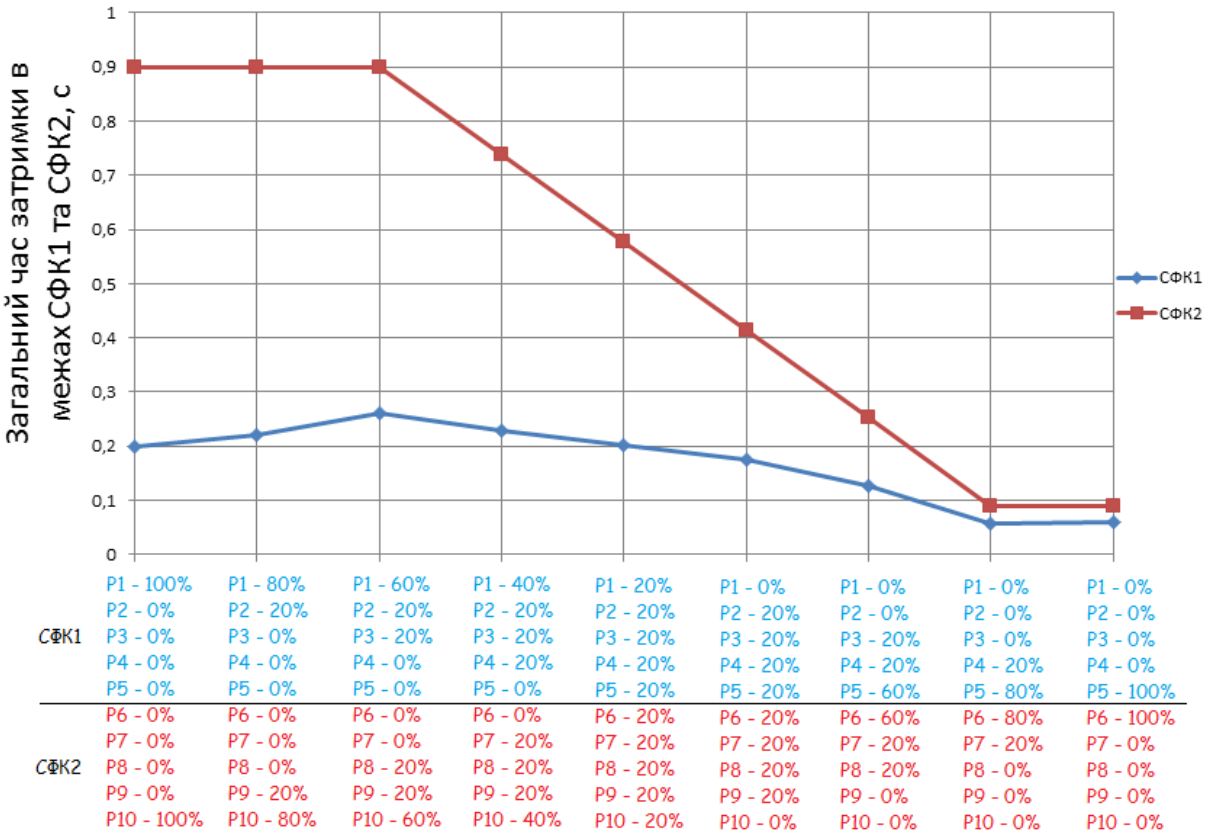

Рис. 2. Залежність середнього часу затримки від розподілу ймовірностей спрацьовування процедур в межах СФК

З результатів цього дослідження (рис. 2) видно, що загальна затримка на виході кожної СФК зменшується при перерозподілі ймовірностей спрацьовування процедур всередині самої СФК.

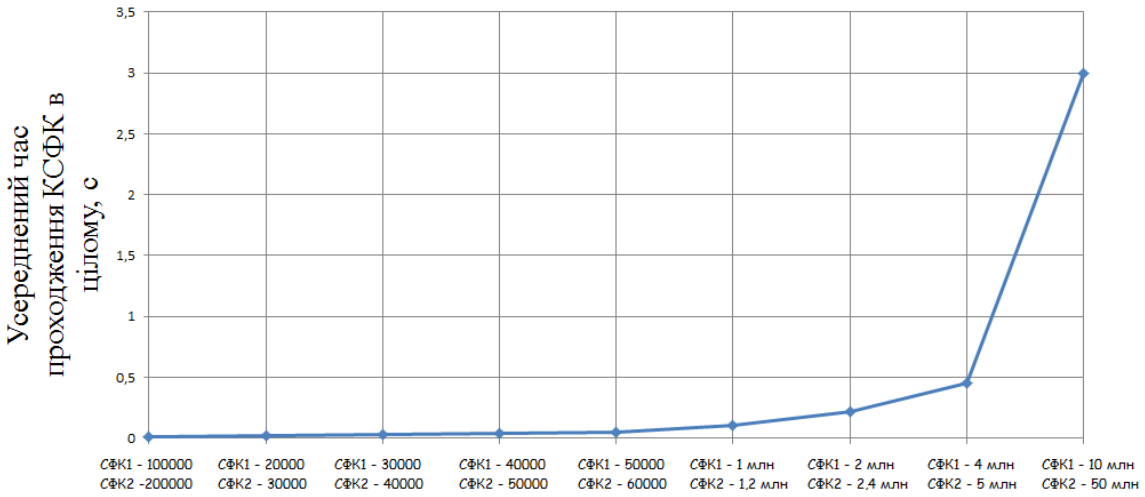

Рис. 3. Залежність середнього часу затримки від кількості записів в списках блокування

В даному випадку зменшення часу в процесі виконання моделювання досягається шляхом збільшення ймовірності спрацьовування процедури, що мінімально впливає на час затримки в межах СФК (в наведеному прикладі це процедура, що опрацьовує мінімальну кількість записів). Де Р1-Р5 це процедури СФК1, а Р6-Р10 це процедури СФК2.

Під час третього дослідження було розглянуто залежність середнього часу затримки від кількості записів у списках блокування (рис. 3). Під час цього дослідження було змінено кількість записів у списках відповідних процедур. З рис. 3 видно, що при збільшенні кількості записів у «чорному/білому» списках загальний час проходження КСФК (час додаткової затримки) також лінійно зростає.

В межах четвертого дослідження було встановлено залежність середнього часу затримки від часу обробки одного запису (кількість записів у списках блокування фіксована, ймовірність спрацьовування процедур та СФК також фіксована). Отримані результати дослідження представлені на рис. 4. Як видно з рис.4 загальний час затримки у КСФК лінійно зростає за рахунок зростання середнього часу обробки одного запиту.

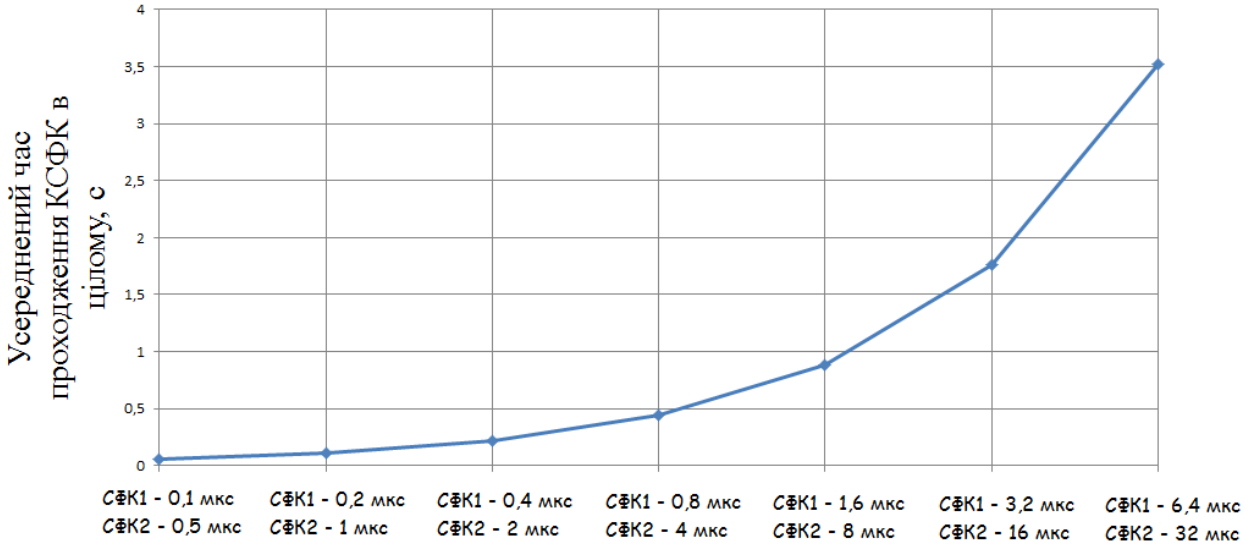

Рис. 4. Залежність середнього часу затримки від часу обробки одного запису

Проведені дослідження, в цілому, продемонстрували що запропонована концепція АКСФК, може зменшити загальний час додаткової затримки при обробці URI у КСФК за рахунок сортування процедур всередині СФК на 37%. Цей показник був досягнутий шляхом порівняння стаціонарної комплексної системи фільтрації контенту та адаптивної комплексної системи фільтрації контенту, де, в свою чергу, при обробці 100тис. запитів, загальний час затримки стаціонарної системи становить 0,3375 с, в той час як адаптивна система показала результат в 0,2125 с за рахунок сортування процедур в системі фільтрації контенту.

Література

1. Воробієнко П.П. Комп'ютерна програма “Мультимедійний навчальний дистанційний курс безпечного користування ресурсами мережі Інтернет” (“OnlineSafety.info”) / П.П. Воробієнко, В.А. Каптур // Свідоцтво про реєстрацію авторського права на твір № 65910 від 06.06.2016.

2. Каптур В.А. Комплексні системи фільтрації контенту в мережі Інтернет / В.А. Каптур // Наукові праці ОНАЗ ім. О.С. Попова, 2013, №1. − С. 16−21.

3. Каптур В.А. Метод адаптивної оцінки URI в комплексних системах фільтрації контенту / В.А. Каптур, О.А. Князєв // Наукові праці ОНАЗ. – Одеса, 2016. – № 1. – С. 35-45.

4. Д.А. Зайцев, Т.Р. Шмелева. Моделирование телекоммуникационных систем в CPN Tools 2008. – С. 1−21.

УДК 681.3.06:006.354

Ковальчук Л.В., Кучинська Н.В., Поречна Д.М.
Національний технічний університет України "Київський політехнічний інститут"
n.kuchinska@gmail.com

ОЦІНКИ ПРАКТИЧНОЇ СТІЙКОСТІ МОДИФІКОВАНИХ СТАНДАРТІВ БЛОКОВОГО ШИФРУВАННЯ УКРАЇНИ ТА РОСІЇ ВІДНОСНО ЦІЛОЧИСЕЛЬНОГО РІЗНИЦЕВОГО КРИПТОАНАЛІЗУ

***Анотація**. розглянуто одну з актуальних модифікацій різницевого криптоаналізу, а саме цілочисельний різницевий криптоаналіз, отримані науково обґрунтовані оцінки практичної стійкості до цілочисельного різницевого криптоаналізу модифікованих стандартів блокового шифрування України та Росії. Проведено порівняльний аналіз отриманих значень з відповідними параметрами для випадкових вузлів заміни, щодо яких проведено статистичні дослідженя.*

Питання удосконалення існуючих та побудови нових ефективних алгоритмів шифрування з обґрунтованою стійкістю є надзвичайно актуальним. Сьогодні симетричні блокові алгоритми шифрування є основним криптографічним засобом забезпечення конфіденційності при обробці інформації в сучасних інформаційно-телекомунікаційних системах. Переважна більшість сучасних блокових шифрів спроектовані схожим чином і містять у своїй структурі композицію ключового суматора, блоку підстановки і оператора перестановки, лінійного над полем F_2 або його деяким розширенням. Тому задача оцінювання стійкості таких шифрів до лінійного, білінійного та різним модифікаціям різницевого криптоаналізу або зводиться до задачі побудови верхніх оцінок середніх ймовірностей таких композицій, або містить її як підзадачу [1-11].

Цілочисельні диференціали використовувалися, як для криптоаналізу, так і для побудови колізій геш-функцій в багатьох роботах; досить повний перелік посилань на такі роботи, а також обгрунтування використання саме цілочисельних диференціалів можна знайти в [8-10]. Зауважимо, що аналітичні складнощі, що виникають у зв'язку з наявністю

біта переносу при модульному додаванні, посилюються тим, що оператор перестановки не є лінійним щодо цієї операції. У відомих роботах, в яких розглядались немарковські та узагальнено марковські блокові шифри, в тому числі ГОСТ-подібні та ″Калина″-подібні, будувались оцінки практичної стійкості лише відносно класичного, тобто побітового різницевого криптоаналізу. Питання побудови оцінок стійкості до цілочисельного різницевого криптоаналізу там не розглядалось. Основні означення, що стосуються марковських та узагальнено марковських блокових алгоритмів можна знайти в [2, 12].

В доповіді розглядається модифікований ГОСТ-подібний алгоритм. Модифікована раундова функція такого алгоритму має вигляд: $f_k(u,v)=(v,u+\varphi(v+k))$, де $x=(u,v)\in V_n$, $n=2m$, $u,v,k\in V_m$, k - раундовий ключ, $\varphi: V_m\times V_m\to V_m$ - раундове перетворення алгоритму, а + є додаванням за модулем 2^m. Такий блоковий алгоритм є марковським шифром відносно операції додавання за модулем 2^m, що дозволяє отримати оцінки практичної стійкості для такого алгоритму, використовуючи отримані раніше авторами верхні оцінки імовірностей цілочисельного раундового диференціалу для раундового перетворення алгоритму ГОСТ. В такому випадку, якщо 4-бітові вузли заміни обрані з рекомендованих [13], але з найменшими значеннями параметрів (dke2 або dke7) такими, що $\max\limits_{\alpha,\beta\in V_n\setminus\{0\}} d^{\varphi}(\omega_i,\omega_{i+1})\le 2\cdot 0{,}375$, то $\max\limits_{\Omega} EDP(\Omega)\le 0{,}0024\approx 2^{-9}$. В результаті проведених досліджень запропоновано вузли заміни, які дозволяють підвищити стійкість вказаного алгоритму до цілочисельного різницевого криптоаналізу.

Модифікація алгоритмів шифрування ″Калина″ (визначений у ДСТУ 7624:2014) та ″Кузнєчік″ (визначений у ГОСТ Р 34.12 2015) з раундовими функціями вигляду $f_k(x)=A\circ S(x*k)$, де $x\in V_n$ - відкритий текст, $n=pu$, $p\ge 2$, $x=(x_p,....,x_1)$, $x_i: V_u\to V_u$, $i=\overline{1,p}$, $k\in V_n$ - раундовий ключ, $*$ - операція побітового або модульного додавання, $S=(s^{(p)},...,s^{(1)})$, $s^{(i)}: V_u\to V_u$ - блок підстановок, полягає в тому, що матриця оператора, оберненого до A є булевою. В залежності від ключового суматора будь-який алгоритм з вказаною раундовою функцією буде або марковським або узагальнено марковським відносно модульного додавання. Зауважимо, що шифр ″Кузнєчік″, є марковським шифром відносно операції побітового додавання. Авторами отримано оцінки практичної стійкості вказаних модифікованих алгоритмів, використовуючи отримані раніше в [3] верхні оцінки імовірностей цілочисельного раундового диференціалу. Так для модифікованої раундової функції алгоритму ″Кузнєчік″ із побітовим додаванням у ключовому суматорі, з урахуванням рекомендованого до використання одного вузла заміни, який позначено π, отримано верхні оцінки імовірностей цілочисельного раундового диференціалу $\max\limits_{\alpha,\beta\in V_n\setminus\{0\}} d^{f}(\alpha,\beta)\le 0{,}08984375$. Звідки для 10 раундів зашифрування (враховуючи, що останній раунд не використовує нелінійну заміну, а лише побітове додавання ключа) середню (за ключами) імовірність узагальненої різницевої характеристики можна оцінити наступним чином $EDP(\Omega)\le 3{,}814\cdot 10^{-10}\approx 2^{-31}$.

Щодо модифікованого алгоритму ″Калина″ з побітовим ключовим суматором та її чотирьох вузлів заміни, визначених стандартом, то найбільше значення верхніх оцінок імовірностей цілочисельного раундового диференціалу будуть мати вузли заміни π_1 та π_3: $\max\limits_{\alpha,\beta\in V_n\setminus\{0\}} d^{f}(\alpha,\beta)\le 0{,}09375$. Для модифікованого алгоритму ″Калина″ з модульним ключовим суматором найбільше значення буде досягатись на вузлі π_2: $\max\limits_{\alpha,\beta\in V_n\setminus\{0\}} d^{f}(\alpha,\beta)\le 0{,}10546875$. Звідки, для 10 раундів шифрування (враховуючи, що

останній раунд не використовує нелінійну заміну, а лише модульне додавання ключа) $EDP(\Omega) \le 5{,}9 \cdot 10^{-11} \approx 2^{-34}$.

Наведені результати, дозволили оцінити практичну стійкість модифікованих ГОСТ-подібного та ″Калина″-подібних алгоритмів блокового шифрування відносно цілочисельного різницевого криптоаналізу. Також встановлені оцінки верхніх меж практичної стійкості модифікованого алгоритму ″Кузнєчік″ до цілочисельного РК у двох випадках: коли у ключовому суматорі реалізована операція модульного додавання або побітового додавання. Порівняння отриманих значень зі статистичними розподілами відповідних параметрів дає привід припускати, що при проектуванні шифру ″Кузнєчік″, окрім стійкості до класичного побітового РК, могла бути врахована необхідність практичної стійкості і до цілочисельного РК. Неможливо стверджувати напевно, чи був такий тип атаки розглянутий авторами шифру при проектуванні його S-блоку. Варто зазначити, щодо інших сучасних алгоритмів, стійкість до цілочисельного різницевого криптоаналізу не розглядалася ні при побудові шифру AES, ні шифру ″Калина″. Якщо припущення – вірне, то ″Кузнєчік″ стає першим алгоритмом шифрування, який би використовував нелінійні вузли заміни за умовчуванням із близькими до практично досяжних найменших значень параметрів ,отриманих авторами.

Література

1. Олексійчук А.М. Криптографічні параметри вузлів заміни, що характеризують стійкість ГОСТ-подібних блокових шифрів відносно методів лінійного та різницевого криптоаналізу / Олексійчук А.М., Ковальчук Л.В., Пальченко С.В.// Захист інформації. – 2007. – № 2. – С. 12 – 23.

2. Ковальчук Л. В., Пальченко С. В., Скрипник Л.В. Застосування теорії узагальнених марковських шифрів для оцінювання стійкості сучасних блокових алгоритмів до методів різницевого криптоаналізу. – Науково-технічний збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». – 2009. – № 2 (19). – С. 45-56.

3. Ковальчук Л.В. Побудова верхніх оцінок середніх імовірностей цілочисельних диференціалів композицій ключового суматора, блока підстановки та лінійного (над деяким кільцем) оператора / Ковальчук Л., Кучинська Н., Скрипник Л. //Науково-технічний збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». – 2015. – №1(29). – С.33-45.

4. Kovalchuk L., Alekseyshuk A., Upper Bounds of Maximum Value of Average Differential and Linear Characteristic Probabilities of Feistel Cipher with Adder Modulo 2^n, // Theory of Stochastic Processes. – 2006. – Vol. 12(28). – № 1, 2. – P. 20 – 32.

5. Ковальчук Л. Обобщёные марковские шифры: оценка практической стойкости к методу дифференциального криптоанализа // Труды Пятой Общероссийской научной Конференции “Математика и безопасность информационных технологий” – (МаБИТ-06), 25-27 октября 2006. – С. 595-599.

6. Олексійчук А.Н., Ковальчук Л.В., Пальченко С.В. Криптографічні параметри вузлів заміни, що характеризують стійкість ГОСТ-подібних блокових шифрів відносно методів лінійного та різницевого криптоаналізу // Захист інформації. – 2007. – № 2. – С. 12 – 23.

7. Алексейчук А., Ковальчук Л., Шевцов А., Скрыпник Л. Оценки практической стойкости блочного шифра ««Калина»» относительно разностного, линейного билинейного методов криптоанализа. // Труды Седьмой Общероссийской научной Конференции “Математика и безопасность информационных технологий” – (МаБИТ-08), 30 октября – 2 ноября 2008. – С. 15-20.

8. X. Wang, H. Yu. How to Break MD5 and Other Hash Functions. // Advances in Cryptology EUROCRYPT'05, Lectures Notes in Computer Science 3494, Springer-Verlag, 2005. – P. 19-35.

9. S. Cotini, R.L. Riverst, M.J.B. Robshaw, Y. Lisa Yin. Security of the RC6™ Block Cipher, http//www.rsasecurity.com/rsalabs/rc6/.

10. Tomas A.Berson Differential cryptanalysis mod 2^{32} with applications to MD5 // Advanced in Cryptology. – CRYPTO'98 (LNCS 372). – 1999. – P. 95-103.

11. Ковальчук Л., Кучинская Н. Построение верхних оценок средних вероятностей целочисленных дифференциалов раундовых функций блочных шифров определенной структуры. //«Кибернетика и системный анализ» – 2012, – №5. – С. 71 – 81.

12. Lai X. Markov ciphers and differential cryptanalysis / X. Lai, J.L. Massey, S. Murphy. // Advances in Cryptology – EUROCRYPT'91, Proceedings. – Springer Verlag, 1991. – pp. 17-38.

13 Наказ Адміністрації Держспецзв'язку №114 Про затвердження Інструкції про порядок постачання і використання ключів до засобів криптографічного захисту інформації Редакція від 27.06.2013 [Електронний ресурс] // Режим доступу: – http://zakon3.rada.gov.ua/laws/show/z0729-07 - Назва з екрану.

УДК 210.5.021

Ковбель М.М.
Державний університет телекомунікацій, Україна,
м. Київ
maxim5555565@gmail.com
Науковий керівник – Д.Т.Н. , С.Н.С Наконечний В.С.

ДОСЛІДЖЕННЯ ІСНУЮЧИХ ОЗНАК ІНФОРМАЦІЙНИХ АТАК

Створена з високою ефективністю та з багатою функціональністю інформаційна систем (ІС), дозволяє в даний час реалізувати її в самих різних сферах життя сучасного суспільства. ІС автоматизуватимуть та підвищуватимуть ефективність обробки інформації шляхом застосування відповідного програмного і апаратного забезпечення. Однак, використання ІС одночасно загострює і проблеми захисту ресурсів цих систем від загроз інформаційної безпеки. Не існує загальноприйнятої класифікації загроз інформаційної безпеки. Один з варіантів класифікації може бути виконаний за такими ознаками:

- Метою реалізації;
- За принципом впливу на систему;
- За характером впливу на систему;
- Через появу використовуваної помилки захисту;
- За способом впливу атаки на об'єкт;
- Об'єкту атаки;
- використовуваних засобів атаки;
- За станом об'єкта атаки.

Реалізація однієї або декількох навмисних загроз є атакою. При цьому атака являє спробу подолання захисту автоматизованої системи (АС), ступінь успіху якої залежить від уразливості системи і ефективності захисних заходів.

Ефективний захист від потенційних мережевих атак неможлива без їх детальної класифікації, що полегшує їх виявлення і завдання протидії їм.

В даний час відомо безліч різних типів класифікаційних ознак інформаційної безпеки. В якості таких ознак може бути вибрано, наприклад, поділ на пасивні і активні, зовнішні і внутрішні атаки, свідомі й несвідомі і т.д. Розгляд існуючих класифікацій почнемо з роботи Пітера Мелла "Комп'ютерні атаки: що це і як їм протистояти". У ній всі можливі мережеві атаки діляться на наступні типи:

- Віддалене проникнення (від англ. remote penetration);
- Локальне проникнення (від англ. Local penetration;
- Віддалений відмова в обслуговуванні (від англ. Remote denial of service);
- Локальний відмову в обслуговуванні (від англ. Local denial of service);

- Атаки з використанням мережевих сканерів (від англ. Network scanners);
- Атаки з використанням сканерів вразливостей (від англ. Vulnerability scanners);
- Атаки з використанням зломщиків паролів (від англ. Password crackers);
- Атаки з використанням аналізаторів протоколів (від англ. Sniffers).

Таким чином, застосування існуючих класифікацій не можна назвати раціональним. Існує об'єктивна необхідність у створенні нової гнучкої класифікаційної схеми можливих атак., Незважаючи на те, що деякі з існуючих класифікацій мало застосовні на практиці, їх активно використовують при виборі системи виявлення вторгнень атак і їх експлуатації.

Література

1. Лукацкий А.В. Железная защита на границе сети PC Week/RE № (435)21`2004 от 15.6.2011. – С. 23.

2 Лукацкий А.В. Обнаружение атака. –2-е изд., перераб. и доп. – СПб.: БХВ-Петербург, 2007. – 608 с.

3. Гошко С.В. Технологии борьбы с компьютерными вирусами. М.: Солон-Пресс, 2009. – 352с.

4. Касперский Е. Компьютерное Zловредство / Е. Касперский. – М.: ООО «Питер Пресс», 2008. – 207 с.

5. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. – М. ДМК Пресс, 2010. – 544 с.

УДК 323:351:34

Кононович В.Г., Паноян Г.Г.
ОНПУ
wwe543@mail.ru

ЛОГИКО-ИСТОРИЧЕСКИЙ АНАЛИЗ МЕТОДОВ ПРЕОДОЛЕНИЯ КЛАССИЧЕСКОЙ ПРЕСТУПНОСТИ И КИБЕРПРЕСТУПНОСТИ

Аннотация. *Исследуется логико-историческими методами условия, причины и методы преодоления резкого роста киберпреступности и инцидентов кибербезопасности. Проводятся аналогии методов противодействия преступности в эпоху ранней промышленной революции и в современную эпоху построения общества высоких технологий. Предложены методы: привлечение хакеров к решению задач устранения уязвимостей и других задач кибербезопасности; осуществление научно-технологических прорывов, как например, создание «иммунной» системы кибербезопасности, внедрение системы определения идентичности и др. Полученные результаты позволят усовершенствовать системы и технологии кибербезопасности.*

Многочисленные статистические данные свидетельствуют о неблагополучном состоянии сферы информационной безопасности и киберпреступности. Инструменты кибератак стали использоваться для получения преимущества в информационном влиянии и кибервойнах. «Формируются спецподразделения, которые имеют целью: ведение разведывательной работы в сетях, защиты собственных сетей, блокирования и «обвала» структур противника с использованием возможностей киберпространства [1]». Среди стратегических аспектов кибербезопасности Украины формулируются проблемы «выстраивания эффективных механизмов защиты национальных интересов государства и необходимости выработки общего видения проблем кибербезопасности как государственными органами, так и бизнес-структурами [2]».

Целью данной работы является определение путей преодоления современной киберпреступности путем логико-исторического исследования причин, условий и методов борьбы с преступностью аналогичных в прошлом и настоящем.

Введение. *Преступность* – это форма социального поведения людей, нарушающая нормальное функционирование обществ. «*Компьютерная преступность* – это относительно массовое, исторически изменчивое социальное явление, которое имеет определенное территориальное и временное распространение и представляет целостную систему единичных общественно опасных деяний, где ЭВМ, сети и представленная в них информация есть орудием совершения преступлений или предметом преступных посягательств [3]». *Киберпреступность* – это «незаконные собирание, хранение, использование, уничтожение, распространение, персональных данных, незаконных финансовых операций, воровство и жульничество в Интернет [4]». К киберпреступлениям может быть отнесено любое преступление, совершенное в электронной среде. *Кибербезопасность* – это состояние защищенности жизненно важных интересов человека и гражданина, общества и государства, что достигается комплексным применением совокупности правовых, организационных, информационных мероприятий. [4].

Очерки борьбы с преступностью в эпоху ранней промышленной революции. Человечество сталкивается с резким ростом преступности не первый раз. В XVIII—начале XX века способы ведения преступности были менее развитыми и утонченными, чем сейчас. Уровень преступности является важнейшим показателем состояния общества. В стабильном, традиционном обществе население привязано к месту жительства и своим общинам, мало развита городская жизнь, существует строгий социальный контроль, социальная структура иерархизирована, вертикальная социальная мобильность низка, общинные связи сильно развиты и общественные цели преобладают над личными. В таком обществе обычно наблюдается низкая преступность. Наоборот, для индустриальных и урбанизированных обществ, доминируют общественные связи, сильно развит индивидуализм, личный успех является важнейшим в системе ценностей, население располагает большой свободой и инициативой, характерна более значительная преступность. Но особенно высокого уровня преступность достигает в обществах, испытывающих серьезные изменения в культурных, социальных и политических ориентациях. Вот типовые случаи.

Франция. В течение столетия страна пережила четыре революции (1789, 1830, 1848, 1870 гг.) и целый ряд глубоких социально-политических потрясений; в ней неоднократно менялась форма государственного устройства. В начале 19 века французская полицейская служба занимается выслеживанием и арестами политических противников королей. В 1810 году была создана Сюртэ. Префект полиции барон Паскье поручил борьбу с преступностью Эжену Франсуа Видоку – бывшему каторжнику, неоднократно сбегавшему из тюрем. Видок набирал сотрудников по принципу: «Только преступник может побороть преступление». За год 12 сотрудников Видока, прошедшие у него железную выучку, арестовали 812 убийц, воров, взломщиков, грабителей и мошенников, ликвидировал притоны. В 1833 году Видок вышел в отставку и организовал первое в мире частное сыскное агентство. Пришедшие на смену руководители Сюртэ не изменили принципов работы: многие бывшие преступники состояли на службе в качестве филеров и сотрудников. Другими словами, Видок заложил систематические (научные) основы криминалистики. В 1883 году получило признание развитие криминалистики Альфонса Бертильйона. А в 1895 году, уже в Англии, Френсис Гальтон добился дактилоскопического контроля уголовных преступников.

Англия. Девятнадцатый век был веком расцвета Великобритании. Великобритания была политической империей, которая контролировала большие территории по всему миру. Войны с Наполеоном, были окончены, и оружие, одежда и другие товары уже не требовались в таких количествах. Безработицу усилило возвращение 300 тысяч солдат. Быстро повысился уровень преступности. От такой жизни многие безработные уходили в города. Что привело к огромному потоку преступности в крупных городах. В отличие от Франции, преувеличенно болезненное (как сейчас в Интернет) представление англичан о гражданских свободах, привело к тому, что общественность усматривала в полиции угрозу гражданским свободам. Пока в 30-х года 19 века лондонцы не стали буквально тонуть в болоте преступлений, насилия и беззакония. Из-за такого понимания гражданских свобод

Англия столетиями не имела настоящей полиции. Поддержание порядка и охрана собственности считалась делом самих граждан. В 1832 году был принят закон о реформе общества. Среди прочего был создан Скотланд-ярд (шотландский двор).

Россия. Данные о преступности в масштабе всей России стали собираться с 1803 г., после образования Министерства юстиции в 1802 г. Ситуация в России была аналогичной, включая мордобой и порку, где создание в 1842 году и дальнейшая деятельность сыскной полиции, которую связывают с именами К. Л. Шерстобитова, И. Д. Путилина и др.

Преступность в эпоху общества высоких технологий. Сравнительная таблица. Сегодня киберпреступность – масштабная проблема, а вредоносные программы пишутся с целью незаконного получения денег. Финансовые операции проводятся через Интернет.

В начале смены тысячелетий влиятельнейшие государства мира стали создавать первые отряды киберполиции. В США первая киберполиция была создана в далеком 2001 году. По данным американских властей, в 2000-ом году жертвами компьютерных взломщиков стали 85% компаний и правительственных организаций. В России в 2015 году были предприняты попытки создания «киберкопов» – которые будут следить за порядком в Сети. 15 октября 2015 года в Украине стартовал набор в киберполицию. Министром внутренних дел Арсеном Аваковым было озвучено, что будет создана киберполиция, в которой будут работать так называемые «белые хакеры». Совершения преступлений в сфере компьютерных технологий имеют очень высокую латентность, которая составляет 85-90%. Законодательство очень часто является некомпетентным в расследовании подобных инцидентов. Во многих случаях, компании, потерпевшие хакерские атаки, не хотят огласки, из-за боязни потери авторитета. Произведем сравнение условий и способов решения проблем с ростом преступности в разные эпохи (табл. 1).

Таблица 1

Сравнение факторов, влияющих на преступность, в разные эпохи

Влияющие факторы	Сравнение содержания факторов, влияющих на преступность в эпоху:	
	ранней промышленной революции	перехода к обществу высоких технологий
1. Преступность	Классическая	Киберпреступность
2. Причины преступности	Беззаконие, урбанизация, низкий интеллектуальный уровень большинства общества, слабые моральные устои	Глобализация, уязвимости технологий, несовершенство юридической и правовой базы, поиск легкой наживы, алчность, антиобщественные идеи и пр.
3. Уровень свободы	Раскрепощение личности. Свободная продажа своего труда на рынке труда	Обеспечение прав человека. Свобода пользования информацией
4. Движущая сила	Капитал. Земельная собственность.	Информация, интеллект. Ресурсы киберпространства
5. Смена целей правопорядка	От защиты короля, к защите общественного порядка и граждан	К защите государства, общества, граждан и борьба с киберпреступностью
6. Создание спец-органов	Полиция (Сюрте, Скотланд ярд и пр.)	Киберполиция, Центры обработки инцидентов, CIRT of Ukraine
7. Научно-техн. прорывы	Антропометрические описания преступников, дактилоскопия	Детектор лжи, «иммунная» защита, управление определением идентичности
8. Кадры	Выпускники университетов.	Выпускники вузов, специалисты ИТ
9. Специалисты	Принятие преступников в полицию	Привлечение хакеров в киберполицию
10. Участие граждан	Узкое	Широкое взаимодействие государства, бизнес-структур и граждан
11. Цель преступлений	Под ударом находится частная собственность	Под ударом находится секретная и прочая информация, реальное оборудование и устройства, инфраструктура и процессы
12.Юридическая и правовая система	Создание юридической и правовой базы капиталистических обществ и отношений	Создание системной юридической и правовой базы виртуальных сообществ, технологий и отношений.

Из табл. 1 следует, что многое уже сделано, но преодоление киберпреступности еще на «полпути». С юридической точки зрения киберпространство – это не публичная собственность. Технологии и компьютерные сети, из которых состоит киберпространство, принадлежит транснациональным компаниям, которые их обслуживают.

Выводы. Еще не все возможности использованы для выполнения задач преодоления киберпреступности. С одной стороны, мешают халатность, некомпетентность лиц, нанятых для решения проблем киберпреступности, недостаточное финансирование соответствующих лиц и органов и т.п. С другой стороны, киберпреступность не может быть искоренена окончательно. Информационные, когнитивные и иные технологии будут развиваться. С ними неизбежно будут появляться уязвимости и ошибки. Нельзя обойти стороной и проблемы подготовки кадров. Дальнейший исход зависит от конкретных физических лиц. Поэтому важен пересмотр отношений к методам решения этой проблемы от правительств сильнейших держав мира, необходим конструктивный и совместный подход.

Список литературы

1. Дубов Д.В. Кібербезпека: світові тенденції [Електронний ресурс] / Д.В. Дубов, М.А. Ожеван // Доповідь на Міжнародній конференції 26 травня 2011 р. – К.: НІСТ, 2011. – 30 с. – Режим доступу: http://www.niss.gov.ua/articles/510.

2. Дубов Д.В. Стратегічні аспекти кібербезпеки [Текст] / Д.В. Дубов // Стратегічні пріоритети. – № 4 (29), 2013. – С. 119 – 126.

3. Інформаційна безпека держави: підручник / [В.М. Петрик, М.М. Присяжнюк, Д.С. Мельник та ін.] ; в 2 т. – Т. 2. – К., 2016. – 328 с.

4. Кавун С. В. Економічна та інформаційна безпека підприємств у системі консолідованої інформації : навч. посібн. / С. В. Кавун, А. А. Пилипенко, Д. О. Ріпка. – Х. : Вид. ХНЕУ, 2013. – 364 с.

УДК 004.056.5:343.326

[1]Корченко О.Г., [2]Ахметов Б.С., [1]Гнатюк С.О.
[1]Національний авіаційний університет,
[2]Казахський національний дослідницький університет ім. К.І. Сатпаєва
s.gnatyuk@nau.edu.ua

МОДЕЛЬ ФОРМУВАННЯ ВИМОГ ЩОДО ЗАХИСТУ ЦИВІЛЬНОЇ АВІАЦІЇ ВІД КІБЕРЗАГРОЗ

Анотація. *Проблема кібертероризму носить глобальний характер і досить гостро постає у сучасному інформаційному суспільстві. Актуальним стає захист критичних інфраструктур, а в деяких галузях, наприклад, у цивільній авіації рівень критичності значно підсилюється підвищеним ступенем комунікації та взаємодії між наземними системами і повітряними суднами, а впровадження сучасних інформаційних та комунікаційних технологій породжує цілу низку нових уразливостей та потенційних загроз. Існуючі розробки не в повній мірі враховують сучасні вимоги та специфіку діяльності цивільної авіації. Виходячи з цього, на базі керівних документів щодо безпеки міжнародної цивільної авіації, запропонована базова модель формування вимог до забезпечення кібербезпеки авіаційної галузі.*

Проблема кібертероризму [1] носить глобальний характер і досить гостро постає у сучасному інформаційному суспільстві. Провідні держави світу все більше уваги приділяють кіберзахисту власних критичних інфраструктур. Одним з важливих об’єктів критичної інфраструктури є транспортна система (поряд, наприклад, з енергетичною, нафто- та газотранспортною системами), несанкціоноване втручання у роботу якої може призвести до

значних економічних збитків, людських жертв і руйнування загальнодержавної інфраструктури. Особливої уваги заслуговує цивільна авіація (ЦА) [2], рівень критичності якої значно підсилюється підвищеним ступенем комунікації та взаємодії між наземними системами і повітряними суднами, а впровадження сучасних інформаційних та комунікаційних технологій (ІКТ) з одного боку підвищує ефективність і спрощує формальності у діяльності ЦА, а з іншого – породжує цілу низку нових уразливостей та потенційних загроз. Стандарт ІСАО [3] декларує необхідність для кожної держави, яка є членом ІСАО, розробляти методи захисту ІКТ, що використовуються для цілей ЦА, від актів незаконного втручання, які можуть поставити під загрозу безпеку міжнародної ЦА. Керівний документ Європейської конференції ЦА (ЕСАС) [4] визначає необхідність включення заходів щодо забезпечення захисту відповідної галузі від кіберзагроз (КЗ) до національної програми безпеки ЦА та інших національних програм (контролю якості, навчання і підготовки персоналу з питань безпеки ЦА тощо). Відповідно до [3-4] обов'язково необхідно ідентифікувати та захищати системи, які містять інформацію, що має критичне значення для безпечного виконання польотів і безпечної діяльності ЦА – це так звані критичні авіаційні інформаційні системи (КАІС) [5], орієнтовний перелік яких наведено у відповідному керівному документі [6]. Несанкціонований доступ (НСД) і використання КАІС може призвести до виникнення загроз безпеці пасажирів, екіпажу та наземного персоналу, з огляду на що важливим є забезпечення їх кібербезпеки (КБ) шляхом захисту від НСД, попередження втручання в роботу КАІС та виявлення атак на них.

Більшість відомих робіт орієнтована на розробку або загальних підходів до забезпечення КБ, або створення методів, моделей та засобів щодо забезпечення конфіденційності, цілісності й доступності інформації, що обробляється, зберігається чи передається за допомогою сучасних ІКТ. Таким чином, відповідно до поточного стану досліджень, не в повній мірі враховуються сучасні вимоги, задекларовані в керівних документах щодо безпеки авіації, та специфіка діяльності ЦА. З огляду на це, метою роботи є розробка базової моделі формування вимог до забезпечення КБ ЦА на базі керівних документів, пов'язаних з безпекою міжнародної ЦА.

Для формування державної системи КБ у галузі ЦА необхідно забезпечити виконання низки вимог, які містяться у різних керівних документах щодо безпеки ЦА (стандартах, рекомендованих практиках та національних програмах). Для розробки базової моделі формування вимог, введемо відповідну базову множину всіх вимог $\mathbf{R}$:

$$\mathbf{R} = \{\bigcup_{i=1}^{n} \mathbf{R}_i\} = \{\mathbf{R}_1, \mathbf{R}_2 \ldots \mathbf{R}_n\}, \tag{1}$$

де $\mathbf{R}_i \subseteq \mathbf{R}$, $(i = \overline{1,n})$ – множини наборів вимог відповідних керівних органів; n – загальна кількість вимог, а

$$\mathbf{R}_i = \{\bigcup_{j=1}^{m_i} \mathbf{R}_{ij}\} = \{\mathbf{R}_{i1}, \mathbf{R}_{i2} \ldots \mathbf{R}_{im_i}\}, \tag{2}$$

при чому $\mathbf{R}_{ij}$ $(i = \overline{1,n}\,;\ j = \overline{1,m_i})$ – множини наборів вимог; m_i – кількість вимог i-го набору.

З урахуванням (2) вираз (1) можна представити у наступному вигляді:

$$\mathbf{R} = \{\bigcup_{i=1}^{n} \mathbf{R}_i\} = \{\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{m_i} \mathbf{R}_{ij}\}\} = \{\{\mathbf{R}_{11}, \mathbf{R}_{12}, ..., \mathbf{R}_{1m_1}\}, \{\mathbf{R}_{21}, \mathbf{R}_{22}, ..., \mathbf{R}_{2m_2}\}, ..., \{\mathbf{R}_{n1}, \mathbf{R}_{n2}, ..., \mathbf{R}_{nm_n}\}\}, \ (i = \overline{1,n}\,;\ j = \overline{1,m_i}). \tag{3}$$

Множини наборів вимог $\mathbf{R}_{ij} \subseteq \mathbf{R}_i$ визначимо таким чином:

$$\mathbf{R}_{ij} = \{\bigcup_{k=1}^{r_{ij}} R_{ijk}\} = \{R_{ij1}, R_{ij2} \ldots R_{ijr_{ij}}\}, \tag{4}$$

де R_{ijk} $(i = \overline{1,n}\,;\ j = \overline{1,m_i}\,;\ k = \overline{1,r_{ij}})$ – вимоги з множини набору вимог $\mathbf{R}_{ij}$; r_{ij} – кількість таких вимог у кожній з множин ij-го набору.

Тоді вираз (3) з урахуванням (4) матиме такий вигляд:

$$\mathbf{R} = \{\bigcup_{i=1}^{n} \mathbf{R}_i\} = \{\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{m_i} \mathbf{R}_{ij}\}\} = \{\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{m_i} \mathbf{R}_{ij} \{\bigcup_{k=1}^{r_{ij}} R_{ijk}\}\}\} = \{\{\{R_{111}, R_{112}, ..., R_{11r_{11}}\}, \{R_{121}, R_{122}, ..., R_{12r_{12}}\}, ...,$$
$$\{R_{1m_1 1}, R_{1m_1 2}, ..., R_{1m_1 r_{nm_1}}\}\}, \{\{R_{211}, R_{212}, ..., R_{21r_{21}}\}, \{R_{221}, R_{222}, ..., R_{22r_{22}}\}, ..., \{R_{2m_2 1}, R_{2m_2 2}, ..., R_{2m_2 r_{nm_2}}\}\}, ... \quad (5)$$
$$\{\{R_{n11}, R_{n12}, ..., R_{n1r_{n1}}\}, \{R_{n21}, R_{n22}, ..., R_{n2r_{n2}}\}, ..., \{R_{nm_1 1}, R_{nm_1 2}, ..., R_{nm_n r_{nm_n}}\}\}\},$$

де

$R_{111}, R_{112}, ..., R_{11r_{11}}, R_{121}, R_{122}, ..., R_{12r_{12}}, ..., R_{1m_1 1}, R_{1m_1 2}, ..., R_{1m_1 r_{nm_1}}, R_{211}, R_{212}, ..., R_{21r_{21}}, R_{221}, R_{222}, ..., R_{22r_{22}}, ...,$

$R_{2m_2 1}, R_{2m_2 2}, ..., R_{2m_2 r_{nm_2}}, ..., R_{n11}, R_{n12}, ..., R_{n1r_{n1}}, R_{n21}, R_{n22}, ..., R_{n2r_{n2}}, ..., R_{nm_1 1}, R_{nm_1 2}, ..., R_{nm_n r_{nm_n}}$ – елементи базової множини, які відображають вимоги щодо забезпечення ЦА від КЗ.

Таким чином, у цій роботі запропоновано базову модель формування вимог до забезпечення кібербезпеки цивільної авіації, яка за рахунок введення базової множини вимог, які містяться у різних керівних документах щодо безпеки ЦА, та відповідних підмножин, що характеризують базову множину, дає можливість формалізувати повну множину вимог, які необхідно забезпечити для захисту ЦА від КЗ.

Література

1. Гнатюк С.О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи / С.О. Гнатюк // Безпека інформації. — Том 19, №2. — 2013. — С. 118-129.
2. Харченко В.П. Кибертерроризм на авиационном транспорте / В.П. Харченко, Ю.Б. Чеботаренко, О.Г. Корченко, Є.В. Паціра, С.О. Гнатюк // Проблеми інформатизації та управління: Зб. наук. пр. : Вип. 4 (28). — К. : НАУ, 2009. — С. 131-140.
3. Приложение 17 к Конвенции о международной гражданской авиации «Безопасность. Защита международной гражданской авиации от актов незаконного вмешательства». — Изд. 9. — 2011. — 60 с.
4. Doc 30 «Политика ЕКГА в сфере авиационной безопасности» (Restricted). — Изд. 13. — 2010. — 138 с.
5. Гнатюк С.О. Сучасні критичні авіаційні інформаційні системи / С.О. Гнатюк, Д.В. Васильєв // Безпека інформації. — Том 22, №1. — 2016. — С. 51-57.
6. Doc 8973 ICAO «Руководство по авиационной безопасности» (Restricted). — Изд. 8. — 2011. — 748 с.

УДК 004.056.5(045)

[1]Корченко А.А., [2]Ахметова С.Т., [1]Казмирчук С.В.
[1]Национальный авиационный университет,
[2]Казахский национальный исследовательский технический университет им. К.И. Сатпаева
annakor@ukr.net
sanzira52@mail.ru
sv.kazmirchuk@gmail.com

ПРЕОБРАЗОВАНИЯ ИНТЕРВАЛОВ В НЕЧЕТКИЕ ЧИСЛА ДЛЯ СИСТЕМ АНАЛИЗА И ОЦЕНИВАНИЯ РИСКОВ ИНФОР МАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. *При решении задач оценивания рисков информационной безопасности в слабоформализованной среде чаще всего необходимо выполнять обработку данных в нечетких условиях. Для реализации такого процесса используют системы, в которых оценивание осуществляется на основе лингвистических переменных, базирующихся на эталонных нечетких числах, определяемые экспертами в процессе настройки систем. За основу эксперт берет интервалы значений и на основе своих заключений, преобразовывает в нечеткие числа. Эффективность использования таких систем оценивания повысится, если будет предусмотрена возможность автоматизированного трансформирования интервалов*

без привлечения экспертов. Для решения такой задачи предлагается метод преобразования, упрощающий процедуру формирования эталонов, за счет реализации процесса трансформирования интервалов в нечеткие числа и минимизирующий влияние человеческого фактора.

Известны методы анализа и оценивания рисков информационной безопасности [1-4] в которых для отображения общего результата оценки используются лингвистическая переменная (ЛП) «СТЕПЕНЬ РИСКА» (***DR***), которая определяется кортежем [3] <***DR***, $\underset{\sim}{T}_{DR}$, X_{DR}>, $\underset{\sim}{T}_{DR} = \bigcup_{j=1}^{m} \underset{\sim}{T}_{DR_j}$. Для каждого из термов $\underset{\sim}{T}_{DR_1}, ..., \underset{\sim}{T}_{DR_j}, ..., \underset{\sim}{T}_{DR_m}$ задается свой интервал значений [dr_1; dr_2[, …, [dr_j; dr_{j+1}[,…, [dr_m; dr_{m+1}]. Трансформирование интервалов значений реализовывают эксперты на основе своих заключений. Часто на практике возникают ситуации, когда такое преобразование в дальнейшем может привести к неточностям при расчёте конечных результатов из-за несогласованности мнений или ошибок экспертов. Поэтому автоматизация этого процесса для минимизации такого рода ошибок является актуальной задачей.

Исходя из актуальности, целью данной работы является разработка метода преобразования интервалов в нечеткие числа (НЧ), который в дальнейшем позволит автоматизировать процесс трансформации и сведёт к минимуму влияния человеческого фактора.

Так как в указанных системах [1-4] чаще всего для реализации процесса анализа и оценивания рисков используются трапециевидные НЧ, реализуем преобразование интервалов в НЧ вида $\underset{\sim}{T}_j = (a_j; b_{1j}; b_{2j}; c_j)$, где $\underset{\sim}{T}_j$ – терм-множества ($j = \overline{1,m}$, m – количество термов); a, c и b_{1j}, b_{2j} – соответственно абсциссы нижнего и верхнего основания трапециевидного НЧ.

Работу метода по преобразованию интервалов представим в виде выполнения последовательности следующих этапов:

Этап 1 – Определение корректирующих параметров: $h_j = \frac{k_{j+1} - k_j}{4}$, где k_j – числовые значения интервалов для оценивания риска ($j = \overline{1,m}$).

Этап 2 – Вычисление значений абсцисс НЧ: $a'_j = k_j - h_j$; $c'_j = k_{j+1} + h_j$; $b'_{1j} = k_j + h_j$; $b'_{2j} = k_{j+1} - h_j$.

Этап 3 – Определение базового значения сдвига и поправка термов: $sf = b'_{11} - k_1, a''_j = a'_j - sf$; $c''_j = c'_j - sf$; $b''_{1j} = b'_{1j} - sf$; $b''_{2j} = b'_{2j} - sf$, где sf - параметр сдвига.

Этап 4 – Нормирование результирующих НЧ: $a_j = (a''_j \times k_{m+1}) / b''_{2m}$; $c_j = (c''_j \times k_{m+1}) / b''_{2m}$; $b_{1j} = (b''_{1j} \times k_{m+1}) / b''_{2m}$; $b_{2j} = (b''_{2j} \times k_{m+1}) / b''_{2m}$, где $j = \overline{1,m}$.

При этом для $\underset{j=1}{\overset{m}{\forall}}(a_j, b_{1j}, b_{2j}, c_j) < 0$, соответственно $a_j = b_{1j} = b_{2j} = c_j = 0$, а для $\underset{j=1}{\overset{m}{\forall}}(a_j, b_{1j}, b_{2j}, c_j) > k_{m+1}$, соответственно $a_j = b_{1j} = b_{2j} = c_j = k_{m+1}$.

Таким образом, предложен метод преобразования интервалов в НЧ в котором за счет реализации процедур корректировки параметров, формирования новых значений абсцисс, определения базового значения сдвига, поправки термов и нормирования результирующих НЧ позволяет формализовать процесс формирования эталонов без участия экспертов соответствующей предметной области.

Для расширения возможностей представленного метода, можно осуществить трансформирование интервалов в другие классы параметрических НЧ, например, треугольных.

Литература

1. Казмирчук С.В. Анализ и оценивания рисков информационных ресурсов в нечетких условиях / С.В. Казмирчук // Защита информации – 2013. – Том 15 №2 (59). – С. 133-140.
2. Казмирчук С.В. Интегрированный метод анализа и оценивания рисков информационной безопасности / С.В. Казмирчук, А.Ю. Гололобов // Защита информации – 2014. – №3. – С. 252-261.
3. Корченко А.Г. Анализ и оценивание рисков информационной безопасности / А.Г. Корченко, А.Е. Архипов, С.В. Казмирчук. // Монография. – К.: ООО «Лазурит-Полиграф», 2013. – 275 с.
4. Mazin Al Hadidi, Jamil S. Al-Azzeh, B. Akhmetov, O. Korchenko, S. Kazmirchuk, M. Zhekambayeva. Methods of Risk Assessment for Information Security Management, International Review on Computers and Software (IRECOS). – 2016. – V. 11 - №2. – P. 81-91.

УДК 004.056:534.6

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

ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ДАТЧИКІВ РОЗБИТТЯ СКЛА СИСТЕМ ОХОРОННОЇ СИГНАЛІЗАЦІЇ

Анотація. *Проведено експериментальне дослідження датчиків розбиття скла систем охоронної сигналізації на предмет виявлення процесу акустоелектричного перетворення. Встановлено, що датчики володіють вказаною залежністю та побудовано залежності нормованих рівнів вихідної напруги від частоти на виході сигнальних ланцюгів досліджуємих датчиків. Запропоновано проводити спецобстеження приміщень де циркулює інформація з обмеженим доступом з метою унеможливлення витоку акустичної інформації.*

Аналіз принципів побудови датчиків систем охоронної сигналізації показує, що до їх складу входять елементи з "мікрофонним ефектом", володіючих властивостями прямого акустоелектричного перетворення. Це, як правило, високочутливі мікрофони. До таких датчиків відносяться датчики розбиття скла, вібраційні або комбіновані датчики.

Зовнішній вигляд та конструкція комбінованого ІЧ-датчика і датчика розбиття скла DSC LC 102 та датчика розбиття скла DSC LC 105 показано на рис. 1.

Рисунок 1 – Датчики DSC LC 102 та DSC LC 105

Ланцюги живлення, передачі інформації та функціонального контролю датчиків поєднуються з пультами прийомно-контрольними які розташовані за межами контрольованої зони [1].

Таким чином, ситеми охоронної сигналізації об'єктів інформаційної діяльності, де циркулює інформація з обмеженим доступом, можуть потенційно утворювати технічний канал витоку акустичної інформації, а саме акустоелектричний канал [2]. Існуючі канали необхідно виявляти, аналізувати природу їх утворення та приймати міри щодо запобіганню витоку акустичної інформації за межі контрольованої зони.

Для дослідження рівнів наведеного електричного сигналу в сигнальних ланцюгах датчиків системи охоронної сигналізації фірм TEXECOM та DSC залежно від частоти опромінюючого гармонічного сигналу в діапазоні частот акустичного сигналу розроблена лабораторна установка. Лабораторна установка включає джерело гармонічного сигналу змінної частоти, звукоізольовану камеру в якій розміщено акустичний випромінювач та досліджуваний датчик сигналізації. Зовнішній вигляд установки представлено на рис 2.

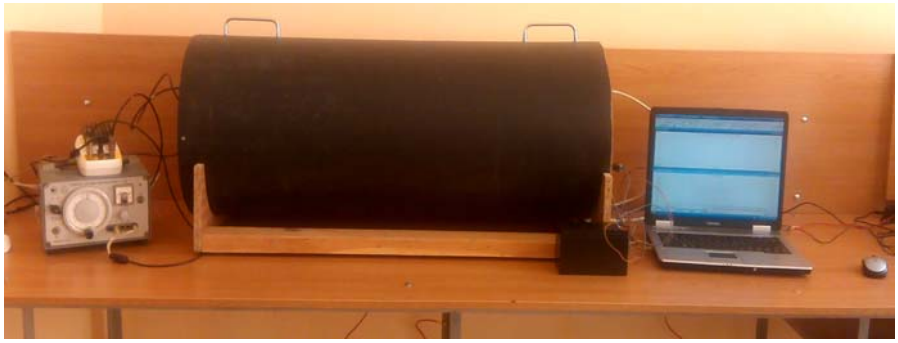

Рисунок 2 – Зовнішній вигляд установки

В якості джерела гармонічного сигналу використовувався генератор гармонічного сигналу звукової частоти Г3-106 з послідовно включеним підсилювачем потужності, а в якості опромінювача в звукоізольованій камері використовувався широкосмуговий гучномовець. Для оцінки рівня наведеного сигналу в сигнальних ланцюгах датчиків використовувалися засоби частотного та часового аналізу.

В якості звукоізольованої камери прийнята поліетиленова труба діаметром 0,5 м та довжиною 1,2 м. В якості звукопоглинаючого матеріалу вибраний поролон, котрий забезпечував рівень звукоізоляції близько 20-40 дБ.

Екрануюча здатність до впливу зовнішніх електромагнітних полів забезпечувалась використанням суцільного екрану виготовлено із оцинкованої сталі, розміщеного по внутрішній стінці труби. Розрахунки ефективності екранування проведені по методиці описаній в [4] складають для електричної складової близько 200 дБ, магнітної складової близько 50 дБ, що достатньо для проведення досліджень.

Дослідження проводилися шляхом опромінення вибраного датчика встановленого всередині камери на середньо геометричних частотах октавних смуг 125, 250, 500, 1000, 2000, 4000, 8000 Гц відповідно при постійному значенні звукового тиску в місці встановлення датчика. Величина наведеного сигналу в ланцюгах передачі інформації оцінювалася з допомогою аналізатора спектру під'єднаного до датчика через попередній підсилювач. Датчик LC-102 опромінювався фрагментом музикальні фонограми.

Результати наведених величин нормованих напруг в залежності від частоти опромінюючого гармонічного сигналу приведені на рис. 3.

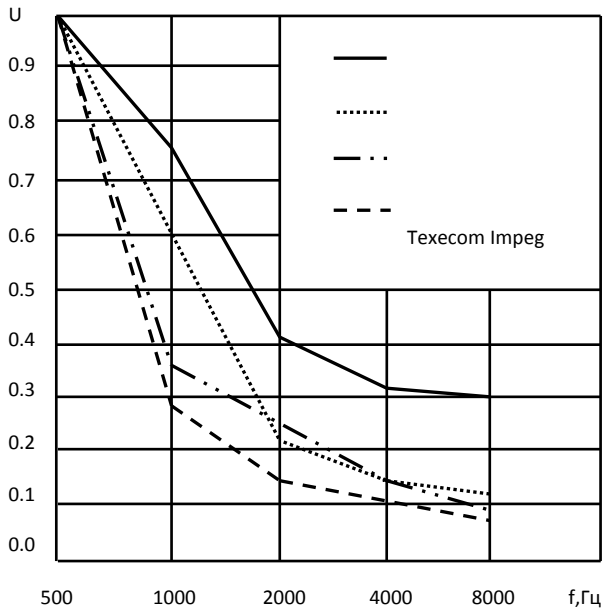

Рисунок 3 – Результати експериментальних досліджень

На рис 4, для прикладу, представлено спектрограми вихідних сигналів датчика LC-105 на частотах опромінення 500 та 1000 Гц відповідно.

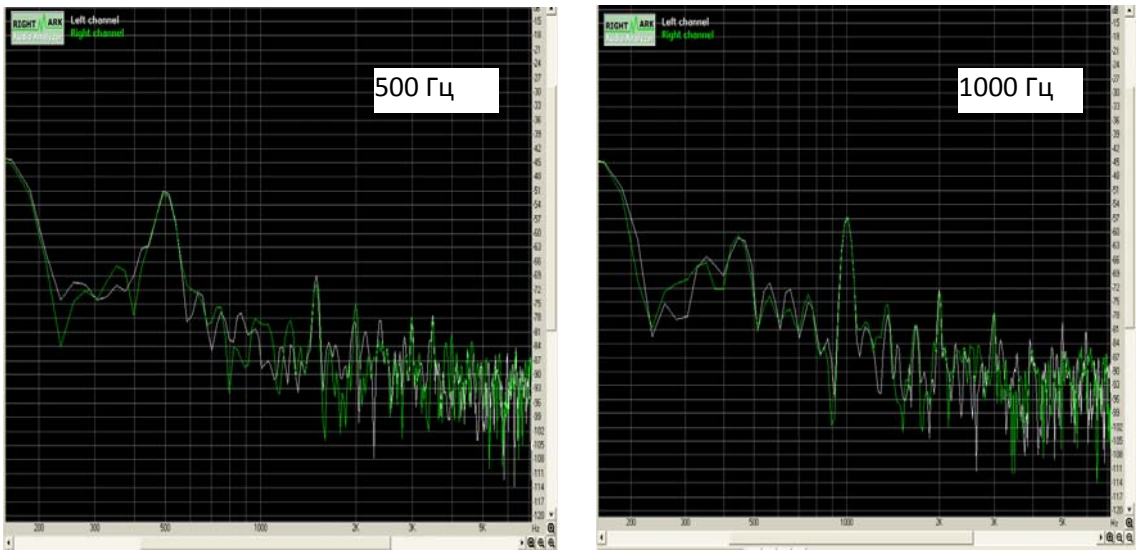

Рисунок 4 – Спектрограма вихідного сигналу датчика LC-105
на частоті опромінення 500 Гц та 1000 Гц

При експериментальних дослідженях була записана музикальна фонограма яка має достатню розбірливість при суб'єктивній оцінці.

Висновки. Проведені дослідження показали, що використання вказаних датчиків в складі охоронних систем на об'єктах інформаційної діяльності, де циркулює інформація з обмеженим доступом, є проблематичною, через можливість несанкціонованого отримання інформації за рахунок ефекту акустоелектричного перетворення. При їх застосуванні в охоронних системах необхідно проводити спеціальні дослідження.

Проведені дослідження є достатньо коректними. Для подальших наукових досліджень необхідно допрацювати лабораторну установку та методику досліджень, з метою врахування амплітудно-частотних характеристик підсилюючих та опромінюючих пристроїв.

Розрахунок послівної розбірливості мови згідно методики [3] вимагає уточнення в зв'язку з тим, що розмову можна записати на диктофон та багатократно прослухати, а тексти є зв'язаними.

Література

1. Магауенов Р. Г. Системы охранной сигнализации: основы теории и принципы построения: Учебное пособие. – М.: Горячая линия-Телеком, 2004. – 367 с.

2. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009. – 508 с.

3. Покровский Н.Б. Расчет и измерение разборчивости речи. – М.: Связьиздат, 1962. – 90 с.

4. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации. – М.: НПЦ «Аналитика», 2008. – 436 с.

УДК 004.056

В.В. Литвинов, д.т.н., професор
Трунова О.В., к.пед.н., доцент
Войцеховська М.М., інженер обчислювального центру
Чернігівський національний технологічний університет
e-mail: KafedraPI@yandex.ua

МОДЕЛЬ КУЛЬТУРИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

Анотація. *Запропонована модель культури інформаційної безпеки організації. Розглянуті її основні рівні: поверхневий, середній, глибинний. Описаний принцип управління та вдосконалення культурою інформаційної безпеки в основу якого покладено цикл Демінга, що містить наступні етапи: попередня оцінка, стратегічне планування, оперативне планування, здійснення, оцінка результатів. Вказані елементи та методи оцінки культури. Для оцінки стану культури інформаційної безпеки організації запропоновані інструменти, а саме експертні системи, що базуються на нечітких моделях, метод MAI, факторний та кластерний аналіз.*

Професійна діяльності ІТ-спеціаліста щоденно пов'язана з інформацією, її накопиченням, зберіганням та/або перетворенням. Лише наявність культури ІБ, усвідомлення і прийняття в повній мірі відповідальності, що покладена на спеціаліста, може зробити дієвими всі технічні та технологічні засоби і процеси ІБ.

Поняття культури ІБ знаходиться на стику інформаційної та корпоративної культур. Культура ІБ − це сукупність відомостей про те, як створити і зберегти інформаційну безпеку особистості, тобто стан захищеності індивіда від шкідливих впливів (інформаційно-психологічна безпека) і як створити стан захищеності інформації, що належить індивіду (безпека інформації). Також культура ІБ − процес створення і збереження стану захищеності індивіда і його інформації від шкідливих впливів на основі наявних компетенцій, а також постійне їх вдосконалення, що приводить до повного задоволення інформаційних потреб. Виходячи з визначення даного поняття, можна сказати, що процес формування культури ІБ в організаціях складається з процесів створення та підвищення корпоративної та інформаційної культур. Однак не всі заходи відносяться до цього процесу, а тільки ті, які стосуються ІБ.

Для того, щоб визначити ситуацію стосовно формування культури ІБ на рівні організації, слід розглянути модель культури ІБ, яка є невід'ємною складовою організаційної

культури: *поверхневий рівень* – артефактів та створень, визначається як видимий, але ще не інтерпретований, – фізичний вплив на формування культури ІБ співробітників за допомогою проведення навчання та контролю рівня компетенцій; *середній рівень* – колективних цінностей, норм та компетенцій, що є частково помітним та свідомим, – збереження рівня культури ІБ організації за рахунок постійного інформування співробітників з питань ІБ для підвищення безпеки організації в усіх її проявах; *глибинний рівень* – основних припущень та переконань, що є неусвідомленим та прихованим – усвідомлення, що кожен працівник є носієм культури ІБ, а тому і учасником організаційної культури загалом рисунок1.

Управління культурою ІБ, як і організаційною культурою в цілому, можливо лише при ретельному, глибокому та тривалому процесі напрацювання, оцінювання та комплексного застосування позитивних управлінських рішень. Формування ефективної корпоративної культури – процес складний та тривалий, потребує критичного оцінювання та постійного вдосконалення.

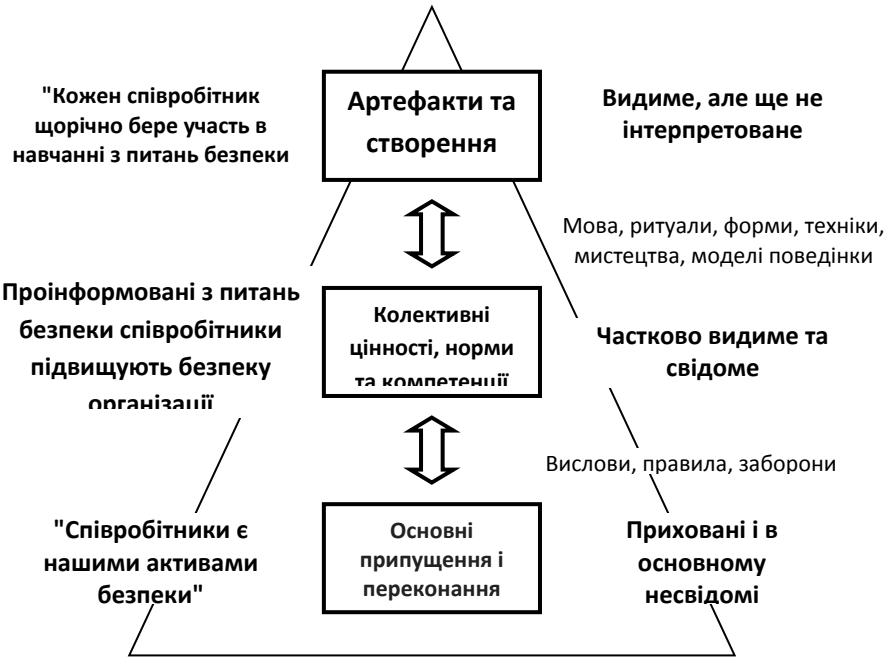

Рисунок 1 – Модель культури ІБ організації

В основі принципу управління та вдосконалення організаційної культури, як і культури ІБ, покладено цикл Демінга. По відношенню до культури ІБ цикл Демінга набуває вигляду, що представлений на рисунку 2.

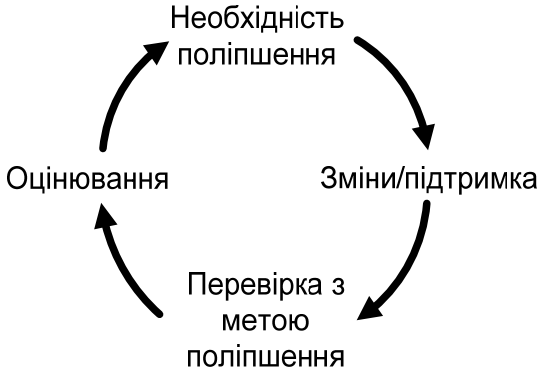

Рисунок 2 – Цикл управління культурою ІБ

Циклу управління культурою ІБ містить наступні п’ять етапів [2]:

1. Попередня оцінка (аналізі фактично наявної культури ІБ):

2. Стратегічне планування: визначення цілей; сегментація (розділення) членів організації.

3. Оперативне планування: інструменти внутрішнього маркетингу; інструменти управління людськими ресурсами; інструменти організаційного розвитку.

4. Здійснення.

5. Оцінка результатів.

Для того, щоб культура ІБ зробила істотний внесок у розвиток ІБ, вона повинна володіти рядом методів для вивчення культури безпеки. Оскільки основні припущення і переконання апріорі неможливо піддати кількісному оцінюванню, то для проведення вимірювання компетенцій, як правило, використовують оповідальні опитування, участь у спостереженнях та групових заняттях. Нажаль, поки що не існує жодного унікального набору інструментів та методів для дослідження культури ІБ. Питання досліджень і розробок в цій області залишається відкритим і потребує уваги. Найбільш доцільним при аналізі моделі культури ІБ організації є використати змішаного методу, реалізація якого наведена в табл. 1 [1, 2].

Таблиця 1

Елементи та методи оцінки культури ІБ

<table>
<tr><th>Метод / Елемент</th><th>Аналіз документів (джерел)</th><th>Анкетування</th><th>Групові заняття</th><th>Опитування</th><th>Спостере-ження</th></tr>
<tr><td>Артефакти та створення</td><td rowspan="3">Аналіз політики безпеки</td><td></td><td></td><td rowspan="3">Опитування відпові-дального за безпеку</td><td>Аудит</td></tr>
<tr><td>Колективні цінності, норми та компетенції</td><td rowspan="2">Анкетування співробітників усіх рівнів</td><td></td><td></td></tr>
<tr><td>Основні припущення і переконання</td><td></td><td></td><td></td></tr>
</table>

Для виявлення основних прогалин між політикою ІБ організації і її сприйняттям працівниками, тобто отримання оцінки стану культури ІБ організації доцільно використовувати експертні системи, що базуються на нечітких моделях, що лінгвістично оцінюють відповіді співробітника. Для зменшення наявного набору факторів пропонуємо здійснювати методом MAI, а для встановлення менш незалежних змінних – факторний аналіз.

Залежно від результатів оцінки рівня культури ІБ, повинні бути прийняті конкретні заходи для збереження або зміни культури за допомогою більш радикальних заходів, що повинні підтримуватися якісною навчальною програмою, можливо, в поєднанні з існуючими навчальними програми, що повинні базуватися на основних положеннях політики культури організації та професійних компетенціях співробітників, усі наявні культурні заходи повинні бути перероблені.

Для отримання можливості визначити правильні заходи з підвищення культури ІБ, визначаються цільові групи співробітників для направленого впливу на основі методів сегментації, зокрема кластерного аналізу. Визначені наступні групи: «*задоволені*» – співробітники, що задоволені політикою організаційної та ІБ, і майже дотримуються певних правил; «*небезпека приходить ззовні*» – співробітники, що вбачають всі небезпеки за межами компанії, вважають, що відповідальність за ІБ цілком покладена на співробітників служби безпеки організації; «*необережні*» – співробітники, які не бачать жодних проблем і вважають розгляд питання щодо політики та правил безпеки зайвим; «*незадоволені*» – співробітники, що незадоволені реальним станом існуючої інформаційної політики, та прагнуть підвищити

рівень безпеки. Кластеризація допоможе при визначенні відповідних заходів з боку співробітників служби безпеки та розробці відповідних інструментів для дієвого впливу на цільову групу.

При порівнянні фактичної та цільової культури ІБ можна визначити правильні інструменти для впливу на персонал та реалізацію цільової культури. Культура не може бути нав'язана набором правил. Лише крок за кроком культура ІБ може бути розроблена на основі внутрішніх комунікацій, підготовки кадрів, належної освіти та на особистої поведінки керівників (лідерів).

Література

1. Rotvold G. How to Create a Security Culture in Your Organization // Information Management Journal. 2008. Nov/Dec. URL: http://findarticles.com/p/articles/mi_qa3937/is_200811/ai_n31111129/?tag=content;col1

2. Schlienger, T. and Teufel, S. (2003). Information Security Culture - From Analysis to Change. 3rd Annual Information Security South Africa Conference, Johannesburg, South Africa, ISSA: http://icsa.cs.up.ac.za/issa/2003/Publications/

УДК 621.391 (043.2)

Одарченко Р.С.
Абакумова А.О.
Національний авіаційний університет, м. Київ
odarchenko.r.s@mail.ru

КЛАСИФІКАЦІЯ DoS АТАК В СУЧАСНИХ СТІЛЬНИКОВИХ МЕРЕЖАХ

Анотація. *В роботі пронаналізовано сучасну архітектуру концепції Інтернету речей. Показана актуальність проведення досліджень в даному напрямку. Було розглянуто основні види мережевих атак в сенсорних підсистемах стільникових мереж у відповідності до еталонної моделі взаємодії відкритих систем, зокрема, фізичного, канального, мережевого, транспортного та прикладного рівнів, з огляду на проблеми забезпечення інформаційної безпеки. Особливу увагу у роботі приділено DoS атакам. Тому було визначено проблемні місця систем захисту саме до них та наведено їх таксономію.*

Інтернет речей (IoT) – концепція обчислювальної мережі фізичних об'єктів, оснащених вбудованими технологіями для взаємодії один з одним або з зовнішнім середовищем, яка розглядає організацію таких мереж як явище, здатне перебудувати економічні та суспільні процеси, що виключає з частини дій і операцій необхідність участі людини [1]. Зв'язок між окремими вузлами в таких мережах може бути забезпечений за допомогою безпроводових технологій різних поколінь (Wi-Fi, Bluetooth, ZigBee, 4G, 5G). Більш детально зупинимося саме на розгляді саме стільникових мереж.

В результаті проведеного аналізу [2-4] було виявлено наступні проблеми і уразливості стільникових мереж в концепції Інтернету речей:

1) DoS-атаки в Інтернеті речей;
2) Прослуховування в Інтернеті речей;
3) Захоплення вузлів в Інтернеті речей;
4) Фізична безпека датчиків.

Як видно, проблемних місць в стільникових мережах доволі багато. Тому на думку автора, необхідно їх розділити на декілька складових підсистем, які потребують підвищення рівня захисту. Таким чином, предметом розгляду даної роботи було обрано стільникову мережу, в якій однією із актуальних задач є оцінка імовірності виникнення та протидії DoS атакам.

Таким чином метою роботи є визначення вразливостей стільникових мереж в архітектурі Інтернету речей до DoS атак, їх класифікація.

Поставлена мета передбачає вирішення наступних завдань:

1. Оцінка імовірності виникнення DoS атак в архітектурі Інтернету речей;
2. Дослідження проблемних місць в архітектурі стільникових мереж Інтернету речей;
3. Дослідження класифікацій DoS атак в стільникових мережах та визначення найбільш небезпечних типів атак;

Тепер перейдемо до детального розгляду вразливостей саме безпроводових сенсорних мереж (БСМ), які можуть нести величезну загрозу в стільниковій мережі. В загальному розумінні сенсорна мережа – це безліч маленьких зчитувальних пристроїв (датчиків), здатних 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 [5]. На рис. 1 [6] показано, наприклад, схему потенційної DoS атаки в сенсорній мережі.

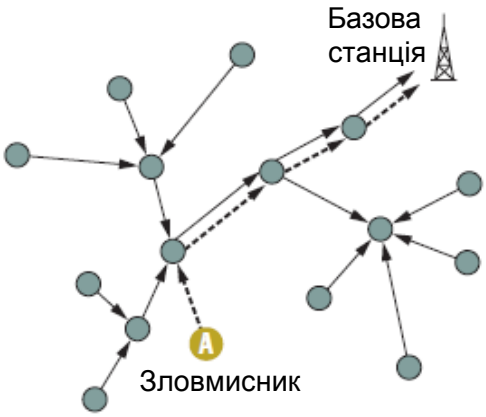

Рисунок 1 – Схема потенційної DoS атаки в сенсорній мережі

Втрати від дії DoS атак залежать від конкретних додатків, що використовуються на сенсорних датчиках. Наприклад, в сенсорній мережі «розумне місто» (smart city) такими додатками можу бути: моніторинг шуму, світла, забруднення навколишнього середовища, руху транспортних засобів, екстрена медична послуга і ін. [7]. В даному прикладі сенсорної мережі для багатьох з наведених додатків наслідки атак DoS можуть бути виражені фінансовими втратами.

На сенсорні вузли та базову станцію можуть бути направлені наступні типи DoS атак в залежності від різних параметрів (рис. 2). В [8] наведено дану таксономію більш детально із повним аналізом DoS атак, в залежності від природи їх виникнення. А в таблиці 1 [9] показаний розподіл DoS атак за рівнями моделі OSI.

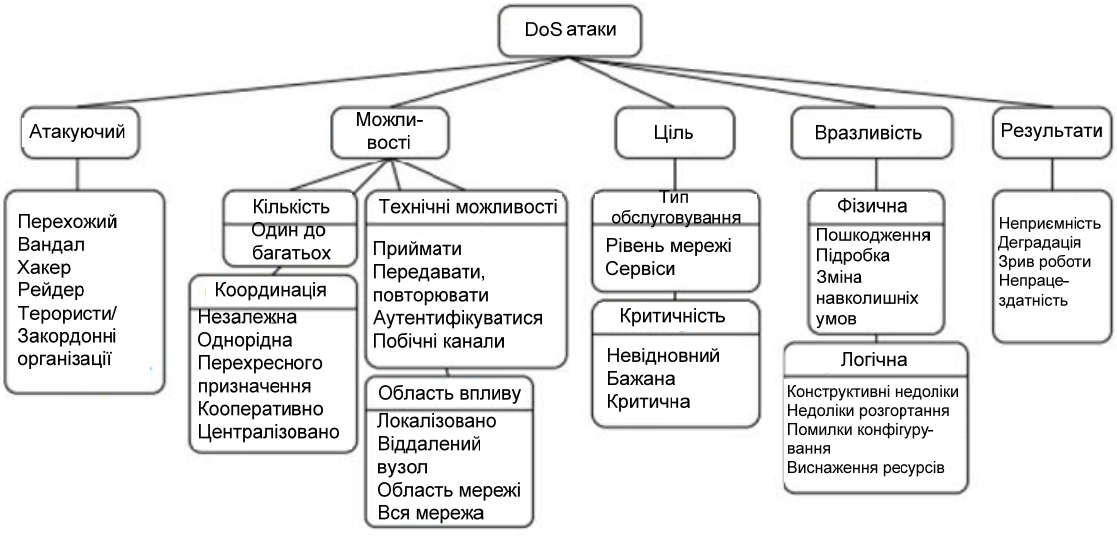

Рисунок 2 – Таксономія DoS атак в безпроводових сенсорних мережах

Таблиця 1

Розподіл DoS атак за рівнями моделі OSI

Рівень	Тип атаки	Заходи протидії
Фізичний рівень	JAMMING (глушіння)	Розширення спектру, пріоритетні повідомлення, картування областей
	TAMPERING (підробка)	Випробувальні пакети проти підробки, використання нечутливих до відмов протоколів
Канальний рівень	Колізії	Корегувальне кодування
	Виснаження	Обмеження швидкості передавання даних
	Збір інформації	Використання захисту проти повторних відправлень, сильна аутентифікація на канальному рівні
Мережевий рівень	Фальсифікація маршрутної інформації	Аутентифікація, використання захисту проти повторних відправлень
	Селективне просування	Використання різних маршрутів, підтвердження доставки
	Sinkhole атака	Перевірка надмірності
	Атака Sybil	Аутентифікація, надмірність, моніторинг
Транспортний рівень	Флуд атаки	Клієнтські пазли
	Розсинхронізація	Аутентифікація
Прикладний рівень	DoS атака на базі маршруту	Аутентифікація, використання захисту проти повторних відправлень
	Перепрограмування	

Висновки. Очевидним є те, що Інтернет речей робить наше життя простіше, але існують значні труднощі в його використанні. Однією з таких проблем є DoS-атаки в розподіленій архітектурі доступу, що можуть бути використані зловмисниками для здійснення крадіжок з незахищених пристроїв, а також використання їх в якості ботів для атаки на треті особи. Таким чином, можна сміливо стверджувати, що дослідження, присвячені проблемам, виявленим в даній роботі, і пошукам шляхів їх вирішення, являються вкрай актуальними, що в майбутньому дозволить підвищити рівень забезпечення безпеки в сенсорних підмережах стильникових мереж зокрема, та у всій архітектурі Інтернету речей.

Література

1. «Интернет вещей» — реальность или перспектива? http://www.mate-expo.ru/ru/article/internet-veshchey-realnost-ili-perspektiva

2. Интернет вещей открывает киберпреступникам новое поле деятельности http://www.klaipeda1945.org/sensatsii/34031/

3. Эксперты предупредили о растущем количестве киберугроз в сфере «Интернета вещей» http://www.securitylab.ru/news/480244.php

4. Интернет вещей ставит под угрозу безопасность пользователей http://umvs.kr.ua/internet-veschej-stavit-pod-ugrozu-bezopasnost-polzovatelej

5. http://sibac.info/studconf/tech/xxxii/42203

6. G.V. Crosby, N. Pissinou, and J. Gadze, “A Framework for Trust-Based Cluster Head Election in Wireless Sensor Networks,” Proc. 2nd IEEE Workshop Dependability and Security in Sensor Networks and Systems, IEEE Press, 2006, pp. 13–22.

7. Матвеев В.А., Морозов А.М., Бельфер Р.А. Оценка уровня риска угрозы безопасности фрода в сети VoIP по протоколу SIP // Электросвязь. – 2014. – №6 – С. 35–38

8. Anthony D. Wood and John A. Stankovic A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks

9. Annie Jenniefer1, John Raybin Jose2 Techniques for Identifying Denial of Service Attack in Wireless Sensor Network: a Survey International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 6, June 2014.

УДК 621.396(043.2)

Поліщук Ю.Я., Шаховал О.А., Мовчан М.С.
Національний авіаційний університет,
liya7954@gmail.com; shakhoval.al@gmail.com
Науковий керівник – к.т.н., доцент Гнатюк С.О.

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОЇ БЕЗПЕКИ УКРАЇНИ В СУЧАСНИХ УМОВАХ

Анотація. *З поліпшенням технологічного процесу в різних сферах життєдіяльності інформаційна безпека та кібербезпека стали основою суспільства та держави, що зобов’язує до створення стратегії кібербезпеки та сприяння її реалізації. У роботі було визначено переваги та недоліки стратегії кібербезпеки України, зокрема у контексті інформаційно-психологічної безпеки, та, у зв’язку із цим, розроблено класифікацію маніпулятивних методів впливу. Отримані результати мають стратегічне значення для забезпечення безпеки українського суспільства в контексті інформаційної війни та можуть бути використані для здійснення профілактичних і заходів протидії негативним інформаційним впливам.*

З огляду на постійне збільшення ризику виникнення нових кіберзагроз та їх еволюції, збільшення впливу на особу, суспільство, кожній державі необхідно мати продуману та чітку, комплексну стратегію кібербезпеки. Стратегія кібербезпеки України [1] була прийнята 15 березня 2016 року. Метою документу є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, а тому потрібно передбачити забезпечення не лише інформаційно-технічної безпеки, а й психологічної.

Відповідно до ISO/IEC 27032, *кіберпростір* – це сукупність апаратних засобів, ПЗ та користувачів, що взаємодіють між собою. Невід’ємним компонентом функціонування будь-якої системи є людина та її свідомість (підсвідомість), яка є об’єктом інформаційно-психологічного впливу (ІПсВ) – фактично в інформаційній безпеці з’являється новий об’єкт захисту. Забезпечення інформаційно-психологічної безпеки (ІПсБ) та контрзаходи для протидії ІПсВ мають бути закріплені на законодавчому рівні.

До основних методів проведення спеціальних інформаційних операцій належать: дезінформування, пропаганда, диверсифікація громадської думки, психологічний тиск, поширення чуток [2]. Саме недопущення їх реалізації забезпечує ІПсБ держави.

Дезінформування найяскравіше розкривається у формі термінологічного «мінування»: так як у вітчизняній стратегії відсутній понятійний апарат, це може спричинити до неправильного визначення понять, що може призвести до хибних дій в забезпеченні кібербезпеки.

Стратегією передбачено використання позитивної *пропаганди*, що проявляється в підвищення цифрової грамотності громадян та культури безпекового поводження у кіберпросторі, проведення кібернавчань для суб’єктів кіберпростору тощо.

Психологічний тиск, поширення чуток, диверсифікація громадської думки – прояви впливу, якому піддається Україна з боку Російської Федерації [3].

Окремим проявом *психологічного тиску* у документі є обмеження участі у заходах, що спрямовані на забезпечення інформаційної безпеки та кібербезпеки будь-яких суб'єктів господарювання, які знаходяться під контролем держави-агресора, або держав чи осіб, стосовно яких діють обмежувальні заходи. Також у стратегії введено поняття активного кіберзахисту як засобу стримування військових конфліктів та загроз у кіберпросторі.

Діяльність спецслужб у кіберпросторі та атаки на урядові і приватні веб-сайти в мережі Інтернет, що мають політичний підтекст та впливають на суспільну свідомість, може здійснюватися з метою *диверсифікації громадської думки, поширення чуток, дезінфомації.*

Однією із найбільших прогалин в площині ІПсБ Стратегії кібербезпеки України є маніпулювання суспільною думкою.

Для кращого висвітлення даної проблеми варто більш детально розглянути поняття ІПсБ, під яким зазвичай розуміють стан захищеності громадян, окремих груп та соціальних верств, масових об'єднань людей і населення загалом від негативних ІПсВ [4].

Сьогодні не є секретом, що сучасні мас медіа будь-якими методами ІПсВ намаються «налаштувати» мислення суспільства у напрямку, яке вигідне для певного кола осіб і, тим самим, створити так званих жертв «маніпуляцій». Узагальнюючи визначення поняття «маніпуляція», доцільно зазначити, що під останнім слід розуміти *процес впливу одним індивідом на іншого з метою виконання волі першого*.

Існує широке коло засобів, за допомогою яких можна керувати поведінкою людини, її думками та відчуттями. Маніпулювання здійснюється в трьох основних сферах: ідеологічній, економічній, соціальній та в рамках міжособистісної, групової та масової комунікації. Особливу важливість в останні роки набула маніпуляція масовою свідомістю і масовою поведінкою, суб'єктом або інструментом якої найчастіше виступають ЗМІ.

Для вирішення завдань і досягнення цілей маніпулятивного впливу (МВ) існують комунікативні методи (технології, прийоми), узагальнену класифікацію яких розроблено, відповідно до механізмів впливу, тобто впливом на свідомість людини, та представлено в [5].

Досліджуючи сферу ІПсБ, важливим фактором є визначення та побудова моделей МВ для подальшого оцінювання МВ мас медіа на особу та соціальну групу.

Формальну модель мас медіа можна представити таким чином:

$$MassMedia = <Content, Members, Channel>, \quad (1)$$

де *Content* – інформаційне наповнення; *Members* – члени інформаційного середовища; *Channel* – канал, яким передається інформація. Тоді як формальна модель каналу, яким передається інформація, з огляду на (1) визначається:

$$Channel = \{Broadcast\ media, Digital\ media, Outdoor\ media, Print\ media, organizing\ and\ public\ speaking\},$$

де *Broadcast media* – кіно, радіо, музика, чи телебачення; *Digital media* – інтернет і мобільні засоби масової комунікації; *Outdoor media* – реклама, плакати або рекламні щити на комерційних будівлях, вагонах метро, повітряна реклама тощо; *Print media* – книги, комікси, журнали, газети, брошури; *Organizing and Public speaking* – публічні виступи.

Інформаційне середовище мас медіа можна представити:

$$InfSpace = < MethInfl, Channel, Members>,$$

де *MethInfl* – сукупність методів МВ; *Channel* – сукупність каналів, якими буде здійснюватися передача інформації; *Members* – члени інформаційного середовища.

$$MethInfl = <MythInfl, PsTechInfl, InfFlInfl, EmotInfl, SocCntr, LogicInfl, EmtSphInfl>,$$

де *MythInfl* – методи міфологічного маніплювання; *PsTechInfl* – методи маніпулятив-них психо-технологій; *InfFlInfl* – методи маніпуляції за допомогою управління потоками або інформаційним середовищем; *EmotInfl* – методи ціннісно-емоційного маніпулювання; *SocCntr* – методи соціального контролю; *LogicInfl* – методи маніпулювання раціональними переконуючими аргументами; *EmtSphInfl* – методи контролю над емоційною сферою.

Виходячи із розроблених формальних моделей, формалізована модель МВ мас медіа матиме вигляд: (див. рис.1) [6], у якій $IFAgent$ – це агент впливу, тобто особа, яка посилає певну інформацію – $Content$ (C); Ch – канал, яким передається (включає використання $P_j = (1,2,3), P \subset M_t$); $M1, M2, M3$ – члени інформаційного середовища або окремі особи.

У загальному алгоритм впливу, відповідно до цієї моделі, можна описати так (рис. 1):

1) агент впливу (окрема особа) передає інформацію (контент); 2) інформація проходить через канали, в цьому випадку під каналом розуміється мас медіа, яка використовує методи МВ; 3) інформація, взаємодіє з точками впливу (страхи, почуття, стереотипи); 4) інформація створює вплив на особу або соціальну групу.

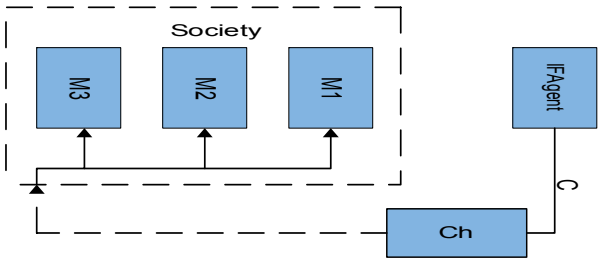

Рисунок 1 – Модель МВ мас медіа

З огляду на розроблену формалізовано модель постає питання обчислення імовірності успіху МВ, яке можна розрахувати за законом біноміального розподілу:

$$P = C_n^k v_0^k (1 - p_0)^{n-k},$$

де p_o – ймовірність, n – к-сть об'єктів МВ, k – об'єкт МВ.

Відповідно для декількох груп МВ n_t, $t = 1, \dots, N$, матимемо елементарні ймовірності p_{ot}, що підвищить точність опису процесів МВ. Математичне очікування при такому розбиті:

$$M = \sum_{t=1}^{m} [n_t p_{ot}].$$

При потужності декількох об'єктів впливу:

$$N = \sum_{t=1}^{m} n_t,$$

Ефективність МВ в цьому випадку можна оцінити таким відношенням, яке завідомо менше одиниці:

$$E_{MD} = \frac{M}{N} = \frac{\sum_{t=1}^{m} [n_t p_{ot}]}{\sum_{t=1}^{m} n_t}$$

Отже, можна зробити висновок, що стратегія не враховує всі можливі шляхи ІПсВ на особу, суспільство, державу та способи і засоби захисту. Це виявляє необхідність створення та прийняття окремого законодавчого акту, який регулював би діяльність, яка стосується ІПсБ, особливо в теперішніх умовах тимчасової окупації території України Російською Федерацією, ескалації конфлікту на Сході держави, економічної кризи та поступового руйнування міжнародного іміджу.

Література

1. Стратегія кібербезпеки України [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/documents/962016-19836.

2. Петрик В.М., Присяжнюк М.М, Мельник Д.С. та ін.. Інформаційна безпека держави: підручник в 2 т.. – Т.1 / за заг. ред. Остроухова В.В. – К.: ДНУ «Книжкова палата України», 2016, – 264 с.

3. Стратегія національної безпеки України [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/287/2015 .
4. Петрик В.М. Щодо визначення інформаційної безпеки та її різновидів / Петрик В.М. // Форми та методи забезпечення інформаційної безпеки держави: Збірник матеріалів міжнародної наук.-практ. конф. (м. Київ, 13 березня 2008 р.). – К.: Видавець Захаренко В. О., 2008. – С. 160–164.
5. Polishchuk Yu., Gnatyuk S., Seilova N. Mass media as a channel of manipulative influence on society // Ukrainian Scientific Journal of Information Security, 2015, vol. 21, issue 3, p. 301-308.
6. Поліщук Ю.Я. Алгоритм реалізації методів медіа-маніпулятивного впливу // IV Все-українська науково-практична конференція молодих вчених і студентів з міжнародною участю «Проблеми та перспективи розвитку авіації та космонавтики»: тези доп. міжнар. наук.-практ. конф., 28-29 жовтня 2015 р., К. – С. 24.

УДК 004.056.5 (045)

Положенцев А.А.,
Національний авіаційний університет,
artem.polozhencev@gmail.com
Науковий керівник – Гнатюк В.О.

МЕТОД ОЦІНКИ ЕФЕКТИВНОСТІ РОБОТИ ГРУП РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ

Анотація. В роботі було розроблено метод оцінки ефективності роботи груп реагування на кіберінциденти, який в подальшому може використовуватись керівниками для аналізу та оцінки ефективності роботи команди, з метою покращення як індивідуальних, так і загальних результатів роботи відділу реагування. Метод складається з декількох етапів: визначення показників роботи CERT, потім виділення з них ключових та побудова панелі індикаторів, яка дозволить візуалізувати отримані показники у зручний для керівника вигляд.

Вступ. Сьогодні інформаційна безпеки особи, суспільства і держави є однією з головних складових національної безпеки в цілому, так як інформаційно-комунікаційні технології широко використовуються в будь-яких сферах життя. Проблема інформаційної безпеки не втрачає своє актуальності в сучасному світі, а навпаки, починає носити глобальний характер. Команди реагування на кіберінциденти (типу CERT – Computer Emergency Response Team) з кожним роком отримують все більше завдань для розслідування. Саме через це з'являється необхідність оцінювати та аналізувати ефективність роботи CERT, тому що даний чинник є одним з ключових для інформаційної безпеки, як окремої організації, так і держави в цілому. Проведений аналіз показав, що оцінці ефективності роботи CERT не відводиться достатньо уваги, що може негативно вплинути на рівень інформаційної безпеки.

Метою роботи є розробка методу оцінки ефективності роботи груп реагування на кіберінциденти, який на основі загальних показників діяльності CERT та багатофакторного кореляційно-регресійного аналізу дозволить визначити ключові показники діяльності CERT та побудувати панель індикаторів.

Проаналізувавши існуючі методи оцінки роботи персоналу зазначимо, що жоден з методів не є універсальним, можна виділити як переваги так і недоліки кожного з них, також, варто відмітити, що для досягнення максимального результату в оцінці є можливим використання декількох методів одночасно, крім того слід зважати на специфіку роботи організації, підрозділ якої оцінюється. Обрані методи мають відповідати структурі

підприємства, характеру діяльності персоналу, цілям оцінки, бути простими і зрозумілими; включати як якісні, так і кількісні показники тощо. Зважаючи на це, було розроблено метод який поєднує переваги відомих методів, мінімізує недоліки та враховує специфіку роботи CERT.

Розроблений метод складається з трьох етапів: 1. визначення показників роботи CERT; 2. визначення ключових показників роботи CERT, 3. побудова панелі індикаторів (ПІ). Далі детальніше розглянемо кожен етап:

Для першого етапу за були взяті базові показники роботи CERT [1]. Основні з яких: пріоритет вирішення кіберінциденту, ступінь впливу кіберінциденту, терміновість вирішення кіберінциденту, лінія підтримки, категорія інциденту, оцінка клієнта, повнота наданої інформації, кількість додатково задіяних фахівців для вирішення кіберінциденту, кількість задіяних ресурсів, вартість заходів реагування на кіберінцидент тощо.

Для другого етапу потрібно, з вказаних у першому етапі показників роботи CERT, відібрати ключові KPI (Key Performance Indicators) [2] шляхом проведення багатофакторного кореляційно-регресійного аналізу. Багатофакторний кореляційно-регресійний аналіз дає змогу оцінити міру впливу на досліджуваний результативний показник кожного із введених у модель факторів при фіксованому положенні на середньому рівні інших факторів. Рівняння, за допомогою якого виражається кореляційний зв’язок між кількома ознаками називають рівнянням множинної регресії. Коефіцієнти множинної регресії показують ступінь середньої зміни результативної ознаки (ефективності роботи CERT) при зміні відповідної факторної ознаки (параметрів ефективності) на одиницю за умови, що всі інші фактори, які включені до рівняння регресії, залишаються постійними (фіксованими) на одному рівні [3]. Тіснота зв’язку при множинній кореляції визначається за допомогою коефіцієнта множинної кореляції, який приймає значення від 0 до ±1, («-» - зв’язок обернений, «+» - прямий). Саме цей показник є ключовим для визначення. Крім даних ключових показників під час кореляційно-регресивного аналізу використовуються також такі показники як коефіцієнти еластичності (показують, на скільки відсотків змінюється величина результативної ознаки при зміні відповідного фактора на один відсоток при фіксованому значенні інших факторів.), бета-коефіцієнти (Бета-коефіцієнти показують, на скільки середньоквадратичних відхилень зміниться результативна ознака при зміні відповідного фактора на одне значення середньоквадратичного відхилення), коефіцієнт детермінації. Всі ці розрахунки можна подати у вигляді машинограми, яку можна спроектувати в додатку MS Excel за допомогою спеціального пакету аналізу. На основі отриманих даних виокремлюються найбільш вагомі параметри, (ступінь залежності яких буде більше від 0,5) які і вважаються KPI.

Завершальним етапом розробленого методу є побудова ПІ, за допомогою якої і буде проходити моніторинг, аналіз та управління ефективністю роботи CERT. Панель індикаторів це інструмент для візуалізації та аналізу інформації про бізнес-процеси і їх ефективність. Дані, що виводяться на панель індикаторів, зазвичай представлені у вигляді ключових показників ефективності. Сама система панелей індикаторів може бути складовою частиною корпоративної інформаційної системи, або виступати як самостійний додаток [4]. Панель індикаторів дозволить представити отримані дані в зручній формі – діаграмах, графіках або схемах даних. Для кожної організації, в залежності від її оперативних, планових та стратегічних цілей дана панель складається індивідуально.

Таким чином, у роботі розроблено метод оцінки ефективності роботи груп реагування на кіберінциденти, який за рахунок загальних показників діяльності CERT та багатофакторного кореляційно-регресійного аналізу дозволяє визначити ключові показники діяльності CERT та побудувати панель індикаторів. Цей метод та сформовані на його основі засоби будуть корисними керівникам команд реагування на кіберінциденти для моніторингу, аналізу, оцінки та управління ефективністю роботи CERT.

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. Система KPI (Key Performance Indicator): разработка и применение показателей бизнес-процесса. Показатели эффективности. – [Електронний ресурс]. – Режим доступу: http://www.businessstudio.ru/procedures/business/kpi/, (05 августа 2016).

3. Мармоза А.Т. Теорія статистики / А.Т. Мармоза // Підручник для студентів вищих навчальних закладів. – К. 2013. – С. 333-397.5

4. 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.

УДК 621.373

Романюков М.Г.
ГУНП в Одеській області
kolyanr21@gmail.com

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПОБІЧНОГО ЕЛЕКТРОМАГНІТНОГО ВИПРОМІНЮВАННЯ SSD ТА HDD НАКОПИЧУВАЧІВ

Анотація: *Сучасні методи обробки інформації, що містять державну таємницю або комерційні, технологічні секрети, проходять етапи обробки на персональних комп'ютерах. Засобам електроно-обчислювальної техніки (ЕОТ): флеш носіям, магнітним дискам, принтерам, клавіатурі та іншим комплектуючим властиві побічні електромагнітні випромінювання та наводи(далі ПЕМВН). Інформація в цих пристроях передається послідовним кодом, всі параметри цього коду стандартизовані та добре відомі.*

Проведено огляд проблем виникнення електромагнітного випромінювання від засобів електронно-обчислювальної техніки та наведена порівняльна характеристика результатів вимірювання побічних електромагнітних випромінювань від SSD(solid-state drive) та HDD(hard disk drive) накопичувачів за допомогою комплексу АКОР-2ПК.

Перехоплення електромагнітних випромінювань базується на широкому використанні різного типу радіоприймальних засобів аналізу і реєстрації інформації та інших (антенні системи, широкосмугові антенні підсилювачі, панорамні аналізатори та ін.) які, як правило, розміщені за межами контрольованого периметра, що створює проблеми по виявленню таких пристроїв. Також ведеться перехоплення інших електромагнітних випромінювань: радіолокаційних, радіонавігаційних систем управління та електромагнітних сигналів, що виникають в електронних засобах за рахунок самозбудження, акустичного впливу, паразитних коливань і навіть сигналів персонально-обчислювальної машини (далі ПЕОМ), що виникають при видачі інформації на екран [4].

Для здійснення активного радіотехнічного маскування ПЕМВН використовуються пристрої, що створюють шумове електромагнітне поле в діапазоні частот від декількох кГц до 2000 МГц. Для даних цілей використовуються надширокосмугові передавачі РІАС-АЗ, Базальт-5ГЕШ, DELTA-7, які мають сертифікат відповідності ДССЗЗІ України [5].

До недавнього часу на вітчизняному ринку та ринку країн СНД були представлені такі комплекси для вимірювання ПЕМВН: SMV-8,5, SMV-11, SMV-41, Элмас, ESH-3, АКОР-2ПК.Вимірювальні приймачі ЕЛМАС, ESH-3, АКОР-2ПК автоматизовані та обладнані інтерфейсами за стандартом IEEE-488, що дає можливість керувати режимами роботи приймача за допомогою зовнішньої ПЕОМ .

Цифровий комплекс вимірювання ПЕМВН реалізовано на основі автоматизованого комплексу виявлення радіовипромінювань. АКОР-2ПК являє собою аналізатор спектру та високочутливий селективний вимірювальний приймач для частотного діапазону від 10 Гц до 3000 МГц. [2, 3].

З появою на сучасних ринках твердотілих накопичувачів SSD (комп'ютерний запам'ятовувальний пристрій на основі мікросхем пам'яті), виникає потреба провести дослідження та порівняльну характеристику вимірювання побічного електромагнітного випромінення від SSD та HDD накопичувачів, що можна реалізувати за допомогою цифрового комплексу вимірювання ПЕМВН АКОР-2ПК [1, 3].

Основна відмінність SSD від звичних HDD накопичувачів – це відсутність будь-яких рухомих деталей. Інформація на таких пристроях зберігається в спеціальних енергонезалежних мікросхемах, також відомих як NAND SSD. Для яких характерні свої переваги:

– відсутність рухомих частин;

– висока швидкість читання/запису, що перевершує пропускну здатність інтерфейсу жорсткого диска (SATA II 3 Gb/s, SATA III 6 Gb/s, SCSI і т. д.);

– низьке енергоспоживання;

– повна відсутність шуму через відсутністю рухомих частин і охолоджувальних вентиляторів;

– висока механічна стійкість;

– широкий діапазон робочих температур;

– стабільність часу зчитування файлів незалежно від їх розташування або фрагментації;

– малі габарити та вага;

– великий модернізаційний потенціал як у самих накопичувачів так і у технологій їх виробництва.

– менша чутливість до зовнішніх електромагнітних полів.

Та недоліки:

– обмежена кількість циклів перезапису;

– проблеми сумісності SSD накопичувачів з застарілими і навіть багатьма актуальними версіями ОС сімейства Microsoft Windows;

– ціна за гігабайти SSD-накопичувачів істотно вище ціни за гігабайти в HDD.

За допомогою комплексу АКОР-2ПК проведено дослідження тактових частот та рівнів сигналу на можливість зняття інформації за рахунок ПЕМВН. Дослідження проводились з використанням вимірювальної антени АИ5-0 для вимірювання електричної складової поля та застосуванням методу примусової активізації, який полягає у активізації каналу еталонним сигналом, що дозволяє ідентифікувати випромінювання, і виміряти рівні що виникають в результаті ПЕМВН [6].

Для тестування було обрано HDD WDC WD5000AAKX-221CA1 та SSD Kingston SSDNow SKC300S37A/120G.

Під час тестування HDD диску було виявлено інформативні сигнали на наступних частотах: 120.011 Мгц та 750.113 Мгц. Графічне зображення спектру яких приведено на рис. 1 та рис. 2 відповідно.

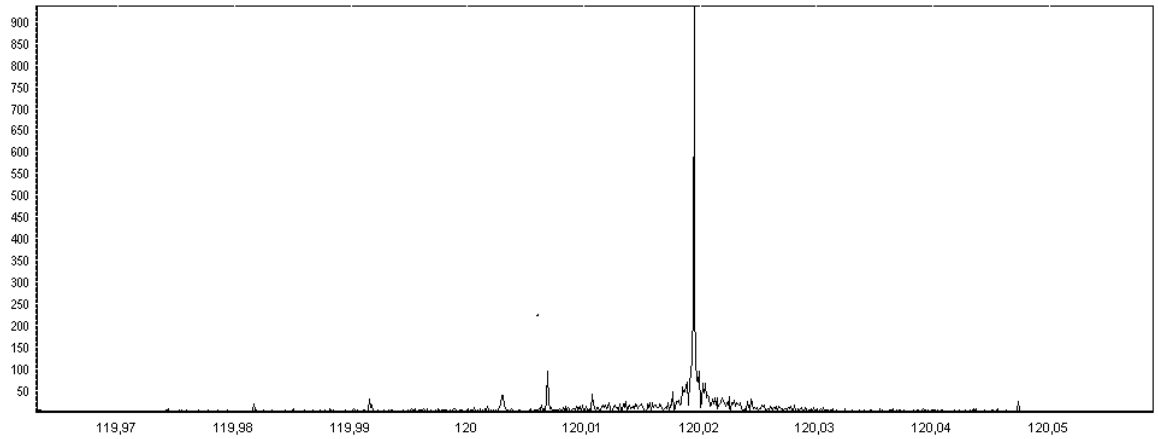

Рисунок 1 – Спектр сигналу частоти 120.011 Мгц

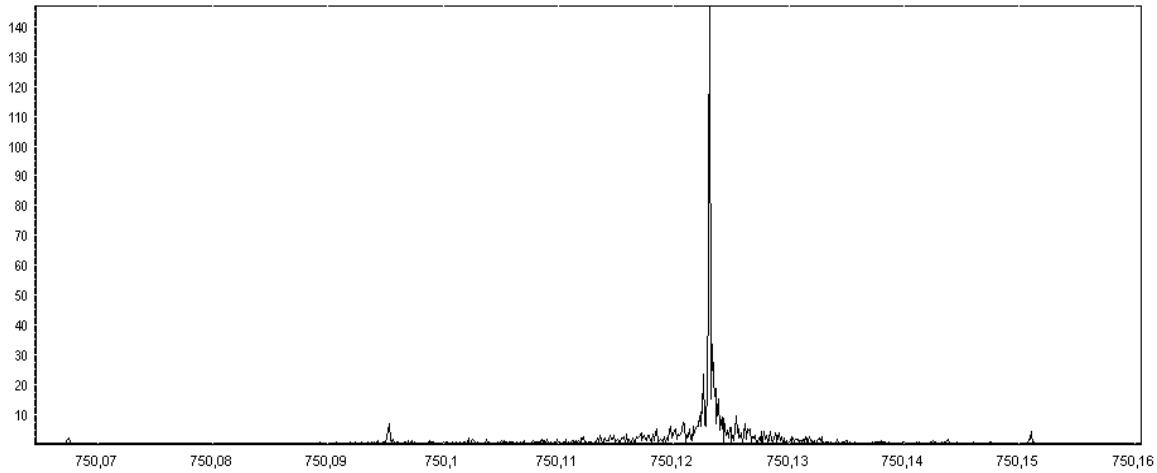

Рисунок 2 – Спектр сигналу частоти 750.113 Мгц

Таким чином проведено порівняльну характеристику SSD та HDD накопичувачів та їх побічних електромагнітних випромінювань за допомогою автоматизованого комплексу АКОР-2ПК, та отримано наступні результати:

- швидкість читання-запису SSD накопичувачів в декілька разів перевищує швидкість читання-запису HDD;
- HDD накопичувачі в режимі роботи споживають майже в 2 рази більше енергії ніж SSD;
- ударостійкість SSD накопичувачів перевищує ударостійкість HDD в 23 рази в режимі роботи та в 4 рази в режимі зберігання інформації;
- відсутність будь-якого шуму під час роботи твердотілих накопичувачів пояснюється відсутністю рухомих частин конструкції, на відміну від HDD;
- фізичні розміри та вага HDD значно перевищує твердотілий аналог;
- досить значна перевага в даних тактової частоти та зниження тривалості імпульсу SSD свідчить про досить швидкий обмін даними накопичувача;
- отримання інформативних частот під час вимірювання HDD утворює реальну загрозу витоку інформації каналом ПЕМВН;
- на сьогоднішній день вартість твердотілих накопичувачів залишається досить високою, порівняно з HDD.

Література

1. Закон України «Про інформацію». – К.: ВР України, 1992. – 15 с.

2. Технические условия ТУ У 33.2-13847488.001-2003 согласованы с ДСТСЗИ СБ Украины (исх.№18/3-1513 от 19.08.2003 г.). Сертификат соответствия № UA1.105.118216-03

от 31.12.2003 г. [Електронний ресурс] – Режим доступу: http://www.akor.mksat.net/production.htm.

3. В.Б. Дудикевич / Дослідження побічного електромагнітного випромінювання від флеш носіїв // В.Б. Дудикевич, І.С. Собчук, Л.М. Ракобовчук, В.С. Зачепило // Системи обробки інформації. – 2011. – № 3. – с.112-116

4. Конахович Г.Ф. Защита информации / Г.Ф. Конахович. – М.: МК-Пресс, 2005. – 281 с.

5. Перелік засобів загального призначення, які дозволені для забезпечення технічного захисту інформації, необхідність охорони якої визначено законодавством України [Електронний ресурс] Режим доступу: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=234237&cat_id=39181. 6. SSD – преимущества и недостатки [Електронний ресурс] – Режим доступу: http://katode.ru/ssd-preimushhestva-i-nedostatki/.

УДК 004.056.53

Самусь В.П., Гізун А.І.
Національний авіаційний університет.
victorsamus@gmail.com

ПРОБЛЕМИ ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ПЛАТІЖНИХ СИСТЕМ В АСПЕКТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОСОБИСТОСТІ ТА СУСПІЛЬСТВА

Анотація. *Досліджено можливість викрадання та неправомірного заволодінням фінансовими активами особистості. Проаналізовано та порівняно існуючі платіжні операції. Визначено незахищені та проблемні місця в проведенні Інтернет-платежів. Наведено практичні рекомендації для запобігання отримання фінансової вигоди стороннім особам та сервісам. В ході дослідження виявлено, що тільки правильне налаштування облікового запису та використання практичних порад дозволяє забезпечити інформаційну безпеку особистості.*

Глобальний розвиток фінансово-економічних зв’язків в суспільстві набирає значних обертів з поширенням інформаційних технологій. Для проведення традиційних фінансових операцій достатньо мати комп’ютер або телефон з активною мережею Інтернет. Еволюція поширення паперової готівки та розвиток високої технології стали причиною створення нового способу організації системи платежів EFTS (Electronic Funds Transfer System). Сучасний бізнес швидко змінює традиційні форми розрахунків і переміщується в мережу Інтернет. Зробити переказ, заплатити за комунальні послуги стало надзвичайно легко. Це полегшувало роботу і не потребувало використання великої кількості готівки. Хоча система електронної організації ефективніша, але поступається в деяких аспектах паперовій [1]. Наприклад, паперовий документ дозволяє отримати квитанцію, що практично унеможливлює шахрайство. Останнім часом збільшилось число злочинів пов’язаних з неправомірним переміщенням коштів з чужого рахунку на власний.

Метою роботи є визначення та дослідження базових процесів проведення Інтернет-платежів в електронних платіжних системах, визначення їх особливостей та порівняння специфіки роботи, а також розробка практичних рекомендацій для запобігання отримання фінансової вигоди сторонніми особами.

Основою всіх фінансових операцій користувачів є платіжна система – це платіжна організація, члени платіжної системи та сукупність відносин, що виникають між ними при проведенні переказу коштів. Існують фізичні та електронні платіжні системи, зосередимось на досліджені роботи останніх. Традиційними представниками є: WebMoney, PayPal, Perfect Money, Yandex.Money, Qiwi та інші. Основними функціями є: реєстрація і підтримка віртуальних рахунків клієнтів, можливість поповнення та виводу коштів на рахунки за

допомогою інших способів, проведення операцій між рахунками клієнтів, збереження інформації про операції та стан рахунків, захист від несанкціонованого доступу і захист конфіденційної інформації клієнта і технічна підтримка клієнтів. Робота електронних платіжних систем базується на електронних грошах.

Електронні гроші – це так звана грошова вартість, яка зберігається на технічному пристрої і дозволяє виконувати платежі. На даний момент зберігають їх на двох видах носіїв: старт-карти і пам'ять комп'ютера. Більшість платіжних систем зберігають електронні гроші в пам'яті комп'ютера. Так, електронні гроші є традиційним видом розрахунку для фрілансерів та користувачів мережі Інтернет. Неправомірно заволодіти електронними грошами можна в двох випадках: в результаті платіжної операції і отримання доступу до облікового запису користувача.

Платіжна операція – це процес в результаті якого електронні гроші надсилаються з одного рахунку на інший. В результаті цього змінюється власник електронних грошей. Існує декілька видів платіжних операцій: прямий переказ, переказ з протекцією, ваучер і переказ з використанням третьої сторони. Прямий переказ – це операція передачі електронних грошей від одного користувача до іншого без застосування додаткових мір безпеки. Для проведення операції достатньо ввести номер рахунку, необхідну суму та коментар платежу. Переказ з протекцією проходить аналогічно прямому переказу але застосуванням додаткового коду, який дозволить отримати електронні гроші. В результаті неправильного введення або закінчення терміну дії гроші повертаються до відправника. Код протекції складається з 6 цифр і анулюється після 8 неправильних введень. Ваучер – це сертифікат чи скретч карта, що підтверджує право власності на певну суму електронних грошей. Для використання достатньо ввести номер в спеціальне поле платіжної системи. Переказ з використанням третьої сторони – це складна операція з залученням третьої сторони, яка гарантує зберігання, переказ і отримання електронних грошей на умовах погоджених з відправником і отримувачем [2]. Характеризується найскладнішим процесом проведення та додатковою комісією від третьої сторони.

Прямий переказ є самим небезпечним видом платіжної операції. Стороння особа створивши віртуальний рахунок може запропонувати послугу, а після отримання електронних грошей просто зникне, перевівши баланс через пункти обміну і отримавши готівку. Своєчасне блокування не дозволить перешкодити зловмиснику. В 94% випадків неправомірне заволодіння трапляється в результаті прямих переказів. Ця проблема дуже поширена, так як люди не використовують платежів з протекцією чи залученням третьої сторони. Код протекції захистить користувача послуги від недобросовісного отримувача в разі повідомлення його після проведення операції. Лише 3% неправомірного заволодіння електронними коштами відбувається через операції з протекцією. 2% і 1% це ваучери і операції з залученням третьої сторони.

Неправомірний доступ до облікового запису може відбутись в результаті введення даних на фішинговому сайті, перехоплення через відкриті канали передачі даних та враження вірусами. Для запобігання викрадання електронних коштів та отримання даних зловмисниками потрібно налаштувати свій обліковий запис. Для цього потрібно ввімкнути авторизацію з двох і більше етапів, підтвердження платежів з використання SMS чи технології E-num [3]. Також, потрібно ввести ліміти на оплату операцій, які б не перевищували середню суму операцій на 10%. Зміна ліміту повинна проводитись з введенням секретного слова. На всіх пристроях де використовується платіжна система повинен бути встановлений антивірусний захист з оновленням бази сигнатур. Потрібно користуватись тільки ліцензованим програмним забезпеченням, не зберігати на комп'ютер додаткове ПО. Також, при проведенні платежів звертати увагу чи захищене підключення до веб-сайту. Наведені практичні поради суттєво знизить шанси зловмисника отримати доступ до облікового запису платіжної системи.

Висновок. В ході проведеного дослідження був розглянутий понятійний апарат функціонування електронних платіжних систем. Була наведені функції роботи платіжних

систем, а також їх функції. Проаналізовано види платіжних операцій, то можливі варіанти неправомірного отримання даних облікового запису користувачів платіжних систем. Сформовано та наведено практичні поради для запобігання отримання електронних грошей зловмисниками та сторонніми особами. В подальшому планується створення та впровадження рекомендацій для безпечного використання платіжних систем.

Література

1. Закон України «Про платіжні системи і переказ грошей в Україні» від 05.04.01 р. № 2346. [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2346-14.

2. Формы оплаты // [Електронний ресурс]. – Режим доступу: http://studio24web.com/category/formy-oplaty.

3. Пиріг С.О. Платіжні системи Навч. посібн. /С.О.Пиріг. – К.: Центр учбової літератури, 2008. – 240 с.

УДК 621.391

Севастєєв Є.О., Гордійчук В.В.
ОНАЗ ім. О.С.Попова
Seva.odessa@gmail.com
Науковий керівник д.т.н., проф. Захарченко М.В.

ИНФОРМАЦИОННАЯ ЕМКОСТЬ НАЙКВИСТОВСКОГО ЭЛЕМЕНТА ПРИ ПОЗИЦИОННОМ И ТАЙМЕРНОМ КОДИРОВАНИИ

Аннотация. *Сравниваются позиционное и таймерное кодирование по критериям временных затрат на передачу соответствующих кодовых ансамблей и информационной емкости найквистовского элемента*

При передаче данных в современных системах связи используют принципы позиционного кодирования. Общий вид представления числа N в позиционной системе исчисления

$$N = \beta_n a^{n-1} + \beta_{n-1} a^{n-2} + \ldots + \beta_1 a^0, \quad (1)$$

Число a – представляет число различимых с заданной вероятностью различных состояний информационного параметра.

Длительность сигнала каждой цифры β_i (1) равна длительности найквистового элемента $t_0 = 1/\Delta F$.

Позиционное кодирование включает в себя:

Определение объема алфавита, соответствуюшей объему числу реализациий кодовых конструкций N_p (числа символов);

Нумерацию конечного счетного числа множества букв в десятичной системе счисления.

Определение числа элементов в кодовом слове по формуле:

$$m = \left| \log_a N_p \right|, \quad (2)$$

где a – позиционность канала (число состояний информационного параметра),

N_p – объем алфавита .

Например, при передаче символов русского языка по двоичному каналу $m = \log_2 32 = 5$ бит. Оценим энтропию и информационную емкость одного найквистовского элемента при посимвольной передаче для позиционного кодирования. При первичном алфавите в 32 символа энтропия H кодового слова равна

$$H = \lceil \log_2 32 \rceil = 5 дв.ед.$$

Следовательно, при передаче посимвольно отдельных букв в каждом кодовом слове, состоящего из 5 двоичных единиц содержится 5 бит информации, информационная емкость одного найквистового элемента будет:

$$I_н = \frac{\log_2 32}{5} = 1 дв.ед.$$

Для увеличения информационной емкости одного найквистового элемента необходимо чтобы число реализаций увеличивалось более чем в 2 раза при увеличении интервала реализаций на один элемент.

$$\frac{N_p(m+1)}{N_p(m)} > 2 \qquad (3)$$

Оценим эффективность использования для этих целей таймерных сигнальных конструкций. В таймерных сигнальных конструкциях в отличии от позиционного кодирования информация заложена не в виде сигнала на интервале найквистового элемента, а в длительностях отдельных отрезков сигнала i и местах их положения. Требование к отрезкам, из которых состоят кодовые слова следующие:

1. каждый из отрезков в кодовом слове $t_0 \le \tau_{ei} = t_0 + k\Delta$, где $k \in 0 \div k_0$ – целые числа;

2. число отрезков в кодовом слове длинной m найквистовских элементов $1 < i < m$. При $i = m$ возможна одна реализация.

3. Величина $\Delta = \frac{t_0}{s}$, где $s \in 1 \div s_0$ определяет минимальную величину длин отдельных отрезков в одной или различных кодовых комбинациях и должны обеспечивать минимальную вероятность измерения длины отрезка на приеме.

Такой принцип формирования кодового слова обеспечивает установление переходного процесса на приеме, и различимость длин отрезков в кодовом слове, позволяет избежать межсимвольных искажений. Можно показать, что меняя длительности отрезков можно резко увеличить число различных комбинаций на заданном интервале m найквистовых элементов [2]

$$N = \frac{((ms - i(s-1))!}{(ms - is)!i!}, \qquad (4)$$

Так, например, при заданном $S = 5$ и $m = 5$, для $i = 3$ $N_p = 286$, а при $s = 7$, что апробировано для городской телефонной сети, $N_p = 680$, что в более чем в 20 раз больше по сравнению с позиционным кодированием.

Построим таблицы, определяющие количество реализаций при *m=const*. Фиксация параметра *m* позволяет не усложнять структуру декодера, так как на приемной стороне заранее известен размер кодового слова. В таблице рассмотрим зависимость количества реализаций от параметров *i* и *s*.

Таблица 1

Количество реализаций ТСК в зависимости от i и s, при m=5

s \ i	1	2	3	4	5
2	9	28	35	15	1
3	13	55	84	35	1
4	17	91	165	70	1
5	21	136	286	126	1
6	25	190	455	210	1
7	29	253	680	330	1

8	33	325	969	495	1

Теперь рассмотрим наиболее важный параметр – количество информации, которое можно передать на временном интервале T_c. Информационная емкость одного найквистовского элемента согласно выражению [3]

$$I_н = \frac{\log_2 N_p}{m} \tag{5}$$

Таблица 2

Информационная емкость найквистовского элемента при *m*=5, в зависимости от *s* и *i*

s \ i	1	2	3	4
2	0,633985	0,961471	1,025857	0,781378
3	0,740088	1,156272	1,278463	1,025857
4	0,817493	1,301559	1,473264	1,225857
5	0,878463	1,417493	1,631974	1,395456
6	0,928771	1,513971	1,765945	1,542849
7	0,971596	1,596599	1,881878	1,673264
8	1,008879	1,668859	1,984071	1,790257

Из таблицы видно, что информационная емкость одного найквистовского элемента растет с ростом параметра s и также растет до определенного значения параметра *i*. Можно сказать, что оно стремится к 2, что в два раза больше чем при позиционном кодировании.

Выводы. Увеличение информационной емкости найквистовского элемента возможно реализовать за счет перехода от позиционного к таймерному кодированию, что обеспечит выигрыш в пределе до двух раз.

Литература

1. Захарченко М.В. Системи передавання даних. – Т. 1: Завадостійке кодування: підручник [для студентів вищих технічних навчальних закладів] / М.В. Захарченко. – Одеса : Фенікс, 2009. – 448 с.

2. Методи підвищення ефективності використання каналів зв'язку / [Захарченко М.В., Гайдар В.П., Улеев О.П., Липчинський О.І.]. – К.: Техніка, 1998. – 248 с.

3. Захарченко Н.В. Эффективность компенсации избыточности кода при использовнии таймерных сигналов/ Н.В. Захарченко, В.Е. Басанов // Моделювання та інформаційні технології: зб. наук. праць. – Вип. 31. – К.: 2005. – С. 6-13.

УДК 621.391.1

Севастєєв Є.О.
ОНАЗ ім. О.С.Попова
Seva.odessa@gmail.com
Науковий керівник д.т.н., проф. Захарченко М.В.

СВОЙСТВА АНСАМБЛЕЙ ТАЙМЕРНЫХ СИГНАЛОВ С ПЕРЕМЕННЫМ ЧИСЛОМ ИНФОРМАЦИОННЫХ ОТРЕЗКОВ

Аннотация. *В докладе показано, как изменяется количество реализаций кодовых слов на интервале T_0 при изменении информационных параметров сигналов, также*

показаны особенности ансамблей таймерных сигналов при фиксировании информационных параметров s=const *и m*=const.

Современные системы связи в большинстве своем используют позиционное блоковое кодирование, — то есть представления символа через коэффициенты системы исчисления соответствующей алфавиту канала. Типичной моделью канала в наши дни является двоично-симметричный канал, алфавит такого канала содержит два символа («0» или «1»), а количество информации, которое можно передать в одном минимальном элементе $I = \log_2 2 = 1$. Каждый символ согласованый с пропускной полосой канала и имеющий длительность $t_0 = 1/\Delta F$ называют Найквистовским элементом. При таком методе передачи модуляция происходит через временной интервал кратный t_0, что является основным недостатком позиционного кодирования, так как на временном интервале T_c блока состоящего из m найквистовских элементов может быть только m моментов модуляции, а количество информации в блоке возрастет в m раз.

В таймерных сигнальных конструкциях информационным параметром является длительность и взаимное положение моментов модуляции на интервале сигнальной конструкции [1].

Количество реализаций для таймерных сигнальних конструкций на временном интервале $T_c = m \cdot t_0$ определяется выражением

$$\mathrm{Np} = \sum_{\mathrm{i}=1}^{\mathrm{m}} C^{i}_{ms-i(s-1)}\ , \qquad (1)$$

где i количество моментов модуляции, $s = t_0/\Delta$, определяется параметрами реального канала.

В случае $i = m$ алфавит таймерного кода будет состоять из одного символа.

В табл. 1 приведены число реализаций ансамблей таймерных кодов на интервалах $m \in 4 \div 10$ найквистовских элементов для позиционного и таймерного кодирования $s = 3,4,7; i = 2,4,5$.

Приведенная таблица наглядно демонстрирует, что с ростом m при i=const, s=const число реализаций увеличивается, так же с ростом s при m=const, i=const число реализаций увеличивается. При этом рост числа реализаций при больших s и m значительно быстрее, чем при позиционном кодировании. Однако, не стоит забывать, что рост s ограничен межсимвольными искажениями, или требуемой вероятностью ошибки в канале.

Таблица 1

Число реализаций таймерных кодов в зависимости от *i, s, m*

i	s	m = 4	5	6	7	8	9	10
		$2^m = 16$	32	64	128	256	512	1024
2	3	28	55	91	136	190	253	325
	4	45	91	153	231	325	435	561
	7	120	253	435	666	946	1275	1653
	3	20	84	220	455	816	1330	2024

3	4	35	165	455	969	1771	2925	4495
	7	120	680	2024	4435	8436	14190	22100
5	3	0	1	56	462	2002	6188	15504
	4	0	1	126	1287	6188	20349	53130
	7	0	1	792	11628	65780	237336	658008

Технологично для получения необходимой мощности используемого ансамбля целесообразно использовать подмножества кодовых слов с различным числом информационных отрезков i при одних и тех же значениях m и s. Например, сформируем множество кодовых слов для передачи различных комбинаций на интервале $T_c=5t_0$, $s=7$. Указанные значения позволяют передавать по каналам ГТС с вероятностью ошибки $p_{err}<5\cdot10^{-5}$ [2].

Рассчитаем суммарное количество реализаций значения согласно выражению (1):

$$N_p = \sum_{i=1}^{5} C_{35-6i}^{5} = 1263$$

Таким образом на интервале $T_c=5t_0$ можно реализовать кодовых слова, каждое из которых содержит $\lceil \log_2 1263 \rceil = 10$ бит. Следовательно емкость одного найквистовского элемента составляет 10/5=2 бита, что в два раза больше по сравнению с позиционным кодированием.

Выводы. Применение таймерных кодов с переменным количеством информационных отрезков i может обеспечить рост информационной емкости одного найквистовского элемента до двух раз по сравнению с позиционным кодированием.

Литература

1. Захарченко М.В. Системи передавання даних. – Т. 1: Завадостійке кодування: підручник [для студентів вищих технічних навчальних закладів] / М.В. Захарченко. – Одеса : Фенікс, 2009. – 448 с.

2. Методи підвищення ефективності використання каналів зв'язку / [Захарченко М.В., Гайдар В.П.,Улеев О.П., Липчинський О.І.]. – К.: Техніка, 1998. – 248 с.

УДК 004.7:621.396.2

Скітер І.С.,
ЧНТУ
skiteris@mail.ua
Скітер А.І.,
ОНАЗ ім. О.С.Попова.
skiterigors@gmail.com

ВИЯВЛЕННЯ DDOS АТАК НА ОСНОВІ АНАЛІЗУ ПРОФІЛЮ КОМП'ЮТЕРНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ EWMA-СТАТИСТИКИ

Анотація. *Сформована задача виявлення аномалій трафіку з врахуванням його стохастичної природи. В якості основного обраний метод EWMA, який дає змогу проводити згладжування динамічного ряду спостережень за вхідним трафіком. Ідентифікація аномального трафіку проводиться за верхньою межею порогового відхилення від*

«центральної лінії» та k послідовних перевищень межі, що зменшує похибки першого роду. Проведена імітація атак на віртуальну комп'ютерну мережу, розроблені та апробовані методи групування трафіку для оптимізації чутливості, максимальної достовірності виявлення атак на мережу та максимально точного часу визначення атаки.

Системи виявлення мережевих вторгнень (СВВ) в інформаційні системи (ІС) застосовуються як один із заходів оборони ІС і включають в себе виявлення ознак атак, розробку методів та засобів виявлення несанкціонованого проникнення крізь системи захисту. Цій темі присвячені роботи Н. Семенова [1], В. Бабенко[2], Р. Фаткієвої [3] та ін.

Системи виявлення аномалій (СВА) працюють, спираючись на нормальний профіль (НП) мережі і реагують при аномальному відхиленні параметрів трафіку мережі від нормального. Ефективність СВА залежить від методів отримання та обробки інформації про параметри мережі [3], [4]. Основою систем, орієнтованих на використання статистичних методів є формування НП мережі [1]. Будь-яке відхилення від нього вважається несанкціонованою діяльністю. Універсальність статистичних методів полягає в тому, що для виявлення аномалій в системі немає потреби визначення типів атак, та їх властивостей [4].

EWMA-статистика (Exponentially Weighted Moving Average) – методологія розрахунку ковзної середньої з експоненційним розподілом вагів, які асимптотично зменшуються з часом [5]. Використовуються контрольні карти на базі граничної межі, центральної лінії, значення показника що досліджується для визначення стану мережі [6]. Аналіз на основі EWMA враховує випадкову і циклічну компоненту коливань рівня активності мережі, так як розраховується на основі динамічних рядів даних. Основними показниками EWMA методу є: пороговий коефіцієнт β, показник чутливості λ, інтервал ковзкої середньої q.

Пороговий коефіцієнт β показує на скільки відсотків поточне значення параметру мережі повинно перевищити середнє, розраховане за EWMA, щоб його можна було вважати аномальним. Аномальним є показник X_t в момент часу t при виконанні умови:

$$X_t \geq (\beta + 1)\bar{x}_{t-1}, \tag{1}$$

де $\bar{x}_t = (1-\lambda)X_t + \lambda\bar{x}_{t-1}$ – середнє значення параметру за EWMA для масиву даних до t.

Ваговий коефіцієнт λ контролює динаміку зміни трафіку шляхом зміни відхилень і зменшує кількість помилок першого роду при аналізу мережі на наявність аномалій [7].

Інтервал згладжування q - кількість значень показника вхідного трафіку для визначення відповідної ковзкої середньої і розраховується за формулою:

$$q = 2/\lambda - 1. \tag{2}$$

При зміні чутливості в межах $(0 < \lambda \leq 1)$ кожному λ відповідає значення $\sigma_{s(t)}$:

$$\sigma_{S(t)} = \sqrt{\frac{1}{n-1}\sum_{t=1}^{n-q-1}(X_t - S_t)^2}\ . \tag{3}$$

Оптимальним вважається значення λ, якому відповідає умова:

$$\lambda_{opt} : \overline{\sigma_{S(t)}} \to \min \quad , \text{де} \quad \overline{\sigma_{S(t)}} = \frac{1}{n-1}\sigma_{S(t)}. \tag{4}$$

Контрольні карти в методиці EWMA включають верхню та нижню граничні межі:

$$\begin{cases} \Delta^- = Z_0 - 3\sigma_Z \\ \Delta^+ = Z_0 + 3\sigma_Z \end{cases} \quad , \text{де} \quad \sigma_Z = \sqrt{\sigma^2_{EWMA}} = \sqrt{\frac{\lambda}{2-\lambda}\sum_{t=1}^{n}(X_t - Z_0)^2}\ . \tag{5}$$

Використання алгоритму, приведеного вище, дає змогу проводити результативний статистичний аналіз мережі на предмет наявності аномалій.

При скануванні, конвертації, обробці даних виявлені недоліки: брак оперативної пам'яті в ОС, аварійне закриття WireShark; при наявності аномалії кількість рядків у скан-файлі перевищує ємність таблиці MS Excel; скан-файли займають багато місця на жорсткому диску; час аналізу даних залежить від характеристик апаратного забезпечення (табл. 1, 2).

Таблиця 1

Розмір файлу з результатами сканування в різні проміжки часу

Час сканування (хв)	Нормальний стан мережі		Аномальний стан мережі	
	Розмір файлу	Кількість рядків в звіті Excel	Розмір файлу	Кількість рядків в звіті Excel
5	1.6 MB	8 145	15 MB	35 849
10	4 MB	15 904	25 MB	55 684
120	2.1 GB	142 653	4,6 GB	1 035 659
180	3,5 GB	201 334	8 GB	4 250 457

Таблиця 2

Час обробки даних в залежності від розміру отриманої вибірки

Розмір файлу	Відкриття в програмі WireShark	Аналіз в MS Excel		
		Групування даних	Статистичний аналіз	Побудова графіків
25 MB	1 хв	8 хв	25 хв	0,2 с
635 MB	23 хв	53 хв	2,8 год	1,3 с
4,6 GB	1,5 год	2,5 год	8,6 год	5,5 с

Основні вимоги до використання методики наступні:

- сканування мережі доцільно проводити протягом 8 годин, створюючи новий звіт кожну годину: формується НП, усувається проблема браку рядків у MS Excel:
- формування профілю для EWMA-аналізу проводити скануванням кожну 1 год.
- при скануванні мережі для EWMA-аналізу новий звіт створювати кожні 10 хв.: скорочення часу на сортування, групування та аналізу даних з 6 год. до 3,3 год;
- EWMA-аналіз доцільний після методу СКВ: звільнення ресурсів системи.

Вхідні дані представлені результатами 8 годинного сканування мережі протягом двох тижнів. Отримано 112 скан-файлів кожну 1 год. З метою імітації DoS та DDoS атак протягом години мережа спеціально перенавантажувалась завантаженням декількох великих файлів. Після сканування розраховано середнє арифметичне значення, значення довірчих меж: $\overline{Y} = 108{,}871$; $Y^{+} = 136{,}008$; $Y_{-} = 87{,}097$ та значення СКВ $\sigma = 256{,}143$, яке перевищує верхню допустиму межу, що свідчить про наявність аномалії. Для зменшення ризику хибного реагування здійснене комплексне використання методу СКВ та методу EWMA. Розрахунок центральної лінії й довірчих меж для НП був проведений на основі годинного сканування нормального функціонування мережі: час розбито на 60 інтервалів по 1 хв. кожний. Імітація атаки проводилась на 10-15-й, 24-28-й та 45-49 хвилинах сканування. Варіанти із менших інтервалів у 1,2,3, 15 та 20 хвилин виявили недоцільність вибору через великий час обробки та аналізу (біля 3-х год.), та неможливість точного встановлення часу виникнення аномалії. У якості значення параметру чутливості для здійснення статистичного аналізу було обрано $\lambda = 0{,}2$,середнє значення довжини пакетів по інтервалам $\overline{X} = 3038{,}717$. Реалізація методу представлена на рис. 1.

Рисунок 1 – Контрольна карта EWMA-аналізу даних годинного сканування

Експериментально встановленне оптимальне значення показника чутливості $\lambda = 0{,}2$. При значенні $\lambda < 0{,}2$ за аномалію сприймається навіть невелике відхилення. При значенні $\lambda > 0.3$ – є велика ймовірність пропустити атаку.

Висновки

Розроблений та доповнений математичний апарат використання статистичних методів аналізу трафіку компютерної мережі. Експериментально доведена ефективність обраних методів для виявлення аномалій трафіку мережі, а також розроблені макроси на мові Visual Basic для MS Excel з метою полегшення обробки та аналізу даних користувачу.

Метод СКВ та EWMA-аналіз дозволяють ідентифікувати та підтвердити атаку на систему та визначити час вторгнення. Причому, при наявності потужного апаратного забезпечення, можна виявити час атаки з точністю до секунди.

При проведенні статистичного аналізу трафіку мережі доцільно перевірку мережі на наявність аномалій першочергово проводити методом СКВ; при ідентифікації наявності аномалій проводити повторний аналіз методом EWMA з метою виключення хибного реагування; оскільки обробка та аналіз результатів 6 десятихвилинних сканувань трафіку в сумі займає менше часу ніж обробка результатів одного одногодинного сканування, проводити саме їх статистичну обробку з метою більш точного визначення часу здійснення атаки.

Література

1. Семенов Н. А. Применение статистических методов обнаружения DDoS-атак в локальной сети / Н. А. Семенов, А. Ю. Телков. // Вестник ВГУ, Серия: Системный анализ и информационные технологии. – 2012. – №1. – С. 82–87.

2. Иванов В.В. Статистическая модель сетевого трафика: автореферат диссертации [Text] / В.В. Иванов. – Дубна., 2009. – С. 30.

3. Фаткиева Р.Р. Модель обнаружения атак на основе анализа временных рядов // Труды СПИИРАН. 2012. – Вып. 21. – С. 71–79.

4. Бабенко Г. В. Анализ современных угроз безопасности информации, возникающих при сетевом взаимодействии. / Г. В. Бабенко. [Text] // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. – 2010. – №2. – С. 149–152.

5. Brown H. Some observations on adaptive forecasting / H. Brown, S. Wage. [Text] // Management Science. – 1964. – №3.

6. Brown R. G. The fundamental theorum of exponential smoothing. Oper. Res / R. G. Brown, R. F. Meyer. [Text] // Management Science. – 1961. – №5

7. Winters P. R. Forecasting sales by exponentially weighted moving averages / P. R. Winters. [Text] // Management Science. – 1960. – №3.

УДК 003.26:351:007

Солодухіна Н.В.,
ОНПУ
amersylvie@gmail.com
Науковий керівник – к.т.н., доц. Кононович В.Г.

МОДЕЛЬ ПРОЦЕСУ УПРАВЛІННЯ ПРИ САМООРГАНІЗАЦІЇ СИСТЕМ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Анотація. *Вирішується задача моделювання процесу управління системою інформаційної, інформаційно-психологічної та кібернетичної безпеки об'єктів із саморганізацією. Конкурентна взаємодія внутрішніх компонентів об'єкта захисту приводить до виявлення параметрів порядку Запропонована спрощена математична модель соціальної активності за методикою формування «Моделі утворення дискусійної групи» і з використанням апарату звичайних диференціальних рівнянь. Модель дозволяє проводити дослідження характеру динаміки взаємодії компонентів об'єкта захисту і виконувати пошук умов та можливих управляючих факторів процесу забезпечення безпеки. Отримані результати дозволять підвищити ефективність управління системою інформаційної, інформаційно-психологічної та кібернетичної безпеки.*

Дана робота відноситься до сфери забезпечення інформаційної безпеки держави в частині управління системами інформаційної, інформаційно-психологічної та кібернетичної безпеки. Проблеми моделювання процесів управління безпекою ускладнюються рядом факторів. Моделювання процесів управління всіма видами безпеки в умовах самоорганізації об'єктів захисту є порівняно новою проблемою і тому актуальною. Основи забезпечення інформаційної безпеки держави викладено у [1]. Концептуальні підходи до інформаційної безпеки представлено в [2]. Соціальна природа інформаційної безпеки відображена у [3]. Властивості інформаційно-психологічно безпеки надано в [4]. Засоби економічної та інформаційної безпеки консолідованої інформації розкриті у [5]. Прикладом моделювання соціальної організації може служити робота [6].

Метою даної роботи є розробка засобів моделювання процесів управління системами інформаційно-психологічної та кібернетичної безпеки в умовах самоорганізації захищених соціальних та кібернетичних об'єктів.

Визначення основних понять та об'єктів захисту, що функціонують в умовах інформаційної війни та прискореної соціальної динаміки. "Інформаційне управління – це процес вироблення та реалізації управлінських рішень у ситуації, коли управляючий вплив носить неявний характер і об'єкту управління надається інформація щодо ситуації, орієнтуючись на яку цей об'єкт начебто сам обирає лінію своєї поведінки" [7, с. 94]». Інформаційний процес – складне переплетення усвідомленого та неусвідомленого впливу джерела інформації на всі рівні людської психіки.

Сукупність різного роду інформаційних процесів, інформаційних систем, системи масової свідомості та психіки складають систему більш складного порядку – інформаційний простір [8, с. 13]». «У загальному випадку під інформаційною безпекою розуміється такий стан інформаційного середовища при якому гарантується розвиток цього середовища і її використання в інтересах особистості, суспільства і держави, а також захищеність від будь-яких загроз [див. 5, с. 121]». Управління розуміється як «процес організації такого цілеспрямованого впливу на об'єкт, у результаті якого цей об'єкт переводиться у потрібний стан [див. 8, с. 16]».

Поняття про самоорганізацію складних кібернетичних та соціальних об'єктів. Наука про самоорганізацію це синергетика. Синергетикою ставляться актуальні питання сучасності – знаходження оптимальних темпів технологічного та технічного прогресу, ефективного управління розвитком суспільства та еволюцією людини і навколишнього

середовища. Синергетика вивчає ряд фундаментальних явищ світу, відкритих у нелінійній динаміці та притаманних багатьом іншим сферам науки.

Синергетика ставить своєю основною задачею пізнання загальних процесів і принципів, які лежать у основі процесів самоорганізації самої різної природи: фізичних, хімічних, біологічних, технічних, економічних, соціальних тощо. Основні принципи синергетики полягають у наступному [9]. Синергетика досліджує кооперативні явища у нелінійних, нерівноважних, нестаціонарних відкритих системах. Ці дослідження пов'язані з вивченням процесів самоорганізації у складних динамічних системах. У цьому випадку спостерігаються кооперативні процеси, які приводить до виникнення нових властивостей системи взаємодіючих динамічних підсистем. Одна з таких властивостей – **самоорганізація**, яка проявляється в самоузгодженості взаємодії підсистем, що дає можливість говорити про виникнення упорядкованої структури (*патернів*), чи навіть нової системи. Виникнення самоузгодженості пов'язано з прагненням системи до певного стійкого стану. Цей стан на мові динамічних систем називається **аттрактором**, що означає притягуюча множина. Поява нової системи пов'язана із втратою стійкості і переходом початкової системи у новий стійкий стан. Процес переходу носить назву **біфуркація**. Зміни, які проходять близько до точок нестійкості, залежать від низки відносно не багатьох факторів, які називаються **параметрами порядку** (ПП) і визначають поведінку підсистем динамічної системи, ніби «підпорядковуючи» її деякій єдиній структурі поведінки. Самі підсистеми формують ПП і, таким чином, виникає, свого роду зворотний зв'язок, а точніше круговий причинний зв'язок. Зміни ПП проходять значно повільніше, ніж зміни «підпорядкованих» їм підсистем. Виникнення ПП пов'язано із взаємодією чи конкуренцією підсистем. ПП відрізняються від **управляючих параметрів** тим, що останні є зовнішніми впливами, які змінюють ПП. Загальна послідовність процесу може бути представлена наступними фазами: 1) відносно стабільний стан втрачає стійкість внаслідок зміни внутрішнього стану чи зовнішніх обмежень; 2) біфуркація, яка зумовлена новим елементом у системі або впливом на управляючий параметр, що приводить до подальшої самоорганізації системи; 3) по завершенню процесу самоорганізації еволюціонуюча система переходить у новий відносно стабільний стан.

Під соціальною самоорганізацією прийнято розуміти стихійне об'єднання людей, що спрямовується єдиною метою [6, с. 17]. Групова свідомість розглядається як система групових понять, правил, образів сприймання, яка самоорганізовується. При моделюванні масштабної самоорганізації, яка охоплює великі маси людей, моделюються механізми утворення і розвитку соціальних рухів і використовується апарат звичайних диференційних рівнянь. У менш масштабній самоорганізації моделюється утворення малих груп і використовується матричний апарат. Конкурентна взаємодія внутрішніх компонентів системи приводить до виявлення ведучої, яка може покласти початок розвитку небезпечних явища або їхнього повторення. Іншими словами – виявляються параметри порядку модельованої динамічної системи. Далі вивчається характер взаємодії компонент і виконується пошук умов попередження катастрофічного наслідку. Після цього в систему включаються управляючі фактори і досліджується задача управління.

Математична модель. Розглянемо найпростішу модель. Відомо, що кількість інцидентів з кібербезпекою невпинно зростає. Розробимо модель самоорганізації, яка описувала б об'єднання людей, групова свідомість яких формується на протилежній ідеї – ідеї боротьби з кіберзлочинністю. Скористуємось методикою розробки моделей соціальної активності, викладеної в роботі Колесіна і названої «Модель утворення дискусійної групи [див. 6, розд. 2.1]». В даній методиці припускається, що у процесі прямого чи опосередкованого спілкування M людей формується ідея, що об'єднує їх у групу. Нехай N – число людей, які об'єдналися в групу. Використаємо характеристику «яскравості» групового самовираження, тобто, нехай V – рівень розвитку ідеї, яка об'єднує людей у групу.

«Формування групової свідомості полягає у виявленні елементів, ефективних для досягнення групової мети. Виявлення ефективного елемента відмічається по росту частоти його прояву серед членів групи. Елемент, який перейшов деяку рубіжну частоту, вважається

визнаним групою, прийнятим до ужитку, а значить такий, що став елементом групової свідомості. Нехай ω_i – частота проявів i-го елемента, а $\Delta\omega_i$ – приріст частоти за час $\Delta t = 1$. Тоді відношення $\Delta\omega_i / \Delta t$ називаємо *інтенсивністю* формування i-го елемента групової свідомості. Нехай n – число елементів, які перейшли рубіж частоти до моменту часу t, а Δn – приріст за час Δt. Тоді $\Delta n / \Delta t$ називаємо інтенсивністю формування групової свідомості або яскравістю групового самовираження [див. 6, с. 19]». При цьому розуміється, що безпосереднє або опосередковане спілкування носить відкритий характер. Враховуючи всі ці припущення складаємо балансні рівняння для M і N, та допоповнюємо їх рівнянням для параметру порядку V:

$$\begin{cases} \dfrac{dM}{dt} = \alpha VM + \beta N, \\ \dfrac{dN}{dt} = \alpha VM - \beta N, M + N = const, \\ \dfrac{dV}{dt} = cM - mV, \end{cases} \quad (1)$$

де αVM – інтенсивність об'єднання прихильників ідеї боротьби з кіберзлочинністю, βN – інтенсивність виходу із нього, «cM – інтенсивність формування ідеї («тим більша, чим більша маса M, в якій вона формується), mV – інтенсивність розпаду ($m = 1/TV$, TV – характерна тривалість зберігання уявлень, які відображають дану ідею) [див. 6, с. 60]».

Початковими умовами можуть бути припущення, що у початковий момент не було ні ідеї, ні її носіїв: $V(0) = 0$, $N(0) = 0$. На слайдах презентації даної доповіді показані результати дослідження властивостей системи.

Висновки. Отримані результати дозволять підвищити ефективність управління системою інформаційної, інформаційно-психологічної та кібернетичної безпеки.

Література

1. Петрик В.М. Забезпечення інформаційної безпеки держави: підручник / В.М. Петрик, М.М. Присяжнюк, Д.С. Мельник та ін.; за заг. ред. О.А. Семченка та В.И. Петрика. – К.: «Книжкова палата України», 2015 – 672 с.
2. Жук Е.И. Концептуальные основы информационной безопасности / Е.И. Жук // Электронное научно-техническое издание. – М.: Издатель ФГБОУ ВПО «МГТУ им. Н.Э. Баумана». Эл. № ФС 77 – 48211, 2010. – 38 с. – Режим доступа: technomag.bmstu.ru/doc/143237.html.
3. Владимирова, Т.В. Социальная природа информационной безопасности [Текст] : монография / Т.В. Владимирова ; АНО содействия развитию соврем. отечеств. науки. Изд. дом «Научн. обозрение». – М.: Изд. Дом «Научн. обозрение», 2014. – 239 с.
4. Петрик В.М. Информационно-психологическая безопасность в эпоху глобализации: учебное пособие / В.М. Петрик, В.В. Остроухов, А.А. Штоквиш; под ред. В.В. Остроухова. – К., 2008. – 544 с.
5. Кавун С. В. Економічна та інформаційна безпека підприємств у системі консолідованої інформації : навчальний посібник / С. В. Кавун, А. А. Пилипенко, Д. О. Ріпка. – Х.: Вид. ХНЕУ, 2013. – 364 с.
6. Колесин И.Д. Принципы моделирования социальной организации: Учебное пособие. – СПб.: Издательство «Лань», 2013. – 288 с.
7. Информационная безопасность системы организационного управления. Теоретические основы : в 2 т. / Н.А. Кузнецов, В.В. Кульба, Е.А. Микрин и др.; [отв. ред. Н.А. Кузнецов, В.В. Кульба] ; Ин-т пробл. передачи инф. РАН. – М.: Наука, 2006. Т.1 – 495 с.
8. Стюгин М. Оценка безопасности системы информационного управления Российской Федерации [Электронный ресурс] / М. Стюгин. – Режим доступа: http://psyfactor.org/lib/styugin4.htm.

9. Большой психологический словарь / под ред. *Б.Г. Мещерякова, В.П. Зинченко* – 3-е изд., доп. и перераб. – СПб.: ПРАЙМ-ЕВРОЗНАК, 2006. – 672 с.

УДК 004.78:681.139.3

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»,
Поліщук К.В.,
Одеська національна академія зв'язку ім. О.С.Попова
kerikanpsn@gmail.com
Науковий керівник – к.ф.н., Стайкуца С.В.

АНАЛИЗ УГРОЗ, РИСКОВ И УЯЗВИМОСТЕЙ СОВРЕМЕННЫХ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ

Аннотация. *В работе представлены критерии оценки систем видеонаблюдения в аспекте безопасности. С позиции критериев оценки проведен анализ угроз, рисков и уязвимостей современных систем видеонаблюдения. Фундаментальные критерии анализа, - принципы построения, технологии, этапы "жизненного" цикла, коммуникационная среда, способы записи видеопотоков, выбор вендора рассмотрены более детально. Результаты анализа позволят всем участникам взаимодействия (проектантам, вендорам, инсталляторам, корпоративным и частным заказчикам) проектировать, строить и эксплуатировать системы видеонаблюдения с более высоким уровнем защищенности.*

Системы видеонаблюдения, как одни из самых популярных в категории технических средств охраны, прочно закрепились на позициях эффективных систем безопасности. За последнее десятилетие из "достаточно дорогого удовольствия" системы видеонаблюдения стали доступным средством безопасности, найдя свое применение в государственном и коммерческом секторах вне зависимости от вида хозяйственной деятельности компании. Системы видеонаблюдения постоянно менялись, адаптируясь под технологическую "эволюцию", которая произошла в сфере телекоммуникаций [1].

Традиционно системы видеонаблюдения классифицируют по типам применяемого оборудования. Так, долгий период время эта классификация включала аналоговые и цифровые системы, добавив с недавних пор в свой состав гибридные решения. Как альтернатива также используется классификация, которая базируется не на технологических решениях, а на типах используемых сигналов. При таком подходе системы видеонаблюдения уже подразделяют на аналоговые, комбинированные, гибридные и сетевые [2]. Для правильного выбора необходимой технологии видеонаблюдения и программно-аппаратного состава необходимо хорошо понимать специфику предприятия, основные цели и задачи системы, а также выбрать подходящий формат построения системы видеонаблюдения [3].

Рассмотрим основные угрозы, уязвимости и риски, современных систем видеонаблюдения. Для объективности анализа предлагается рассматривать уровни защищенности систем видеонаблюдения с учетом основных критериев, а именно: принципа построения системы видеонаблюдения, жизненного цикла, выбранной технологии, компонентного состава, коммуникационной среды, способа записи видеопотока, вендора оборудования, уровня квалификации собственного персонала и представителей проектно-монтажной компании, типа угрозы (внутренняя или внешняя), типа воздействия на систему (физическое или логическое), а также наличия договоров обслуживания и реального проведения технического обслуживания.

Выбор правильного принципа построения системы видеонаблюдения на базовом уровне дает возможность прогнозировать угрозы безопасности. Так, в настоящее время существует 2 основных принципа построения систем видеонаблюдения: принцип ”одеяла” и принцип ”специфического подхода” [4]. Принцип “одеяла” предполагает распределенную инфраструктуру объекта, наличие бюджета, большое количество видеокамер, массивы данных, штат операторов. В противоположность представленному примеру, метод ”специфического” подхода используется для наблюдения за конкретными объектами и в условиях ограниченного бюджета. Основные признаки – минимальная инфраструктура, малое количество видеокамер, небольшой штат с высокой квалификацией персонала, использование принципов превентивности. С позиции уровня защищенности неправильный выбор принципа построения системы видеонаблюдения может приводить появлению целого ряда рисков, как стратегических, так и тактических.

Примером стратегического риска могут выступать нарушения в количественном и качественном наполнении ”жизненного” цикла систем видеонаблюдения. Известно, что каждый из этапов жизненного цикла систем безопасности имеет свои цели и задачи, начиная от формирования требований к системе (обследование объекта, использование опросного листа, составление технического задания), далее – документирования процесса (подготовка эскизного и рабочего проектов, рабочей документации) и ее эффективной эксплуатации (монтажные и пусконаладочные работы, обслуживание). Нарушения на любом этапе неминуемо приводят к появлению рисков и снижают уровень защищенности системы в целом. Так, строительство системы видеонаблюдения без проектной документации не позволяет составить общую ”модель угроз”, увидеть в системе ”узкие” места и ликвидировать их еще на уровне эскизного проектирования. На этапе введения системы видеонаблюдения в эксплуатацию компании-инсталляторы часто формируют ”вопиющую” уязвимость – оставляют пароли вендоров “по умолчанию”, предоставляя возможность потенциальным злоумышленникам получить доступ к системам [5]. По мнению авторов, уязвимостям с паролями ”по умолчанию” на территории Украины подвержены около 1 500 000 видеокамер.

Независимо от выбранной технологии, в структуре любой системы видеонаблюдения присутствуют 3 участка: оконечное оборудование, коммуникационная среда, центральная часть. В некоторых случаях участки совмещаются, например, если видеокамера пишет сама на себя (применение SD-карты) совмещены сторона оконечного оборудования и центральная часть. На каждом из участков могут присутствовать свои угрозы. Так, на оконечное оборудование (видеокамеры) могут быть направлены такие противоправные действия нарушителя, как вандализм, блокирование объектива, засветка, изменение углов обзора видеокамеры (поворот, расфокусировка) и т.д.

При построении любой системы видеонаблюдения используется коммуникационная среда – проводная, беспроводная или комбинированные решения. Основные проводные решения основываются на применении коаксиального кабеля, кабеля типа ”витая пара”, волоконно-оптического кабеля. В беспроводных решениях широко применяются такие технологии, как Wi-Fi, Wi-Max, GSM, CDMA, реже – Bluetooth. Классические угрозы коммуникационной среды – повреждения кабельной инфраструктуры, перехват сигналов с видеокамер, подмена контента, блокировка (глушение) канала связи и т.д. Например, при использовании беспроводного решения на основе Wi-Fi система видеонаблюдения может быть подвержена тем же атакам, которые часто встречаются в классических информационных сетях – Wardriving, DDoS, MITM, глушение, модификация, создание ложной точки доступа. Системы видеонаблюдения в своем “историческом” понимании (Closed - circuit television, системы видеонаблюдения замкнутого типа) меньше подвержены сетевым атакам по причине своей изолированности. Но желание пользователей получить удаленный доступ к системам CCTV приводит к использованию статического (иногда - динамического) IP-адреса, включению CCTV в глобальную информационную сеть, а значит – перехода от изолированности к открытости со всеми ее рисками.

Как уже отмечалось, многие факторы, влияющие на уровень защищенности системы видеонаблюдения, закладываются на этапах проектирования системы, выборе принципа построения, целей, задач и компонентного состава. Так, требования к количеству видеокамер и качеству изображения напрямую влияют на способы записи видеопотоков и коммуникационную составляющую, как следствие – на ее центральную часть. Основные способы записи видеопотоков с указанием рисков представлены в табл.1.

Таблица 1

Основные способы записи видеопотоков с указанием рисков

№	Способ записи видеопотока	Основные риски
1	SD-карта	Кража архива вместе с видеокамерой, Короткий цикл записи из-за небольшого объема памяти
2	Видеорегистратор	Уязвимости прошивки
3	Видеозапись на базе ПК	Зависимость от сторонней программно-аппаратной части
4	Видеосервер	Качество оборудования и условия гарантийной (послегарантийной) поддержки Наличие ремонтно-восстановительного фонда
5	VSaaS	Полная зависимость от поставщика услуги VSaaS Вопросы конфиденциальности информации

Выбор “оптимального” вендора также напрямую влияет на уровень защищенности системы видеонаблюдения. Так, отсутствие должного качества элементов системы видеонаблюдения приводит к аварийным ситуациям – отсутствию видеосигнала, выгоранию электроники, перегреву, зависанию, проблемам с прошивкой и т.д.

Детальное исследование уязвимостей систем видеонаблюдения, основных рисков и угроз подразумевает составление гипотетических “моделей угроз” по базовым критериям с применением инструментов анализа рисков [6]. Визуализация угроз их подробное описание позволит минимизировать потенциальные риски на всем ”жизненном” цикле системы видеонаблюдения.

Выводы. Представленный анализ защищенности систем видеонаблюдения показывает наличие угроз и уязвимостей. В перспективе будут проведены экспериментально-статистические исследования, направленные на вероятностную оценку возникновения рисков, а также, учитывая “модель угроз”, подготовку алгоритмов защитных мероприятий для систем видеонаблюдения. Защитные мероприятия должны рассматриваться с позиции полного ”жизненного” цикла, с учетом основных критериев оценки уровня защищенности, а также позиции комплексности, взаимодополняемости и носить цикличный и динамический характер.

Литература

1 Сучасні телекомунікації: мережі, технології, безпека, економіка, регулювання, Довгий С.О., Воробієнко П.П., Гуляєв К.Д., за загальною редакцією члена-кореспондента НАН України Довгого С.О., Київ “Азимут-Україна”, 2013. – 607 с.

2 Гіль О.А. Дослідження методів організації та застосування систем відео спостереження / О.А.Гіль, С.В. Стайкуца // Матеріали 68-ї науково-технічної конференції профес.-викл. складу, науковців, аспірантів та студентів ”, ОНАЗ ім. О.С.Попова. – Одеса, 2013. – С. 34-35.

3 Фесюков О.С. Дослідження методів застосування систем відеоспостереження на прикладі сільськогосподарської галузі / О.С.Фесюков, В.Й.Кільдішев // Матеріали 69-ї науково-технічної конференції профес.-викл. складу, науковців, аспірантів та студентів ”, ОНАЗ ім. О.С.Попова. – Одеса, 2014.

4 А. Лыткин. IP - видеонаблюдение. Наглядное пособие // Издательство “Авторская книга”, 2011. – 200 с.

5 Шпионим через приватные камеры видеонаблюдения [электронный ресурс] http://pikabu.ru/story/shpionim_cherez_quotprivatnyiequot_kameryi_videonablyudeniya_3294899.

6 Стайкуца С.В. Аналіз загроз безпеки телекомунікаційних компаній з розробкою методології захисту / С.В. Стайкуца, О.С. Семенов // Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS’2016)”, НАУ, МТУ ”Миколаївська політехніка”. – Миколаїв – Коблево, 2016. – С. 48-50.

УДК 004.057.5

Теліженко К.О.,
Теліженко О.Б.
LLC Verum Visum, м.Київ
tel63@ukr.net

ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ У ВІРТУАЛЬНИХ ПРОСТОРАХ

Анотація. *Розглядаються вразливості у структурі побудови та функціонування соціальних просторів у віртуальній реальності. Пропонується методика захисту інформації, що циркулює у віртуальних просторах.*

Одним з перспективних напрямів розробки сучасних програмних засобів є розвиток соціальних просторів у віртуальній реальності. Однак, методика захисту персональних даних, що циркулює у віртуальному просторі, а також ідентифікації віртуальних аватарів розроблена частково та лише для конкретних реалізацій. Ефективним засобом захисту інформації у віртуальних просторах може стати механізм встановлення електронного цифрового підпису (ЕЦП) при передачі даних між сервером та клієнтом. Подібна методика практикується при формуванні ЕЦП для захисту записів камер зовнішнього спостереження, наприклад, при фіксації автомобільних номерів порушників правил дорожнього руху.

Розробка програмного забезпечення (ПЗ) для захисту інформації, що циркулює у віртуальних просторах, передбачає реалізацію мережного протоколу обміну даних з використанням ЕЦП та шифрування. ПЗ також передбачає зв’язок з центром управління ключами (ЦУК). ЦУК відповідно має взаємозв’язок з центром сертифікації ключів, що надає можливість використовувати легітимні (сертифіковані) на Україні алгоритми шифрування. Створення сертифікаційних центрів з технічної точки зору не є складною. Однак, можуть виникнути юридичні проблеми у разі виникнення суперечок про відмову від авторства або підробки підпису. Тобто, ці центри повинні нести юридичну відповідальність за достовірність сертифікатів, що видаються.

У якості стандарту цифрового підпису може розглядатися, наприклад, національний стандарт на еліптичних кривих ДСТУ 4145-2002. Протоколи встановлення та перевірки цифрового підпису трохи ускладнюють механізми передачі зображень, але при сучасних технологіях втрата часу у режимі on-line не буде помітною.

Висновки. Механізм використання ЕЦП дозволить зберегти цілісність зображень, здійснити автентифікацію джерела зображень та забезпечити неможливість відмови від факту підпису конкретного зображення. При цьому ЕЦП реалізується таким чином, що він легко перевіряється та здійснити перевірки підпису може мати можливість кожен користувач без отримання доступу до таємного ключа.

УДК 621.391

Тихонов В.И.,
victor.tykhonov@onat.edu.ua,
Тахер А.,
abidalla_2004@yahoo.com,
Тихонова Е.В.,
elena.tykhonova@onat.edu.ua
ОНАЗ ім. О.С. Попова.

ПРИМЕНЕНИЕ ПРИНЦИПОВ МНОГОУРОВНЕВОЙ ГРАММАТИКИ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация. *Предложен способ защищенного кодирования персональных данных на основе многоуровневой формальной грамматики. Первый уровень формальной грамматики описывает взаимодействие смежных узлов сети, а второй - взаимодействие произвольных узлов сети по открытым протоколам. Третий уровень формальной грамматики соответствует защищенным прикладным процессам и протоколам, параметры и таблицы кодирования которых могут динамически изменяться в процессе обмена данными.*

При проектировании сети следующего поколения проблемой является обеспечение транспортной системой качества обслуживания многопродуктового потока данных. Традиционные модели интегрированного и дифференцированного обслуживания (IntServ/DiffServ), применение протоколов RSVP и NSIS не обеспечивают достаточный уровень масштабируемости для широкого практического применения [1]. Современная концепция программно-конфигурируемой сети (SDN) показывает эффективность SDN архитектуры в некоторых областях [2], хотя такая сеть достаточно сложна для управления и приводит к значительным задержкам обратной связи. В последние годы в 4G сетях мобильной связи активно внедряется услуга передачи голоса по сети LTE (VoLTE). Однако, эта технология не полностью эквивалентна передаче голоса по IP (VoIP), так как надежные голосовые соединения устанавливаются только в пределах конкретной автономной системы. Таким образом, интеграция различного рода телекоммуникационных услуг на базе сети с пакетной коммутацией остается нерешенной проблемой. Кроме того, на прикладном уровне актуальным вопросом является защита персональных данных индивидуальных и корпоративных пользователей сети; при этом система защиты должна быть хорошо масштабируемой от простых и быстрых алгоритмов до высокой степени защиты. Удовлетворение такого многообразия требований приводит к сложным протоколам многоуровневой инкапсуляции данных, чрезмерной избыточности заголовков и снижению эффективности использования сетевого оборудования и каналов связи. *Целью данного исследования является разработка единого общего подхода к представлению многопродуктового потока в транспортной сети на основе принципов многоуровневой формальной грамматики, в которой каждый уровень может обладать своими свойствами защищенности данных.*

Представление цифрового потока в виде последовательности символов формальной грамматики

Представим последовательный цифровой поток F в телекоммуникационном канале в виде последовательности символов формальной грамматики первого уровня G^1, имеющей фиксированный алфавит $A^1 := S^1 \bigcup L^1$, где S^1 – фиксированное множество синтаксических знаков первого уровня, L^1 - фиксированное множество букв первого уровня. Элементы $a^1 \in A^1$ образуют неограниченное множество слов W^1 первого уровня грамматики; выделим два открытых подмножества S^2 и T^2 внутри множества W^1: $S^2 \bigcup T^2 \subset W^1$, где элементы $s^2 \in S^2$ - это синтаксические знаки, а элементы $t^2 \in T^2$ - это ключевые слова (теги) второго

уровня грамматики. Оставшуюся часть множества W^1 ($L^2 := W^1 \setminus S^2 \bigcup T^2$) назовем неограниченным открытым множеством $d^2 \in D^2$ букв второго уровня грамматики (или информационных слов, т.е. данных). Таким образом, три множества $G^2 := \langle S^2, T^2, D^2 \rangle$ представляют собой базис грамматики G^2 второго уровня. Синтаксис SX грамматики G^2 определяет набор правил $r^2 \in R^2$ построения корректных предложений $sn \in SN$. Каждое предложение sn грамматики G^2 обязательно включает в себя команду $c \in C$ и может содержать сегмент с информационными данными $d^2 \in D^2$. Различные комбинации элементов $s^2 \in S^2$, $t^2 \in T^2$ и $d^2 \in D^2$ образуют неограниченное открытое множество предложений: $\{SN\} := \{s^2, t^2, d^2\}$.

Команды из множества $c \in C$ интерпретируются (т.е. выполняются) на приемной стороне канала связи, рис. 1. В конечном итоге, два фиксированных множества синтаксических знаков S^1 и S^2, а также фиксированное множество правил R^1 первого уровня и первоначальное открытое множество R^2 правил второго уровня определяют открытую грамматику G^2 второго порядка. В процессе эволюции грамматики G^2 все большее количество элементов множества D^2 будет резервироваться в качестве ключевых слов (т.е. будет исключаться из множества D^2 и включаться во множество тегов T^2). Текстовый файл, интерпретируемый грамматикой G^2, состоит из множества предложений грамматики G^2; данный файл маркируется предложениями начала и конца файла (“Start-file” и “End-file”).

На рисунке 1 показан принцип синхронной передачи потока символов между соседними узлами телекоммуникационной сети с помощью конвейерных транспортных модулей (СТМ), циркулирующих циклически с фиксированной частотой в обоих направлениях дуплексного канала. Полу-бесконечный поток символов имеет начальную точку (сброс) и не имеет фиксированной конечной точки (т.е. он может длиться до бесконечности). Модули СТМ имеют фиксированный максимальный размер поля полезной нагрузки в зависимости от применяемой технологии канального уровня OSI (например, 1500 байт для кадра Ethernet). Частота циркуляции СТМ зависит от пропускной способности канала. На отправляющей стороне симплексного канала последовательность символов разбивается на блоки в соответствии с размером полезной нагрузки СТМ. В свою очередь, принимающая сторона восстанавливает последовательность символов из потока СТМ, объединяя поля полезной нагрузки СТМ. Таким образом, принимающая сторона (дискретный автомат) оперирует потоком символов, как будто он виртуально подключен к порту узла-отправителя.

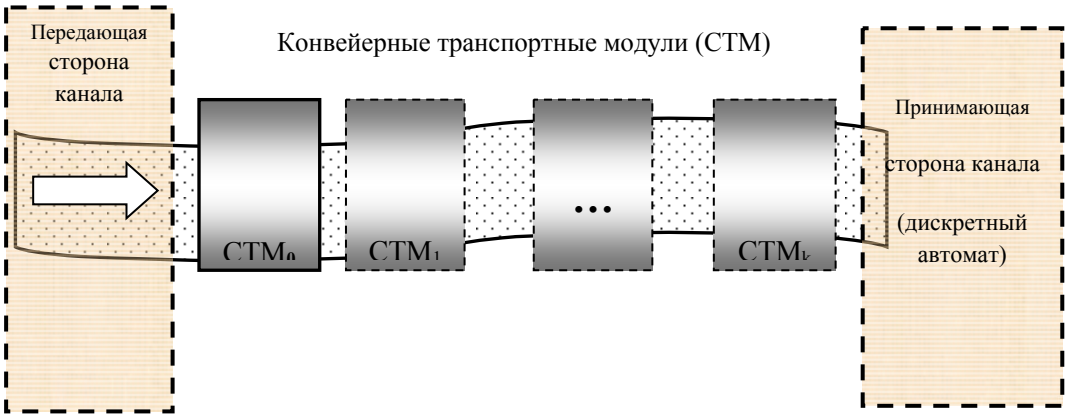

Рисунок 1 – Синхронная передача потока символов в коммуникационном канале

Аналогичным образом, можно построить практически неограниченное множество различных грамматик вышестоящих уровней – третьего, четвертого и т.д. Согласно предложенной в Одесской национальной академии связи трехуровневой модели интегрированной технологии телекоммуникаций UA-ITT, первые два уровня взаимодействия открытых систем могут быть построены как соответствующие грамматики двух нижних уровней [3]. При этом протоколы передачи данных между объектами сетевой инфраструктуры могут быть открытыми для обеспечения возможности их унификации и стандартизации. Третий (прикладной) уровень обеспечивает кодирование и декодирование персональных данных конечных пользователей. Каждая группа пользователей может строить собственные грамматики, неизвестные и закрытые для несанкционированного доступа. Сложность грамматики определяет степень ее защищенности от взлома. Эту степень можно плавно регулировать длиной таблиц кодировки ключевых слов и синтаксических знаков грамматики третьего уровня, а также динамическим переключением подмножеств грамматики между различными сеансами связи или даже в одном сеансе.

Выводы

Интеграция телекоммуникационных услуг и обеспечение защищенности персональных данных, передаваемых по сети, продолжает оставаться актуальной проблемой в отношении сетевых технологий следующего поколения. Данная работа обосновывает унифицированный подход к представлению цифрового потока в телекоммуникационной сети на основе многоуровневой формальной грамматики. Это расширяет возможности для обеспечения совместимости различных открытых систем, позволяя создавать большое количество прикладных протоколов на основе первоначального стандартного мета-протокола.

Литература

1. Analysis of existing Quality of Service signaling protocols (RFC 4094). – 2005. – Режим доступа: https://tools.ietf.org/html/rfc4094.

2. Packet and Circuit Network Convergence with OpenFlow / Das, S., Parulkar,G., McKeown, N. and others // proceedings of Optical Fiber Communication (OFC), collocated National Fiber Optic Engineers Conference (21-25 March, 2010). – San Diego, 2010. – P. 1-3. – Режим доступа: http://yuba.stanford.edu/~nickm/papers/Openflow-OFC10_invited.pdf.

3. Integrated telecommunication technology for the next generation networks / P.P.Vorobiyenko, V.I.Tikhonov // Proceedings of the ITU Kaleidoscope Academic Conference (22-24 April 2013). – Kyoto, Japan, 2013. – P. 187-193.

УДК 621.391.31 + 004.056.53

Шестак Я.В., e-mail: lucenko.y@ukr.net
Огбу Д.О., e-mail: jamesybone@yahoo.com
КНУ имени Тараса Шевченко, Киев
Научный руководитель – д.т.н., проф. Оксиюк А.Г.,
зав. каф. кибербезопасности и защиты информации,
КНУ имени Тараса Шевченко, Киев

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ОЦЕНИВАНИЯ ЗАЩИЩЕННОСТИ СЛОЖНЫХ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Аннотация. *В рамках сложившейся ситуации на рынке ИТ-технологий, относительно роста телекоммуникационных технологий, их развития, параметризации, инновационности, неуклонно возрастает потребность в обеспечении требуемого уровня*

безопасности и анализе защищенности, с целью предотвращения несанкционированного доступа к информации, ее блокирования, а также нарушения функционирования информационно – телекоммуникационных систем. Работа посвящена актуальной задаче разработки алгоритма определения вероятности защищенности информационно–телекоммуникационной системы от существующих угроз современными средствами защиты.

Нормативной основополагающей защищенности сложных распределенных информационно-телекоммуникационных систем, является Закон Украины «О защите информации в информационно-телекоммуникационных системах» от 05.07.1994 № 80/94-ВР. Который, регулирует отношения в сфере защиты информации в информационных, телекоммуникационных и информационно-телекоммуникационных системах, приводит взаимосвязанную совокупность организационных и инженерно-технических мероприятий, средств и методов защиты информации [1]. В свою очередь, Техническая лаборатория Информации (ITL) в Национальном институте стандартов и технологий (NIST) предоставляет техническую документацию и стандарты по защите информации относительно сложных распределенных информационно-телекоммуникационных систем, которая, на сегодня, является фундаментом в обеспечении защиты последних.

Хотя вопрос защищенности сложных систем, является юридически урегулированным, практические вопросы возникают, как следствие оценивания защищенности.

На сегодняшний день, в сложных распределенных информационно-телекоммуникационных системах выделяют пять основных способов воздействия на информацию.

Основным является нарушение конфиденциальности информации или несанкционированный доступ к ней.

Нелегальное приобретение платных информационных услуг, либо же незаконное использование вычислительных мощностей.

Длительность передачи информации, здесь важным аспектом выступает актуальное время передачи информации, которое во многих случаях играет немаловажную роль в сохранности передачи и актуальности результата.

Изменение маршрутов передачи сообщения, с целью их копирования либо подмену содержимого.

Искажение начальной информации либо же нарушение целостности информации. Этот аспект возникает при полной или частичной потере информации (потеря вызывается вирусами, некомпетентной передачей, слиянием двух видов информации (поврежденной и достоверной) и т.д.).

Оценка уровня защищенности производится посредством определения совокупности вероятных угроз с помощью конкретного средства защиты, учитывая отдельные функции всех программных и программно-аппаратных средств защиты, а также уровня опасности угрозы для сложной распределенной информационно-телекоммуникационной системы.

С математической точки зрения это выглядит так [2]:

$$Q = \sum \{c_k + i_k + a_k + S_k\}/_4 \cdot p_k \cdot z_k \qquad (1)$$

где c_k – конфиденциальность

i_k – целостность информации;

a_k – доступность информации;

S_k – наблюдаемость информации;

p_k – весовой коэффициент угрозы;

z_k – коэффициент успешного выполнения защиты.

Уровень защиты информации определяется защищенностью каждого отдельного ресурса из совокупности, предназначенной для защиты системы.

На сегодняшний день, рынок информационных технологий, представляет множество программных решений, направленных на оценивание уровня защищенности сложных систем. Фундаментальной основой эффективного определения уровня защищенности выступает системный и систематический подходы, направленные на решение комплекса задач, основанных на модульном разбиении системы.

Информационные технологии оценивания направлены на выявление наиболее уязвимых мест сложных распределенных информационно-телекоммуникационных систем, безопасность, которых может быть нарушена в первую очередь. Либо же недостатки, которых, нарушитель может использовать для нанесения вреда безопасности системы в целом.

Начальным этапом анализа является структуризация системы, которая производится по нескольким направлениям (выделение информационных объектов, пространственная и функциональная структуризация). Последняя говорит о реструктуризации сложной системы на функциональные подсистемы.

Пространственная структуризация основана на выявлении частей сложной системы, которые находятся на расстоянии и значительно отличаются по требованиям к уровню защищенности.

После структуризации системы производится оценка уязвимости, целостности, наблюдаемости, конфиденциальности, защищенности каждого объекта по отдельности с детальным обоснованием каждого критерия.

Следующим этапом, выступает этап построения модели событий рисков. Здесь, основным фактором, является выявление уровня опасности каждой отдельной угрозы, которая определена на начальном этапе. Результатом данного анализа является детальное описание событий риска, их последствий, уровня угроз, возможности реализации (возникновения). Так же важным критерием является степень воздействия на систему и вероятные потери информации.

После сравниваются статистические данные в количественном выражении с имеющимися полученными ранее (если таковы есть), это производится с целью определения оценки уровня вероятности события риска, и для того, чтобы отметить динамику частоты возникновения события риска по выявленному направлению.

На основании этого, используя математический алгоритм вычисления рассчитывается уровень защищенности сложных распределенных информационно-телекоммуникационных систем, приводится ожидаемый ущерб от каждого выявленного события рисков, как математическое ожидание величины ущерба.

Описанный механизм позволяет оценить защищенность сложных систем и на основании этого пользователь может определить актуальные меры по защите сложных распределенных информационно-телекоммуникационных систем, что на сегодня является приоритетным направлением в сфере ИТ-технологий.

Литература

1. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України // Відомості Верховної Ради України. – 1994. – № 31. – Ст.286.

2. Глыбовский П.А., Глухов А.П., Пономарев Ю.А., Шиленков М.В. Подход к оцениванию и прогнозированию уровня защищенности информационных и телекоммуникационных систем // Труды СПИИРАН. –2015. – Вып. 42. – С. 180-195.

УДК 004.056.5

Юдін О.Ю.
ДержНДІ Спецзв'язку
alex@ukrdeftech.com.ua

СВІТОВИЙ ДОСВІД ЩОДО ВИЗНАЧЕННЯ ГАЛУЗЕЙ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. *Проведений аналіз нормативно-правових актів провідних держав світу щодо віднесення галузей до критичної інфраструктури. Результати аналізу викладені у вигляді зведених даних щодо секторів критичної інфраструктури. Також, з урахуванням законодавства України та Європейського союзу, запропонований перелік секторів та підсекторів критичної інфраструктури України.*

Актуальність дослідження

Актуальними проблемами впровадження систем захисту критичної інфраструктури при забезпеченні національної безпеки України є те, що:

- захист об'єктів критичної інфраструктури в Україні відноситься до компетенції низки відомств в межах їх завдань і має фрагментарний характер, що відбивається в паралельному функціонуванні систем, призначених для захисту об'єктів та населення від окремих типів загроз (техногенного, природного або соціально-політичного характеру) [1];
- об'єкти критичної інфраструктури України категоруються на основі галузевих (відомчих) підходів, виходячи з міркувань та критеріїв забезпечення безпеки за окремими складовими національної безпеки (економічної, державної, політичної, енергетичної, екологічної, гуманітарної тощо) [2];
- в національному законодавстві здобули визначення такі об'єкти, як: підприємства, які мають стратегічне значення для економіки та безпеки держави; важливі державні об'єкти; об'єкти, які підлягають охороні і обороні в умовах надзвичайних ситуацій і в особливий період; особливо важливі об'єкти електроенергетики, нафтогазової галузі; потенційно небезпечні та об'єкти підвищеної небезпеки; нерухомі пам'ятки культурної спадщини [3-7].

Попри істотні досягнення в становленні системи захисту національної безпеки України, існує ціла низка труднощів і проблем, пов'язаних із захистом критичної інфраструктури, що потребують розв'язання, а саме:

- невідповідність національної нормативно-правової бази, положенням міжнародних документів, зокрема в тій частині, що регулює питання захисту об'єктів критичної інфраструктури, на фоні декларування курсу на євроінтеграцію;
- відсутність нормативних документів, вимог, методологій щодо оцінки загроз об'єктам, що є критичними для життєдіяльності держави, загальної методології оцінки ризиків для об'єктів критичної інфраструктури.

Приведене вище дає підстави для виконання дослідження стосовно визначення галузей критичної інфраструктури.

Терміни, які використовуються в доповіді, мають наступні значення [8]:

- критична інфраструктура - системи, виведення з ладу або руйнування яких може призвести до ефекту послаблення економічної безпеки в промисловості, безпеки населення або держави;
- об'єкт критичної інфраструктури - елемент критичної інфраструктури вплив на який може мати наслідки, що призведуть до послаблення національної безпеки, включаючи безпеку людини і громадянина, суспільства та держави.

Предмет дослідження

Предметом дослідження та аналізу стали нормативні документи США, Європейського союзу, окремих країн Європейського союзу (Естонської Республіки, Австрійської

Республіки, Чеської Республіки, Французької Республіки, Нідерландів, Федеративної Республіки Німеччини, Польської Республіки, Республіки Словенія, Республіки Словаччина, Королівства Іспанія, Королівства Швеція, Швейцарської Конфедерації, Сполученого королівства Великої Британії та Північної Ірландії), Австралійського союзу, Канади, Японії, Турецької Республіки та Індії. Також були проаналізовані національні нормативні документи [3-7].

Результати дослідження

За результатами дослідження підготовлені зведені дані стосовно кожної розглянутої країни щодо секторів критичної інфраструктури та зроблено співставлення секторів критичної інфраструктури до галузей критичної інфраструктури, які входять до їх складу.

	Енергетика	Інформаційні, телекомунікаційні технології	Водопостачання	Продовольство	Здоров'я	Фінанси	Суспільний та правовий порядок та безпека	Цивільна адміністрація	Транспорт	Хімічна та ядерна промисловість	Космос та дослідження	Інше
AU	+	+	+	+	+	+	+	+	+		+	
BE	+	+				+			+			
CZ	+	+	+	+		+		+	+			Аварійні служби
DK	+	+		+	+				+			
EE	+	+	+	+	+	+	+	+	+			
FI	+	+	+	+	+	+	+		+			
FR	+	+	+	+	+	+	+	+	+		+	Промисловість
DE	+	+	+	+	+	+	+		+			Засоби масової інформації та культура
LV	+								+			
HU	+	+	+	+	+	+	+		+			Промисловість
IT	+								+			
MT	+	+			+	+		+	+			
NL	+	+	+	+		+	+	+	+	+		
PL	+	+	+	+	+	+		+	+	+		Аварійні служби
SK	+	+	+		+				+			Промисловість / Пошта
ES	+	+	+	+	+	+		+	+	+	+	
UK	+	+	+	+	+	+		+	+			Аварійні служби
CH	+	+	+	+	+	+		+	+			Промисловість
SI	+	+	+	+	+	+			+			Захист навколишнього середовища
SE	+	+	+	+	+	+	+	+	+			Промисловість, торгівля, соц. захист
EU	+	+	+	+	+	+	+	+	+	+	+	
USA	+	+	+	+	+	+			+	+		Промисловість, Засоби масової інформації та культура

AU	+	+	+	+	+	+			+			Інформаційна безпека, Стійкість до відмов
CA	+	+	+	+	+	+		+	+			Промисловість, безпека
JP	+	+	+		+	+		+	+			
TR	+	+	+						+			Промисловість
UA	+	+	+	+	+	+			+	+	+	Промисловість, стандартизація, метрологія та сертифікація, гідрометеорологічна діяльність

Література

1 Бірюков Д.С. “Про доцільність та особливості визначення критичної інфраструктури в Україні”. Аналітична записка // [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/1026.

2 Анализ угроз и уязвимостей индустриальных автоматизированных систем управления / Гончар С., Леоненко Г., Юдин А. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2013. Випуск 2 (26).

3 Україна. Закони. “Про об’єкти підвищеної небезпеки” : офіц. текст : [прийнятий Верховною Радою 18 січня 2001 р.]. - К.: Відомості Верховної Ради України, 2001, № 15, ст.73.

4 Постанова Кабінету Міністрів України № 83 від 04.03.2015 “Про затвердження переліку об'єктів державної власності, що мають стратегічне значення для економіки і безпеки держави”.

5 Постанова Кабінету Міністрів України № 339 від 15.05.2013 “Про затвердження переліку особливо небезпечних суб’єктів підприємницької діяльності - боржників, припинення діяльності яких потребує здійснення спеціальних заходів із запобігання заподіянню можливої шкоди життю та здоров’ю громадян, майну, спорудам, навколишньому природному середовищу”.

6 Постанова Кабінету Міністрів України № 1170 від 28.07.2003 “Про затвердження переліку особливо важливих об'єктів електроенергетики, які підлягають охороні відомчою воєнізованою охороною у взаємодії із спеціалізованими підрозділами інших центральних органів виконавчої влади”.

7 Розпорядження Кабінету Міністрів України № 578-р від 27.05.2009 “Про затвердження переліку особливо важливих об'єктів нафтогазової галузі”.

8 XVII Міжнародна науково-практична конференція “Безпека інформації у інформаційно-телекомунікаційних системах”. Доповідь О.Ю.Юдіна “Зміст понять “кібернетична безпека” та “об’єкт критичної інфраструктури” з огляду на термінологію іноземних нормативних документів”, стор. 100. Матеріали науково-практичної конференції; м. Київ, 26-28 травня 2015р. / Держспецзв’язку, Інститут комп’ютерних інформаційних технологій Національного авіаційного університету / Редкол.: О.В. Корнейко (голова) та ін.. – К.: Держспецзв’язку, 2015. – 142с.

ЗМІСТ