Горбенко Юрій Іванович, канд. техн. наук, АТ «Інститут інформаційних технологій», перший заступник головного конструктора, Україна.

Yuriy Horbenko, candidate. technical of Sciences, JSC "Institute of Information Technologies", first deputy chief designer, Ukraine.
E-mail: gorbenkou@iit.kharkov.ua.
Orcid ID: 0000-0003-0073-9107.

Кожухівська Ольга Андріївна, д-р техн. наук, Державний університет інформаційно-комунікаційних технологій, доцент кафедри інформаційної та кібернетичної безпеки; Київ, Україна.

Olga Kozhuhivska, Dr. Tech. of Sciences, State University of Information and Communication of technologies, associate professor of the department of information and cybernetic security, Kyiv, Ukraine.
E-mail: rsg.o.i.v@gmail.com.
Orcid ID: 0009-0008-2176-9149.

Борсуковський Юрій Володимирович, канд. техн. наук, Державний університет інформаційно-комунікаційних технологій, доцент кафедри інформаційної та кібернетичної безпеки; Київ; Україна.

Yuryi Borsukovskiy, Candidate of Sciences. technical Sciences, State University of Information and Communication Technologies, associate professor of the department of information and cybernetic security, Kyiv, Ukraine.
E-mail: gmbyurii@gmail.com.
Orcid ID: 0000-0003-1973-2386.

DOI: 10.18372/2410-7840.26.18836
УДК 004.056.53

ОБҐРУНТУВАННЯ ІМОВІРНОСТІ УНЕМОЖЛИВЛЕННЯ ВИЗНАЧЕННЯ НАЯВНОСТІ СИГНАЛІВ В СЕРЕДОВИЩАХ ЇХ ПОШИРЕННЯ

Сергій Іванченко, Василь Некоз

Проведено обґрунтування унеможливлення визначення наявності сигналів в середовищах їх поширення В якості моделі каналу розповсюдження інформації було використано дискретно-неперервний канал. Інформація вироблялась від дискретного джерела, де кожному з інформаційних символів ставились у відповідність неперервні реалізації, які поширювались неперервним середовищем із завадою. Прийом сигналів здійснюється засобами, які можуть бути ефективними. З точки зору убезпечення інформації від неконтрольованого порширення та забезпечення її захищеності в середовищі поширення, як правило, використовують два фактори: згасання амплітуди хвилі (сигналу) при її поширенні у фізичному середовищі; спотворююча дія завади, що має місце в середовищі поширення сигналу та руйнує його форму. Однак, використання цих факторів, що могло б забезпечити повну, майже абсолютну безпеку інформації, є питанням складним, а то і неможливим. Адже сигнали, що поширюються у просторі, відповідно до законів фізики здійснюють це у вигляді електромагнітних чи інших хвиль, або потоків елементарних (заряджених) частинок. Вони можуть поширюватись на досить великі відстані, а теоретично майже до нескінченності, ефективність перехоплення яких повністю визначається ефективністю засобів прийому. Для вирішення зазначеного питання, що має широке застосування у менеджменті інформаційної безпеки, є ризик орієнтований підхід, який не вимагає абсолютного убезпечення, а допускає можливість не виконання вимоги з безпеки з деяким певним допустимим ризиком [2]. Цей ризик, як правило, визначається допустимими збитками, які може понести власник активів, і при цьому результативність виробничих процесів не порушиться.

***Ключові слова**: інформаційна безпека, кібербезпека, інформаційно-комунікаційні системи, системи захисту інформації, інформаційний сигнал, дискретний канал.*

ВСТУП

Забезпечення ризику в каналах витоку вимагає вирішення актуального завдання, а саме обґрунтування сукупності взаємозв'язаних показників, які мають надати можливість трансформування захищеності від ризику безпеки до енергетичних умов в середовищі поширення.

Паралельно при цьому одним із основних питань є обґрунтування зв'язку імовірності неможливості впевненого визначення ознак інформаційного сигналу та граничного відношення сигнал/завада, яке також вимагає окремого вирішення.

ОСНОВНА ЧАСТИНА

Обґрунтування сукупності показників для забезпечення безпеки інформації від неконтрольованого поширення на основі унеможливлення визначення ознак інформаційних сигналів

Зазначені показники повинні забезпечити виконання вимоги з захищеності інформації від неконтрольованого поширення в усіх можливих середовищах, та мати поміж собою зв'язок, який би дозволяв стверджувати про еквівалентність цих показників з допустимим ризиком безпеки – ступенем невиконання вимог. Нехай задано якісну вимогу, якою є неможливість визначення оз-

нак небезпечного сигналу в технічному каналі витоку. Задано допустимий ризик інформаційної безпеки [2].

Ризик безпеки кількісно виражає потенційну небезпеку, що приводить до збитків, та може бути представленим як добуток імовірності реалізації загрози p_r і ціни *Price* наслідків від неї:

$$R = p_r \times Price . \quad (1)$$

По суті ризик це загальний показник якості, який кількісно характеризує ступінь або рівень захисту. Якщо задати його граничне допустиме значення $R_{\text{гр.доп.}}$, то можливе впровадження ризик орієнтованого підходу із забезпечення захисту інформації в тому числі і від витоку технічними каналами.

Слід зазначити, що впровадження ризик орієнтованих підходів є досить зручним та перспективним. Переваги цього підходу полягають в тому, що він дозволяє автоматизоване управління безпекою. А автоматизація управління – це забезпечення повного циклу управління інформаційною безпекою (цикл Шухарта-Демінга: планування, виконання, перевірка якості, вплив на покращення якості). Це підвищення швидкодії реагування на зміни в загрозах. Це підвищення ефективності керування в цілому.

Очевидно, що ціну можливих збитків *Price* і межі ризиків $R_{\text{гр.доп}}$, має встановлювати власник інформації, інформаційних ресурсів, як суб'єкт, що зацікавлений у потрібному ступені захисту та ефективному управлінні інформаційною безпекою власних ресурсів [2]. Однак не для всякої інформації існує її ціна.

По-перше, інформація не є об'єктивною, а тому одна і та ж інформація для різних суб'єктів може мати різну важливість та, умовно кажучи, різну ціну, яка водночас може бути і нульовою, і досить високою.

По-друге, інформація може бути пов'язана із глобальними, міжнародними процесами, щодо яких не може існувати єдиної цінової шкали. Так, наприклад, чи можна відповісти на питання: скільки коштує планета Земля, або як порахувати ціну озера чи гори тощо.

По-третє, ярким прикладом щодо неможливості надати ціни інформації є секретна інформація (державна таємниця). Не зважаючи на те, що її розголошення може нанести великі збитки, які можна порахувати, все таки між кількістю секретної інформації та можливими збитками у випадку її витоку немає жорсткої залежності, а тому *Price* секретної інформації є досить складним питанням та на даний час не є нормативно визначеним.

Конфіденційна інформація немає ціни тому, що вона безцінна. Безпека конфіденційної інформації є однією із запорук успішного функціонування різноманітних установ тощо. Тому, одним із показників, що може бути застосованим в якості ризику безпеки, є не можливі кількісні збитки, а, як вже вище зазначалося, імовірність ризику p_r, тобто імовірність того, що може бути реалізована загроза. Гранична допустима імовірність ризику $p_{r\,\text{гр.доп.}}$ є технологічним показником, який має забезпечувати система захисту та може бути знайденою із формули (1):

$$p_{r\,\text{гр.доп.}} = \frac{R_{\text{гр.доп.}}}{Price} . \quad (2)$$

Так, система захисту буде ефективною в тому разі, якщо її показники надійно забезпечуватимуть $p_{r\,\text{гр.доп.}}$ і цим самим вказана система доведено гарантуватиме інформаційну безпеку із заданим ризиком.

Нехай задано межу імовірності ризику $p_{r\ \text{гр доп.}}$ – умову безпеки конфіденційної інформації, яка має бути виконаною посередництвом технологічних показників у своїх розрахункових межах. Цій імовірності можна поставити у відповідність імовірність визначення ознак небезпечного сигналу, оскільки ця подія є протилежною до захищеності інформації від неконтрольованого поширення. Іншими словами імовірність неможливості визначення цих ознак матиме вид:

$$p_{\text{нвос}} = 1 - p_{r\,\text{гр.доп.}} . \quad (3)$$

Імовірність $p_{\text{нвос}}$ є мірою того, що вирішальна схема, як це було обґрунтовано в попередньому розділі прийматиме рішення, що сигнал відсутній в той час, коли в ТКВ він все таки має місце. Формально це виглядає наступним чином:

$$p_{\text{нвос}} = p\left\{ Z_{\Delta\,\text{пор.}}(u) < -\frac{P_{\Delta\,\text{пор.}}}{2} \right\} , \quad (4)$$

де $P_{\Delta\,\text{пор.}}$ – потужність різницевого сигналу відносно порогового сигналу:

$$P_{\Delta\,\text{пор.}} = \frac{1}{T}\int_0^T c^2_{\Delta\,\text{пор.}}(t)dt , \quad (5)$$

де $Z_{\Delta\,\text{пор.}}(u)$ – взаємна потужність сигналу на виході каналу та різницевого сигналу відносно порогового сигналу:

$$Z_{\Delta\,\text{пор.}}(u) = \frac{1}{T}\int_0^T u(t)c_{\Delta\,\text{пор.}}(t)dt , \quad (6)$$

$c_{\Delta\ \text{пор.}}$ – різницевий сигнал відносно порогового сигналу:

$$c_{\Delta\ \text{пор.}}(t) = c_{q}(t) - c_{\Delta\ \text{пор.}}(t). \qquad (7)$$

В свою чергу, нерівність (4) є результатом роботи вирішальної схеми в дискретно-неперервному каналі, яка вираховує цю нерівність через енергетичні показники на вході приймача. Як відомо, в наближеному виді таким показником є відношення сигнал/завада, яке забезпечує нерівність у фігурних дужках співвідношення (4) в середньому з імовірністю $p_{\text{нвос}}$:

$$p_{\text{нвос.}} = p(y = y_0) = f(\text{сигнал/завада}). \qquad (8)$$

Сукупність показників захищеності інформації зі структурою їх зв'язків для забезпечення заданого ризику безпеки на основі унеможливлення визначення ознак небезпечного сигналу в просторі можна представити у виді як показано (рис. 1).

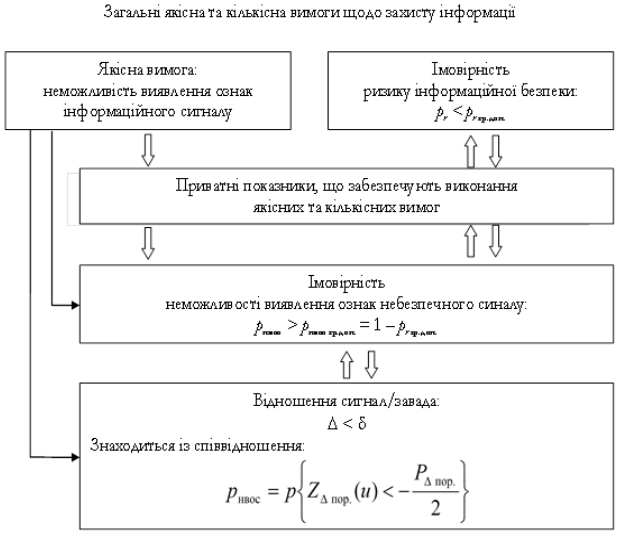

Рис. 1. Сукупність показників захищеності інформації для забезпечення ризику безпеки та структура їх зв'язків на основі унеможливлення визначення ознак інформаційного сигналу в каналах витоку

Із невирішених питань залишається встановлення зв'язку між імовірністю неможливості визначення ознак інформаційного сигналу та відношенням сигнал/завада в точці можливого здійсненні аналізу та прийому, які забезпечуватимуть заданий гранично допустимий ризик безпеки.

Обґрунтування зв'язку імовірності неможливості впевненого визначення ознак інформаційного сигналу та відношення сигнал/завада

Відповідно до отриманого критерію та побудованої вирішальної схеми оптимального приймача [3] обґрунтуємо співвідношення що встановлює зв'язок між імовірністю неможливості впевненого визначення ознак інформаційного сигналу та відношення сигнал/завада як показників захищеності інформації в середовищі поширення. Зазначене обґрунтування здійснимо для довільного розподілу апріорних імовірностей джерела, та для приватного випадку, коли засоби ІКС постійно працюють.

Для цього згідно з стратегією врахування демаскуючих ознак за максимумом демаскування реалізацій інформаційних знаків, знайдемо ймовірності неможливості визначення демаскуючих ознак інформаційного сигналу $p_{\text{нвос}}$ для загального розподілу апріорних імовірностей джерела та неможливості впевненого визначення демаскуючих ознак сигналу $p_{\text{нввос}}$ для випадку неперервної роботи джерела інформації.

Очевидно, що ймовірність неможливості визначення демаскуючих ознак інформаційного сигналу $p_{\text{нвос}}$ буде забезпечуватися випадковим збігом таких обставин, коли в кожному такті інформаційного знака виконуватиметься нерівність [3]:

$$\lambda_{kq/0}(u) = \frac{\omega_k(u / x_q)}{\omega_k(u / x_0)}. \qquad (9)$$

Нехай задано двійкове дискретне джерело витоку інформації з бернуліївським розподілом ймовірностей. Задано канал, як дискретно-неперервний канал з адитивною гауссівською завадою, через який витікають дискретні знаки у виді деяких неперервних реалізацій.

Нехай вирішальна схема (рис. 2), є вирішальною схемою оптимального прийому дискретної інформації, яка, спостерігаючи за джерелом через адитивний канал з гауссівською завадою, з максимальною вірністю визначає, чи є в каналі ознаки сигналу, чи ні [4].

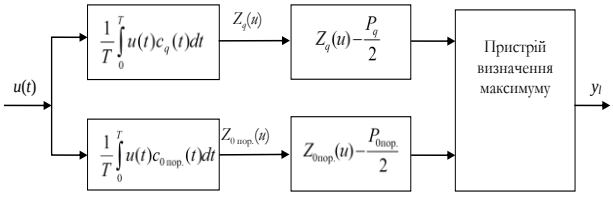

Рис. 2. Вирішальна схема оптимального приймача з описом умови неможливості впевненого визначення ознак інформаційного сигналу за максимумом демаскування реалізацій інформаційних знаків

Зауважимо, що визначення цих ознак має здійснюватися під час роботи джерела інформації. Тому імовірністю неможливості визначення цих ознак є ніщо інше які імовірність помилкового рішення на прийомі про те, що джерело не

виробляє інформації. Незалежно від того з якого об'єму алфавіту джерело виробляє інформаційні дані, за обраною стратегією визначення ознак інформаційного сигналу, граф станів та перехідних процесів в дискретному каналі з точки зору приймача матиме вид (рис. 3).

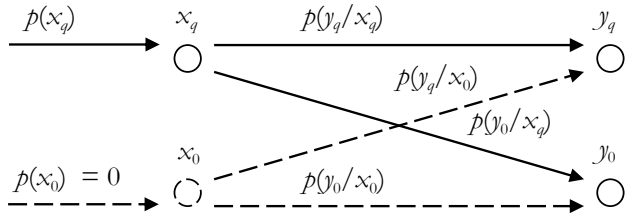

Рис. 3. Граф станів та перехідних процесів в дискретному каналі

На рис. 3 стан входу каналу x_q обирається вирішальною схемою окремо із всіх N станів щодо прийому даних за максимумом демаскування ознак інформаційного сигналу $s_q(t)$, $x_q \in \max\{x_1 \vee x_2 \vee x_3 \vee \ldots \vee x_{N-1} \vee x_N\}$, $q = 1 \div N$. Він є узагальненням роботи технічного засобу або системи обробки та передачі інформації, яке є джерелом інформації, та найгіршим випадком з точки зору невизначення зазначених ознак.

Стан входу x_0 – це стан, за якого технічний засіб або система не працюють. Тобто джерело інформації не виробляє та, відповідно, сигнал на вхід каналу не потрапляє. Відсутність сигналу формально позначили "нульовою" реалізацією $s_0(t)$ або $c_0(t)$, де $s_0(t) = 0$ та $c_0(t) = 0$.

На рис. 3 стан входу каналу x_0 та стрілки від нього показані пунктиром, оскільки реально цей стан виключається із процесу при виявленні ознак інформаційного сигналу в каналах витоку інформації. Тому апріорні імовірності $p(x_0) = 0$ та $p(x_q) = p(x_1 \vee x_2 \vee x_3 \vee \ldots \vee x_N) = 1$, а зображення переходів від x_0 є необхідними з точки зору математичної коректності.

Станами виходу каналу є: $y_l = y_q$ – рішення вирішальної схеми про те, що мають місце в каналі ознаки небезпечного сигналу; $y_l = y_0$ – рішення вирішальної схеми про те, що відсутні ознаки інформаційного сигналу.

Із всього зазначеного очевидно, що імовірністю неможливості визначення ознак сигналу в каналі вирішальною схемою, яка є найкращою щодо визначення цих ознак, є імовірність $p_{\text{н.в.о.с.}} = p(y_0/x_q)$.

По аналогії до вирішальних схем оптимального прийому, що були вже розглянутими раніше, та відповідно до вирішальної схеми на рис. 3 ця імовірність може бути знайденою як імовірність того, що виконується нерівність:

$$p_{\text{нвос}} = p(y_0 / x_q) = \\ = p = \left\{ \begin{array}{l} \dfrac{1}{T}\displaystyle\int_0^T u(t)c_q(t)dt - \\ -\dfrac{P_q}{2} + \dfrac{N_q}{2T}\ln p(x_q) < \\ < \dfrac{1}{T}\displaystyle\int_0^T u(t)c_0(t)dt - \\ -\dfrac{P_0}{2} + \dfrac{N_0}{2T}\ln p(x_0) \end{array} \right\}, \qquad (10)$$

де:

$$u(t) = c_q(t) + n(t). \qquad (11)$$

Не складно побачити, що за умови $p(x_0) = 0$ та $p(x_q) = 1$ співвідношення (10) прийме вид та дорівнюватиме нулю, оскільки нічого не може бути меншим за від'ємну нескінченність:

$$p_{\text{нвос}} = p(y_0 / x_q) = \\ = p = \left\{ \begin{array}{l} \dfrac{1}{T}\displaystyle\int_0^T u(t)c_q(t)dt - \\ -\dfrac{P_q}{2} < -\infty \end{array} \right\} = 0. \qquad (12)$$

І дійсно це буде так. Це зручно показати за допомогою рис. 4 на прикладі роботи вирішальної схеми оптимального приймача двійкових знаків. Якщо сигнал на вході приймача $u > c_0$, то приймач приймає рішення y_1, тобто вважає, що джерело виробило знак x_1; якщо $u < c_0$, то приймач приймає рішення y_2, тобто вважає, що джерело виробило знак x_2. Відповідно, імовірності вірних $p(y_1/x_1)$ і $p(y_2/x_2)$ та помилкових $p(y_1/x_2)$ і $p(y_2/x_1)$ вирішень (рис. 4) представляють собою площі під відповідними кривими.

З графіків видно, що чим меншою буде різниця між ослабленими сигналами c_1 та c_2 або чим більшою буде потужність завади (виражається через розмах графіків) тим більшими будуть площі під кривими та імовірності помилкових вирішень.

Однак, відсутність сигналів на вході приймача виражається однією точкою $u = c_0$, а тому її імовірність $p(y_0/x_1 \vee x_2) = 0$.

Таким чином є очевидним, що унеможливлення визначення ознак інформаційного сигналу в середовищах неконтрольованого поширення інформації відносно оптимального приймача є складним, а то й неможливим.

Нехай задано двійкове дискретне джерело витоку інформації з бернуліївським розподілом

ймовірностей. Задано канал, як дискретно-неперервний канал з адитивною гауссівською завадою, через який витікають дискретні знаки у виді деяких неперервних реалізацій.

Нехай на вході приймача формується суміш сигналу та завади, за якою вирішальна схема приймає рішення щодо того чи передавався хоча б один із знаків, чи ні. В такому разі граф станів перехідних процесів матиме вид (рис. 5).

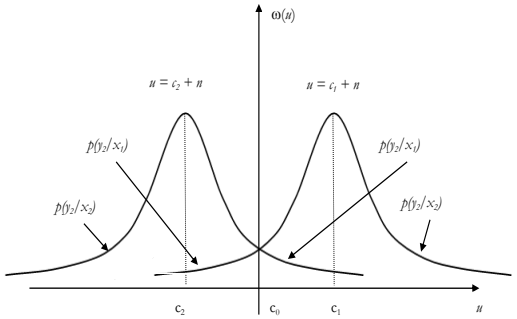

Рис. 4. Щільності розподілу ймовірностей випадкової величини u на вході приймача щодо двійкових гіпотез вирішень

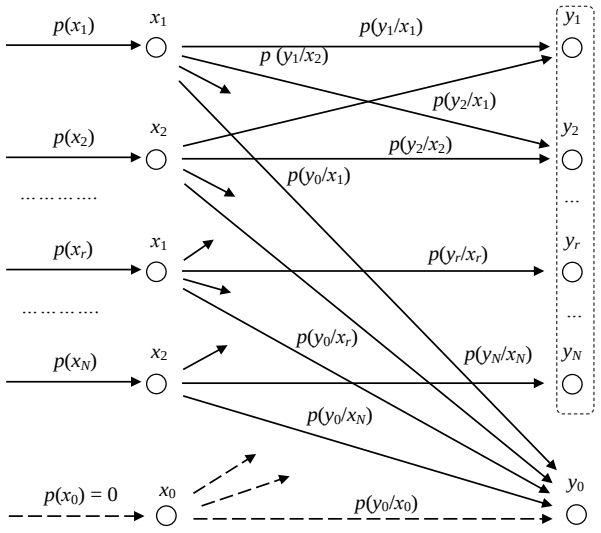

Рис. 5. Граф станів та перехідних процесів в дискретному двійковому каналі з можливістю невиявлення ознак інформаційного сигналу

Нехай на виході каналу побудовано оптимальний приймач, що на рис. 3 має не "нульовий" поріг чутливості, який на основі обробки прийнятого $u(t)$ оцінює наявність ознак небезпечного сигналу $c_0(t)$, $c_1(t)$, $c_2(t)$,…, $c_r(t)$,…, $c_N(t)$.

Зазначимо, що всі реальні приймачі мають як завгодно малий, але певний "ненульовий" поріг чутливості, що визначається його власними шумами.Поріг чутливості – це той проміжок значень сигналів навколо "нуля", в межах якого приймач "не бачить" ненульових реалізацій. Це проміжок, в якому приймач не має можливості впевненого визначення їх ознак небезпечного сигналу і здійснює судження, що скоріше за все сигнал відсутній. В такому разі "нульова" реалізація вже не дорівнюватиме нулю, а перебуватиме у проміжку значень (рис. 6):

$$c_0(t) \in \left[-c_{\text{пор}};+c_{\text{пор.}}\right]. \qquad (13)$$

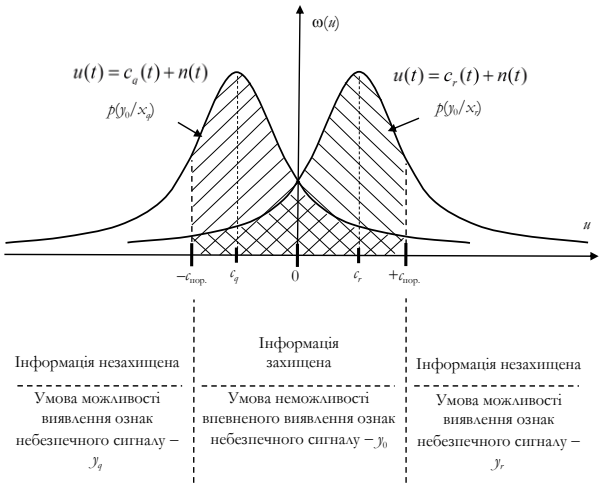

Рис. 6. Шкала стану приймача з "ненульовим" порогом чутливості щодо умов можливості/неможливості визначення ознак інформаційного сигналу в каналі з адитивною гауссівською завадою

Судячи з графу станів на рис. 6 та того, що $p(x_0) = 0$, імовірність неможливості вже впевненого визначення ознак інформаційного сигналу в середовищі неконтрольованого поширення інформації може бути знайденою через математичне сподівання (рис. 5):

$$p_{\text{н.в.в.о.с}} = p(y_0) = \sum_{r=1}^{N} p(x_r)\,p(y_0 / x_r). \qquad (14)$$

Аналогічним чином (14) імовірність $p(y_0/x_r)$ може бути знайденою як добуток k площ під кривими щільностей розподілу ймовірностей випадкових величин u_i, $i = 1, 2, 3, \ldots, k$,що описують суміш сигналу c_{ri} та шумового процесу n_i в середовищі поширення цього ж сигналу, в кожному з k відліків (рис.6). Це є допустимим, оскільки випадковою складовою є білий шум, для якого будь-які два відліки є статистично незалежними.

В роботі [4] показано, що за теоремою Котельникова кількість відліків k доцільно брати не більше ніж $2FT$, де F – смуга пропускання приймача, в якому повністю зосереджений спектр сигналу $c_r(t)$, T – період (тривалість розряду) сигналу $c_r(t)$.

Слід зазначити, що k може бути будь-яким та визначається засобами прийому. Однак, це не впливатиме на зменшення захищеності інформації. Так, якщо k буде малим ($k < 2FT$), то прийом сигналів буде не самим кращим і імовірність не-

можливості впевненого визначення ознак небезпечного сигналу буде більшою ніж на справді. Якщо k буде великим ($k > 2FT$), то в зв'язку з обмеженням спектру шумів між відліками з'явиться кореляційна залежність, яка не приводитиме до зменшення імовірності неможливості впевненого визначення ознак небезпечного сигналу. Адже всі зайві (понад $2FT$) відліки матимуть деяку статистичну (кореляційну) залежність, із-за кореляції (неортогональності) будуть проекційними повторами попередніх (з числа $2FT$) відліків та не матимуть додаткової інформативності.

Таким чином, умовна імовірність визначатиметься як добуток по всім $2FT$-відлікам:

$$\begin{aligned} p(y_0 / x_r) &= \prod_{i=1}^{2FT} p(y_{0i} / x_{ri}) = \\ &= \prod_{i=1}^{2FT} p\left\{-c_{\text{пор.}} \le u_i \le +c_{\text{пор.}}\right\} = \\ &= \prod_{i=1}^{2FT}\left\{-c_{\text{пор.}} \le c_{ri} + n_i \le +c_{\text{пор.}}\right\} = \\ &\prod_{i=1}^{2FT}\left\{-c_{\text{пор.}} - c_{ri} \le n_i \le +c_{\text{пор.}} - c_{ri}\right\} = \\ &= \prod_{i=1}^{2FT}\frac{1}{T}\int_{-c_{\text{пор.}}-c_{ri}}^{+c_{\text{пор.}}-c_{ri}} \omega(n)dn = \\ &= \prod_{i=1}^{2FT}\frac{1}{T}\int_{-c_{\text{пор.}}-c_{ri}}^{+c_{\text{пор.}}-c_{ri}} \frac{1}{\sqrt{2\pi\sigma_n^2}} e^{-\frac{n^2}{2\sigma^2}} dn. \end{aligned} \quad (15)$$

Для приведення у співвідношенні (15) інтегралу щільності нормального розподілу до виду інтегралу Лапласа зробимо заміни:

$$\begin{aligned} &\frac{n}{\sigma} = \eta, \ldots dn = \sigma dn, \\ &\eta_{\text{гр.}\pm} = \frac{n_{\text{гр.}\pm}}{\sigma} = \frac{\pm c_{\text{пор.}} - c_{\text{ri.}}}{\sigma}. \end{aligned} \quad (16)$$

З врахуванням замін (16) співвідношення (15) прийме вид:

$$p(y_0 / x_r) = \prod_{i=1}^{2FT}\frac{1}{T}\int_{\frac{-c_{\text{пор.}}-c_{ri}}{\sigma}}^{\frac{+c_{\text{пор.}}-c_{ri}}{\sigma}} \frac{1}{\sqrt{2\pi\sigma_n^2}} e^{-\frac{n^2}{2}} dn. \quad (17)$$

Якщо шумовий процес є ергодичним процесом, то його дисперсію (квадрат середньоквадратичного відхилення) можна замінити потужністю завади $P_з$, та виразити через спектральну щільність N_0:

$$\sigma^2 = P_з = N_0 F. \quad (18)$$

Таким чином, співвідношення імовірності неможливості впевненого визначення ознак небезпечного сигналу в каналі витоку інформації, що означено формулою (14), з врахуванням поправка (18) має вид:

$$p_{\text{н.в.в.о.с.}} = \sum_{r=0}^{N} p(y_0 / x_r)\prod_{i=1}^{2FT}\frac{1}{T}\int_{\frac{-c_{\text{пор.}}-c_{ri}}{\sqrt{N_0 F}}}^{\frac{+c_{\text{пор.}}-c_{ri}}{\sqrt{N_0 F}}} \frac{1}{\sqrt{2\pi}} e^{-\frac{n^2}{2}} dn. \quad (19)$$

Формула (19) дозволяє знаходження імовірності неможливості визначення ознак сигналу за його демаскуванням в середньому по всім реалізаціям. Щодо означених вище стратегій визначення, це є стратегія 2.

За максимумом демаскування небезпечного сигналу, це відповідає означеній вище стратегії 1, співвідношення імовірності (19) дещо спроститься:

$$p_{\text{н.в.в.о.с.}} = \prod_{i=1}^{2FT}\frac{1}{T}\int_{\frac{-c_{\text{пор.}}-c_{ri}}{\sqrt{N_0 F}}}^{\frac{+c_{\text{пор.}}-c_{ri}}{\sqrt{N_0 F}}} \frac{1}{\sqrt{2\pi}} e^{-\frac{n^2}{2}} dn. \quad (20)$$

ВИСНОВКИ

Таким чином, отримано сукупність показників щодо здійснення визначення ознак інформаційних сигналів . Для забезпечення ризику безпеки обґрунтовано структуру їх зв'язків на основі унеможливлення прийому інформаційних сигналів.

Обґрунтовано аналітичний зв'язок імовірності неможливості прийому інформаційного сигналу з гранично допустимим відношенням сигнал/завада. Показано, що за його виконання визначення сигналів в середовищі поширення не дозволить розпізнаванню ознак. Отримані аналітичні співвідношення дозволяють нескладно здійснювати розрахунки відносно заданого ризику безпеки, аналізувати ризик безпеки відносно заданих умов безпеки.

ЛІТЕРАТУРА

[1]. Іванченко С.О., Некоз В.С. Унеможливлення визначення ознак небезпечного сигналу як спосіб захисту інформації від витоку технічними каналами. Збірник наукових праць "Спеціальні телекомунікаційні системи та захист інформації". К.: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2023. Вип. № 1 (37) С. 54-66.

[2]. Information technology. Security techniques. Information security management systems. Requirements [ISO/IEC 27001:2013].

[3]. Іванченко С.О., Некоз В.С. Обґрунтування критерію оптимальності прийому для побудови вирішальної схеми щодо визначення ознак небезпечного

сигналу. Збірник наукових праць "Спеціальні телекомунікаційні системи та захист інформації". К.: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2023. Вип. № 2 (38) С. 48-60.
[4]. Науково-дослідна робота. Розробка методів щодо виявлення цифрових детермінованих сигналів в неперервному середовищі з випадковими процесами. К.: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2023.
[5]. Про державну таємницю: Закон України від 21 січ.1994 р. № 3855-XII.
[6]. Про інформацію : Закон України від 2 жовт. 1992 р. № 2657-XII.
[7]. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 лип. 1994 р. № 80/94-ВР.
[8]. Про затвердження Концепції технічного захисту інформації в Україні: Постанова Кабінету Міністрів України від 8 жовт. 1997 р. N 1126.
[9]. Батаєв О.П., Ковтун І.В., Корольова Н.А. Теорія електричного зв'язку: навч. посіб. Харків, 2010. 650 с.

JUSTIFICATION OF THE PROBABILITY OF DETERMINING THE PRESENCE OF SIGNALS IN THE ENVIRONMENT OF THEIR PROPAGATION

The substantiation of the impossibility of determining the presence of signals in the media of their distribution was carried out. A discrete-continuous channel was used as a model of the information distribution channel. Information was produced from a discrete source, where each of the information symbols was matched by discontinuous implementations that propagated through a continuous medium with interference. Reception of signals is carried out by means that can be effective. From the point of view of securing information from uncontrolled dissemination and ensuring its security in the distribution environment, as a rule, two factors are used: attenuation of the wave (signal) amplitude during its propagation in the physical environment; the distorting effect of interference that takes place in the medium of signal propagation and destroys its shape. However, the use of these factors, which could ensure complete, almost absolute security of information, is a difficult issue, if not impossible. After all, signals propagating in space, in accordance with the laws of physics, do so in the form of electromagnetic or other waves, or streams of elementary (charged) particles. They can spread over fairly long distances, and theoretically almost to infinity, the effectiveness of their interception is completely determined by the effectiveness of the means of reception. To solve this issue, which is widely used in information security management, there is a risk-oriented approach that does not require absolute security, but allows the possibility of not fulfilling the security requirement with a certain acceptable risk [2]. This risk, as a rule, is determined by the permissible losses that the owner of the assets can incur, and at the same time the effectiveness of production processes will not be disturbed.
Keywords: information security, cyber security, information and communication systems, information protection systems, information signal, discrete channel.

Іванченко Сергій Олександрович, доктор технічних наук, професор, професор Спеціальної кафедри № 1 Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського".

Serhiy Ivanchenko, doctor of technical sciences, professor, professor of the Special Department No. 1 of the Institute of Special Communication and Information Protection of the National Technical University of Ukraine "Ihor Sikorskyi Kyiv Polytechnic Institute".
E-mail: soivanch@ukr.net.
Orcid ID: 0000-0003-1850-9596.

Некоз Василь Сергійович, викладач Спеціальної кафедри № 3 Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського".

Vasyl Nekoz, teacher of the Special Department No. 3 of the Institute of Special Communication and Information Protection of the National Technical University of Ukraine "Ihor Sikorskyi Kyiv Polytechnic Institute".
E-mail: nvs20141987@gmail.com.
Orcid ID: 0000-0001-5091-0529.

DOI: 10.18372/2410-7840.26.18837
УДК 004.056

ДОСЛІДЖЕННЯ СТІЙКОСТІ ДО АТАК ВІДТВОРЕННЯ ПРОТОКОЛІВ ДИСТАНЦІЙНОГО КЕРУВАННЯ З ВИКОРИСТАННЯМ РАДІОКАНАЛУ 433 МГЦ

Ольга Михайлова, Артем Стефанків

У цій статті виявляються критичні вразливості протоколу EV1527, які широко використовуються в системах дистанційного керування, зокрема в домашніх автоматизаційних системах. Зосереджуючись на детальному аналізі структури протоколу та потенційних слабких місць, дане дослідження оцінює ризики атак повторного відтворення, які можуть здійснюватися шляхом перехоплення та повторної трансляції радіосигналів. Результати роботи демонструють значну вразливість цього протоколу до таких атак через відсутність криптографічного захисту переданих даних. У рамках цієї роботи було проведено експериментальні випробування з використанням програмно-керованого трансивера HackRF One, що дозволило відт-