ISSN 2519-2310

# CS&CS Journal


KARAZIN UNIVERSITY
CLASSICS AHEAD OF TIME

1(17) 2020

## COMPUTER SCIENCE AND CYBERSECURITY

## КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ
MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені В.Н.КАРАЗІНА
ХАРЬКОВСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ имени В.Н. КАРАЗИНА
V.N. KARAZIN KHARKIV NATIONAL UNIVERSITY

# КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА
# КОМПЬЮТЕРНЫЕ НАУКИ И КИБЕРБЕЗОПАСНОСТЬ
# COMPUTER SCIENCE AND CYBERSECURITY
# (CS&CS)

**Issue 1(17) 2020**

Заснований 2015 року

Міжнародний електронний науково-теоретичний журнал
Международный электронный научно-теоретический журнал
International electronic scientific journal

The journal publishes research articles on theoretical, scientific and technical problems of effective facilities development for computer information communication systems and on information security problems based on advanced mathematical methods, information technologies and technical means.

Journal is published quarterly.
Approved for placement on the Internet by Academic Council of the Karazin Kharkiv National University (June 23, 2020, protocol No. 10)

The journal has Digital Object Identifier: **10.26565/2519-2310**.



**Editorial office**:
V.N. Karazin Kharkiv National University
Svobody Sq., 6, office 315a, Kharkiv, 61022, Ukraine *(North building of University, 3th floor)*
**Phone**: +38 (057) 705-10-83
**E-mail**: *cscsjournal@karazin.ua*
**Web-page**: *http://periodicals.karazin.ua/cscs (Open Journal System)*

Published articles have been internally and externally peer reviewed

# TABLE OF CONTENTS

**Issue 1(17) 2020**

УДК 519.111: 621.391 DOI: 10.26565/2519-2310-2020-1-01

# СОКРЫТИЕ ИНФОРМАЦИИ В ИЗОБРАЖЕНИЯХ С ИСПОЛЬЗОВАНИЕМ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Алексей Смирнов[1], Людмила Горбачова[2], Александр Кузнецов[2]

[1] Центральный украинский национальный технический университет, пр. Университетский 8, Кропивницкий, 25006, Украина
[2] Харьковский национальный университет им. В.Н. Каразина, пл. Свободы, 4, Харьков, 61022, Украина

dr.smirnovoa@gmail.com, lusyag23@gmail.com, kuznetsov@karazin.ua

**Рецензент:** Николай Карпинский, д.т.н., проф., Университет Бельско-Бяла, ул. Виллова 2, 43-309 Бельско-Бяла, Польша
mkarpinski@ath.bielsko.pl

Поступила: Январь 2020

***Аннотация.*** *В работе рассматриваются техники сокрытия информационных сообщений в контейнерах-изображениях с использованием технологии прямого расширения спектра. В основе этой технологии лежит использование слабокоррелированных псевдослучайных (шумовых) последовательностей. Модулируя информационные данные такими сигналами, сообщение представляется в шумоподобном виде, что существенно затрудняет его обнаружение. Сокрытие состоит в добавлении модулированного сообщения к контейнеру-изображению. Если интерпретировать это изображение как шум в канале связи, тогда задача сокрытия пользовательских данных эквивалентна передаче шумоподобного модулированного сообщения по каналу связи с шумом. При этом предполагается, что шумоподобные сигналы слабокоррелированы, как друг с другом, так и с контейнером-изображением (или его фрагментом). Однако последнее предположение может не выполняться, т.к. реалистичное изображение не является реализацией случайного процесса, его пиксели имеют сильную корреляцию. Очевидно, что выбор псевдослучайных расширяющих сигналов должен учитывать эту особенность. В работе исследованы различные способы формирования расширяющих последовательностей. Выполнена оценка интенсивности битовых ошибок (Bit Error Rate, BER) информационных данных, а также искажений контейнера-изображения по среднеквадратической ошибке (Mean Squared Error, MSE) и пиковому отношению сигнал/шум (Peak signal-to-noise ratio, PSNR). Полученные экспериментальные зависимости наглядно подтверждают преимущество использования последовательностей Уолша. В ходе исследований получены наименьшие значения BER. Даже при небольших значениях мощности сигналов расширяющих последовательностей ($P \approx 5$) величина BER в большинстве случаев не превышала 0,01. Это представляет собой лучший результат из всех рассмотренных в работе вариантов расширяющих последовательностей. Значения PSNR при использовании ортогональных последовательностей Уолша, в большинстве случаев, сопоставимо с другими рассмотренными вариантами. Однако для фиксированного значения PSNR использование преобразования Уолша приводит к значительно меньшим величинам BER. Отмечено, что перспективным направлением является использование адаптивно формируемых дискретных последовательностей. Так, например, если правило формирования расширяющих сигналов будет учитывать статистические свойства контейнера, то можно существенно снизить BER. Также, другим полезным результатом может быть повышение PSNR при фиксированном (заданном) значении BER. Основной целью работы является обоснование выбора расширяющих последовательностей для снижения BER и MSE (увеличения PSNR).*

***Ключевые слова:*** *стеганография; технология прямого расширения спектра; псевдослучайная последовательность, расширяющие сигналы.*

## 1 Введение

Для сокрытия факта передачи и самого существования информационного сообщения традиционно используют различные стеганографические техники [1-4]. С развитием компьютерных наук и цифровых методов обработки информации стеганографическое сокрытие сообщений стало очень распространенным, его используют при обработке изображений, аудио, текстовых документов и пр. Это довольно эффективный и надежный способ организации скрытых каналов передачи данных. Для стороннего наблюдателя передаваемые (*например, посредством электронной почты*) контейнеры, содержащие сокрытые в них информационные сообщения, ничем не отличаются от обычных пользовательских файлов. Это дает возможность организовать скрытый канал связи (КС), не вызывая подозрения о своих намерениях, причем детектировать такие каналы чрезвычайно сложно [1, 2].

Одним из перспективных направлений в развитии современной стеганографии являются

техники встраивания данных в контейнеры-изображения на основе технологи прямого расширения спектра [5-17]. Эта технология традиционно используется в системах связи для повышения скрытности передачи данных по КС с шумами [12-17]. Информационные данные модулируются расширяющей спектр псевдослучайной (*шумовой*) последовательностью. При передаче полученные сигналы в статистическом смысле неотличимы от естественного шума, что повышает скрытность связи. Кроме того, реализуемые методы корреляционного приема позволяют обеспечить исправление произошедших ошибок, что повышает помехоустойчивость связи. Эти и многие другие преимущества технологии прямого расширения спектра позволяют строить надежные и безопасные системы связи. Например, можно организовать связь со значительно меньшей мощностью передатчика, что обеспечивает экологичность связи; применение больших ансамблей (*множеств*) расширяющих последовательностей позволяет повысить абонентскую емкость множественного доступа и т.д. [18-21]. Подобный подход можно применять и в компьютерной обработке цифровых изображений. Интерпретируя изображение, как шум в КС и используя технологию прямого расширения спектра можно организовать сокрытие информационных сообщений без видимого (*демаскирующего*) искажения контейнера. Такие техники и составляют предмет исследований данной статьи.

## 2 Технология прямого расширения спектра для сокрытия сообщений в изображениях

В первых работах по использованию технологии прямого расширения спектра в цифровой стеганографии выдвигалась идея использования псевдослучайных (*шумовых*) последовательностей в качестве «носителя» информационных сообщений [5-11]. Например, для двоичного случая модулированное сообщение $S$ получают умножением отдельных информационных бит $b_i$ (*представляемых в полярном виде* $b_i \in \{-1,1\}$) на расширяющий шумовой сигнал $\varphi_i$:

$$S = \sum_i b_i \varphi_i \qquad (1)$$

причем $\varphi_i$ принадлежит ансамблю (множеству) слабокоррелированных друг с другом псевдослучайных последовательностей (ПСП):

$$\forall \varphi_i \in \varphi = \{\varphi_0, \varphi_1, ..., \varphi_{M-1}\}.$$

Это означает, что коэффициент корреляции двух разных сигналов (*вычисляемый как скалярное произведение последовательностей*) примерно равен нулю:

$$\forall i \neq j : \rho(\varphi_i, \varphi_j) \approx 0.$$

Выражение (1), которое описывает процесс модуляции информационных бит $b_i \in \{-1,1\}$ расширяющими сигналами $\varphi_i$, традиционно используется в широкополосной системе связи с прямым расширением спектра. Поскольку расширяющий сигнал $\varphi_i$ по своим статистическим свойствам подобен шуму, то полученное модулированное сообщение $S$ слабоотличимо от шумов в канале связи, что и позволяет осуществить скрытую передачу. Действительно, передаваемые сообщения приобретают вид шумоподобных последовательностей, а за счет большой мощности множества $\varphi$ и прямого расширения частотного спектра обеспечивается высокая скрытность и имитостойкость организовываемых каналов связи [18-21]. В системах с кодовым разделением каналов CDMA (*Code Division Multiple Access*) каждый сигнал $\varphi_i$ назначается отдельной паре абонентов, т.е. увеличение мощности $M$ множества $\varphi = \{\varphi_0, \varphi_1, ..., \varphi_{M-1}\}$ позволяет повысить абонентскую емкость систем связи, т.е. существенно удешевить передачу данных [18,19].

Стеганография с использованием прямого расширения спектра использует эти техники в различных файлах-контейнерах. Например, интерпретируя контейнер-изображение $I$, как естественный шум в канале связи можно организовать передачу информационных сообще-

ний «внутри» изображения [5-17]. В работах [5-11] в качестве сигналов $\varphi_i$ предлагалось использовать формируемые генераторами ПСП последовательности, после чего сформированный по правилу (1) сигнал $S$ поэлементно суммируется с контейнером-изображением $I$:

$$N = I + S \tag{2}$$

Таким образом, полученное изображение-стеганоконтейнер $N$ формируется посредством добавления к исходному изображению $I$ модулированного сообщения (1). Это аналогично тому, как в системах связи передаваемое модулированное информационное сообщение $S$ «складывалось» с естественным фоновым шумом (*помехой*).

На приемной стороне, как и в системах связи, информационное сообщение восстанавливается с использованием корреляционного приема. Для двоичного случая для извлечения $j$-ого бита вычисляют коэффициент корреляции между сигналом $\varphi_j$ и принятым $N$:

$$\rho\left(N,\varphi_j\right) = I\varphi_j + \varphi_j \sum_i b_i \varphi_i \tag{3}$$

В системах связи естественный шум и шумовой сигнал $\varphi_i$ статистически независимы (*некоррелированы*). Следуя подобным интерпретациям логично предположить, что аналог шума – контейнер-изображение $I$ также некоррелирован с расширяющими сигналами, т.е. $\rho\left(I,\varphi_j\right) = I\varphi_j \approx 0$. Различные шумовые сигналы также некоррелированы друг с другом, т.е. $\forall j \neq i : \varphi_j\varphi_i \approx 0$. В этом случае $\rho\left(N,\varphi_j\right) \approx b_j\varphi_j\varphi_j$, т.е. значение $b_j$ можно определить по знаку $\rho\left(N,\varphi_j\right)$:

$$b_j = sign\left[\rho\left(N,\varphi_j\right)\right] \tag{4}$$

К сожалению, для стеганографических приложений, когда используется контейнер-изображение $I$, предположение $\rho\left(I,\varphi_j\right) = I\varphi_j \approx 0$ в (3) может не выполняться. Действительно, если для сокрытия информационного сообщения используется реалистичное изображение (*т.е. не являющееся реализацией некоторого датчика случайных величин*), то тогда может наблюдаться существенная корреляция $I$ и $\varphi_i$. В этом случае восстановление информационных бит в соответствии с выражением (4) может быть ошибочным.

В данной работе исследуются различные способы формирования множества $\varphi = \{\varphi_0, \varphi_1, ..., \varphi_{M-1}\}$ и проведена оценка интенсивности битовых ошибок (*BER - Bit Error Rate*) при извлечении сообщения из изображений-контейнеров (*N*). В частности, исследован предложенный в работах [7,8,10,11] нелинейный способ формирования последовательностей с нормальным гауссовым распределением, а также ортогональные последовательности Уолша [22] и псевдослучайные последовательности, с равномерно распределенными на интервале (-1, 1) элементами. Также, в рамках работы проведена оценка искажения изображения-контейнера по среднеквадратической ошибке (СКО) и пиковому отношению сигнал/шум (*Peak signal-to-noise ratio, PSNR*). Эти две характеристики (*BER* и *PSNR*) наглядно демонстрируют возможности по достоверной (*безошибочной*) и скрытной (*без демаскирующих искажений изображения-контейнера*) передачи информационных сообщений с использованием технологии прямого расширения спектра.

## 3 Порядок исследований

Для проведения исследований различных способов сокрытия информации в контейнерах-изображениях используют несколько показателей эффективности.

Для оценки правильности восстановленных данных (*их достоверности, безошибочности*) используют *BER* [23]. *BER* - количество битовых ошибок $N_{error}$, деленное на общее количество переданных бит $N_{total}$:

$$BER = \frac{N_{error}}{N_{total}} \tag{5}$$

*BER* - это единичный показатель производительности, часто выражаемый в процентах[23]. Мы оценивали *BER* в абсолютных величинах, т.е. непосредственно по (5). Для оценки искажений контейнера-изображения используют *MSE* и *PSNR* [23-25].

Для монохромного $m \times n$ изображения *I* и его искаженного ошибками приближения (*Noisy Approximation*) *N* значение *MSE* определяют выражением:

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I_{i,j} - N_{i,j}]^2 \tag{6}$$

*PSNR* характеризует отношение между максимально возможной мощностью сигнала и мощностью искажающего шума. *PSNR* обычно выражается в логарифмической шкале (*dB*):

$$\begin{aligned} PSNR &= 10 \cdot \log_{10}\left(\frac{I_{\max}^2}{MSE}\right) = 20 \cdot \log_{10}\left(\frac{I_{\max}}{\sqrt{MSE}}\right) = \\ &= 20 \cdot \log_{10}(I_{\max}) - 10 \cdot \log_{10}(MSE). \end{aligned} \tag{7}$$

где $I_{\max}$ есть максимально возможное значение пикселя изображения.

Если пиксели кодируются $m$-ми битными величинами, тогда $I_{\max} = 2^m - 1$. Например, для наиболее простого случая с $m = 8$ имеем $I_{\max} = 255$ и значение *PSNR* рассчитывается по (8):

$$PSNR = 20 \cdot \log_{10}(255) - 10 \cdot \log_{10}(MSE) \tag{8}$$

При проведении экспериментов были использованы различные изображения (*размером 256×256 эл.*) при кодировании каждого монохромного пикселя одним байтом [7,8,10,11]. Так в частности, в рамках экспериментов обработке подвергалось стандартное тестовое изображение *Lenna* размером 256×256 пикселей. Приводимые далее результаты, представляют собой усредненные значения, полученные для нескольких различных изображений. Для усреднения результатов использовались формулы квадратичной регрессии с интерполяцией полученных результатов (*встроенная функция regress и interp системы MathCad*).

Следует отметить, что приводимые здесь результаты соответствуют использованию различных расширяющих последовательностей, но без применения помехоустойчивого кодирования. Например, в работе [8] для снижения *BER* применяются блоковые коды в режиме прямого исправления ошибок. В данной работе приводятся оценки *BER* без использования помехоустойчивых кодов. В этом смысле полученные результаты могут быть сопоставлены с уже имеющимися, известными данными.

## 4 Результаты исследований

При проведении исследований мы реализовали несколько вариантов формирования множества расширяющих сигналов $\varphi = \{\varphi_0, \varphi_1, ..., \varphi_{M-1}\}$. Для каждого способа формирования расширяющих последовательностей осуществлялась вставка информации в различные контейнеры-изображения и выполнялась оценка значений *BER*, *MSE* и *PSNR* (*как в (5-8)*). Основное внимание было акцентировано на сравнении полученных результатов, с целью определения лучшего способа формирования последовательностей $\varphi_i$.

### 4.1 Использование нелинейной модуляции

В работах *Lisa M. Marvel* и др. [7, 8, 10, 11] для использования технологии прямого расширения спектра предлагалось использовать нелинейное правило формирования множества $\varphi = \{\varphi_0, \varphi_1, ..., \varphi_{M-1}\}$:

$$(\varphi_i)_j = \begin{cases} \Phi^{-1}((u_i)_j), b_i = -1; \\ \Phi^{-1}((u'_i)_j), b_i = 1, \end{cases} \quad (9) \qquad \text{где} \qquad (u'_i)_j = \begin{cases} (u_i)_j + 0.5, u_i < 0.5; \\ (u_i)_j - 0.5, u_i \geq 0.5, \end{cases} \quad (10)$$

$(u_i)_j$ - равномерно распределенная на интервале (0,1) случайная величина, а $\Phi^{-1}$ представляет собой обратную кумулятивную функцию распределения для стандартной гауссовой случайной величины.

Таким образом, расширяющие спектр последовательности из $\varphi = \{\varphi_0, \varphi_1, ..., \varphi_{M-1}\}$ представляют собой реализацию случайной величины, распределенной по нормальному закону с нулевым средним и единичным среднеквадратичным отклонением. Эта случайная реализация вычисляется в соответствии с (9), т.е. с использованием метода обратного преобразования (*The Inverse Transformation Method*) [26].

Для практической реализации нелинейного правила (9) и (10) были использованы встроенные в *MathCad* функции $rnd(x)$ и $dnorm(p, \mu, \sigma)$: $\Phi^{-1}(x) = dnorm(x, 0, 1)$; $(u_i)_j = rnd(1)$.

Очевидно, что правило (1) для вычисления модулированного сигнала $S$ при таком способе формирования множества $\varphi = \{\varphi_0, \varphi_1, ..., \varphi_{M-1}\}$, следует записать в следующем виде:

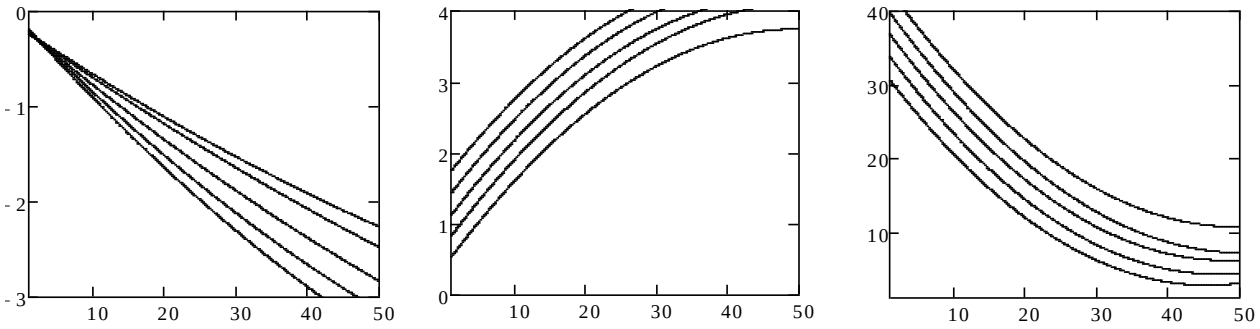
$$S = \sum_i \varphi_i \quad (11)$$

Как известно [7-8,10-11], непосредственное использование расширяющих последовательностей для сокрытия информации в изображениях-контейнерах, приводит к значительным битовым ошибкам в извлеченных данных. Для этого предлагалось повышать мощность расширяющих сигналов. Таким образом, выражение (11) запишем как

$$S = \sum_i P\varphi_i \quad (12)$$

где $P$ - положительное значение, кратно увеличивающее мощность (*power*) расширяющих сигналов последовательностей $\varphi_i$.

В серии проведенных экспериментов авторами реализовано сокрытие данных в изображениях-контейнерах с использованием выражений (9), (10), (12). Полученные результаты для различных значений $P$ представлены на рис. 1, где приведены различные случаи для $k = 1, 2, 4, 8, 16$ и $P = 2^i, i = 0, 1, ..., 6$. Число слагаемых в (1) и (12) определяется числом $k$ информационных бит, скрываемых в одном изображении-контейнере.




*a) BER (P)* *b) MSE (P)* *c) PSNR (P)*

Рис. 1 - Результаты моделирования с использованием выражений (9), (10), (12)

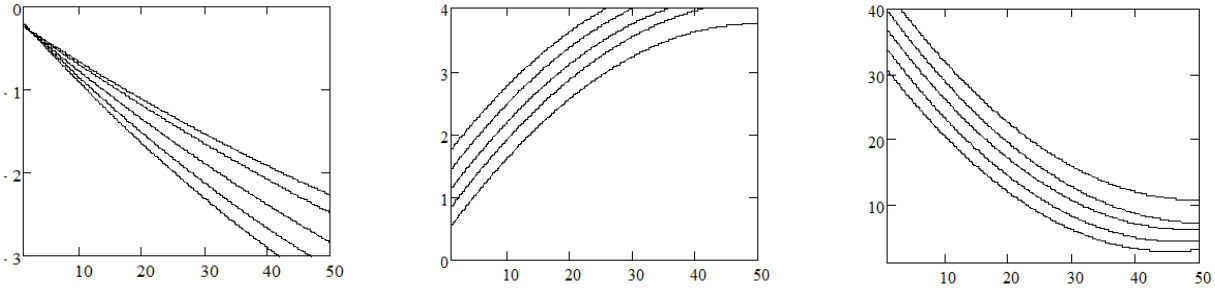
Если множество сигналов $\varphi = \{\varphi_0, \varphi_1, ..., \varphi_{M-1}\}$ формировать по упрощенной схеме (13):

$$(\varphi_i)_j = \Phi^{-1}((u'_i)_j), (u'_i)_j = \begin{cases} (u_i)_j + 0.5, u_i < 0.5; \\ (u_i)_j - 0.5, u_i \geq 0.5, \end{cases} \quad (13)$$

то для сокрытия данных можем использовать аналог выражения (1) в следующем виде:

$$S = \sum_i Pb_i\varphi_i \quad (14)$$

Данный способ формирования расширяющих сигналов нами также был исследован, а полученные результаты представлены на рис 2.




*a) BER (P)* *b) MSE (P)* *c) PSNR (P)*

Рис. 2 – Результаты моделирования с использованием выражений (13) и (14)

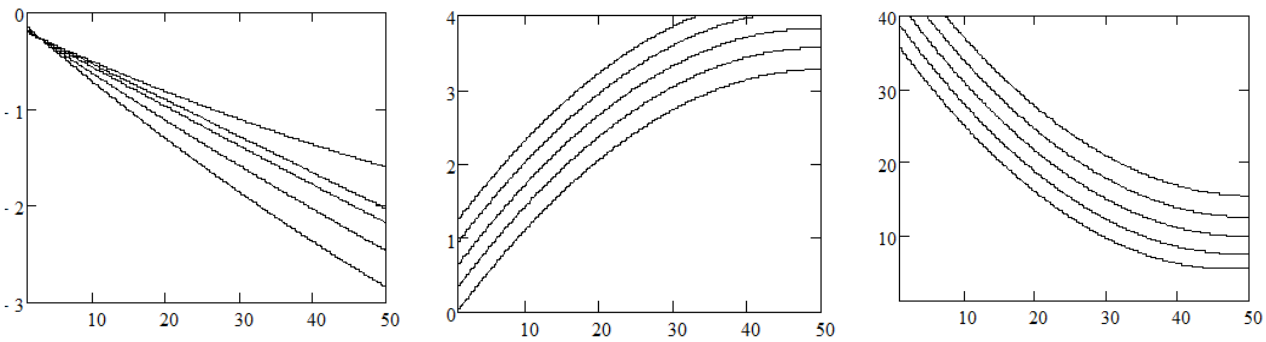
Анализ представленных данных позволяет утверждать, что оба способа формирования расширяющих последовательностей дают практически одинаковые результаты. В сери проведенных экспериментов правило (9), (10) было лишь немногим лучше по значению *PSNR* (*из-за логарифмической шкалы это различие практически не заметно*). Также следует отметить высокое значение *BER*, например, уже при «мощности» расширяющих сигналов $P \approx 20$ это значения, в большинстве случаев, находится в диапазоне 0,1 ... 0,01 (*практически граничное значение целесообразности использования помехоустойчивого кодирования*).

**4.2 Использование случайных чисел, равномерно распределенных на интервале (-1,1)**

Другой способ формирования множества $\varphi = \{\varphi_0, \varphi_1, ..., \varphi_{M-1}\}$, который мы исследовали, состоял в использовании равномерно распределенных на интервале (-1,1) случайных чисел. Для моделирования данного варианта использована встроенная функция $rnd(x)$ системы *MathCad*, а правило формирования последовательностей имело вид:

$$(\varphi_i)_j = rnd(2) - 1 \quad (15)$$

Результаты исследований эффективности сокрытия информации в соответствии с правилом (13) для различных соотношений $k$ и $P$ приведены на рис. 3.




*a) BER (P)* *b) MSE (P)* *c) PSNR (P)*

Рис. 3 – Результаты моделирования с использованием выражений (15) и (14)

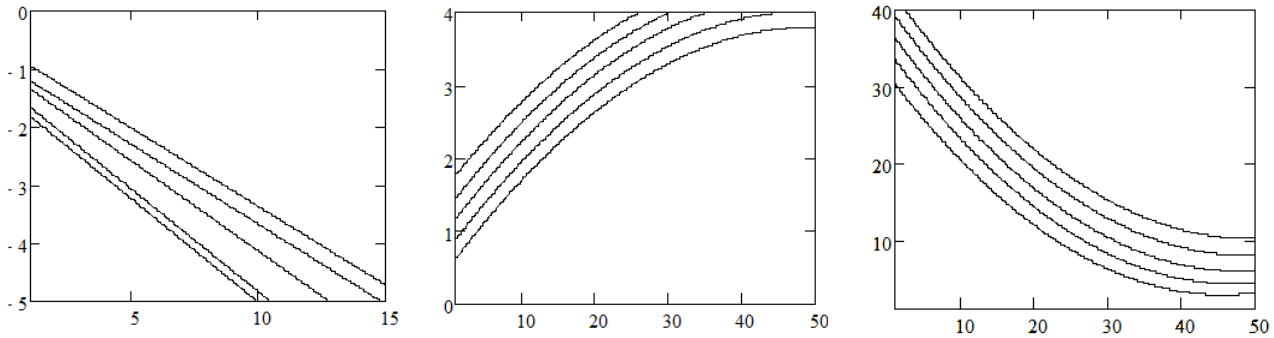
Приведенные на рис. 3 результаты практически сопоставимы с данными, полученными для случая нелинейной модуляции (9), (10), а также для упрощенного варианта (13). В данном случае наблюдается, лишь незначительное повышение *BER*, однако *PSNR* при этом также увеличилось. В целом, можно утверждать, что выявленные отличия невелики и эти способы формирования расширяющих последовательностей практически равноценны.

### 4.3 Использование ортогональных последовательностей Уолша

В своих исследованиях мы также использовали ортогональные дискретные последовательности Уолша (*Walsh*). Такие сигналы образуются из строк матрицы Адамара (*Hadamard matrix*) $H_{2^i}$, формируемой по рекуррентному правилу:

$$H_{2^i} = \begin{bmatrix} H_{2^{i-1}} & H_{2^{i-1}} \\ H_{2^{i-1}} & -H_{2^{i-1}} \end{bmatrix}, \; H_1 = [1]. \tag{16}$$

Итеративное повторение правила (16) позволяет сформировать любую матрицу Адамара $H_{2^i}$ порядка $2^i$, $i = 1, 2, \ldots$. Строки (или столбцы) сформированных матриц взаимно ортогональны, т.е. их скалярное произведение равно нулю. В ходе проведенного моделирования было использовано правило (16), а строки матрицы $H_{2^i}$ интерпретировались, как элементы множества $\varphi = \{\varphi_0, \varphi_1, \ldots, \varphi_{M-1}\}$. Полученные результаты приведены на рис. 4.




*a) BER (P)* *b) MSE (P)* *c) PSNR (P)*

Рис. 4 – Результаты моделирования с использованием ортогональных последовательностей Уолша и выражения (14)

Зависимости на рис. 4 наглядно подтверждают преимущество использования последовательностей Уолша. Так, в ходе исследований получены наименьшие значения *BER*. Даже при небольших значениях $P \approx 5$ величина *BER*, в большинстве случаев, не превышала 0,01, что представляет собой наилучший результат из всех рассмотренных вариантов расширяющих последовательностей.

Значения *PSNR* при использовании ортогональных последовательностей Уолша, в большинстве случаев, сопоставимо с рассмотренными ранее вариантами. Однако для фиксированного значения *PSNR* использование преобразования Уолша приводит к значительно меньшим величинам *BER*.

## 5 Выводы

Полученные в ходе моделирования зависимости показывают, что использование технологии прямого расширения спектра действительно может являться перспективным решением задачи сокрытия информационных сообщений в изображениях-контейнерах (стеганографии).

Интерпретируя изображение, как шум в КС можно организовать скрытный канал передачи данных, причем искажения изображения могут быть не велики. В тоже время, основное предположение о некоррелированности расширяющих последовательностей с контейнером-переносчиком информации (*или его отдельной частью/фрагментом*), может быть ошибочным. В этом случае при восстановлении информационных (*скрытых*) данных будет получен

высокий уровень ошибок. Следовательно, важным элементом такой стеганосистемы является корректный выбор расширяющих последовательностей.

В данной работе были проанализированы несколько вариантов построения расширяющих последовательностей для целей синтеза стеганосистемы. В частности, рассмотрен один из известных алгоритмов [11] с нелинейной модуляцией по правилу (9), (10), на примере которого исследована эффективность подобной стегановставки по показателям *BER*, *MSE* и *PSNR*. Полученные данные частично совпадают с известными результатами из [7,8,10,11], что косвенно подтверждает адекватность представленных результатов.

Также исследованиям были подвергнуты и другие способы формирования расширяющих последовательностей (*для целей сокрытия данных в контейнерах-изображениях*). Моделирование показало, что применение упрощенного правила (13), равно как и использование последовательностей с равновероятными на интервале (-1,1) значениями, не приводит к существенному ухудшению результатов *(показатели BER и PSNR отличаются не значительно)*.

В ходе экспериментов изучено применение расширяющих последовательностей Уолша. Анализ данных результатов свидетельствует, что этот вариант наиболее удачный, поскольку при сопоставимых значениях *PSNR* достигается значительно меньшая величина ошибок. Действительно, как следует из представленных результатов, величина *BER* значительно ниже, чем для других вариантов использованных расширяющих последовательностей.

Подчеркнуто, что потенциально интересным направлением дальнейших исследований является использование адаптивно формируемых дискретных последовательностей. Так, например, если правило формирования расширяющих сигналов будет учитывать статистические свойства изображения-контейнера, то можно существенно снизить *BER*, либо вовсе получить практически безошибочную передачу. Также, другим полезным эффектом может быть повышение *PSNR* при фиксированном (*например, наперед заданным*) значении *BER*.

В рамках дальнейших исследованиях будут представлены результаты моделирования ряда других способов формирования расширяющих последовательностей, рассмотренных в наших предыдущих работах [27-31].

## Ссылки


[1] “Digital Watermarking and Steganography,” 2008. doi:10.1016/b978-0-12-372585-1.x5001-3.

[2] F. Y. Shin, “Digital Watermarking and Steganography,” Dec. 2017. doi:10.1201/9781315219783.

[3] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," in Computer, vol. 31, no. 2, pp. 26-34, Feb. 1998. doi: 10.1109/MC.1998.4655281.

[4] I. V. S. Manoj, “Cryptography and Steganography,” International Journal of Computer Applications, vol. 1, no. 12, pp. 63–68, Feb. 2010. doi:10.5120/257-414.

[5] A. Z. Tirkel, C. F. Osborne and R. G. Van Schyndel, "Image watermarking-a spread spectrum application," Proceedings of ISSSTA'95 International Symposium on Spread Spectrum Techniques and Applications, Mainz, Germany, 1996, pp. 785-789 vol.2. doi: 10.1109/ISSSTA.1996.563231.

[6] J. R. Smith and B. O. Comiskey, “Modulation and information hiding in images,” Lecture Notes in Computer Science, pp. 207–226, 1996. doi:10.1007/3-540-61996-8_42.

[7] L. M. Marvel, C. G. Boncelet, R. Jr., and Charles T., “Methodology of Spread-Spectrum Image Steganography,” Jun. 1998. doi:10.21236/ada349102.

[8] L. M. Marvel, C. G. Boncelet and C. T. Retter, "Spread spectrum image steganography," in IEEE Transactions on Image Processing, vol. 8, no. 8, pp. 1075-1083, Aug. 1999. doi: 10.1109/83.777088.

[9] M. Kutter, “Performance Improvement of Spread Spectrum Based Image Watermarking Schemes through M-ary Modulation,” Lecture Notes in Computer Science, pp. 237–252, 2000. doi:10.1007/10719724_17.

[10] F. S. Brundick and L. M. Marvel, “Implementation of Spread Spectrum Image Steganography,” Mar. 2001. doi:10.21236/ada392155.

[11] Patent No.: US 6,557,103 B1, Int.Cl. G06F 11/30. Charles G. Boncelet, Jr., Lisa M. Marvel, Charles T. Retter. Spread Spectrum Image Steganography. Patent No.: US 6,557,103 B1, Int.Cl. G06F 11/30. – № 09/257,136; Filed Feb. 11, 1999; Date of Patent Apr. 29, 2003

[12] Fan Zhang, Bin Xu and Xinhong Zhang, "Digital image watermarking algorithm based on CDMA spread spectrum," 2006 12th International Multi-Media Modelling Conference, Beijing, 2006, pp. 4 pp.-. doi: 10.1109/MMMC.2006.1651359.

[13] T. T. Nguyen and D. Taubman, "Optimal linear detector for spread spectrum based multidimensional signal watermarking," 2009 16th IEEE International Conference on Image Processing (ICIP), Cairo, 2009, pp. 113-116. doi: 10.1109/ICIP.2009.5414121.

[14] E. Nezhadarya, Z. J. Wang and R. K. Ward, "Image quality monitoring using spread spectrum watermarking," 2009 16th IEEE International Conference on Image Processing (ICIP), Cairo, 2009, pp. 2233-2236. doi: 10.1109/ICIP.2009.5413955.

[15] S. Ghosh, P. Ray, S. P. Maity and H. Rahaman, "Spread Spectrum Image Watermarking with Digital Design," 2009 IEEE International Advance Computing Conference, Patiala, 2009, pp. 868-873. doi: 10.1109/IADCC.2009.4809129.
[16] H. O. Altun, A. Orsdemir, G. Sharma and M. F. Bocko, "Optimal Spread Spectrum Watermark Embedding via a Multistep Feasibility Formulation," in IEEE Transactions on Image Processing, vol. 18, no. 2, pp. 371-387, Feb. 2009. doi: 10.1109/TIP.2008.2008222.
[17] A. Samčović and M. Milovanović, "Robust digital image watermarking based on wavelet transform and spread spectrum techniques," 2015 23rd Telecommunications Forum Telfor (TELFOR), Belgrade, 2015, pp. 811-814. doi: 10.1109/TELFOR.2015.7377589.
[18] V. P. Ipatov, "Spread Spectrum and CDMA," Mar. 2005. doi:10.1002/0470091800.
[19] "Introduction to CDMA Wireless Communications," 2007. doi:10.1016/b978-0-7506-5252-0.x5001-7.
[20] "The Generalized CDMA," CDMA: Access and Switching, pp. 1–28. doi:10.1002/0470841699.
[21] S. Hara and R. Prasad, "DS-CDMA, MC-CDMA and MT-CDMA for mobile multi-media communications," Proceedings of Vehicular Technology Conference - VTC, Atlanta, GA, USA, 1996, pp. 1106-1110 vol.2. doi: 10.1109/VETEC.1996.501483.
[22] S. S. Agaian, H. G. Sarukhanyan, K. O. Egiazarian, and J. Astola, "Hadamard Transforms," Aug. 2011. doi:10.1117/3.890094.
[23] "Probability Theory of Bit Error Rate," Optical Bit Error Rate, 2009. doi:10.1109/9780470545430.ch7.
[24] J. Korhonen and J. You, "Peak signal-to-noise ratio revisited: Is simple beautiful?," 2012 Fourth International Workshop on Quality of Multimedia Experience, Yarra Valley, VIC, 2012, pp. 37-38. doi: 10.1109/QoMEX.2012.6263880
[25] "Data Compression," 2007. doi:10.1007/978-1-84628-603-2.
[26] L. Devroye, "Non-Uniform Random Variate Generation," 1986. doi:10.1007/978-1-4613-8643-8.
[27] Yu.V. Stasev, A.A. Kuznetsov, A.M. Nosik. "Formation of pseudorandom sequences with improved autocorrelation properties." Cybernetics and Systems Analysis, vol. 43, Issue 1, pp. 1-11, January 2007. DOI: 10.1007/s10559-007-0021-2
[28] N.I.Naumenko, Yu.V.Stasev, A.A.Kuznetsov. "Methods of synthesis of signals with prescribed properties." Cybernetics and Systems Analysis, vol. 43, Issue 3, pp. 321-326, May 2007. DOI: 10.1007/s10559-007-0052-8
[29] O.Karpenko, A.Kuznetsov, V.Sai, Yu.Stasev. "Discrete Signals with Multi-Level Correlation Function." Telecommunications and Radio Engineering, vol. 71, 2012 Issue 1. pp 91-98. DOI: 10.1615/TelecomRadEng.v71.i1.100
[30] A. Kuznetsov, S. Kavun, V. Panchenko, D. Prokopovych-Tkachenko, F. Kurinniy and V. Shoiko, "Periodic Properties of Cryptographically Strong Pseudorandom Sequences," 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, Ukraine, 2018, pp. 129-134. doi: 10.1109/INFOCOMMST.2018.8632021
[31] A. Kuznetsov, O. Smirnov, D. Kovalchuk, A. Averchev, M. Pastukhov and K. Kuznetsova, "Formation of Pseudorandom Sequences with Special Correlation Properties," 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT), Lviv, Ukraine, 2019, pp. 395-399. doi: 10.1109/AIACT.2019.8847861

**Reviewer:** Mikołaj Karpiński, Dr. of Sciences (Eng.), Full Prof., University of Bielsko-Biala, Bielsko-Biala, Poland.
E-mail: mkarpinski@ath.bielsko.pl

Received: January 2020.

**Authors:**
Oleksii Smirnov, Central Ukrainian National Technical University, avenue University, 8, 25006, Kropivnitskiy.
E-mail: dr.smirnovoa@gmail.com
Ludmila Gorbacheva, student of CSD, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: lusyag23@gmail.com
Alexandr Kuznetsov, Doctor of Sciences (Eng.), Full Prof., V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: kuznetsov@karazin.ua

**Hiding information in images using pseudo-random sequences.**

**Abstract.** In this article are discussed techniques of hiding information messages in cover image using direct spectrum spreading technology. This technology is based on the use of poorly correlated pseudorandom (noise) sequences. Modulating the information data with such signals, the message is presented as a noise-like form, which makes it very difficult to detect. Hiding means adding a modulated message to the cover image. If this image is interpreted as noise on the communication channel, then the task of hiding user's data is equivalent to transmitting a noise-like modulated message on the noise communication channel. At the same it is supposed that noise-like signals are poorly correlated both with each other and with the cover image (or its fragment). However, the latter assumption may not be fulfilled because a realistic image is not an implementation of a random process; its pixels have a strong correlation. Obviously, the selection of pseudo-random spreading signals must take this feature into account. We are investigating various ways of formation spreading sequences while assessing Bit Error Rate (*BER*) of information data as well as cover image distortion by mean squared error (*MSE*) and by Peak signal-to-noise ratio (*PSNR*). The obtained experimental dependencies clearly confirm the advantage of using Walsh sequences. During the research, the lowest *BER* values were obtained. Even at low values of the signal power of the spreading sequences ($P \approx 5$), the *BER* value, in most cases, did not exceed 0,01. This is the best result of all the sequences under consideration in this work. The values of *PSNR* when using orthogonal Walsh sequences are, in most cases, comparable to other considered options. However, for a fixed value of *PSNR*, using the Walsh transform results in significantly lower *BER* values. It is noted that a promising direction is the use of adaptively generated discrete sequences. So, for example, if the rule for generating expanding signals takes into account the statistical properties of the container, then you can significantly reduce the value of *BER*. Also, another useful result could be increasing *PSNR* at a fixed (given) value of *BER*. The purpose of our work is to justify the choice of extending sequences to reduce *BE*R and *MSE* (*increase PSNR*).

**Keywords:** Steganography; Direct spectrum Spreading technology; Pseudorandom sequence; Spreading signals.

**Рецензент:** Микола Карпінський, д.т.н., проф., університет Бельсько-Бяла, Бельсько-Бяла, Польща.
E-mail: mkarpinski@ath.bielsko.pl

Надійшло: Січень 2020.

**Автори:**
Олексій Смірнов, Центральній український національний технічний університет, Кропивницький, 25006, Україна.
E-mail: dr.smirnovoa@gmail.com
Людмила Горбачова, студентка факультету комп'ютерних наук, Харківський національний університет імені В. Н. Каразіна, Харків, 61022, Україна.
E-mail: lusyag23@gmail.com
Олександр Кузнецов, д.т.н., проф., Харківський національний університет імені В. Н. Каразіна, Харків, 61022, Україна.
E-mail: kuznetsov@karazin.ua

**Приховування інформації в зображеннях з використанням псевдовипадкових послідовностей.**

**Анотація.** У статті розглядаються техніки приховування інформаційних повідомлень в контейнерах-зображеннях з використанням технології прямого розширення спектра. В основі цієї технології лежить використання слабокорельованих між собою псевдовипадкових (шумових) послідовностей. Модулюючи інформаційні дані такими сигналами, повідомлення видається в шумоподібному вигляді, що суттєво ускладнює його виявлення. Приховування полягає в додаванні модульованого повідомлення до контейнера-зображення. Якщо інтерпретувати це зображення як шум у каналі зв'язку, тоді завдання приховування призначених для користувача даних еквівалентна передачі шумоподібного модульованого повідомлення по каналу зв'язку з шумом. При цьому передбачається, що шумоподібні сигнали слабокорельовані як один з одним, так і з контейнером-зображенням (або його фрагментом). Однак останнє припущення може не виконуватися, тому що реалістичне зображення не є реалізацією випадкового процесу, його пікселі мають сильну кореляцію. Очевидно, що вибір псевдовипадкових розширюючих сигналів повинен враховувати цю особливість. В роботі досліджено різні способи формування розширюючих послідовностей. Виконана оцінка інтенсивності бітових помилок (*Bit Error Rate, BER*) інформаційних даних, а також спотворення зображення - контейнера за середньоквадратичною помилкою *(mean squared error, MSE*) та піковому відношенню сигнал/шум (*Peak signal -to-noise ratio, PSNR*). Отримані експериментальні залежності наочно підтверджують перевагу користування послідовностей Уолша. В ході досліджень отримані найменші значення *BER*. Навіть при невеликих значеннях потужності сигналів розширюючих послідовностей ($P \approx 5$) величина *BER*, в більшості випадків, не перевищувала 0,01. Це являє собою кращий результат з усіх розглянутих в роботі варіантів розширюючих послідовностей. Значення *PSNR* при використанні ортогональних послідовностей Уолша, в більшості випадків, можна порівняти з іншими розглянутими варіантами. Однак для фіксованого значення *PSNR* використання перетворення Уолша призводить до значно менших величинам *BER*. Відзначено, що перспективним напрямком є використання дискретних послідовностей, які адаптивно формуються. Так, наприклад, якщо правило формування розширюючих сигналів буде враховувати статистичні властивості контейнера, то можна істотно знизити *BER*. Також, іншим корисним результатом може бути підвищення *PSNR* при фіксованому (заздалегідь заданому) значенні *BER*. Головною метою роботи є обгрунтування вибору розширюючих послідовностей для зниження *BER* і *MSE* (*збільшення PSNR*).

**Ключові слова:** стеганографія; технологія прямого розширення спектра; псевдовипадкова послідовність; сигнали розширення.

УДК 004.056.5: 342.922/951 DOI: 10.26565/2519-2310-2020-1-02

# ДОСЛІДЖЕННЯ ЯВИЩА КІБЕРБУЛІНГУ ТА АНАЛІЗ ШЛЯХІВ ПРОТИДІЇ ЙОГО ПРОЯВАМ

Валерія Гайкова, Сергій Малахов

Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, Харків, 61022, Україна
valeriagaikova98@gmail.com, mailgate@meta.ua

**Рецензент**: Володимир Хома, д.т.н., проф., Опольський політехнічний Університет, Ополе, Польща
xoma@wp.pl

Надійшло: Березень 2020.

***Анотація:*** *В роботі досліджено основні характеристики Інтернет-травлі (кібертравлі або кібербулінгу). Розглянуті основні особливості проявів цього явища. Виконано аналіз існуючих видів кібербулінгу і їх окремих характеристик. Розглянуто приклади законодавчих актів різних країн щодо протидії кібербулінгу. За результатами огляду наявної нормативно-правової бази різних країн, зроблений висновок про істотний дефіцит відповідних норм законів. Підкреслено, що в сучасному світі жертвою Інтернет-травлі може стати будь-хто. При цьому, ризик стати жертвою кібербулінгу практично не залежить від будь яких факторів (наприклад, фінансового становища жертви, її віку, статі, соціального стану та ін.). Відзначено, що комунікації, які здійснюється в кіберпросторі надають користувачам можливість заздалегідь та ретельно вибирати інформацію про себе, яку вони хочуть оприлюднити. У більшості випадків це сприяє тому, що люди демонструють тільки свої «позитивні» сторони (наприклад, при спілкування в чатах). В результаті цього у мережевих співрозмовників часто виникають помилкові взаємні симпатії, внаслідок чого вони необачно вступають в довірчі відносини. Таким чином відбувається ідеалізація партнера по мережевої комунікації, та будь-яка його інформація починає сприйматися набагато більш чуйно, аніж при прямій «фізичній» комунікації. Цей ефект з «успіхом» використовується при проведенні акцій кібербулінгу, коли одна людина спочатку викликає максимальну довіру іншого, а потім різко змінює тактику спілкування, стаючи немотивовано віроломним і агресивним. Підкреслено, що явище кібербулінгу є дуже недооціненим і тому являє собою серйозну проблему.*

*Виконано короткий огляд існуючих технологій і засобів протидії цьому явищу. Проведено порівняння їх ефективності. Систематизовано критерії, яким повинна відповідати сучасна і ефективна технологія протидії кібербулінгу. Представлені приклади вдалої реалізації захисту користувачів у деяких найбільш популярних соціальних мережах. Акцентовано увагу на тому, що для протидії кібербулінгу, в теперішній час, в переважній більшості випадків, використовують технології захисту на основі обмежень. Головна мета відповідних засобів захисту полягає у тому, щоб максимально локалізувати небажаний контент (з точки зору існування ознак кібербулінгу).*

*За результатами роботи стверджується, що і в подальшому кібербулінг буде тільки поширюватись. Це обумовлено постійним збільшенням чисельності користувачів нових мережевих сервісів та онлайн майданчиків для спілкування. Висловлено думку, що для активної протидії та ефективного захисту від кібербулінгу потрібно впровадження комплексних організаційно-технічних заходів. На завершенні запропонована загальна оцінка подальшого розвитку кібербулінгу і шляхів вдосконалення відповідних інструментів протидії.*

***Ключевые слова:*** *булінг; кібербулінг; соціальна мережа; інформаційна безпека; контент; захист; технологія; мережева безпека.*

## 1 Вступ

Наш час характеризується стрімким та багатовекторним розвитком інформаційно-комунікаційних технологій, що суттєво змінює характер виробничих, соціально-політичних і морально-етичних відносин, які, в своїй сукупності, формують нові критерії норм поведінки не тільки у сучасному суспільстві, а й у кіберпросторі. Такі речі як смартфон і комп'ютер стали невід'ємною частиною буденного життя сучасної людини. Інтеграція всіх існуючих пристроїв в єдине інформаційне середовище, за рахунок використання глобальної мережі Інтернет, надання функцій мобільності її абонентам та практично безперервний зв'язок, фактично створили нову реальність. Ця реальність спроможна надати людству нову якість життя але, з іншого боку, несе в собі і нові загрози, та фактори ризику нових форматів, і змісту. Так, наприклад, наразі Інтернет використовується майже у всіх сферах життя сучасної людини: - для роботи, навчання, розваг, забезпечення побутових потреб, підтримання соціальних контактів і багато чого іншого. Проте, поряд з великою кількістю позитивних сторін, нові інформаційні технології (ІТ- технології) мають і свої, приховані від непідготовленої людини,

загрози [1]. В цьому сенсі, однією з найгостріших проблем, яка пов'язана з широким використанням нових можливостей ІТ-технологій, є загроза потенційного зіткнення людини (*користувача будь якого онлайн сервісу або пристрою, що має з'єднання з мережею*) з агресивними нападками окремих представників мережевої спільноти, що називають кібербулінгом.

Кібербулінг – це форма залякування, яке відбувається, в тому числі, за рахунок можливостей Інтернет технологій, та використання різних електронних пристроїв (смартфонів, планшетів тощо). Кібербулінг може реалізуватися за допомогою соціальних мереж, електронної пошти, додатків для обмінну миттєвими повідомленнями, текстових повідомлень, форумів, комп'ютерних ігор та багато чого іншого. Принциповим є те, що будь-яке онлайн середовище, яке дозволяє обмінюватися даними, може стати технічною платформою для здійснення Інтернет-травлі [2].

Свого найбільшого поширення кібербулінг набув у молоді, але не слід вважати, що жертвою Інтернет-травлі можуть бути лише представники молодого покоління. В сучасному світі жертвою Інтернет-травлі може стати будь-хто, і це не залежить а ні від фінансового статку, а ні від віку, а ні від статі, соціального стану та іншого.

Актуальність даної роботи обумовлена тим, що по мірі поширення новітніх віртуальних сервісів та комунікаційних технологій, явище кібербулінгу теж набуває все більших масштабів та форм його проявів. Його наслідки можуть бути найрізноманітніші, від тяжкої психічної травми конкретної людини до порушення поточного балансу відносин (*виробничих, соціальних, культурних та ін.*) в рамках цілих соціальних груп або окремих співтовариств. Тому знати цю проблематику та володіти відповідними знаннями щодо можливостей протидії цьому явищу, є важливим напрямком фахових компетенцій сучасних фахівців з інформаційної безпеки (ІБ).

## 2 Основні визначення і характеристики кібербулінгу

В наслідок стрімкого розвитку ІТ-технологій безліч, раніше звичних явищ, в теперішній час, набувають нових форм та масштабів можливих наслідків. Це стосується і питань еволюції прояву взаємної людської агресії, яка існує у віртуальному просторі, і як наслідок, формування певних поведінкових норм мережевої етики, котрі тісно пов'язані з проблематикою протидії можливим наслідкам мережевої агресії та віртуального маніпулювання особистістю.

Булінг (*тобто знущання*) [3] – різновид насильства; навмисне, що не носить характеру самозахисту і не є санкціонованим нормативно-правовими актами держави, довготривале (*повторюване*) фізичне чи психологічне насильство з боку індивіда чи групи, які мають певні переваги (*фізичні, психологічні, адміністративні тощо*) стосовно індивіда, і що відбувається переважно в організованих колективах з певною особистою метою (*наприклад, бажання заслужити авторитет у бажаних осіб і т.і.*).

Булінг був проблемою з найдавніших часів. Хоч більшість людей і намагається жити у цивілізованому, мирному суспільстві, але, нажаль, є люди, які хочуть виплеснути свою агресію на того, хто слабший за них. З часом тривіальний булінг у реальному житті переріс у нове явище, яке називається кібербулінг. Тобто знущання у віртуальному світі.

### 2.1 Джерела походження явища булінгу

Практично неможливо точно сказати коли люди почали проявляти психологічну агресію один до одного. Термін булінг не був публічно визнаний доти, поки відома англійська газета не зробила статтю з даною темою. У 1862 році, через сімдесяти двох років публікацій щотижнева газета «*The Times*» написала свою першу розповідь про булінг [4]. У той час булінг сприймався багатьма як нормальна поведінка. Проте, після того як це явище стало більш поширеним, воно стало привертати до себе все більше уваги дослідників, які хотіли дізнатись більше про ймовірні причини, мотиви та можливі наслідки.

Найбільш значущий момент (*в історичному сенсі*) булінга був у середині 70-х років минулого століття. Професор психології *Dan Olweus* першим провів інтенсивне дослідження явища булінгу серед учнів, використовуючи при цьому свої особисті методи дослідження. Слід

зазначити, що зусилля Олвеуса справили великий вплив на зменшення рівня шкільного насилля та допомогли підвищити безпеку учнів у школі [5].

Розглядаючи явище булінгу принципово важливо підкреслити, що знущання можуть траплятися у різному віці, у різних місцях, у різних соціальних та техногенних середовищах, та як свідчить реальність, з використанням різноманітних технологічних здобутків.

Хоч кожен окремий випадок булінгу по своєму унікальний, у більшості ситуацій є три породжуючи фактори [6]:

1. *Намір*. Випадкова образа, скоріш за все, не є булінгом. Ті, хто знущаються свідомо, добре розуміють, що саме роблять вони, і тому шкода буде навмисною;
2. *Дисбаланс влади*. У більшості випадків кривдник має більшу владу. І зовсім не означає, що кривдник обов'язково більше або сильніше за жертву. Він може, наприклад, займати більш високий пост на роботі, або бути вихідцем з багатої родини тощо;
3. *Повторювання*. Одноразовий образливий вчинок по відношенню до людини не є булінгом. Булінг це навмисна дія, яка згодом буде систематично повторюватись.

Повертаючись до історії слід відмітити, що наприкінці 90-х років XX-го сторіччя наслідки залякування досягли свого піку [7] і прийняли ще один негативний еволюційний поворот. Завдяки поширення доступу до мережі Інтернет, багато підлітків почали використовувати кіберпростір як майданчик для булінгу [5]. Враховуючи те, що в сучасному світі переважна більшість людей для спілкування та роботи використовують дуже широкий спектр різних гаджетів, то явище кібербулінгу набуло нових якостей, поширилось у віртуальному світі і стало великою проблемою, яка безпосередньо впливає не тільки на характер взаємовідносин людей в сучасному мережевому просторі, але і в їх реальному житті.

Офіційний науковий термін «кібербулінг» ввів канадський педагог *Bill Belsey*. Згідно його тлумачення, кібербулінг – це навмисна, повторювана ворожа поведінка окремих осіб чи груп, маючих намір спричинити шкоду іншим, використовуючи при цьому інформаційні і комунікаційні технології [8]. В сучасному розумінні кібербулінг став поширеним явищем у середині 2000-х років, коли звичайні смартфони, як інтегрований засіб мобільних комунікацій, набули популярності та стали повсякденним компонентом сучасного життя.

### 2.1.1 Особливості та мотивації кібербулінгу

Як було зазначено вище, кібербулінг – особливий вид Інтернет комунікації. Серед головних особливостей [9] даного типу комунікацій слід виділити наступні:

- *Безперервність*. Комунікація в мережі Інтернет (*надалі мережі*) майже не має обмежень за часом: - користувачі можуть у будь-який час «вийти» з діалогу, та в будь-який час його продовжити;
- *Мультіконтентність*. Користувачам мережі надаються багаточисельні інструменти і засоби спілкування: - текст, графічні зображення, фото- й відеоматеріали, аудіо контент і тому подібне;
- *Анонімність*. Один з ключових факторів кібербулінгу. Будь-яка людина може реєструватись в мережі під будь-яким неіснуючим образом (*віртуальним аватаром*), який приховує реальну особистість. Це дозволяє деяким користувачам мережі виключити чинник персональної відповідальності за можливі наслідки своїх дій у віртуальному просторі.
- *Опосередкованість*. Інтернет комунікації, в своєї більшості, є непрямим діалогом між її учасниками, котрі часто не знайомі, безпосередньо не бачать один одного, та не можуть використовувати такі невербальні засоби комунікації як: - жести, міміка тощо (*виключенням є відеоконференцзв'язок, але це є не типовий спосіб здійснення кібертравлі*).

Зазначені особливості віртуальної комунікації приваблюють потенційних агресорів, які почувають себе в умовах мережі дуже безпечно та комфортно. Навіть, якщо у реальному житті вони нікому і не завдають шкоди, то в разі використання можливостей IT- технологій, внаслідок помилкового враження про відсутність контролю та безкарність, такі люди можуть почати проявляти свою агресивну сутність по відношенню до інших представників мереже-

вої спільноти. Можна стверджувати, що кібербулінг дозволяє мережевому нападнику уникнути відповідальності, так як, не застосовуючи пряме насильство над жертвою, він в більшості випадків, зможе ухилитись від особистої відповідальності. Більш того, для деяких кіберзлочинців вирішальним плюсом є саме те, що булінгом можна займатись не змінюючи привичного їм образу життя та практично з любого місця, де є доступ до мережі.

З досліджень на цю тему слід звернути увагу на роботи доктора психологічних наук *Al Cooper* [10]. У одній зі своїх робіт він виділив три найпривабливіші, на його думку, аспекти Інтернет-комунікації та назвав їх принципом «Потрійного А» (*від анг. «Triple A» – Anonymous, Accessible and Affordable*): 1 – анонімність; 2 – доступність; 3 – низька ціна.

Про *анонімність* вже було сказано вище. Саме цей аспект робить булінг дуже привабливим для його виконавця. Тут спрацьовує так званий «*ефект дистанціювання*», який передбачає, що мережевий агресор, який знаходиться на відстані від своєї жертви, робить більш жорстокі речі, ніж при звичайному прямому спілкуванні [11].

*Доступність* підключення до Інтернету, також значно полегшує процес кібербулінгу. На сьогоднішній день доступ до Інтернету є майже усюди (*високошвидкісні Ethernet та безпровідне з'єднання*) [1]. Причому, завдяки мобільним пристроям і високошвидкісним бездротовим мережам, цей доступ користувачі отримують практично безперервно [12, 13].

*Низька ціна* – вартість участі в Інтернет комунікації. При наявності у людини комп'ютера або будь-якого мобільного пристрою з доступом до мережі (*корпоративною або напряму з Інтернет*), практично забезпечує його технічну готовність до здійснення потрібних віртуальних комунікацій.

Як вже було зазначено вище, люди які вдаються до кібербулінгу, у реальному житті частіше за все не проявляють ніяких агресивних вчинків. При цьому кібербулінг, в першу чергу, приваблює тих людей, хто бажає миттєво змінити в віртуальному світі свій реальний стан, на іншу, більш сильну або привабливу позицію (*в будь-яких розуміннях*). Перш за все таких людей приваблюють переваги комп'ютерно-опосередкованої комунікації, які описані у «Гіперперсональній моделі комунікації» [14]. Завдяки визначеним особливостям Інтернет комунікації (*анонімність, знижені соціальні рамки, можливість попереднього планування дій, можливість ретельно обміркувати свою відповідь тощо*) онлайн комунікація стає ідеальним засобом для особистої презентації у навмисно перекрученому вигляді.

Комунікація, що здійснюється в кіберпросторі надає користувачам можливість ретельно вибирати інформацію про себе, яку вони хочуть надати в широкий доступ (*оприлюднити*). У більшості випадків це сприяє тому, що люди показують тільки свої «позитивні» сторони (*наприклад, спілкування в чатах*). В результаті цього у співрозмовників часто виникають симпатії один до одного, та вони вступають в довірчі відносини. Таким чином відбувається ідеалізація партнера по мережевої комунікації, і його інформація починає сприйматися набагато більш чуйно, аніж при прямій «фізичній» комунікації. Цей ефект з «успіхом» використовується в кібербулінгу, коли одна людина спочатку викликає максимальну довіру іншого, а потім різко змінює тактику спілкування, стаючи агресивним. В цьому сенсі онлайн комунікація дозволяє нападнику заздалегідь обмірковувати свої наступні дії (*тип контенту і форму його подання*) і, в певній мірі, контролювати часові параметри атаки (*інтенсивність видачі контенту, тривалість пауз та ін.*).

### 2.1.2 Компоненти кібербулінгу

Кібербулінг складається з декількох обов'язкових компонентів (*учасників процесу*), що впливають на те, як саме відбувається кожен конкретний прояв булінгу (*окремі властивості та чисельність кожної з груп*). Практично у кожному випадку учасники кібербулінгу поділяються на три категорії: – агресор, жертва і спостерігач (Рис. 1). Кожний з цих елементів може бути представлений, як в однині, так і в множині, тобто процес може відбуватися в групах. А сам процес може бути реалізований миттєво або бути пролонгованим у часі.

*Агресор* – людина (*або група*), яка навмисно ображає, несе загрозу чи агресію, щоб визвати страх чи страждання у інших.

*Жертва* – той (*група*), кого (*групу*) переслідує агресор. Жертви не можуть легко захищати себе і, по ряду причин, є більш слабкими ніж агресор.

*Спостерігач* – особа (чи група), яка є свідком інциденту, але не є його прямим учасником. В окремих випадках спостерігачі можуть оказувати підтримку жертві, реагуючи проти агресора. Але, вони, також, можуть посилювати «страждання» жертви, що були завдані агресором, опосередковано підтримуючи їх дії.

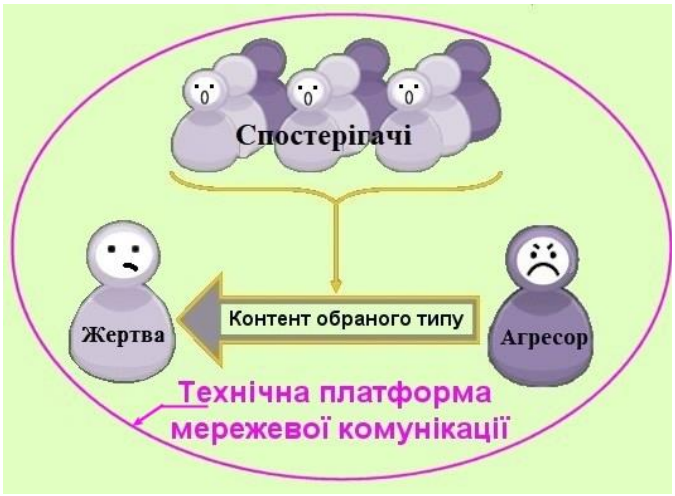



Рис. 1 – Складові процесу кібербулінгу

*Платформа*, на базі якій відбувається кібербулінг, також є дуже впливовим компонентом у цьому явищі. У загальному випадку платформа являє собою сукупність програмно-технічних засобів, а в деяких випадках і каналів зв'язку, за допомогою яких забезпечується функціональна взаємодія її абонентів. Так наприклад, на сьогоднішній день, соціальні мережі є основними комунікаційними платформами, які розгорнути на базі мережі Інтернет.

Соціальна мережа – це Web-платформа для побудови соціальних відносин між людьми зі схожими інтересами і діяльністю [15]. Соціальні мережі являють кожного зі своїх учасників через її особисту сторінку (*профіль, акаунт*), яка переважно містить особисту інформацію та інтереси користувача. Вони також надають користувачам засоби для взаємодії, наприклад, за допомогою миттєвих повідомлень. Сайти соціальних мереж різноманітні і пропонують різні види діяльності, такі як: обмін фото та відео, публікація коментарів та відстеження дій інших користувачів в мережі.

Ще одним обов'язковим елементом процесу кібербулінгу є *контент* та метод, за допомогою яких відбувається кібербулінг. Це може бути відео або фото зображення, комп'ютерна анімація (*включаючи комп'ютерну гру*), статичний текст, будь-яка інфографіка та ін.

Технічні можливості кожної платформи (*наприклад, підтримка можливості ведення чату, можливість передачі мультимедійного контенту, підтримка мобільності абонентів та ін*.) мають істотний вплив на організацію процесу цькування. Також, свої особливості *(наприклад, неспівпадіння видів контентного наповнення або часові параметри комунікації*) має і процес підтримки комунікацій для користувачів різних платформ (*кроссплатформна взаємодія*). Наявність різниці в часі підтримки з'єднання (*різниця в тарифікації послуг в межах кожної платформи*) та забезпечення мобільності абонентів (*доступ до бездротових мереж*) суттєвим образом, можуть змінювати конфігурацію процесу кібербулінгу та, в певній мірі, його наслідки. Таким чином, комбінація всіх зазначених обставин та факторів, обумовлює потенційне різноманіття можливих реалізацій кібербулінгу.

### 2.1.3 Види кібербулінгу

Наразі неможливо точно сказати які є види кібербулінгу. Через те, що це явище відносно нове, та постійно і швидко розвивається, різні дослідники по-різному класифікують прояви кібербулінгу. Ще однією причиною цього є те, що Інтернет-травля з кожним роком все більше поширюється, і разом з тим набуває нових форм і проявів. У межах даної роботи розглядаються тільки два різних трактування існуючих видів кібербулінгу: - точка зору, що поєднує погляди фахівців західних країн світу та сукупна точка зору вітчизняних фахівців за даною проблематикою.

У західній класифікації *Nancy E. Willard*, автор видання «*Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress*» (2007), виділила та організувала кібербулінг у сім різних категорій [16]:

1 – флеймінг (*Flaming*);
2 – домагання (*Harassment*);
3 – поширення чуток (*Denigration*);
4 – кіберсталкінг (*Cyberstalking*);
5 – самозванство (*Impersonation*);
6 – брехливість (*Outing* & *Trickery*);
7 – соціальна ізоляція (*Exclusion*).

Розглянемо кожен вид докладніше.

*Флеймінг*. Під цим видом Інтеренет-залякування розуміють короткі суперечки між учасниками онлайн комунікації. Це можуть бути різноманітні гнівні та образливі коментарі, повідомлення і т.д. Місцем для флеймінгу частіше за все виступають «публічні» майданчики Інтернету (*наприклад, форуми, чати і т.і.*). Часто, такий вид кібербулінгу переростає в затяжну «війну» між його учасниками. Хоч і здається, що флеймінг трапляється між рівними людьми, але інколи, він також може перетворитися на затяжний психологічний нерівноправний терор. Наприклад, це трапляється тоді, коли особа не знає скільки людей її підтримує, і чи буде її позиція підтримана найавторитетнішими учасниками даної комунікації.

*Домагання* (*харасмент*), передбачає регулярні виснажливі нападки на людину. Прикладом може бути постійне надсилання великої кількості образливих електронних листів, текстових повідомлень (*в т.ч. SMS-повідомлень з використанням можливостей платформи стільникового мобільного зв'язку*), електронних повідомлень із неприємними зображеннями і т. ін. Також до цієї категорії можна віднести численні телефонні дзвінки. Відмінність від флеймінгу полягає у тому, що в цьому випадку кількість повідомлень значно більше, і приходять вони, частіше, в односторонньому порядку.

Слід відмітити, що нещодавно з'явилась нова форма харасменту – гріфінг (*griefing, з англійської «grief» - горе, смуток*) [17]. Цей вид булінгу передбачає спрямоване притиснення одного з учасників комп'ютерної гри. Агресори у даному випадку, називаються гріфери. Це група гравців, метою яких є руйнування ігрового досвіду інших учасників гри. При цьому принциповим є той факт, що перемога у грі вже не є пріоритетом у даних гравців.

*Поширення чуток*. Ця категорія кібербулінгу передбачає навмисне розповсюдження неправдивої образливої інформації за допомогою електронних засобів комунікацій. Треба підкреслити, що цей вид кібербулінгу передбачає те, що агресор знає, що інформація є заздалегідь неправдивою. При цьому в якості такої інформації може виступати будь-який доступний контент. Для цього агресори створюють так звані «книги для критики» (*Slam Books*), головним сенсом котрої є розміщення образливих жартів про жертву, а також різноманітних наклепів. Потім, з таких книг обираються «мішені», на котрих інші будуть фокусувати свою агресію. Також прикладом поширення чуток є розсилка різноманітних образливих списків (*наприклад, «хто є хто»*).

*Кіберсталкінг* це скритне вистежування людини, і тих, хто знаходиться поряд із нею. Як правило це робиться анонімно, беручи за мету різноманітні злочинні дії. За допомогою різноманітних сервісів мережі Інтернет злочинець відстежує користувачів-жертв, дізнається про час, місце і всю іншу інформацію, що необхідна для подальшого скоєння злочину.

*Самозванство*, тобто втілення в іншу особу, це коли агресор присвоює собі повноваження або ознаки іншої людини, використовуючи при цьому акаунти жертви у соціальних мережах, пошті, блогах, різноманітних месенджерах і т. і. Для цього злочинець якимось чином *обов'язково* повинен заволодіти автентифікаційними даними жертви, а після нелегітимного проникнення у необхідний мережевий профіль жертви, злочинець здійснює спланована негативну комунікацію, тобто надсилає іншим людям образливу інформацію. Після того, як з адреси жертви (*без її відому*) відбулася відправка злочинних повідомлень, трапляється так звана «хвиля зворотних зв'язків».

При цьому розгублена жертва не розуміє у чому справа. Таким чином, агресор робить провокацію, залишаючись, при цьому, непомітним для всіх сторін здійсненої їм фіктивної комунікації.

*Брехливість* передбачає те, що злочинець якимось чином отримує доступ до чутливої інформації про особу, а потім несанкціоновано розповсюджує її у мережі. У цьому разі за мету агресор ставить знищення репутації жертви, та спробу зміни ставлення до неї інших людей.

Різновидом *брехливості* є секстінг (*Sexting*). До нього відноситься поширення особистих фото відвертого характеру, без згоди жертви, а також повідомлення інтимного змісту за допомогою різних засобів зв'язку. Нажаль, такі дані залишаються у мережі надовго що створює загрозу кар'єрного, психічного і фізичного насилля над жертвою.

*Соціальна ізоляція* є особливо тяжкою категорією булінгу (*особливо для підлітків*). Так як людина є соціальною істотою, то її виключення з певного соціуму, в переважній більшості випадків, може сприйматись дуже тяжко. У онлайн середовищі ізоляція теж несе дуже неприємні наслідки. Ізоляція можлива у будь-яких середовищах, де можливо сформувати різноманітні списки (*наприклад, «найкращі друзі» у соціальній мережі Instagram*), заблокувати користувача, чи сформувати список небажаних повідомлень. В цьому сенсі, відсутність швидкої відповіді на електронне повідомлення теж може бути віднесено до соціальної ізоляції.

В контексті вищезазначеного слід підкреслити, що у деяких фахівців з окресленої проблематики є дещо інша точка зору. Так, наприклад, думка психолога Галини Солдатової [18] стосовно існуючих різновидів кібербулінгу відрізняється від загальноприйнятих критеріїв. Зі своєї сторони вона виділяє три основні види Інтернет-травлі: 1 – флеймінг (*Flaming*); 2 – хейтінг (*Hate*); 3 – тролінг (*Cyber trolls*).

*Хейтінг* передбачає негативні коментарі і неконструктивну критику в адресу об'єкту травлі без обґрунтування або запиту. У час, коли великого поширення здобув такий рід діяльності як блогерство (блогер – людина яка веде свій он-лайн щоденник, у який записує тексти на різні тематики, публікує фото- і відео-контент), хейтінг став дуже критичною проблемою. Слід особливо підкреслити, що даний вид кібербулінгу передбачає саме неконструктивну критику. Це можуть бути коментарі про зовнішність людини, її діяння та багато іншого.

*Тролінг* (*кепкування*) передбачає провокування жертви до діалогу, використовуючи в переважної більшості насмішки чи образливі коментарі. Тролі (*нападники*) можуть бути відносно нешкідливими (*одноразові жарти у коментарях*), але можуть збиратися у цільові групи і водночас атакувати жертву, використовуючи для цього всі наявні ресурси та засоби. За статистичними даними [19], близько чотирьох з десяти користувачів мережі хоч раз принижували чи ображали когось в Інтернеті, а тих, хто був свідком нападу тролей у рази більше.

Кібербулінг все частіше призводить до трагічних випадків. Не розуміючи, що їх вчинки можуть призвести до дуже серйозних наслідків, злочинці стають все більш вигадливими і злими. У США навіть з'явився новий термін «буліцид». Віз означає загибель людини внаслідок булінгу.

### 2.2 Аналіз статистичних даних щодо кібербулінгу

Щоб наглядно підтвердити всю актуальність проблеми кібербулінгу, потрібно звернутися до відповідних статистичних даних. Варто зауважити, що, нажаль, більшість статистичних даних стосуються лише підлітків та дітей.

Задля підтвердження актуальності проблеми поширення кібербулінгу, звернемося до відповідних статистичних даних [20-21]:

– один з трьох підлітків у 30 різних країнах стверджує, що він був жертвою булінгу в Інтернеті, при цьому кожен п'ятий повідомив, що пропустив школу саме через кібербулінг;

– 37 % підлітків у віці від 12 до 17 років піддавалися знущанням в Інтернеті, а у 30 % опитаних, це було не одноразово;

– 23 % студентів повідомили, що вони зробили щось погане по відношенню до іншої людини в Інтернеті;

– 27 % студентів піддавалися зовнішнім образам в мережі;

– 60 % підлітків стали свідками знущань в Інтернеті, але більшість з них не втручалася в цей процес;

– тільки 1 з 10 постраждалих підлітків повідомили дорослим про ці інциденти.

На рис. 2-3 приведено результати опитування підлітків щодо кібербулінгу, які були отримані організацією *Unicef* [22]. Аналіз відповідних даних дозволяє зробити висновок: - в Україні 21,5 % школярів були жертвою Інтернет-травлі, а 4,1 % з них піддаються постійному кібербулінгу (*один чи декілька разів на тиждень*).

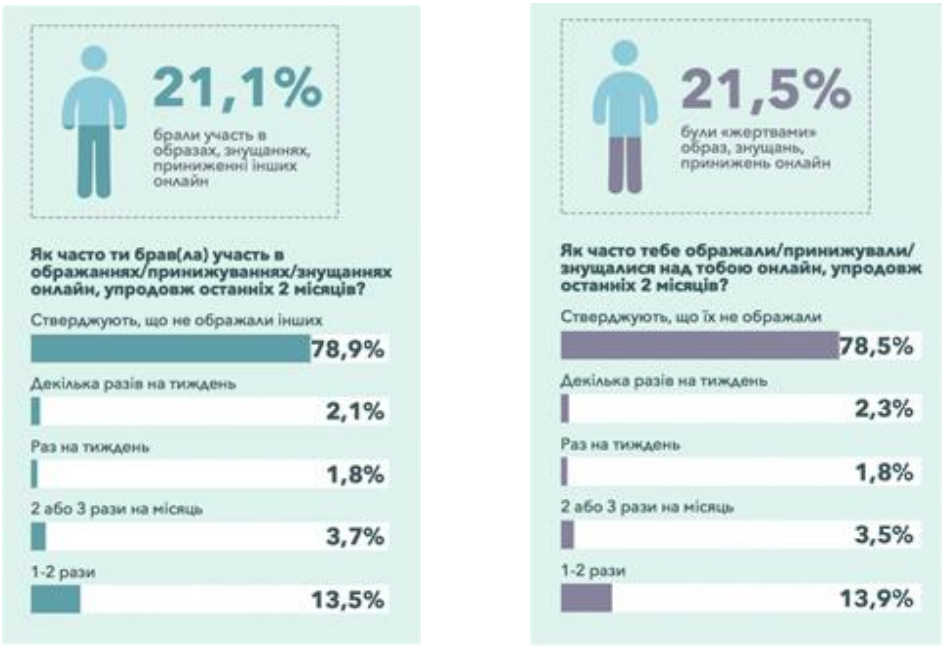



Рис. 2 – Дані щодо кібербулінгу серед підлітків України


Рис. 3 – Час, який підлітки витрачають на соціальні мережі

### 3 Особливості законодавчого врегулювання кібербулінгу

За результатами аналізу найбільш показових прикладів боротьби з кібербулінгом на законодавчому рівні (США [23], Канада [24], Швеція [25], Франція [26], Великобританія [27], Іспанія [28], деякі країни СНД [29-31], Україна [32-36], Південна Африка, Японія, Сінгапур та ін. [37]), можна стверджувати наступне:

1 – в тих випадках коли відсутні прямі норми, що стосуються булінгу і кібербулінгу, такі випадки можуть бути трактовані, як дискримінаційні домагання, якщо вони засновані на расі, кольору шкіри, релігії, віку, статі чи інвалідності тощо. В цьому разі, інколи, для злочинців можуть бути висунуті федеральні звинувачення у переслідуванні (*наприклад, в США*). При цьому, якщо булінг переростає у переслідування, то навчальні заклади, які отримують федеральні (*державні*) кошти, зобов'язані вирішити дану проблему;

2 – в разі федеративного устрою держави, існує розмежування відповідальності на регіональному та федеральному рівнях. Причому баланс відповідних законодавчих актів у кожній окремій країні має свою специфіку. Наприклад, у США кібербулінг, у першу чергу, підпадає під закони штатів. При цьому у більшості штатів у правоохоронних органах навіть є спеціальні підрозділи по боротьбі з кіберзлочинністю [23];

3 – у разі існування відповідної законодавчої бази, ці закони часто поділяються на ті, що стосуються дітей та підлітків, а також закони, які захищають дорослих жертв кібербулінгу чи жертв будь-якого віку [23];

4 – в залежності від конкретної країни, відповідальність за даний тип злочину (*булінгу і кібербулінгу*) може передбачати собою позбавлення волі та/чи штраф у відповідному розмірі;

5 – в більшості країн світу працівники навчальних закладів повинні повідомляти про будь-які відомі їм випадки булінгу, що сталися в їх установах;

6 – в більшості країн з явищем кібербулінгу борються не тільки коли злочин вже відбувся, але й активно розвивають профілактичні міри щодо його запобіганню;

7 – в разі існування відповідної законодавчої бази, її норми, в рівній мірі стосуються випадків кібербулінгу, як у навчальних закладах, так і на робочому місті (*виробництві*);

8 – законодавчі акти ряду країн передбачають норму, яка спонукає свідків проявів кібербулінгу повідомити про це, так як в іншому випадку вони можуть бути притягнуті до відповідальності [24];

9 – в тих країнах де не існує юридичного визначення явища кібербулінгу, використовують діючі закони, норми яких можуть бути застосовані до даних випадків [25, 32]. Таким чином використовуються окремі правові акти, котрі розглядають склад правопорушень, які містять певні ознаки даних явищ;

10 – норми законів деяких країн вимагають, щоб Інтернет провайдери передавали контактні дані осіб, що здійснюють дії із характерними ознаками Інтернет травлі;

11 – ефективною мірою протидії є деанонімізація користувачів мережевих сервісів. Наприклад, в Китаї є закон, згідно якому люди повинні реєструвати в мережі свої реальні імена, завдяки чому вони стають більш відповідальні за свої слова і дії у мережі;

12 – ефективною технічною мірою протидії кібербулінгу є допуск неповнолітніх в Інтернет тільки при наявності на їх гаджетах встановлених програмних фільтрів (*наприклад, в Японії де діє Закон «Про підтримку здорового Інтернет-середовища для молоді»*).

Таким чином, закони, які спрямовані на протидію кібербулінгу, є відносно новими і тому не дуже поширені у світі. Через це в більшості країн, при визначенні заходів покарання для особи, яка причасна до кібербулінгу, використовують норми інших законів. При цьому певною проблемою є те, що та невелика кількість законів, які все ж таки приймаються, націлені на протидію кібербулінгу переважно серед неповнолітніх. Це породжує певний правовий дисбаланс, так як це явище охоплює всі вікові, соціальні та етнічні групи.

## 4. Технології і засоби протидії кібербулінгу

Станом на сьогоднішній день, практично існують три основні шляхи протидії проявам кібербулінгу: 1 – соціальний; 2 – законодавчій; 3 – технічний. У попередньому пункті були розглянуті законодавчі аспекти протидії кібербулінгу, в межах цієї частини основна увага буде приділена технічній стороні питання що розглядається.

Слід підкреслити, що, як і у випадку законодавчих ініціатив, цьому напряму, також, приділялося недостатньо уваги. Однак на сьогодні, із-за значного поширення цього явища, почалася інтенсифікація робіт і за технічним напрямком. Вдалим прикладом цього може бути нідерландська розробка *Friendly ATTAC* [38], яка спеціально націлена на поведінку свідків кібербулінгу. Базисом цього рішення є ствердження, згідно якого соціально вірна реакція свідків даного різновиду злочину, може зменшити масштаб цькування і завдану ним шкоду.

На даний час відомо багато різних технологій захисту даних та забезпечення конфіденційності роботи користувачів в мережі [13, 39-40], але не всі вони підходять для захисту від кібербулінгу. Як вже згадувалося раніше, наразі немає вузькоспеціалізованих програмно-апаратних рішень для ефективного захисту від цієї загрози. Тому розглянемо деякі види технологій мережевого захисту, які у той чи іншій мірі можуть бути корисними у боротьбі з цькуванням у мережі.

Для протистояння булінгу в Інтернет використовують технології захисту на основі певних обмежень. Їх головна мета полягає у тому, щоб локалізувати різноманітний небажаний контент (*з точки зору існування ознак кібербулінгу*). В цьому сенсі слід виділити наступні техно-

логії [41]: – аналіз контенту та поведінки; – фільтрація; – моніторинг; – блокування небажаних користувачів (*контактів*); – звітність; – перевірка віку/особистості (*в якоїсь мірі повноважень*); – освітні технології. Аналіз специфіки роботи цих технологій дозволяє виділити один спільний недолік, а саме: - їх використання сприяє порушенню конфіденційності учасників процесу комунікацій. В цьому контексті слід зауважити, що обмежувальні технології можуть порушувати право людини на свободу інформації та вираження особистої думки.

Перед тим як розглянути деякі із існуючих засобів протидії проявам кібербулінгу, систематизуємо бажані характеристики [42], які повинні забезпечувати відповідні технології захисту (Табл. 1).

Таблиця 1 – Бажані характеристики технологій протидії

| № | Характеристика | Пояснення |
|---|---|---|
| **1** | **Універсальність** | Технологія повинна враховувати існуючи види мережевої травлі, середовища поширення і методи, за допомогою яких це відбувається. |
| **2** | **Безперервність** | Технологія потрібна забезпечити цілодобовий захист у реальному часі. |
| **3** | **Добровільність** *<br><br>* - *в сенсі її використання користувачем.* | Захист повинен грунтуватися на добровільному бажанні користувачів використовувати ці технології (*засоби*).<br>Якщо жертви *(можливо і свідки*) мотивовані використовувати захист, то агресор ніколи не буде брати участь в цьому добровільно, тому що булінг це виключно навмисний акт. |
| **4** | **Конфіденційність** | Технологія не повинна порушувати конфіденційність людини (*або мати чітко декларовані обмеження*). |
| **5** | **Транспарентність** **<br><br>** - *Свобода волевиявлення.* | Кожна людина має право на свободу самовираження, тому технологія повинна забезпечувати (*не порушувати*) баланс інтересів між правами кожної окремої особистості (*користувача комунікаційної платформи*) та прийнятими нормами суспільної моралі. |

Варто зауважити, що такі характеристики, як «Конфіденційність» та «Транспарентність», в кожному окремому випадку, є достатньо дискусійними і, як наслідок, складно формалізуються (*з точки зору синтезу відповідних алгоритмів роботи системи захисту*). В цьому випадку особисте життя людини та її право на свободу вираження повинні бути ретельно збалансовані з потенційними перевагами технології для захисту від кібербулінгу.

### 4.1 Огляд технологій протистояння кібербулінгу

Коротко розглянемо основні з існуючих технологій Інтернет-безпеки та визначимо особливості їх застосування для боротьбі з кібербулінгом [42].

*Аналіз контенту та поведінки.* Аналіз контенту та поведінки практично зводиться до процедур автоматичного вилучення індикативної інформації з будь-яких типів даних. Теоретично, ця технологія може бути вдало використана для виявлення кібербулінгу. Проте, деякі результати схожих задач показують, що автоматично дуже складно розпізнати різні види травлі в різних видах контенту (*складність формалізації прийняття рішення та висока обчислювальна складність морфологічного аналізу контенту*). Так наприклад, *Pendar N.* статистично дослідив здатність автоматично розпізнати сексуальні домагання у повідомленнях, де показники доходили до 95 % випадків [43]. Проте, по-перше, набори даних що використовувались у експерименті були невеликими (*701 розмова*). По-друге, у розмовах, які використовувались для дослідження було зрозуміло, що людина хоче причинити шкоду (*зазвичай, таке трапляється не часто*). Тому, перед тим як цей метод можливо буде використовувати в якості практичного захисту від кібербулінгу, його треба ще значно удосконалити.

Технологія аналізу контенту та поведінки працює у реальному часі, і може бути застосована як добровільно, так і ні. Оскільки для аналізу мережевого контенту потрібно зберігати та інтерпретувати дані про поведінку всіх учасників комунікацій (*що може бути розцінено як обробка особистих даних*), то конфіденційність цих користувачів, потенційно, може постраждати. Хоча виявлення неналежних даних і не обмежує свободу вираження, однак дії, які приймаються після цього, можуть. Наразі, у численних програмних рішеннях, так званого «батьківського контролю» використовуються деякі види аналізу Інтернет-ризиків (*наприклад: - контентні, комунікаційні, споживчі та електронні ризики*) [44-45].

*Фільтрація*. Програмне забезпечення (ПЗ) для Web-фільтрації блокує доступ к Web-ресурсам з небажаним контентом. Методи фільтрації включають в себе «дозволені списки» (*списики Web-сайтів, які дозволено відвідувати*), «заборонені списки» (*списики ресурсів, доступ до яких заблоковано*) та аналіз контенту (*відповідний алгоритм, що приймає рішення, наприклад, на основі появи певних ключових слів і т.і.*). У всіх ПЗ даного типу є два спільних недоліки: – це недостатнє блокування (*неможливість заблокувати деякі ресурси з небажаним контентом*), та надмірне блокування (*помилкове блокування*).

В цілому фільтрація – це більше профілактична міра. І хоча вона не була призначена спеціально для комунікації, фільтрація вхідного та/або вихідного трафіку може відчутно обмежити чи, навпаки, запобігти шкідливому контакту між учасниками кожної окремої комунікації. Проте, як вже було зазначено вище, розпізнавання кібербулінгу на основі комунікації чи контенту, з технічної точки зору, досить складно формалізується, і тому потребує залучення досить серйозних ресурсів (*фінансових, технічних, людських і т. і.*). Ще одним недоліком ПЗ даного типу є те, що фільтрацію можливо обійти. Наприклад, можна замінити початкові терміни, що є заблокованими, на інші, які так само будуть ображати (*наприклад, англійське слово «loser» стає «l o s e r», «LOS3R», «looser» і т.п.*).

Фільтруюча технологія працює у реальному часі, та в переважній більшості випадків, не передбачає зберігання персональних даних користувача, тому не загрожує його конфіденційності. Однак вона не є добровільною, так як користувачі, часто не мають можливість здійснення свого вибору, стосовно наступної фільтрації контенту. Також, блокування комунікації (*фільтрація*) чи запобігання доступу к Web-сайтам, потенційно, може обмежувати параметри обміну інформації та, як слідство, вираження думки.

*Моніторинг.* Дана технологія є більш профілактичною і працює на основі припущення, що користувачі комунікації будуть контролювати свою поведінку, якщо вони знають, що за їх он-лайн активністю хтось або щось слідкує. ПЗ що реалізує дану технологію, теоретично, підходить для всіх типів, середовищ і методів кібербулінгу. Проте на практиці, інциденти, які пов’язані з мережевою травлею, потрібно буде шукати буквально у ручному режимі. Враховуючи, що кібербулінг у багатьох випадках тяжко розпізнати, то з великою часткою впевненості можна стверджувати, що це є дуже ресурсномістка та втомлива робота. Як свідчить відомий досвід ПЗ для моніторингу не є добровільним, тому користувачі зазвичай не знають і не помічають що їх контролюють. Активність реєструються в режимі реального часу, проте, якісь зворотні дії можуть бути зроблені тільки після того, як відповідні записи пройшли аудит експертною стороною (*наприклад, батьками, в разі використання ПЗ типу «батьківській контроль»*). Технологія моніторингу порушує конфіденційність, тому що вся онлайн активність, яка може розглядатись, як особисті данні, фіксується та зберігається для її подальшого аналізу. Свобода слова не зачіпається.

Більша частина програмних рішень для моніторингу трафіку працює в режимі реального часу та не вносить будь-яких затримок у процес комунікацій (*працює в фоновому режимі*).

*Блокування небажаних користувачів (контактів)*. Більшість сучасних додатків обміну миттєвими повідомленнями та соціальних мереж надають користувачам можливість заблокувати інших користувачів, щоб виключити небажаний контакт. Також, соціальні мережі надають можливість заборонити невідомим користувачам зв’язуватись з власником акаунту і отримувати доступ до його профілю. В цьому разі, блокування трапляється у відповідь на минулі інциденти та обмежує шкідливу комунікацію між людьми. Однак, на жаль, ця техно-

логія можлива поки тільки у соціальних мережах і месенджерах. Блокування – це добровольчий акт, який допомагає користувачам контролювати *(в певній мірі суб'єктивно)* своє віртуальне спілкування. Вони можуть блокувати агресорів у будь-який момент, тому ця технологія працює у реальному часі. В даному випадку, блокування ніяк не пов'язане з конфіденційністю користувача, і таким чином практично не обмежує свободу його самовираження.

*Звітність*. Багато існуючих соціальних мереж надають можливість повідомляти про неприємний та незаконний контент (*наприклад, застосувавши функцію «повідомити про порушення»*). Ці донесення, зазвичай, відправляються модераторам платформи, які особисто його переглянуть, і вирішать, варто реагувати на скаргу, чи ні. В даному випадку, принциповим питанням стає дотримання вимог професійної етики, з боку модераторів (*цензорів*), тому що вони отримують доступ до "чутливого" персоніфікованого контенту користувачів. Деякі соціальні мережі, чати, онлайн ігри та форуми також надають можливість повідомити про дії користувача, який, на думку жертви, займається кібербулінгом. В цьому разі модератори також вирішують, як слід поступити з цим користувачем. Нажаль, даний вид захисту можливий тільки якщо є можливість залучення системного цензору, тому він не є універсальним.

Так як всі користувачі комунікаційної платформи можуть повідомляти про небажаний контент, ця технологія є добровільною. Але, вона не працює у реальному часі, тому що модератори перевіряють звіти особисто, а на це потрібен певний час. Конфіденційність не страждає, тому що особисті дані не зберігаються у звітах (*принаймні це не задекларовано*).

*Перевірка віку/особистості*. Перевірки віку та/чи особистості націлені на обмеження небажаних контактів неповнолітніх зі сторонніми дорослими, а також запобіганню доступу неповнолітніх до небажаного контенту. Ця технологія є профілактичною. Перевірка віку та/чи особистості може використовувати публічні та закриті бази даних (БД), які містять інформацію, як про неповнолітніх (*шкільні записи*), так і про дорослих (*наприклад, людей, які здійснили зґвалтування*). Особам які є у цих БД, або користувачам певного віку дозволяється, або навпаки не дозволяється підтримувати зв'язок з деякими іншими групами користувачів.

Дана технологія не є універсальною, тому що вона не націлена на різні форми кібербулінгу. Перевірка віку/особистості може бути як добровільною (*наприклад, при проходженні реєстрації*), так і не добровільною (*наприклад, якщо шкільний сайт дозволяє доступ тільки учням цієї школи*). Технологія працює у реальному часі. Оскільки перевірка віку/особистості потребує збору і зберігання особистих даних, то конфіденційність може бути під загрозою.

*Освітні технології*. Освіта є ще однім, опосередкованим, засобом підвищення мережевої безпеки для неповнолітніх. Освітні технології для боротьби з кібербулінгом – це, здебільшого, різноманітні інтерактивні комп'ютерні ігри та програми, які навчають дітей безпеці в мережі, та їх правильній поведінці у випадках кібербулінгу. Наприклад, «*FearNot!*» – це інтелектуальне віртуальне середовище (*Intelligent Virtual Environment - IVE*) в 3D, де вигадані персонажі розігрують сценарії булінгу. Даний додаток було розроблено для дітей 8-12 років, щоб вони могли спостерігати за подіями з позиції третьої особи. *IVE* пропонує дітям безпечне середовище, яка підтримує соціальне та емоційне навчання. Контрольні дослідження, які були проведені у Німеччині і Великобританії [46], встановили короткочасний ефект запобігання булінгу для жертв у Великобританії.

Оскільки основною метою освітніх технологій є стимулювання правильної поведінки у підлітків, в цілому вони призначені для усіх типів і методів кібербулінгу. Освітні програми зазвичай є обов'язковими, тому це не є добровільною технологією. Здебільшого вони призначені для формування правильної поведінки, тому вони не захищають безпосередньо від проявів кібербулінгу. Також, ці технології не порушують конфіденційність дитини.

Головна проблема, яка пов'язана з використанням освітніх технологій, полягає у їх обмеженій ефективності. У 2010 році *Faye Mishna* та інші [47] провели дослідження, у ході якого зробили огляд трьох освітніх програм. У кінці дослідження вони прийшли до висновку, що участь у цих програмах дає покращення знань про безпеку в Інтернеті, проте зміна поведінки в мережі учасників програми була не суттєва. Тобто, більші знання про безпечне використання Інтернету не обов'язково корелює з меншим онлайн ризиком.

Узагальнені результати основних можливостей існуючих технологій захисту від кібербулінгу наведені у Табл.1-2. Слід підкреслити, що всі технології, які розглядалися, відповідають відразу декільком з приведених в Табл. 2 характеристикам. При цьому, більшість з розглянутих технологій (*перевірка віку/особистості, фільтрація, моніторинг, звітування та блокування небажаних контактів*) не створювались спеціально для захисту від кібербулінгу, та добре захищають від інших загроз [1]. В першу чергу вони призначені для блокування доступу до небажаного контенту, тому їх успіх, в плані захисту від кібербулінгу (*котрий в більшій мірі пов'язано зі спілкуванням*) є досить обмежений.

Таблиця 2 – Результати аналізу різних технологій

| **Технологія** | **Оцінюваний параметр** | | | | |
|---|---|---|---|---|---|
| | Універсальність | Безперервність | Добровільність | Конфіденційність | Транспарентність |
| Аналіз контенту / поведінки | +/- | + | – | +/- | + |
| Фільтрація | +/- | + | – | + | – |
| Моніторинг | +/- | – | – | – | + |
| Блокування контактів | – | + | + | + | + |
| Звітність | – | – | + | + | – |
| Перевірка віку та/або особистості | – | + | +/- | – | + |
| Освітні технології | + | – | – | + | + |

Згідно аналізу характеристик, що були визначені у Табл. 1, та враховуючи специфіку питань, які розглядаються, найбільш відповідною технологією слід вважати блокування небажаних контактів. В цілому можна стверджувати, що у більшості існуючих технологій мережевої безпеки, які в певній мірі адаптовані до умов боротьби з кібербулінгом, є одна спільна особливість: - вони всі намагаються керувати поведінкою користувачів, так чи інакше обмежуючи її! Таким чином, станом на сьогоднішній день, обмеження потенційних агресорів та/або жертв є ефективним напрямом протидії, але навчити їх справлятись саме з інцидентами кібербулінгу, було би значно більш кращим результатом. Проте, поки це лише у перспективі. На практиці ж (*як це вже було зазначено вище*), освітні технології, що застосовують такий метод, слід вважати малоефективними.

### 4.1.1 Комплексування технологій

Показовим прикладом поліпшення рівня захисту від кібербулінгу, є шлях інтеграції декількох різних технологій в межах одного рішення. Вдалим прикладом відповідного ПЗ можна вважати функцію «батьківський контроль», котра може бути реалізована, як на рівні окремого модулю в складі комплексного рішення ІБ (*наприклад, в рішеннях класу Internet Security*), так і у вигляді самостійного спеціалізованого ПЗ [44-45, 48].

Батьківський контроль – це комплексний продукт, який не залежно від типу кінцевого пристрою, одночасно використовує технології моніторингу, фільтрації (*в т.ч. із застосуванням SaaS - Software as a Service*) і аналізу контенту та/або поведінки кінцевого користувача. Традиційно, функції батьківського контролю реалізуються за рахунок застосування 2-х видів контролю: - пасивного і активного [48]. Пасивні методи реалізують наступні функції:

- Обмеження на запуск деяких програм;
- Обмеження на час використання пристрою;
- Обмеження на час використання якоїсь програми;
- Обмеження на відвідування певних Web-ресурсів (*за різними критеріями*).

До активних методів відносяться:

- Відстеження місцезнаходження;
- Перегляд контактів, повідомлень, завантажувань, історії дзвінків;
- Відстеження переглянутого відео/аудіо контенту.

На думку фахівців та Інтернет користувачів, станом на 2019 рік, перелік п'яти найкращих модулів «батьківській контроль» виглядає наступним чином [49]: – *Avira* (Німеччина); – *Blue Coat* (США); – *DrWeb* (Росія); – *BitDefender* (Румунія); – *ContentKeeper* (Австралія).

### 4.2 Кібербулінг і соціальні мережі

На рис. 4 представлена статистична інформація, яка надана *Ditch the Label*, однією з провідних організацій проти знущань. Ці відомості відображають дані опитування студентів, стосовно платформ, на яких вони зазнали кібербулінг.

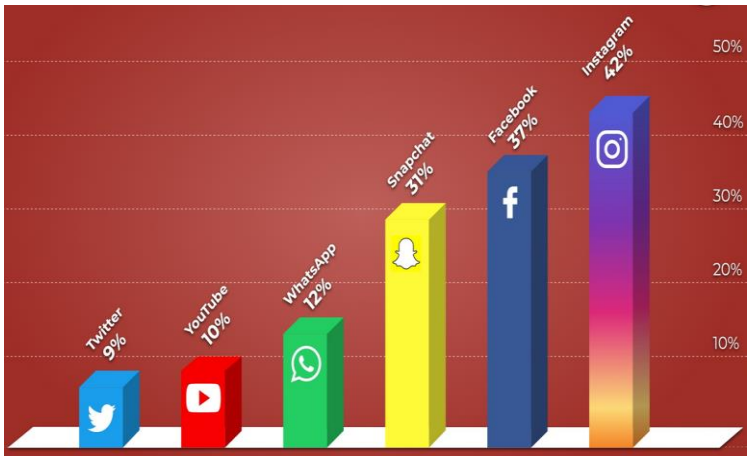



Рис. 4 – Дані щодо кібербулінгу соцмережах

Згідно цих даних, найбільш за все кібербулінгу піддавались користувачі соціальних мереж *Instagram, Facebook* та *Snapchat*. Ці комунікаційні платформи щодня налічують мільйони користувачів і тому проявляють очевидну зацікавленість в ефективній протидії кібербулінгу.

*Facebook.* На сьогодні є найкрупнішою соціальною мережею у світі. Число користувачів, які регулярно (*не менше ніж 1 раз на місяць*) використовують цей ресурс, складає порядку 2,5 мільярди чоловік. Дана платформ активно бореться з різноманітними проявами кібербулінгу. Фахівці цієї мережі поєднали одразу три технології: - блокування контактів (*можливість заблокувати небажаного користувача*); - звітування (*користувач може повідомити про небажаний контент*); - та освітні технології (*«Центр захисту від травлі»*).

У 2013 році *Facebook* запустив свій спеціальний проект «Центр захисту від травлі» [50], котрий позиціонується, як ресурс для підлітків, батьків і викладачів, що потребують підтримки та допомоги з питань, які пов'язані зі знущаннями та іншими конфліктами в мережі. У 2017 році було реалізовано декілька нових додаткових функцій, котрі можуть допомогти попередити булінг та переслідування [51]. Також соціальна мережа у подальшому планує надати своїм користувачам можливість повідомляти про булінг чи переслідування від імені іншого користувача. А наразі тестується ще одна функція, за допомогою якої користувач зможе блокувати появу певних слів в своїх коментарях [52].

*Instagram*. *Instagram* (*власник Facebook*) позиціонує себе, як соціальна мережа для обміну медіа-контентом (*Media sharing networks*). Нажаль, але ця платформа наразі є найпопулярнішою для кібербулінгу. У *Instagram*, так само як і у *Facebook*, присутні технології блокування

контактів та звітування. Тобто, користувачі даної мережі можуть подати скаргу на небажаний коментар та обліковий запис, чи заблокувати його. Також, є можливість зробити свій профіль «закритим» (*тільки для «своїх» підписантів*).

З 2019 року компанія почала вводити нову функцію [53], яка повідомляє користувачів, коли їх коментар до фото чи відео контенту «вважається як образливий». Керівництво мережі повідомило, що вони впроваджують елементи штучного інтелекту (ШІ), котрий може розпізнавати різні види булінгу в рамках їх платформи. Так, перед тим, як небажаний коментар буде опубліковано алгоритм ШІ повідомить відправника про потенційну небезпеку його коментарів. Представники *Instagram* вважають, що такий підхід змусить користувачів ресурсу замислитись стосовно змісту особистих коментарів. Також, проходить апробацію функція «тіньового бану», яка дозволяє користувачам мережі робити коментарі кривдника прихованими для всіх інших користувачів платформи, крім нього самого.

*Twitter.* *Twitter* позиціонується, як соціальна мережа для авторських записів. Наразі, це є найпопулярнішим сервісом мікро-блогів у світі. І хоча *Twitter* знаходиться не на 1-му місті по розповсюдженості кібербулінгу (*лише 9% студентів відповіли, що зустрічались з булінгом на цій платформі*), ця компанія теж активно бореться за безпеку своїх користувачів [54]. Наразі можна виділити 7 способів, за допомогою яких фахівці компанії протидіють кібербулінгу на їх платформі:

1. Розширена фільтрація повідомлень. Користувачі можуть використовувати цей інструмент для багатофакторної фільтрації облікових записів, від яких вони можуть приймати повідомлення. Ця функція призначена для недопущення зловживань з неперевірених облікових записів чи певних користувачів, які мають статус «небажаних»;
2. Розширення способів вимкнути контент. Розширені можливості функції вимкнення повідомлень: - користувачі мають можливість приховати відображення ключових слів чи цілих фраз, та управляти часом блокування відображення небажаних повідомлень. Таким чином, користувач може налаштувати контент, якій він бажає бачити у повідомленнях;
3. Прозорість процедури звітування. Фахівці мережі забезпечили більшу прозорість опрацювання скарг про виявлені зловживання, в наслідок чого користувачі отримують службові повідомлення, стосовно дій, які приймає *Twitter* на їх скаргу щодо булінгу;
4. «Тайм-аут» *(тимчасова перерва активності)*. Якщо твіти (*текстові записи*) користувачів помічені, як образливі, або ті, що іншим чином порушують системні Правила, то активність профілю тимчасово скривається. Таким чином інші користувачі не матимуть змогу переглядати записи цього профілю;
5. Безпечні результати пошуку. Алгоритми ШІ фільтрують результати пошуку, щоб користувачі не отримували контент з облікових записів, які були «вимкнено» (*за скаргою*). Однак, ці дані все ще будуть зберігатися, тому, якщо користувач справді шукає саме їх, то він повинен знайти саме цей контент. Але в цьому разі він/контент не буде відображатись у якості основного результату пошуку;
6. Руйнування образливих записів. Алгоритми ШІ приховують записи, які визначені образливими, чи порушують правила мережевої спільноти. Користувач може переглянути дані твіти, але тільки якщо «зайде» безпосередньо у профіль автора запису;
7. Блокування створення нових образливих профілів. Алгоритми ШІ запобігають створенню нових облікових записів, якщо інші профілі користувача вже були позначені системою, як «образливі». Це унеможливлює створення і наступне використання фальшивих профілів для розсилки спаму, переслідування чи булінгу інших користувачів. Поведінковий алгоритм в межах платформи сканує декілька облікових записів-клонів з однаковими реквізитами, та визначає присутність можливих шахраїв та кривдників.

Узагальнюючи все вище зазначене, можна зробити висновок, що практично усі розглянуті технології протидії кібербулінгу відповідають хоча б одному з визначених критеріїв, однак жодна з них, поки, не відповідає більшості бажаних характеристик (*не кажучи вже про всі*). Скоріш за все це обумовлено тим, що станом на сьогоднішній день майже не існує техноло-

гій, які б були розроблені спеціально задля протидії саме кібербулінгу (*окрім освітніх технологій, хоча і вони є спірними*). Тому, їх ефективність у боротьбі з Інтернет-травлею дуже обмежена. В цьому сенсі, дещо ліпші показники мають програмні рішення класу «батьківський контроль». Вони інтегрують у собі декілька технологій захисту та мають більш таргетований функціонал, завдяки чому забезпечують і більш адекватний рівень парирування спроб проведення кібербулінгу.

## 5 Висновки

Хоча розвиток ІТ- технологій і несе сучасному суспільству багато корисних новацій, він теж, нажаль, має свої, приховані від необізнаних користувачів, негативні наслідки. У нашому випадку, однією з таких негативних сторін, є проблема булінгу, котра в наслідок масштабної інформатизації суспільства, «перейшла» у віртуальне середовище, та відкрила нову, «темну», сторінку в технологічної історії людства – сторінку кібербулінгу. Мета даної роботи полягала в дослідженні явища кібербулінгу, його основних видів, способів реалізації, характеристик та можливостей протистояння його проявам [55]. За результатами аналізу питань за даною проблематикою, можна стверджувати наступне:

1. Хоча явище булінгу досліджується вже декілька десятиліть, однак в його кіберваріації воно ще залишається дуже не вивченим. Так, поки все ще немає чіткого поділу на різні види кібербулінгу, за рахунок чого, кожен дослідник приводить своє бачення цього питання;

2. У плані вироблення консолідованої позиції в протистоянні кібербулінгу, принциповим є той факт, що не у кожній країні світу ведеться офіційна статистика, стосовно масштабів цього явища та його жертв (*наслідків*). А якщо вона і є, то частіше за все, акцент робиться на кібербулінгу у підлітковому середовищі. Однак, як це було підкреслено у роботі, в сучасному світі кібербулінг може стосуватися кожного, і це не залежить від віку, статі, соціального статусу та багатьох інших чинників;

3. За результатами огляду законодавчої бази різних країн, зроблено висновок, про існування гострої нестачі відповідних законів. Наразі, навіть провідні країни світу не мають розвиненої законодавчої бази стосовно протидії Інтернет-травлі;

4. Визначено, що в Україні є закон який регулює булінг (*і кібербулінг зокрема*), але він націлений тільки на учасників навчального процесу;

5. У більшості існуючих технологій мережевого захисту, які так чи інакше адаптовані до умов протидії кібербулінгу, є одна спільна особливість: - вони всі намагаються обмежувати поведінку користувачів. Таким чином, станом на сьогоднішній день, обмеження потенційних агресорів та/або жертв є найбільш ефективним напрямом протидії кібербулінгу;

6. В роботі систематизовано критерії, яким повинна відповідати сучасна технологія протидії кібербулінгу, та представлені приклади вдалої реалізації захисту користувачів у деяких найбільш популярних соціальних мережах. Підкреслено, що наразі є велика нестача спеціальних технологій для ефективної протидії проявам кібербулінгу;

7. Станом на сьогоднішній день, явище кібербулінгу є дуже недооціненим і тому являє собою серйозну проблему. З великою часткою впевненості можна стверджувати, що в подальшому кібербулінг буде тільки поширюватись, адже з кожним роком все більше людей стають активними користувачами все нових мережевих сервісів та онлайн послуг;

8. Для ефективної протидій проявам кібербулінгу потрібно застосовувати виключно комплексний підхід, тобто впроваджувати відповідні заходи в межах всіх зазначених у роботі шляхів протидії: - соціального, законодавчого та технологічного. В межах реалізації кожного з цих заходів, потрібно періодично проводити різноманітні освітні заходи, які будуть інформувати суспільство про особливості проявів цього явища;

9. Ефективним засобом захисту дітей і підлітків від негативного впливу мережевих загроз і проявів кібербулінгу, є захисне ПЗ класу «батьківський контроль». Установка таких рішень на пристрої, якими безпосередньо користуються діти, за умови постійної уваги до змісту log-файлів і коригування налаштувань даних програм, робить цей засіб досить ефективним в протистоянні кібербулінгу.

Однак, незважаючи на всі можливості існуючих технологій батьківського контролю, одних лише програмних засобів явно недостатньо, тому що навіть найпередовіші технічні рішення не замінять довірливої розмови з «близькою» людиною. Як наслідок, не варто нехтувати регулярними бесідами з підлітками і дітьми про правила поведінки в Інтернеті та основні різновиди онлайн загроз. Вже сам факт існування такої бесіди, підтверджує те, що і батьки і діти об'єктивно оцінюють загрози сучасного віртуального світу та готові протистояти потенційним викликам сучасності;

10. Потужним інструментом для подальшого вдосконалення процедури рецензування «спірних» записів користувачів в соціальних мережах, може послужити практика використання фахівцями комунікаційних майданчиків додаткових технічних параметрів, видобутих з пристроїв користувачів (*наприклад, параметри геолокації, поведінковий профіль користувачів, аналіз структури сузір'я контактів, репутаційний рейтинг та ін.*);

11. Основою технологічного фундаменту майбутніх захисних рішень, що протидіють проявам кібербулінгу можуть виступати останні напрацювання в сферах штучного інтелекту, синтезу поведінкових алгоритмів та удосконалення технологій хмарних обчислень.

## Посилання


[1] Маллери Д. Безопасная сеть вашей компании. Защита и администрирование / Пер. с англ. Е. Линдеман. – М.: НТ Пресс, 2007. – 640 с.

[2] What is cyberbullying? // nuedusec. URL: https://nuedusec.com/blog/cyberbullying/, 11.02.2020

[3] Цькування. // wikipedia. URL: https://uk.wikipedia.org/wiki/%D0%A6%D1%8C%D0%BA%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F, 11.02.2020

[4] Hyojin Koo. A time line of the evolution of school bullying in differing social contexts. // Asia Pacific Education Review Copyright 2007 by Education Research Institute 2007, Vol. 8, No. 1, 107-116 URL: https://files.eric.ed.gov/fulltext/EJ768971.pdf, 15.02.2020

[5] History of bullying. // blogspot. URL: http://bullying190.blogspot.com/2012/10/history-of-bullying.html, 15.02.2020

[6] What is bullying? // humanrights. URL: https://humanrights.gov.au/our-work/commission-general/what-bullying-violence-harassment-and-bullying-fact-sheet, 15.02.2020

[7] Columbine Shooting. // history. URL: https://www.history.com/topics/1990s/columbine-high-school-shootings, 21.02.2020

[8] Cyberbullying: An Emerging Threat to the “Always On” Generation // billbelsey. URL: http://www.billbelsey.com/?cat=13, 21.02.2020

[9] А.И. Маренцова. Запугивание и издевательство в сети. Феномен: CYBERBULLYING. Москва, 2015, сс. 16-20.

[10] A. Cooper. Sexuality and the Internet Surfing into the New Millennium. Cyber Psychology and Behavior, Vol. 1, No. 2, 1998, pp. 181-187.

[11] Donegan R. Bullying and Cyberbullying: history, statistics, law, prevention and analysis. – The Elon Journal of Undergraduate Research in Communications, 2012.

[12] Григорьев В.А., Лагутенко О.И., Распаев Ю.А. Сети и системы радиодоступа. – М.: Эко-Трендз, 2005. – 384 с.

[13] Шахнович И.В. Современные технологии беспроводной связи. Издание второе, исправленное и дополненное. - М.: Техносфера, 2006. – 288с.

[14] Hyperpersonal model. // wikipedia. URL: https://en.wikipedia.org/wiki/Hyperpersonal_model, 02.03.2020

[15] Maral Dadvar. EXPERTS AND MACHINES UNITED AGAINST CYBERBULLYING, 2014, pp. 23-25

[16] Mary Howlett-Brandon. CYBERBULLYING: AN EXAMINATION OF GENDER, RACE, ETHNICITY, AND ENVIRONMENTAL FACTORS FROM THE ETHNICITY, AND ENVIRONMENTAL FACTORS FROM THE NATIONAL CRIME VICTIMIZATION SURVEY: STUDENT CRIME NATIONAL CRIME VICTIMIZATION SURVEY: STUDENT CRIME SUPPLEMENT, 2009, p. 8. URL: https://scholarscompass.vcu.edu/cgi/viewcontent.cgi?article=4485&context=etd, 02.03.2020

[17] Грифер. // wikipedia. URL: https://ru.wikipedia.org/wiki/%D0%93%D1%80%D0%B8%D1%84%D0%B5%D1%80, 09.03.2020

[18] Солдатова Г. У., Ярмина А. Н. Кибербуллинг: особенности, ролевая структура, детско-родительские отношения и стратегии совладания, 2019, № 3(35). С. 17–31.

[19] Что значит интернет-тролль, как его отличить? // fb. URL: https://fb.ru/article/245287/chto-znachit-internet-troll-kak-ego-otlichit-kak-zarabatyivayut-trolli-v-internete-kak-vesti-sebya-s-trollyami-v-internete-kak-borotsya-s-trollyami-v-internete, 11.03.2020

[20] 51 Critical Cyberbullying Statistics In 2020. // broadband. URL: https://www.broadbandsearch.net/blog/cyber-bullying-statistics, 20.03.2020

[21] 11 FACTS ABOUT CYBERBULLYING // dosomething. URL: https://www.dosomething.org/us/facts/11-facts-about-cyber-bullying, 16.03.2020

[22] Булінг та кібербулінг у підлітковому середовиші // unicef. URL: https://www.unicef.org/ukraine/bullying-cyberbylling-teens-Ukraine, 20.03.2020

[23] Cyberbullying Laws. // criminal.findlaw. URL: https://criminal.findlaw.com/criminal-charges/cyber-bullying.html, 30.03.2020

[24] Canada: The New Age Of Cyberbullying. // monaq. URL: https://www.mondaq.com/canada/social-media/727084/the-new-age-of-cyberbullying, 30.03.2020

[25] Proskauer. Bullying, Harassment and Stress in the Workplace — A European Perspective, 2013. URL: https://www.internationallaborlaw.com/files/2013/01/Bullying-Harassment-and-Stress-in-the-workplace-A-European-Perspective.pdf, 04.04.2020

[26] French Law Prohibiting Bullying in the Workplace. // thehrdirector. URL: https://www.thehrdirector.com/business-news/diversity_and_equality/french-law-prohibiting-bullying-in-the-workplace/, 04.04.2020
[27] The Law on Cyberbullying. // localsolicitors. URL: https://www.localsolicitors.com/criminal-guides/the-law-on-cyberbullying, 04.04.2020
[28] Ciberacoso, código penal y leyes al acoso. // ciberintocables. URL: https://ciberintocables.com/ciberacoso-codigo-penal/, 05.04.2020
[29] Уголовный Кодекс Республики Беларусь – Статья 189. Оскорбление // koddeksy-by. URL: https://kodeksy-by.com/ugolovnyj_kodeks_rb/189.htm, 07.04.2020
[30] Ответственность за оскорбление в Интернете. // berestovitsa.grodno-region. URL: http://berestovitsa.grodno-region.by/uploads/files/Otvetstvennost-za-oskorblenie-v-Intnrnete.pdf, 10.04.2020
[31] Валентина Алексеевна Мальцева. Защита детей от кибербуллинга. Вопросы уголовно-правового регулирования. 2019, pp. 95-99. URL: https://cyberleninka.ru/article/n/zaschita-detey-ot-kiberbullinga-voprosy-ugolovno-pravovogo-regulirovaniya, 10.04.2020
[32] Конституція України: Редакція від 01.01.2020
[33] Кодекс України про адміністративні правопорушення: Редакція від 14.05.2020
[34] В 2019 суд рассмотрел 310 дел о буллинге. // osvita. URL: https://ru.osvita.ua/school/69377/, 17.04.2020
[35] Проект Закону про внесення змін до деяких законодавчих актів України щодо протидії мобінгу. // w1.c1.rada. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65602, 17.04.2020
[36] Проект Закону про внесення змін до деяких законодавчих актів України щодо забезпечення захисту педагогічних, науково-педагогічних та наукових працівників. // w1.c1.rada. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=67110, 18.04.2020
[37] A Guide to Worldwide Bullying Laws. // hcalawyers. URL: https://www.hcalawyers.com.au/blog/bullying-laws-around-the-world/, 18.04.2020
[38] Friendly Attac. // friendlyattac. URL: https://www.friendlyattac.be/, 23.04.2020
[39] Телекоммуникационные системы и сети: Учебн. пос. В 3-х т. Т. 3. Мультисервисные сети / В.В. Величко, Е.А. Субботин, В.П. Шувалов, А.Ф. Ярославец / Под ред. В.П. Шувалова. – М.: Горячая линия-Телеком, 2005. – 592 с.
[40] Ріпний О.С., Дьяченко О.О., Гостєв О.Л. Аналіз особливостей організації IDS/IPS систем в сучасних інформаційно-телекомунікаційних системах. // Проблеми інформатизації. VII міжнародна НТК. 13-15 листопада 2019. Том 1: секції 1-3. – Ч.: ЧДТУ. – 2019. – С.119.
[41] Internet Safety Technical Task Force, 2008. URL: http://cyber.law.harvard.edu/pubrelease/isttf/, 23.04.2020
[42] Janneke M. van der Zwaan, Virginia Dignum, Catholijn M. Jonkerand Simone van der Hof. On Technology Against Cyberbullying. Chapter 12, 2014, pp. 217-218, 218-225. URL: http://mmi.tudelft.nl/sites/default/files/zwaan_Technology%20against%20b.chapter%202014.pdf
[43] Pendar N. Toward spotting the pedophile telling victim from predator in text chats. In:ICSC'07: Proceedings of the international conference on semantic computing. IEEEComputer Society, 2007, pp 235–241.
[44] Родительский контроль на новом уровне // URL: https://www.securitylab.ru/analytics/423870.php.html
[45] Светлана Шляхтина. Родительский контроль - дело тонкое. // URL: https://compress.ru/article.aspx?id=23035
[46] Watson S. FearNot! An Anti-Bullying Intervention: Evaluation of an Interactive Virtual Learning Environment. 2007. URL: https://www.researchgate.net/publication/30384409_FearNot_An_Anti-Bullying_Intervention_Evaluation_of_an_Interactive_Virtual_Learning_Environment, 27.04.2020
[47] Faye Mishna, Charlene Cook, Tahany Gadalla, Joanne Daciuk, Steven Solomon, Ajita Deodhar. Cyber bullying behaviors among middle and high school students. Vol. 80, No. 3, 2010, pp. 362-374.
[48] Parental controls. // wikipedia. URL: https://en.wikipedia.org/wiki/Parental_controls, 08.05.2020
[49] Рейтинг - лучшие родительские контроли 2019. // anti-malware. URL: https://www.anti-malware.ru/parental_control_test_history, 08.05.2020
[50] Как бороться с травлей. // facebook. URL: https://www.facebook.com/safety/bullying/, 13.05.2020
[51] Facebook introduces new tools to fight online harassment. // engadget. URL: https://www.engadget.com/2017-12-19-facebook-new-tools-fight-online-harassment.html, 13.05.2020
[52] Facebook bullying: How it happens and what to do about it. // comparitech. URL:https://www.comparitech.com/internet-providers/facebook-bullying/, 13.05.2020
[53] Использование ИИ для борьбы с травлей пользователей в Интсаграм. // androidsider. URL:https://androidinsider.ru/novosti/instagram-budet-ispolzovat-ii-dlya-borby-s-travlej-polzovatelej.html, 15.05.2020
[54] How Twitter Is Fighting Harassment & Cyberbullying. // blog.hubspot. URL:https://blog.hubspot.com/marketing/twitter-harassment-cyberbullying, 20.05.2020
[55] Гайкова В. В. Дослідження явища кібербулінгу і аналіз шляхів протидії його проявам : Пояснювальна записка до дипломної роботи бакалавра: напрям підготовки 125 – Кібербезпека / В. В. Гайкова; Харківський національний університет імені В. Н. Каразіна. – Харків: [Б. В.], 2020. – 64 с.

**Рецензент**: Владимир Хома, д.т.н., проф., Опольский Политехнический Университет, Ополе, Польша.
E-mail: xoma@wp.pl

Поступила: Март 2020.

**Авторы:**
Валерия Гайкова, студентка факультета компьютерных наук, ХНУ имени В. Н. Каразина, Харьков, Украина.
E-mail: valeriagaikova98@gmail.com
Сергей Малахов, к.т.н., с.н.с., доцент кафедры, ХНУ имени В. Н. Каразина, Харьков, Украина.
E-mail: mailgate@meta.ua

**Исследование явления кибербуллинга и путей противодействия его проявлениям.**

**Аннотация**. В работе исследованы основные характеристики Интернет травли (кибертравли или кибербуллинга). Рассмотрены основные особенности проявлений этого явления. Выполнен анализ существующих видов кибербуллинга и их отдельных характеристик. Рассмотрены примеры законодательных актов различных стран по противодействию кибербуллингу. По результатам обзора имеющейся нормативно-правовой базы разных стран, сделан вывод о существенном дефиците соответствующих норм законов. Подчеркнуто, что в современном мире жертвой Интернет травли может стать любой человек. При этом, риск стать жертвой кибербуллинга практически не зависит от каких-либо факторов (например, финансового положения жертвы, его возраста, пола, социального положения и др.). Отмечено, что коммуникации, которые осуществляются в киберпространстве, предоставляют пользователям возможность заранее и тщательно выбирать информацию о себе, которую они хотят обнародовать. В большинстве случаев это способствует тому, что люди демонстрируют только свои «положительные» стороны (например, при общении в чатах). В результате этого у сетевых собеседников часто возникают ложные взаимные симпатии, в результате чего они опрометчиво вступают в доверительные отношения. Таким образом, происходит идеализация партнера по сетевой коммуникации, и любая его информация начинает восприниматься гораздо чувствительнее, чем при прямом «физическом» общении. Этот эффект с «успехом» используется при проведении акций кибербуллинга, когда один человек сначала вызывает максимальное доверие другого, а потом резко меняет тактику общения, становясь немотивированно вероломным и агрессивным. Подчеркнуто, что явление кибербуллинга является значительно недооцененным и поэтому представляет собой серьезную проблему. Выполнен краткий обзор существующих технологий и средств противодействия этому явлению. Проведено сравнение их эффективности. Систематизированы критерии, которым должна соответствовать современная и эффективная технология противодействия кибербуллингу. Представлены примеры удачной реализации защиты пользователей в некоторых наиболее популярных социальных сетях. Акцентировано внимание на том, что для противодействия кибербуллингу, в настоящее время, в подавляющем большинстве случаев, используют технологии защиты на основе ограничений. Главная цель соответствующих средств защиты заключается в том, чтобы максимально локализовать нежелательный контент (с точки зрения существования признаков кибербуллинга). Сделан вывод, что и в дальнейшем кибербуллинг будет только распространяться. Это обусловлено постоянным увеличением численности пользователей новых сетевых сервисов и онлайн площадок для общения. Высказано мнение, что для активного противодействия и эффективной защиты от кибербуллинга требуется внедрение комплексных организационно-технических мероприятий. В завершении предложена общая оценка дальнейшего развития кибербуллинга и путей совершенствования соответствующих инструментов противодействия.

**Ключевые слова:** буллинг; кибербуллинг; социальная сеть, информационная безопасность; контент; защита; технология, сетевая безопасность.

**Reviewer:** Volodymyr Khoma, Dr. of Sciences (Eng.), Full Prof., The Opole University of Technology, Opole, Poland.
E-mail: xoma@wp.pl

Received: March 2020.

**Authors:**
Valeriia Haikova, CSD Student, V.N. Karazin Kharkiv National University, Ukraine.
E-mail: valeriagaikova98@gmail.com
Serhii Malakhov, Ph.D., Senior Researcher, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: mailgate@meta.ua

**Research of the cyberbullying phenomenon and analysis of ways to counter its manifestations.**

**Annotation.** The main characteristics of Internet harassment (*cyberbullying*) are investigated in the research. The main features of this phenomenon are considered. The analysis of existing types of cyberbullying and their individual characteristics is made. The examples of legislative acts of different countries is concluded that there is deficiency of relevant rules of low. It is emphasized that anyone can become a victim of in the modern world. At the same time a risk of becoming a victim of cyberbullying does not depend on any factors (*for example financial position of victim, his or her age, sex, social position etc.).* It is noted that communications that are made in cyberspace provide an opportunity for users to choose information they want to make public carefully and in advance. In most cases it contributes to help people show theirs strengths (*for example, when communicating in chats*). In results there is often false sympathy between network interlocutors and they trust each other. So the idealization of the partner happens and any his or her information is perceived more sensitive than during direct communication. This effect is successfully used during cyberbullying, when first one person inspires the trust of another and then changes communication tactics, becoming faithless and aggressive. It is emphasized that the cyberbullying phenomenon is very underestimated and that`s why it is a serious problem. The brief overview of existing technologies and means of counteracting this phenomenon is made. The comparison of their effectiveness is made. The standards that modern and effective technology of cyberbullying resistance must meet are systematized. There are examples of successful realization of user protection in most popular social network. It is emphasized that for cyberbullying resistance nowadays in most cases the protection technologies of it is to localize undesirable content in terms of the existence of cyberbullying. Based on the results of this research it is confirmed that the cyberbullying will spread further. This is due to the constant increase in the number of users of new network services and online platforms for communication. For effective defense against cyberbullying it is required the introduction of organizational and technical measures. At the end it is proposed the general assessment of further development of cyberbullying and the ways to improve appropriate countermeasures.

**Keywords:** Bullying; Cyberbullying; Social Network; Informational Security; Content; Protection; Technology; Network Security.

УДК 004.056.5 DOI: 10.26565/2519-2310-2020-1-03

# ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ ТЕХНОЛОГІЇ HONEYPOT

Тетяна Кохановська, Олексій Нарежний, Олександр Дьяченко

Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, Харків, 61022, Україна
tanya.koh99@gmail.com, o.nariezhnii@karazin.ua, diachenko4@gmail.com

**Рецензент**: Олександр Оксіюк, д.т.н., проф., Київський національний університет імені Т. Шевченка, вул. М. Ломоносова 81, Київ, 03189, Україна.
o.oksiuk@gmail.com

Поступила: Березень 2020.

***Анотація:*** *Визначено роль та головні завдання різних мережевих пасток (Honeypot) при побудові інтегрованих систем безпеки. Розглянуто основні класифікаційні ознаки та особливості первинних налаштувань декількох комерційних засобів. Зроблено висновок, що основні переваги технології Honeypot, серед іншого, полягають в їх гнучкості та масштабованості. Підкреслено, що на даний час поки ще немає досконалих методик ідентифікації і швидкої компрометації мережевих паст. Звернено увагу на те що, тактика мережевої розвідки і методи здійснення мережевих атак постійно прогресують. Враховуючи цей факт постійний аудит даних Honeypot і оперативна реакція на визначені мережеві інциденти та колізії є одним із головних напрямків роботи для фахівців з питань забезпечення вимог корпоративної політики інформаційної безпеки. Відзначено, що архітектура різних пасток, в цілому, достатньо добре відома і тому є потенційно вразливою. Тому, наділяючи пастки більш гнучким (варіативним) сценарним контекстом та скорочуючи час мережевої експозиції можливо підтримувати їх захистний потенціал в досить паритетному стані. Ці обидва напряму потребують більш щільної уваги (докладний аналіз даних log-файлів та корегування алгоритмів роботи поведінкового аватару для створеної пастки) зі сторони персоналу, та вимагають постійної підтримки його професійних компетенцій. За результатами огляду можливостей існуючих Honeypot та узагальнення типових ознак мережевої активності найбільш характерних вузлів (в даному випадку файлового серверу), розглянуто особливості синтезу відповідних поведінкових профілів (аватарів) для корегування роботи програмних пасток. Стверджується, що систематизація правил роботи аватару Honeypot (як сукупності користувальницьких поведінкових алгоритмів) та своєчасна корекція наявних баз поведінкових профілів є завдання, яке важко формалізується. Це обумовлено потенційним різноманіттям варіантів мережевої активності, що притаманна для кожної конкретної мережі та налаштувань наявних мережевих вузлів. В цьому сенсі надлишкова уніфікація (звуження можливого поля поведінкових реакцій) поведінкових профілів Honeypot в значної мірі може полегшити зловмиснику проведення моніторингу та наступної ідентифікації створеної пастки. Тому формування базового набору відповідних мережевих аватарів слід розглядати, не більше, як основу для її подальшої модифікації під специфіку завдань, топологію та інші особливості кожної окремої IT-структури (або особливості їх окремих елементів). Підкреслено, що впровадження технології пасток не підміняє собою інших технологій і інструментів безпеки, а лише ефективно розширює наявний арсенал протидії новим загрозам безпеки (перш за все, як інструмент швидкого реагування). Тому шлях інтеграції Honeypot з іншими, вже розгорнутими рішеннями ІБ, є найбільш збалансованим напрямом для подальшого підвищення загального рівня безпеки мережевих ресурсів.*

***Ключові слова****: Honeypot; вторгнення; інформаційна безпека; ЛОМ; Firewall; IDS; IPS.*

## 1 Вступ

На сьогодняшний день більша частина людства активно користується Інтернетом, а кожна сучасна людина, в той чи іншої мірі є користувачем персонального комп'ютера (ПК) або якогось іншого електронного гаджету. Паралельно зі стрімким розвитком усіх основних напрямків інформаційних технологій (ІТ) постійно вдосконалюються і різноманітні технології проведення мережевих атак та ведення кібершпіонажу. Це напрямок діяльності створює постійну загрозу для безпеки інформаційних ресурсів і є основним спонукальним чинником для організації ефективних заходів протидії різнорідним мережевим загрозам. Саме тому, на постійній основі, необхідно забезпечувати комплексний моніторинг всієї поточної мережевої активності, особливо в частині аналізу змісту, характеру та інтенсивності трансграничного трафіку. Це в першу чергу стосується аналізу трафіку в межах спеціально передбачених демілітаризованих зон та відповідних публічних сервісів (при їх наявності), що передбачають інтенсивну взаємодію з користувачами, які знаходяться за рамками організованого периметра безпеки компанії або окремого користувача. Одним з ефективних засобів ведення моніторингу поточної мережевої активності та виявлення ознак підготовки майбутнього кіберзло-

чина, є використання можливостей технології Honeypot (т.з. вузлів або мереж пасток/приманок). Мета даної роботи полягає у аналізі основних можливостей існуючих Honeypot, та розгляді особливостей подальшого розвитку мережевих пасток, що впроваджують тактику адаптивної протидії (*використання поведінкових сценаріїв*).

## 2. Особливості функціонування та питання класифікації Honeypot

Honeypot (*з англ. - «горщик з медом»*) - програмно-апаратний ресурс, який представляє собою функціональну приманку (або пастку) для потенційних мережевих зловмисників, яка відповідним чином розміщена, налаштована та періодично обслуговується для забезпечення її більш ефективного використання за призначенням [1]. Honeypot (далі HPot) помітно відрізняється від інших поширених технологій забезпечення інформаційної безпеки (ІБ). Так, більшість технологій забезпечення ІБ, що використовуються сьогодні, було спроектовано для вирішення якоїсь однієї задачі [2]. Наприклад, міжмережевий екран (ММЕ) контролює вхідний і вихідний мережевий трафік і використовується, переважно, як засіб блокування будь-якої несанкціонованої мережевої активності (*в т.ч. трафіку*). Системи виявлення вторгнень (*IDS - Intrusion Detection System*) визначають атаки, здійснюючи постійний моніторинг мережі і системної активності користувачів, а мережевий комутатор підтримує адміністрування трафіку згідно створеного для нього ACL (*Access Control List*) і т.і. В цьому сенсі HPot відрізняється від класичних засобів забезпечення ІБ, таких як ММЕ, IDS або систем захисту від витоку даних [2,3] тим, що вони не покликані вирішувати будь-яку конкретну задачу. Навпаки, HPot - гнучкий засіб, який може бути застосовано в різних ситуаціях та в різних масштабах (*точково, використовуючи розподілену структуру або реалізуючи гібридне рішення*). Так наприклад, засоби HPot можуть дозволяти запобігати або виявляти атаки, або тільки імітувати роботу певного ресурсу (*окремого серверу або цілої Scatternet*). Таким чином, HPot поєднують в собі (*в залежності від конкретних завдань, що на них покладені у кожному конкретному випадку*) деяку функціональність практично всіх засобів забезпечення ІБ.

HPot вперше з'явилися з першими комп'ютерними зловмисниками, а роботи по їх створенню та практичному впровадженню проводилися паралельно з дослідженнями *IDS* та *IPS* (*Intrusion Prevention System*, та її різновид *WIPS - Wireless Intrusion Prevention System*). Першою документальною згадкою, за тематикою HPot, була робота Кліффорда Столла *«The Cuckoo's Egg»*, що вийшла у 1990 році. А вже у 2000-х роках HPot стали досить поширеними елементами інтегрованих систем безпеки, що забезпечували ефективну протидію спробам несанкціонованого проникнення до «внутрішнього» периметру безпеки комп'ютерних мереж компаній і установ [1].

В спрощеному трактуванні основне завдання HPot – навмисно виявитися та піддатися атаці зі сторони сторонньої особи або зовнішнього програмного засобу (ПЗ), що згодом дозволить вивчити стратегію зловмисника і визначити перелік засобів за допомогою яких можуть бути проведені будь-які нелегітимні дії проти інформаційних, та апаратних ресурсів мережевої інфраструктури, яка захищається. Конкретна реалізація HPot може являти собою як спеціальний виділений сервер (*фізично або його програмну емуляцію*), так і окремий мережевий сервіс, головне завдання якого – спробувати привернути увагу потенційних кіберзлочинців.
В контексті вищезазначеного слід підкреслити, що HPot є ресурс, який без будь-якого впливу на нього сам, практично, нічого не робить. Фактично HPot збирає певну кількість інформації, після аналізу якої їм формується відповідна статистика щодо методів і способів, якими користуються кіберзлочинці, а також визначається присутність роботи будь-яких нових (*невідомих раніше*) рішень, які згодом можуть бути застосовані при проведенні справжньої атаки. Наприклад, веб-сервер, який не має імені та фактично нікому не відомий, на практиці, не повинен мати і користувачів, що «заходять» на нього. Тому логічно вважати, що всі користувачі, які намагаються все ж таки на нього проникнути, можуть розглядатися, як потенційні порушники. В цьому випадку даний сервер - пастка буде збирати інформацію про характер поведінки цих користувачів (*частота відвідувань, їх IP-адреси, час очікування та ін.*), та про їх способи впливу на неіснуючий сервер. Після аналізу всієї отриманої інформації фахівці, які

обслуговують цю пастку, в певному сенсі повинні скорегувати алгоритм роботи аватару HPot, або іншими словами - модифікувати відповідні поведінкові шаблони так, щоб реакції пастки стали більш адекватні поточним умовам мережевої активності [4]. В цьому сенсі, в разі використання HPot з сильною взаємодією [1], буде вкрай корисно визначення загальної стратегії захисту, яка передбачає більш складні сценарії мережевої «гри» (*наприклад, каскадування HPot та/або непомітне розміщення і активація відповідного програмного "жучка" (cookie, що передані через браузер) на комп'ютері зловмисника та ін.*).

Особливості синтезу профілів мережевої активності вузлів, які захищаються за рахунок впровадження відповідних HPot, розглянемо на прикладі файлового серверу, що розміщується в демілітаризованій зоні за першим (зовнішнім) корпоративним MME. Аналізуючи типові риси роботи такого файлового серверу, можна визначити наступне (Рис. 1(а)):

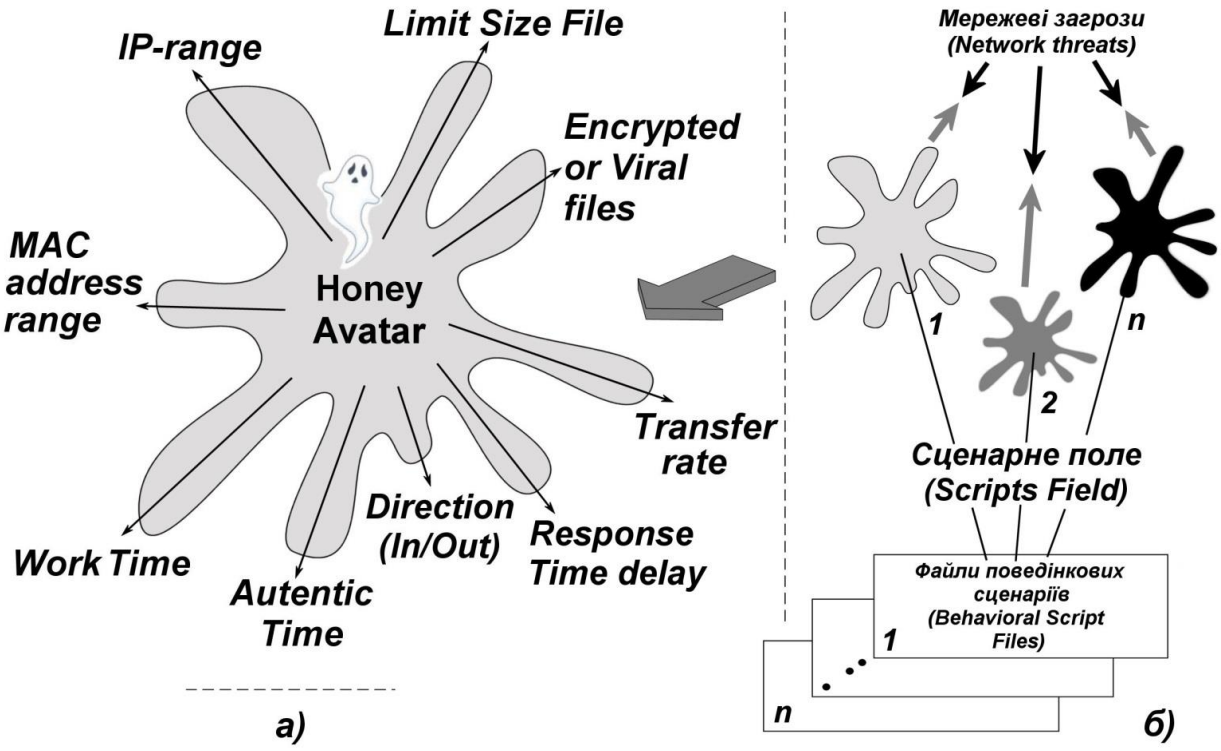



Рис. 1 – Принцип використання поведінкових профілів аватару HPot

- з ним, потенційно, можуть взаємодіяти, як зовнішні користувачі, так і користувачі з будь-якого внутрішнього сегменту локальної мережі (в залежності від їх повноважень). В даному випадку адміністрування доступу до інформаційних ресурсів серверу можливо здійснювати за рахунок управління відповідним адресним простором для IP та MAC адресів взаємодіючих абонентів («*IP range*» та «*MAC address range*»);

- обмеження розміру файлів (як скачуваних, так і тих що записуються/оновлюються на сервері), визначається функцією/правилом «*Limit size file*»;

- швидкість передачі даних з серверу можна регулювати відповідними значеннями функції/правила «*Transfer rate*»;

- затримка часу «відповіді» серверу (аналог функції уповільнення мережевих з'єднань, наприклад, як в HPot «*Tarpit*» (буде розглянуто нижче)), визначається функцією/правилом «*Response Time delay*»;

- дискретне управління можливістю зчитування-запису даних, всіма групами користувачів, визначається відповідними правилами «*Direction – In/Out*»;

- параметр правила «*Autentic Time*» дозволяє регламентувати час проходження процедури зовнішнього підключення (а саме підтвердження повноважень) для незареєстрованих/зареєстрованих користувачів;

- параметр правила «*Time Work*» дозволяє дискретно змінювати час роботи серверу для певних (або всіх) груп користувачів, що забезпечує можливість відтворювати враження спостереження перебігу інтенсивних бізнес процесів або навпаки, існування деяких технологічних пауз.

В цілому, за результатами аналізу характерних рис, що притаманні роботи кожного окремого файлового серверу, можна скласти відповідний профіль його мережевої активності. Узагальнення основних показників кожного профілю, дозволяє синтезувати відповідний аватар для його HPot (Рис. 1(а)), що забезпечить можливість імітувати роботу серверу в найбільш типових умовах мережевого оточення, та впливу актуальних (*або визначених*) мережевих загроз.

Сукупність характерних умов роботи серверу та певних ознак нелегітимного зовнішнього впливу на нього, формують відповідне сценарне поле (*Script Field*), в межах якого саме і діє даний HPot. Таким чином, чим ширше сценарне поле, тим більше можливостей у Honeypot протистояти потенційним загрозам, і тим самим більш ефективніше забезпечувати «прикриття» справжнього серверу [4]. Набір відповідних аватарів HPot, формалізується у вигляді файлів поведінкових сценаріїв («*Behavioral Script Files*», Рис.1(б)), що надає можливостей постійно розширювати спектр протидії (або моніторингу) новим загрозам, та адаптувати окремі характеристики створеної пастки під конкретну ситуацію (на відміну від випадку використання системи HPot *Specter* (*коротко буде розглянуто нижче*), яка реалізована за принципом «як є», де у її користувача немає можливості змінювати вже існуючи сценарії).

Важливо підкреслити, що створені поведінкові аватари HPot можуть мати однаковий склад параметрів, які імітуються, але відрізнятися один від одного інтенсивністю проявив кожного з них (*наприклад, аватари сценаріїв №1 та № 2 на рис.1(б) мають однакову конфігурацію, але різну довжину пліч (інтенсивність) відповідних реакцій*). Також можливо створення суттєво відмінного від інших аватару, якій має принципові відмінності, що надає йому можливостей протидіяти конкретному типу загроз (аватар «n» на Рис. 1(б)). В цьому разі поведінковим аватаром можуть підтримуватися/імітуватися, якісь дуже нетипові можливості, що значно ускладнюють доступ до «цінної» інформації яка зберігається на даному вузлі. Так наприклад, для умов файл-серверу пастки такими перешкодами можуть бути наступні (функція «*Encrypted or Viral Files*» на Рис. 1(а)):

- впровадження механізмів шифрування даних;
- впровадження механізмів багаторівневого (вкладеного) архівування даних;
- розміщення файлів з навмисно інфікованим вмістом та ін.

Зворотною стороною розвиненого сценарного поля HPot, є необхідність епізодичного аудиту його log-файлів і корекція (*т.з. тонка настройка*) файлів поведінкових скриптів. Хоча і цю рутинну процедуру можна в певної мірі автоматизувати, особливо в частині програмованих, епізодичних змін деяких робочих параметрів серверу-пастки (наприклад, зміна параметрів «*Time Work*», «*Transfer rate*» або «*Limit size file*», на рис. 5.1(а)).

Слід зазначити, що аналіз типових профілів мережевої активності для найбільш характерних об'єктів мережевої інфраструктури і подальший синтез відповідних поведінкових аватарів, необхідно проводити для кожного окремого випадку: - типу мережевих вузлів чи цілих мережевих структур (*в т.ч. і окремих мережевих сегментів*).

Так наприклад, у разі створення поведінкового аватару для цілей захисту справжнього поштового серверу, потрібно буде враховувати такі особливості, як:

- необхідність роботи з протоколами (SMTP, POP3 та IMAP);
- підтримка роботи «дозволеного» та «забороненого» списків повідомлень;
- підтримка можливості автоматичної екстракції електронних адрес з отриманого листа, та їх наступне переміщення до списку «заборонених» адресатів;
- оцінка скважністі розсилок з однієї адреси/домену;
- відслідковування розміру отриманих повідомлень і т.і.

Відповідно, врахування індивідуальних рис та ознак для кожного окремого випадку, буде в значної мірі модифікувати склад та взаємовідносини всіх складових аватару (Рис. 1(а)).

### *2.1 Класифікація Honeypot*

В цілому HPot можна класифікувати за багатьма параметрами [5]. До найбільш принципових параметрів слід віднести наступні:

1) Характеристики процесу установки і первинних настроювань HPot. В цьому сенсі, чим більший перелік можливостей підтримує конкретний HPot, тим більш складним є і даний параметр (*особливо складно в умовах розгортання HoneyNet*);
2) Складність використання та поточної підтримки (*наприклад, частота залучення адміністратора для коригування параметрів роботи пастки та аудиту лог-файлів, частота оновлень ПЗ і т.і.*). Як і за першим параметром, чим ширше функціональність HPot, тим складніше його використання, і тим більше часу та зусиль вимагає його налагодження та підтримка;
3) Ступень взаємодії пастки з потенційним зловмисником. Очевидно, що чим більш щільна взаємодія предбачається між HPot та потенційним зловмисником, то тим більша і ймовірність помилки на кожному з етапів роботи створеної пастки. За цім параметром слід розрізняти:
   - - слабкої взаємодії;
   - - середньої взаємодії;
   - - сильної взаємодії. У більшості випадків такий HPot розташовується в контрольованому середовищі (*наприклад, після 1-го (вхідного) MME [2]).* В цілому, одного разу правильно встановлений, ретельно налаштований, та періодично перевіряємий HPot сильного взаємодії, може надати таку інформацію, та дозволити такий спектр можливої активної протидії (в певному сенсі - гри), яку не здатен дати жоден з інших, більш простих, типів пасток. Як наслідок, рівень компетенцій фахівців, що встановлюють та обслуговують відповідній тип HPot, повинні підтримуватися на досить високому рівні;
4) Забезпечуємий рівень імітації. Даний параметр передбачає 3 можливих стана:
   - Простий, що характеризується обмеженою функціональністю імітованого сервісу (*наприклад, тільки відображення вітального повідомлення при зовнішньому з'єднанні*);
   - Середній/вибірковий, що підтримує досить докладну імітацію визначе*ного (окремого*) сервісу, або параметрів мережевої активності вузлу/мережі;
   - Високий - передбачає реалізацію всіх функціональних можливостей імітованого сервісу та/або вузлів мережі. Забезпечує підтримки пулу сценарних аватарів зворотної поведінки пастки при її реакції на спроби проведення мережевих атак;
5) Ступень потенційного ризику в разі компрометації HPot. Загальне правило: - з розширенням функціональних можливостей пастки, зростає вірогідність того, що вона може бути використана для атаки інших систем та/або сервісів. Даний параметр передбачає 3 можливих стана:
   - Низький – можлива атаку тільки проти окремого імітованого сервісу;
   - Середній – притаманний для HPot, що одночасно імітують кілька сервісів;
   - Високий – притаманний для HPot з сильною взаємодією;
6) Обсяг контрольованих параметрів мережевої активності. Найпростішим варіантом є HPot з імітацією окремого системного сервісу, а найбільш інформативним є HPot сильної взаємодії, що реалізує розширений збір всієї потрібної інформації;
7) Забезпечуємий рівень протоколювання мережевої активності (*глибина аудиторського сліду*). Даний параметр передбачае 3 можливих стана:
   - Слабке протоколювання (*зазвичай це HPot слабкої взаємодії, де фіксуються тільки IP-адреса і дані, які надходять зі сторони потенційного зловмисника*);
   - Середнє (*або вибіркове*) протоколювання (*фіксує деякі додаткові дані, наприклад, час приходу даних, ідентифікатори взаємодій і т.і.*);
   - Розширене протоколювання (*зазвичай це HPot сильної взаємодії, де реєструються всі події при взаємодії пастки із зовнішнім оточенням*).

### 3 Основні можливості відомих мережевих пасток

Всі існуючи HPot можна умовно поділити на 2 категорії - відкриті та комерційні [6,7]. До 1-ої категорії слід віднести такі програмні рішення, як: *Honeyd, Jackpot, BackOfficer Friendly* та ін. Характерними представниками комерційних продуктів є*: ManTrap, KFSensor, Specter* та ін. Коротко розглянемо характерні можливості декількох відкритих HPot.

*3.1 Honeyd*. Розроблений у 2002 році Нільсом Провосом (*Niels Provos*). Є *Open Source* рішенням для Unix-платформ. Створювався як виробничий HPot, тобто його імітовані сервіси, більшим чином, спрямовані для виявлення атак та несанкціонованої мережевої активності. Дозволяє створювати віртуальні хости в мережі (*використовується вільний простір IP-адрес*). Для опису віртуальної пастки використовується відносно простий конфігураційний файл. Цій HPot підтримує можливість власної внутрішньої установки (наприклад, додавання імітованих сервісів), та може імітувати різні операційні системи (ОС) на рівні мережевих протоколів. Імітація роботи сервісів досягається шляхом перекомутації з'єднань на робочі сервіси або використанням заздалегідь синтезованих поведінкових сценаріїв, які можна модифікувати та додавати нові. Для імітації роботи сервісів використовується відповідна база даних (*наприклад, характеристики протоколів різних ОС*). Це рішення дозволяє зробити імітацію цілої мережі, тобто створені HPot (хости-пастки) можна об'єднати у *Virtual LAN*. Таким чином, задавши потрібну топологію мережі, схему маршрутизації та визначивши припустимий відсоток втрат пакетів, можна забезпечити імітування реальної робочої мережі (*або її окремого вузлу/вузлів*). Вкрай вдалу адаптацію Honeyd для роботи з ОС сімейства Windows запропонував Майкл Девіс (*Michael Davis*): - від всіх Windows-подібних реалізацій до Unix-систем та маршрутизаторів. В цілому, Honeyd імітує систему не тільки на прикладному рівні, а також на рівні IP-стека, що надає ще більший рівень обміну інформацією зі зловмисником (або ботом-розвідником), завдяки чому цей HPot можна віднести до виду пасток середньої взаємодії.

*3.2 Jackpot.* Цей HPot є кросплатформним додатком (на мові Java), що являє собою імітацію поштового серверу. Розробником цієї системи є Джек Клів (*Jack Cleave*). Так як сервер з розгорнутим на ньому HPot не оголошується як загальнодоступний, то виявити поштовий сервер можна тільки при скануванні мережі (наприклад, з допомогою Nmap). В наслідок цього вся вхідна кореспонденція розглядається, як потенційний спам або, як тестові листи спамерів, які перевіряють його працездатність. В разі класифікації отриманих листів, як спам, вони далі не пересилаються. При цьому, адреси відправників, текст листів та інша (доступна) інформація про хости, з яких була проведена розсилка, зберігаються в базі даних цього HPot (*для інформування адміністратора хосту, з якого була здійснена спам розсилка*). В цілому лист визначається, як спам за наступними правилами:

- кожний наступний лист надходить через короткий проміжок часу від попереднього;
- адреса відправника є в «забороненому» списку адрес (т.з «*Blacklist File*»);
- вміст отриманого листа містить посилання на «заборонений» список адрес;
- у отриманому листі зазначено велику кількість одержувачів (адресатів).

Важливо підкресліти, що дана пастка підтримує можливість уповільнення прийому даних (функція *Tarpit*), що може досить ефективно використовуватися для організації «дрібних» неприємностей потенційному спаммеру. Як наслідок, через прикру «завантаженість каналу зв'язку» спамер розішле відчутно меншу кількість спамерських оголошень. Даний HPot має відносно прості настройки і дозволяє емулювати різні типи поштових серверів. Більш того, є можливість віддаленого адміністрування системи з використанням web-інтерфейсу, а зібрана статистика видається у форматі HTML. В якості певних недоліків, слід мати на увазі те, що при роботі не на ОС Windows, можуть виникати деякі невідповідності.

*3.3 Back Officer Friendly (BOF).* BOF - один з найпростіших HPot, якій може працювати під ОС Unix та Windows. Його перший реліз був представлен ще в 1998 році фахівцями з компанії *NFR Security Inc.* Варто зазначити, що певна частина спеціалістів з питань ІБ не вважають BOF справжнім HPot, однак, виходячи з його основних функціональних можливостей (*утиліта управління віддаленими комп'ютерами*) це рішення можно класифікувати, як

HPot слабкої взаємодії. Так наприклад, при виборі режиму роботи «*Fake Replies*» (*генерування помилкових відповідей*) ця утиліта використовує відповідні інтерактивні сценарії для полегшеної емуляції поточної активності мережевих сервісів. В межах реалізації функціоналу «*Fake Replies*», при фіксуванні нового з'єднання BOF інформує абонента відповідним повідомленням (*із збереженням IP-адреси, з якої надійшов цій запит*) про недоступність даного сервісу, а через заданий час повідомляє його про втрату з'єднання. Таким чином забезпечується моніторинг мережевих подій та підтримка протоколу взаємодії.

В якості недоліків даного HPot слід зазначити відсутність: – детектування «прихованого» сканування; – збереження системи в файл; – модифікації поведінкових сценаріїв; – передачі службових повідомлень по e-mail. Таким чином, за сукупність своїх можливостей та недоліків, дане рішення, в певній мірі, можна вважати ефективною пасткою лише на початку тривалого мережевого протистояння (*фактично, є засобом раннього попередження про підготовку до вторгнення*).

*3.4 LaBrea Tarpit (неофіційна назва «липкий» Honeypot).* Це рішення (створено Томом Ліштоном) вивчає своє близьке мережеве оточення, визначає вільні IP-адреса та створює віртуальні хости, використовуючи для цього саме ці адреси. При спробах встановити з'єднання з подібною пасткою вона припиняє з'єднання, однак не розриває його. Це призводить до сканування мережі, де створені подібні віртуальні хости. Пастка може регулювати темп надходження даних по з'єднанню, оголошуючи число байтів, які вона «спроможна» прийняти в поточний момент часу. Таким чином, відправник (*потенційний зловмисник*) потрапляє в штучно створені умови, будучи вимушеним постійно адаптуватися під заявлені характеристики швидкості прийому даних зі сторони HPot. При цьому перевірка закритого вікна TCP може тривати досить тривалий період (*наприклад, поки додаток, який використовує дане з'єднання, не завершить свою роботу*). Таким чином, потенційний зловмисник потрапляє в неконтрольовану для нього ситуацію уповільнення мережевих з'єднань, що надає можливість стороні, яка захищається, виграти певний час на підготовку більш якісного захисту. В цілому цей HPot може значно уповільнити та відтягнути атаку, але не може завадити потенційним хакерам знайти спосіб щодо його нейтралізації.

Характерними представниками відомих комерційних рішень є: *ManTrap, KFSensor, Specter* та ін. Коротко розглянемо основні властивості деяких з них.

*3.5 ManTrap*. Цей HPot сильної взаємодії від компанії *Recourse Technologies*, котрий крім функцій пастки додатково синтезує добре контрольовану ОС, з якою взаємодіє потенційний порушник периметру безпеки. Більш того, це рішення, в межах однієї фізичній платформи, здатне утворювати контрольоване віртуальне оточення/середовище, з якого атакуючому практично дуже складно «вийти» для компрометації справжньої системи. Таким чином створюються сукупність "пасток", де кожна з них – це повноцінна функціональна ОС, яка має всі можливості, що і справжня система. При цьому передбачена функція настройки кожної окремої "пастки", як реальної фізичної ОС (*наприклад, можна створювати користувачів або запускати процеси і т.і.*). В цілому, використовуючи один комп'ютер, може бути створено до 4-х різних HPot сильної взаємодії. В якості функціональних обмежень ManTrap варто зазначити те, що це рішення підтримує лише деякі ОС, а сам HPot може функціонувати тільки на комп'ютері з ОС Solaris (з використовує особливих параметрів установки). По-друге, в силу того, що цей HPot використовує технологію "віддзеркалювання", то і основа всіх віртуальних ОС – тільки одна.

*3.6 KFSensor*. Цей HPot від компанії *KeyFocus* був створений для використання на системах під управлінням ОС Windows, дозволяє виявляти нелегітимні дії, за рахунок імітації вразливих сервісів ОС-жертви, та за сукупністю своїх можливостей є пасткою середньої взаємодії. Дане рішення підтримує наступні можливості: - віддалене адміністрування (*за допомогою механізмів шифрування і автентифікації*); - сумісність з IDS *Snort*; - емуляція мережевих Windows-протоколів; - має зручний користувальницький інтерфейс. Робота HPot полягає у прослуховуванні певного простору TCP/UDP-портів, а вразі зовнішньому підключення до них пастка ініціює відповідний банер (*зміст котрих можна модифікувати*) запрошення для

кожного імітованого сервісу і розриває з'єднання. В залежності від налаштувань HPot може перекомутовивати з'єднання з порту імітованого сервісу, на реально діючий сервіс іншого комп'ютера, що відбувається непомітно для зовнішнього абонента. Важливою якістю даного HPot є те, що він підтримує базу даних сигнатур, які засновані на складанні характерних ознак мережевих атак, аналогічних правилам IDS *Snort* (*можуть бути імпортовані із Snort*). За рахунок підтримки цього функціоналу, відбувається не тільки виявлення та фіксації активності мережевого зловмисника, а й забезпечується можливість створення власних скриптів відповідей та поведінки, і як наслідок, збільшення бази даних сигнатур мережевих атак. В сукупності все це надає можливість змоделювати, яку саме вразливість намагався використовувати зловмисник для проникнення в систему, що захищається. Крім того, в *KFSensor* реалізована можливість передачі повідомлень про зафіксовані мережеві інциденти по електронній пошті, що дозволяє підтримувати віддалене адміністрування та скоротити час інформування обслуговуючого персоналу, в разі виникнення необхідності оперативного втручання в перетин подій. Однак, на жаль, цей HPot не визначає прихованого сканування, та не може імітувати стек TCP/IP- протоколів.

*3.7 Specter.* Цей HPot від компанії *NetSec*, встановлюється в систему та імітує набір мережевих сервісів (з якими зловмисник взаємодіє), але при цьому зловмиснику не надається доступ до реальної ОС, а спект його дій обмежений передбаченою функціональністю пастки. Для того щоб ускладнити процес ідентифікації пастки для цього HPot можна призначити власне доменне ім'я, адресу, змінити банери сервісів що імітуються (*на більш характерні для кожного окремого випадку*), а також інші специфічні характеристики, що надає додаткової аргументації зловмиснику, що він таки має справу зі справжнім ресурсом. Дане рішення підтримує конфігурування потрібного рівня захищеності імітованого сервісу. Так наприклад, при імітації слабо захищеного файлового серверу, можна реалізувати можливість зовнішнього підключення, використовуючи стандартний вхід для незареєстрованих користувачів, і таким чином дозволити потенційному зловмиснику завантажити заздалегідь підроблений файл. І навпаки, в разі забезпечення високого рівня захисту сервісу, підключення до серверу-пастки може дуже ускладнити, наприклад заборонити підключення з певних IP-адресів. Корисними властивостями *Specter* є те, що він підтримує передачу службових повідомлень HPot на віддалений сервер, та має механізм передачі повідомлень по e-mail або телефонному каналу зв’язку. Однак у користувача цього HPot немає можливості додавати індивідуальні імітовані сервіси (*розширювати поведінку аватару*) або змінювати вже існуючи сценарії. Крім того, сервіси що імітуються працюють тільки з TCP-протоколом, та не підтримують UDP. Також, даний HPot є більш вимогливий до ресурсів, однак і його можливості декілька ширші порівняно з аналогами. В цілому, за сукупністю своїх властивостей *Specter* краще за всього використовувати, як систему раннього попередження про ведення мережевої розвідки або початок проведення мережевих атак.

Як випливає з матеріалів проведеного короткого огляду існуючих HPot, в незалежності від ступеня комерціалізації того чи іншого рішення, їх базовий функціонал практично завжди забезпечує імітацію основних мережевих сервісів і логирование (*з різним ступенем деталізації*) поточної мережевої активності. Таким чином, в основі практично всіх рішень є можливість раннього детектування ознак підготовки мережевої атаки або вторгнення.

## 4 Висновки

1. Надано огляд особливостей використання різних реалізацій програмних HPot, та визначено основні класифікаційні ознаки відомих рішень. Розглянути особливості первинних налаштувань та умов функціонування декількох відповідних комерційних засобів. За сукупністю результатів аналізу визначеної проблематики підкреслено, що основні переваги даної технології полягають в їх гнучкості та масштабованості. Можна стверджувати, що на даний час поки все ще немає досконалих методик ідентифікації та швидкої компрометації мережевих пасток. Проте, тактика мережевої розвідки і методи здійснення атак постійно прогресують,

тому забезпечення оперативної, та адаптивної протидії новим мережевим загрозам слід вважати одним із пріоритетних напрямків роботи для фахівців з питань ІБ.

2. Архітектура існуючих пасток, в цілому, достатньо добре відома і тому, є потенційно вразливою. Однак, можна стверджувати, що наділяючи пастки більш варіативним сценарним контекстом та скорочуючи час мережевої експозиції можливо підтримувати їх потенціал в досить паритетному стані. Ці обидва напряму потребують більш щільної уваги ( *докладний аналіз даних log-файлів і корегування алгоритмів роботи «мережевого аватару»*) зі сторони персоналу, та вимагають постійної підтримки його професійних компетенцій. За результатами аналізу можливостей відомих HPot та узагальнення профілів мережевої активності вузла типу файл-сервер, розглянуто особливості синтезу відповідних поведінкових профілів для корегування роботи програмного аватару відповідної пастки.

3. Систематизація правил роботи мережевого аватару кожної окремої пастки (*як сукупності користувальницьких поведінкових алгоритмів*) та періодична корекція наявних поведінкових профілів, є завданням, що важко формалізувати (*через різноманіття особливостей функціонування як всієї мережі, так і її окремих вузлів*). В цьому сенсі надлишкова уніфікація поведінкових профілів HPot (*для кожного типу вузлів*) в певній мірі може полегшити зловмиснику ідентифікацію діючої пастки. Тому наявність базового набору поведінкових профілів HPot слід розглядати, не більше, як основу для подальшої модифікації аватару під специфіку завдань, топологію та інші особливості кожної мережевої структури [4].

4. Впровадження технології пасток не підміняє інших механізмів мережевої безпеки, а лише ефективно розширює наявний арсенал засобів мережевого моніторингу та протидії новим загрозам (*перш за все, як інструмент попередньої розвідки та швидкого реагування*). Тому шлях комплексування мережевих пасток з іншими рішеннями ІБ, є найбільш збалансованим напрямом подальшого підвищення загального рівня безпеки мережевих ресурсів.

## Посилання

[1] Рузудженк, С., Погоріла, К., Кохановська, Т., & Малахов, С. (2020). Особливості захисту корпоративних ресурсів за допомогою технології Honeypot. Комп'ютерні науки та кібербезпека, (4), 22-29. Retrieved із https://periodicals.karazin.ua/cscs/article/view/15751

[2] Безопасная сеть вашей компании / Джон Маллери, Джейсон Занн и др.; пер. с англ. Е. Линдеманн. – М.: НТ Пресс, 2007. – 640 с.

[3] Ріпний О.С., Дьяченко О.О., Малахов С.В. // Особливості функціонування систем IDS та IPS при реалізації спроб несанкціонованого доступу до корпоративних ресурсів. Матеріали IX міжнародній НТК. 11-12.04.2019. – Х.: НТУ "ХПІ". – 2019. – С.95.

[4] Кохановська Т. А. Дослідження можливостей технології Honeypot : Пояснювальна записка до дипломної роботи бакалавра: напрям підготовки 125 – Кібербезпека / Т. А. Кохановська; Харківський національний університет імені В. Н. Каразіна. – Харків: [Б. В.], 2020. – 45 с.

[5] Технология Honeypot, Часть 2: Классификация Honeypot. DOI: https://www.securitylab.ru/analytics/275775.php (дата звернення: 2.10.2019)

[6] Технология Honeypot, Часть 3: Назначение Honeypot. DOI: https://www.securitylab.ru/contest/283103.php (дата звернення: 24.11.2019)

[7] Красоткин А. Черный лед // СНІР. – 2003. - №7. – С. 98-103.

**Reviewer**: Oleksandr Oksiiuk, Doctor of Sciences (Eng.), Full Prof., Taras Shevchenko National University of Kiev 81 Lomonosova St., Kyiv, 03189, Ukraine. E-mail: o.oksiuk@gmail.com

Received on March 2020.

**Authors:**

Tetiana Kokhanovska, student of CSD, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: tanya.koh99@gmail.com

Oleksii Nariezhnii, Ph.D., Associate Professor, V.N. Karazin Kharkiv National University, Ukraine.
E-mail: o.nariezhnii@karazin.ua

Alexandr Dyachenko, student of CSD, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: diachenko4@gmail.com

**Researching the possibilities of Honeypot technology.**

**Abstract.** The role and main tasks of various network traps (Honeypot) in the construction of integrated security systems are defined. Basic classification signs and features of the primary tuning of a few commercial facilities software solutions. It is concluded that the

main advantages of Honeypot technology, among other things, are their flexibility and scalability. It is emphasized that at present there are no perfect methods of identification and rapid compromise of network traps. Attention is drawn to the fact that network intelligence tactics and methods of network attacks are constantly progressing. Given this fact, the ongoing audit of HP data and prompt response to identified network incidents is one of the main areas of work for staff on compliance with corporate information security policy requirements. It is noted that the architecture of various traps, in general, is quite well known and therefore potentially vulnerable. Therefore, by providing traps with a more flexible (variable) scenario context and reducing the exposure time, it is possible to maintain their protective potential in the parity enough state. Both of these direction require closer attention (detailed analysis of log-files data and adjustment of behavioral avatar algorithms for the created trap) on the part of staff, and require constant support of them professional competencies. Based on the results of reviewing the capabilities of existing Honeypots and generalizing the typical features of network activity of the most characteristic nodes (in this case the file server), the features of synthesis of the corresponding behavioral profiles (avatars) are considered. It is claim that systematization of avatar rules Honeypot (as a set of behavioral algorithms) and timely correction of existing databases of behavioral profiles is a task that is difficult to formalize. This is caused to the potential variety of network activity options that are specific to each network and the individual settings of existing network nodes. In this sense, excessive unification (narrowing of the possible field of behavioral reactions) of behavioral profiles Honeypot can greatly facilitate the attacker to monitor and subsequently identify the trap created. Therefore, the formation of a basic set of relevant network avatars should be considered as a basis for its further modification under a special task, topology and other features of each individual IT structure (or features of their individual elements). It is emphasized that the introduction of trap technology does not replace other security technologies and tools, but only effectively expands the existing arsenal of countering new security threats (primarily as a tool for operational intelligence and rapid response). Therefore, the way to integrate net-traps with other security solutions is the most balanced way to further improve the overall security of network resources.

**Keywords:** Honeypot; Intrusion; Informational security; LAN; Firewall; IDS; IPS.

**Рецензент**: Александр Оксиюк, д.т.н., проф., Киевский национальный университет имени Т. Шевченко, ул. Ломоносова 81, Киев, 03189 Украина. E-mail: o.oksiuk@gmail.com

Поступила: Март 2020.

**Авторы:**

Татьяна Кохановская, студентка факультета компьютерных наук, Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина. E-mail: kate7smith12@gmail.com

Алексей Нарежний, к.т.н., доцент, каф. безопасности информационных систем и технологий, Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина. E-mail: o.nariezhnii@karazin.ua

Александр Дьяченко, студент факультета компьютерных наук, Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина. E-mail: diachenko4@gmail.com

**Исследование возможностей технологии Honeypot.**

**Аннотация**. Определена роль и основные задачи различных разновидностей сетевых ловушек (Honeypot) при построении интегрированных систем безопасности. Рассмотрены основные классификационные признаки и особенности первичных настроек нескольких коммерческих средств. Сделан вывод, что основные преимущества технологии Honeypot, среди прочего, заключаются в их гибкости и масштабируемости. Подчеркнуто, что в настоящее время пока еще нет совершенных методик идентификации и быстрой компрометации сетевых ловушек. Обращено внимание на то, что тактика сетевой разведки и методы осуществления сетевых атак постоянно развиваются. Учитывая этот факт, постоянный аудит данных Honeypot и оперативная реакция на выявленные сетевые инциденты и коллизии, является одним из главных направлений работы для специалистов по вопросам обеспечения требований корпоративной политики информационной безопасности. Отмечено, что архитектура разных ловушек, в целом, достаточно хорошо известна и поэтому является потенциально уязвимой. Поэтому, наделяя ловушки более гибким (вариативным) сценарным контекстом и сокращая время сетевой экспозиции, можно поддерживать их защитный потенциал в достаточно паритетном состоянии. Эти оба направления требуют более пристального внимания (подробный анализ данных log-файлов и корректировка алгоритмов работы поведенческого аватара ловушки) со стороны персонала и постоянной поддержки их профессиональных компетенций. По результатам обзора возможностей существующих Honeypot и обобщения характерных признаков сетевой активности типовых узлов (в данном случае файлового сервера), рассмотрены особенности синтеза соответствующих поведенческих профилей (аватаров) для коррекции работы программных ловушек. Утверждается, что систематизация правил работы аватара для сетевой ловушки (как совокупности пользовательских поведенческих алгоритмов) и своевременная коррекция имеющихся поведенческих профилей, является задачей, которая трудно формализуется. Это обусловлено потенциальным многообразием вариантов сетевой активности, характерных для каждой конкретной сети и настроек имеющихся сетевых узлов. В этом смысле избыточная унификация (сужение возможного поля поведенческих реакций) поведенческих профилей Honeypot, в значительной степени может облегчить злоумышленнику проведения мониторинга и последующей идентификации созданной ловушки. Поэтому формирования базового набора соответствующих сетевых аватаров следует рассматривать, не более чем, как основу для ее дальнейшей модификации под специфику задач, топологию и другие особенности каждой отдельной IT-структуры (или особенности их отдельных элементов). Подчеркнуто, что внедрение технологии ловушек не подменяет собой других технологий и инструментов безопасности, а только эффективно расширяет имеющийся арсенал противодействия новым угрозам безопасности (прежде всего, как инструмент быстрого реагирования). Поэтому путь интеграции Honeypot с другими, уже развернутыми решениями ИБ, является наиболее сбалансированным направлением для дальнейшего повышения общего уровня безопасности сетевых ресурсов.

**Ключевые слова:** Honeypot; вторжение; информационная безопасность; ЛВС; межсетевой экран; IDS; IPS.

УДК 621.327:621.391 DOI: 10.26565/2519-2310-2020-1-04

# ВЕРИФИКАЦИЯ ОТПЕЧАТКОВ ПАЛЬЦЕВ МЕТОДОМ ДЕКОМПОЗИЦИИ МИНУЦИЙ

Ольга Мелкозерова, Сергей Малахов

Харьковский национальный университет имени В.Н. Каразина, пл. Свободы, 4, Харьков, 61022, Украина
olja.mex@gmail.com, mailgate@meta.ua

**Рецензент**: Вячеслав Калашников, д.ф.-м.н., проф., Технологический университет Монтеррея, 64849 Монтеррей, Нуево-Леон, Мексика
kalash@itesm.mx

Поступила: Апрель 2020.

***Аннотация:*** *В настоящее время производится попытка внедрения биометрических технологий в различные сферы общественной и государственной жизни: криминалистика, системы контроля доступа, приложения на мобильных устройствах, банковское дело и т.д. Проблема точности при этом все еще остается открытым вопросом для обсуждения, так как при решении задачи верификации биометрических образцов возникают проблемы дописывания или исчезновения опорных точек, деформация расстояний между ними, линейные и угловые смещения всего образца. Также разработанные биометрические системы не отвечают всем требованиям информационной безопасности, а именно целостности, аутентичности, доступности, неопровержимости, наблюдаемости и конфиденциальности. В статье приведен анализ метода декомпозиции окрестности минуции при верификации отпечатков пальцев, описаны его преимущества и недостатки в сравнении с другими методами. Он основывается на создании локальных структур для каждой минуции отпечатка, так как именно локальные структуры обладают устойчивостью к перемешиванию, угловому и линейному смещениям точек. Построение глобальных структур зачастую не приводит к хорошим показателям точности, так как возникает проблема при центрировании всего образца. Проведен полный перебор испытаний образцов базы данных отпечатков пальцев при их верификации этим методом. Описан алгоритм построения кода для произвольной минуции и алгоритм сравнения двух шаблонов отпечатков. В результатах статьи приведены значения парных сравнений двух шаблонов для истинных и ложных испытаний. Исследованы показатели ложного отказа (FRR – False Rejection Rate), ложного доступа (FAR – False Acceptance Rate), единой эквивалентной ошибки (EER – Equal Error Rate).*

***Ключевые слова:*** *отпечатки пальцев, метод декомпозиции окрестности минуций, минуция.*

## 1 Введение

В настоящее время практически применяются различные способы биометрической идентификации [1]: - отпечатки пальцев; - особенности голоса; - особенности радужной оболочки глаз; - характерные особенности лица и многие другие особенности (*например, параметры походки и другие антропогенные характеристики*).

Одним из наиболее популярных и часто используемых, является способ распознавания по отпечаткам пальцев. Этому способу биометрической идентификации личности посвящено значительное количество публикаций, однако, время от времени, все равно возникают определенные трудности при распознавании отпечатков *(условия применения, ограничения различного характера, несовершенство алгоритмов и т.п.*). Анализ и обобщение характерных предпосылок возникновения подобных трудностей, позволяет утверждать, что причиной тому, как правило, служат [1-6]:

- неоднозначность преобразований;
- флуктуация расстояния между минуциями, что определяется степенью нажатия пользователя пальцем на считывающее устройство сканера и угол поворота пальца при этом;
- проблемы с используемым алгоритмом предобработки отпечатков, для получения их шаблона (*появляются ложные минуции и/или исчезают истинные*).

Проблему угла поворота довольно успешно решают алгоритмы, которые позволяют строить локальные структуры, такие структуры, которые связаны с системой координат каждой отдельной минуции, а не с глобальной системой координат всего отпечатка в целом [2, 3]. К таким методам, например, относится метод построения цилиндрического кода, который дает

неплохие результаты по точности, а также метод декомпозиции окрестности минуции, который является объектом исследования в данной статье.

## 2 Описание метода декомпозиции минуций

Метод декомпозиции минуций относительно прост для понимания и реализации [2]. Его суть заключается в том, что для каждой отдельной минуции строится своя локальная структура, представленная матрицей размерностью 4×9, а весь шаблон имеет размер 4*N*×9 (*где N – количество минуций в первоначальном образце*).

Последовательность шагов для создания локальной структуры каждой минуции имеет следующий вид:

1) Нахождение трех ближайших минуций (Рис. 1);
2) Декомпозиция графа из четырех вершин на три треугольника (Рис. 2);
3) Заполнение матрицы локальной структуры (*размером 4×9*) значениями длин сторон, внутренними углами треугольников и разностью углов прихода минуций, которые принадлежат треугольнику:

$$u_r = \left(s_{r1}, \Delta o_{r1}, \alpha_{r1}, s_{r2}, \Delta o_{r2}, \alpha_{r2}, s_{r3}, \Delta o_{r3}, \alpha_{r3}\right), \quad (1)$$

где $s_{ri}$ – длина стороны треугольника $(i = 1,...3)$; $\alpha_{ri}$ – внутренние углы треугольника, $(i = 1,...3)$; $\Delta o_1 = |o_1 - o_2|$, $\Delta o_2 = |o_2 - o_3|$, $\Delta o_3 = |o_3 - o_1|$ – разница углов прихода минуций, $r = 1,...,4$.

Для реализации всего метода шаги 1-3 нужно повторить для каждой минуции, которая принадлежит данному шаблону.

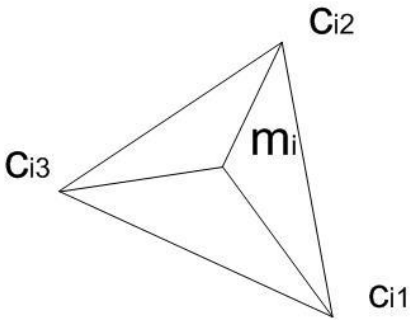



Рис. 1 – Окрестность минуции $m_i$

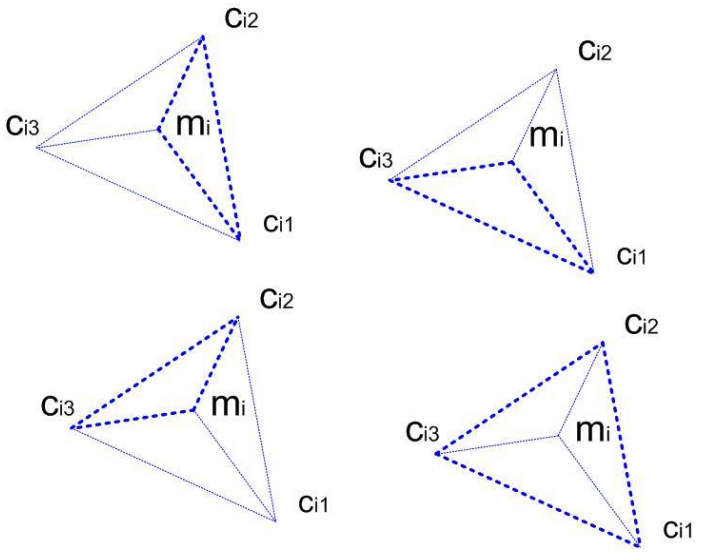



Рис. 2 – Пример декомпозиции окрестности минуции

## 3 Пример построения локальной структуры минуции и сравнение 2-х шаблонов

На рис. 3 приведен пример размещения координат всех минуций, формирующих типовой шаблон. Для индикаторной минуции, с координатами (137; 380), выбираем три ближайшие к ней минуции c1, c2, c3 (их координаты см. в табл. 1).

Проводим декомпозицию (табл. 2) окрестности выбранной минуции. На рис. 4, это треугольники с вершинами координат: - m-c2-c3; - m-c1-c2; - c1-c2-c3; - m-c1-c3.

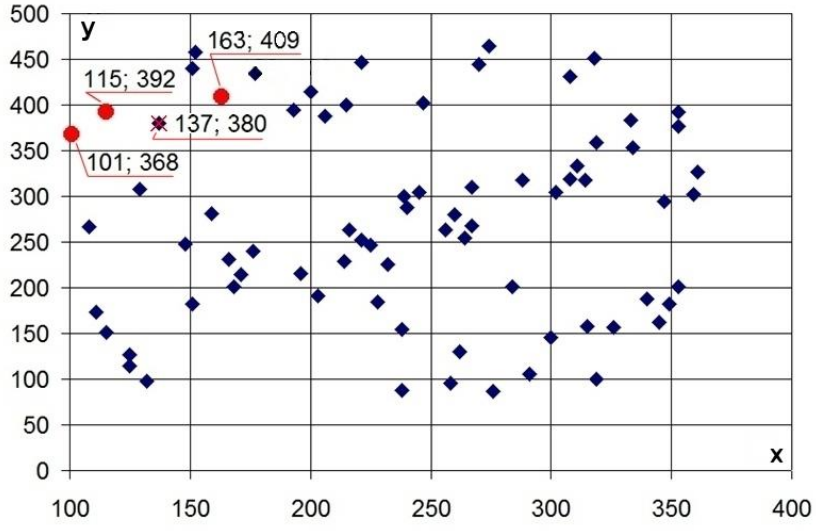



Рис. 3 – Координаты минуции шаблона

*Прим.: Выбор трех ближайших точек (выделены красными маркерами) к минуции для которой строится локальная структура*

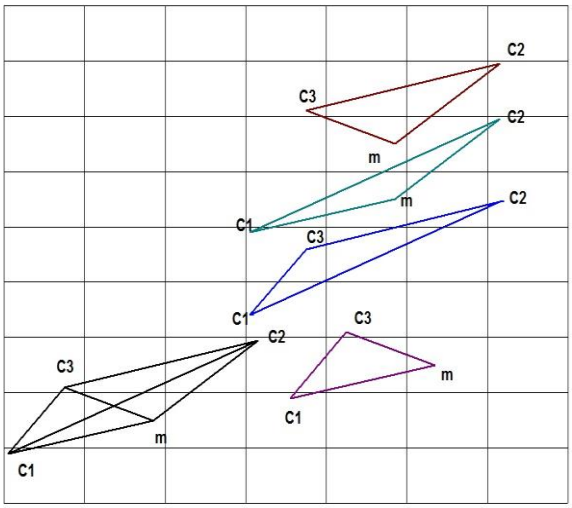



Рис. 4 – Декомпозиция окрестности минуции

Таблица 1 – Координаты точек и угол прихода минуций

| *Обозначение* | *x* | *y* | *θ* |
|---|---|---|---|
| m | 137 | 380 | 0,575959 |
| c1 | 115 | 392 | 0,785398 |
| c2 | 101 | 368 | 0,575959 |
| c3 | 163 | 409 | 0,785398 |

Для сравнения двух шаблонов из $M$ и $N$ минуций [2], имеющих векторы $W^n = \left[w_1^n, w_2^n, w_3^n, w_4^n\right]$ и $W^m = \left[w_1^m, w_2^m, w_3^m, w_4^m\right]$, которые образуются двумя окрестностями минуций $m$ и $n$ (Рис. 5), можно воспользоваться формулой:

$$p_{nm} = \min_{i,j=1,\ldots,4}\left(\left\|w_i^n, w_i^m\right\|\right), \quad (2)$$

где $n = 1,\ldots,N$ и $m = 1,\ldots,M$.

$\left\| w_i^n, w_i^m \right\|$ - евклидово расстояние между векторами $w_i^n$ и $w_i^m$.

Таблица 2 – Заполнение данными матрицы размера 4×9

| *Декомпозиция* | $d_1$ | $\Delta o_1$ | $\alpha_1$ | $d_2$ | $\Delta o_2$ | $\alpha_2$ | $d_3$ | $\Delta o_3$ | $\alpha_3$ |
|---|---|---|---|---|---|---|---|---|---|
| m-c1-c3 | 25.060 | 0.209 | 0.821 | 37.947 | 0.000 | 1.600 | 27.785 | 0.209 | 0.721 |
| m-c2-c3 | 25.060 | 0.209 | 1.802 | 38.949 | 0.209 | 0.840 | 50.922 | 0.000 | 0.500 |
| m-c1-c2 | 37.947 | 0.000 | 2.623 | 38.949 | 0.209 | 0.263 | 74.330 | 0.209 | 0.256 |
| c1-c2-c3 | 27.785 | 0.209 | 2.439 | 50.922 | 0.000 | 0.458 | 74.330 | 0.209 | 0.244 |

Далее сохраняем минимальное значение для каждого ряда:

$$a_n = \min_m (p_{nm}). \tag{3}$$

Итоговое значение сравнения двух шаблонов имеет вид:

$$S = \frac{\sum_{n=1}^{N} (a_n < t)}{\sqrt{N \cdot M}}, \tag{4}$$

где $t$ - некоторое пороговое значение.

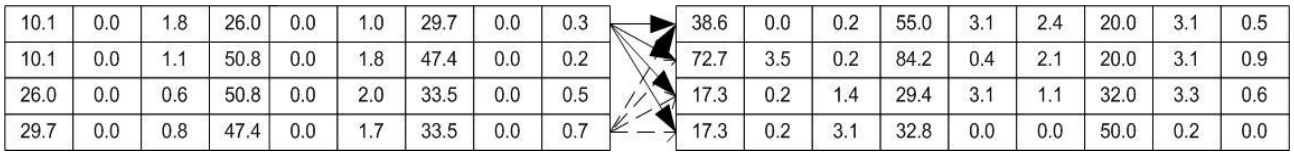



Рис. 5 – Схема сравнения минуций двух шаблонов

## 4 Результаты экспериментов

В рамках моделирования было проведено 78400 ложных и 1372 истинных (*это полный перебор*) испытаний. На рис. 6-7 представлены графики распределений по метрике декомпозиции окрестностей минуций. Таблица 3 содержит значения сравнения шаблонов для нескольких ложных и истинных испытаний. На рис. 8-9 приведены графики *FAR/FRR* (*False Acceptance Rate - уровень ложного принятия*, *False Rejection Rate - уровень ложного отказа*), для каждого типа испытаний, по которым можно определить значение *EER* ≈ 23% *(Equal Error Rate – величина эквивалентной ошибки).*

Табл. 3 – Результаты сравнения шаблонов при ложных и истинных испытаниях

| Значения метрики для ложных испытаний | | | Значения метрики для истинных испытаний | | |
|---|---|---|---|---|---|
| 1_1 | 8_0 | 0,081493 | 0_0 | 0_1 | 0,166248 |
| 1_1 | 8_1 | 0,033013 | 0_0 | 0_2 | 0,306681 |
| 1_1 | 8_2 | 0,049796 | 0_0 | 0_3 | 0,484639 |
| 1_1 | 8_3 | 0,05229 | 0_0 | 0_4 | 0,346349 |
| 1_1 | 8_4 | 0,214177 | 0_0 | 0_5 | 0,28879 |
| 1_1 | 8_5 | 0,051358 | 0_0 | 0_6 | 0,245287 |
| 1_1 | 8_6 | 0,066666 | 0_0 | 0_7 | 0,338063 |
| 1_1 | 8_7 | 0,05912 | 0_1 | 0_2 | 0,386257 |
| 1_1 | 9_0 | 0,281655 | 0_1 | 0_3 | 0,332314 |
| 1_1 | 9_1 | 0,084131 | 0_1 | 0_4 | 0,181061 |
| 1_1 | 9_2 | 0,140809 | 0_1 | 0_5 | 0,34472 |
| 1_1 | 9_3 | 0,18105 | 0_1 | 0_6 | 0,253618 |

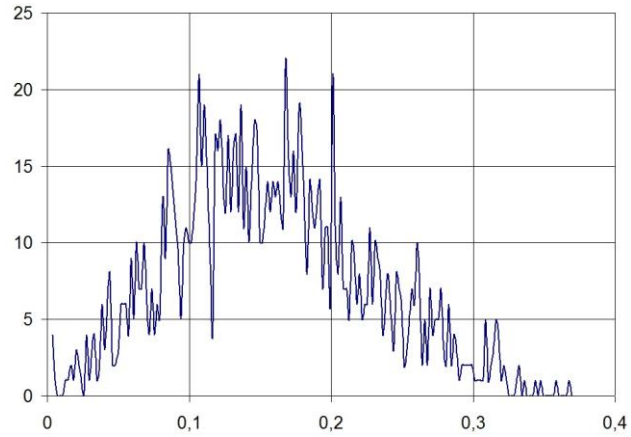



Рис. 6 – Гистограмма распределения истинных испытаний

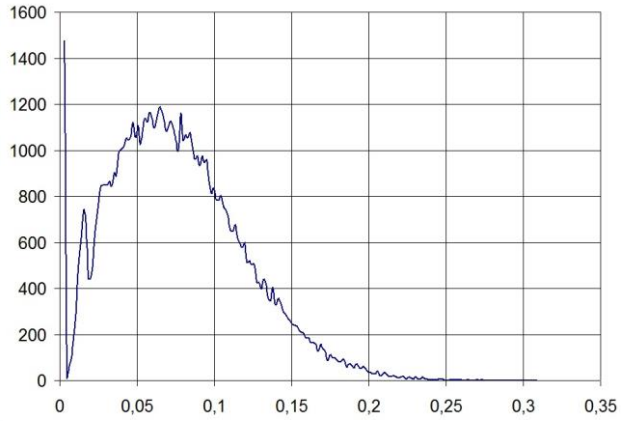



Рис. 7 – Гистограмма распределения ложных испытаний

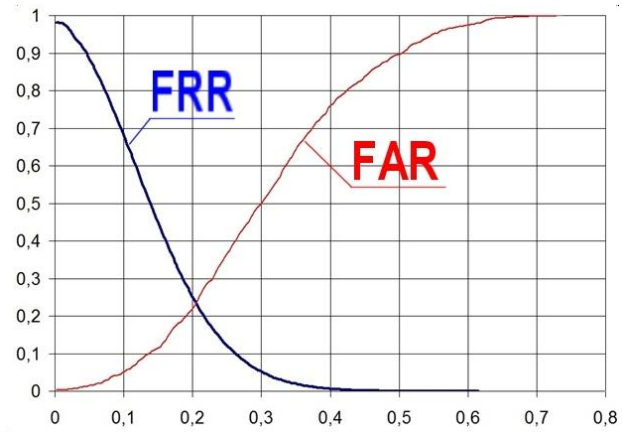



Рис. 8 – Зависимости *FRR* и *FAR*

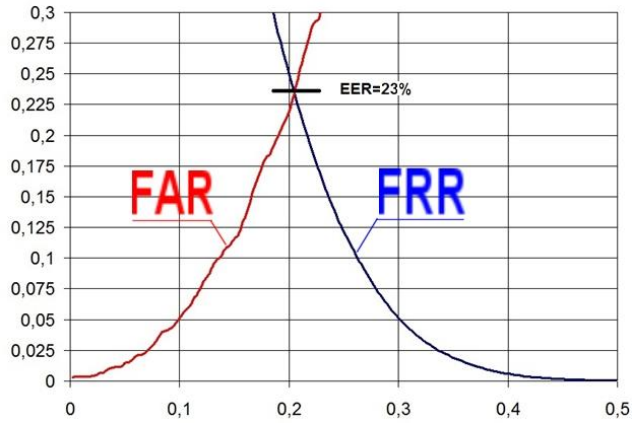



Рис. 9 – Зависимости *FRR* и *FAR*

## 5 Выводы

1. В работе рассмотрено практическое решение задачи верификации отпечатков методом декомпозиции минуций, который позволяет синтезировать локальные структуры для всех минуций, образующих соответствующий шаблон отпечатка.

2. К очевидным преимуществам этого метода следует отнести: - простоту реализации и высокую скорость обработки базы данных. Так, время обработки всей базы данных составляет 42 с, а одного шаблона - 0,17 с. При использовании же цилиндрического кода, полный перебор той же базы данных, занимает 30 мин.

Полный перебор при постановке задачи верификации составляет 60 мин, тогда как при обработке цилиндрического кода это может занять 24 часа.

3. К недостаткам описанного метода следует отнести низкую точность полученных результатов, *EER* = 23%. Однако путем реализации некоторых манипуляций, возможно, некоторое улучшение полученного результата. Например, это может быть построение выпуклой оболочки для координат минуций шаблона, которая будет обеспечивать исключение крайних искаженных точек образца (отпечатка).

## Ссылки

[1] Lantian Li, Chao Xing, Dong Wang, Kaimin Yu, Thomas Fang Zheng, Binary Speaker Embedding, In arXiv:1510.05937v2 31 Mar 2016. https://ieeexplore.ieee.org/document/7918381 - 20.06.2020.

[2] Jin Zhe, Andrew Teoh Beng Jin, Fingerprint template protection with Minutia Vicinity Decomposition. Article, 2011. https://www.researchgate.net/publication/261431544_Fingerprint_template_protection_with_Minutia_Vicinity_Decomposition - 20.06.2020.

[3] Wajih Ullah Baig, Umar Munir, Waqas Ellahi, Adeel Ejaz, Kashif Sardar Minutia texture cylinder codes for fingerprint matching https://arxiv.org/pdf/1807.02251.pdf , Article 2018 - 20.06.2020.

[4] Melkozerova, O., Shlokin, V., Malakhov, S. Mathematical model of the biometric system of fingerprint authentication. Problems of informatization: abstracts of the reports of the seventh international conference on November 13-15, 2019, Pages. 92.
[5] Melkozerova, O., Malakhov, S. Features of automated software testing procedures. Problems of informatization: abstracts of the reports of the seventh international conference on November 13-15, 2019, Pages 36.
[6] Melkozerova, O., Rassomakhin, S. Identification of fingers on the basis of Hamiltonian cycles of local features. the Bulletin of KNU Series "Mathematical Modeling. IT. ACS". Bulletin of V. Karazin Kharkiv National University series «Mathematical Modelling. Information Technology. Automated Control Systems». 2019. Issue 44. Pages 51–65. https://periodicals.karazin.ua/mia/article/view/15767 - 20.06.2020.

**Reviewer**: Vyacheslav Kalashnikov, Doctor of Sciences (Physics and Mathematics), Full Prof., Department of Systems and Industrial Engineering, Campus Monterrey, Monterrey, Mexico. E-mail: kalash@itesm.mx

Received on April 2020.

**Authors:**
Olha Melkozerova, Ph.D., Senior Lecturer, Department of Security of Information Systems and Technologies, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine. E-mail: olja.mex@gmail.com
Serhii Malakhov, Ph.D., Senior Researcher, Associate Professor, Department of Security of Information Systems and Technologies,, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine. E-mail: mailgate@meta.ua

**Fingerprint verification by the method of minutia decomposition.**

**Abstract.** Currently, an attempt is being made to introduce biometric technologies in various spheres of public and state life: forensics, access control systems, applications on mobile devices, banking, etc. The problem of accuracy remains an open question for discussion, because when solving the problem of verification of biometric samples there are problems of addition or disappearance of reference points, deformation of distances between them, linear and angular displacements of the whole sample. Also, the developed biometric systems do not meet all the requirements of information security, namely the integrity, accessibility, authenticity, indisputability, observability and confidentiality. The article presents an analysis of the method of decomposition of minefields during fingerprint verification, describes its advantages and disadvantages in comparison with other methods. It is based on the creation of local structures for each minute of the imprint, because it is the local structures that are resistant to mixing, angular and linear displacement of points. Building global structures often does not lead to good accuracy, as there is a problem of centering the entire sample. A complete list of tests of samples of the database of fingerprints during their verification by this method. An algorithm for constructing a code for an arbitrary minution and an algorithm for comparing two sample templates are described. The results of the article show the value of pairwise comparisons of two templates for true and false tests. The indicators of false rejection rate (*FRR*), false access rate (*FAR*), single equivalent error rate (*EER*) were studied.

**Keywords:** Fingerprints; Method Of Minutia Vicinity Decomposition; Minutia.

**Рецензент**: В'ячеслав Калашников, д.ф.-м.н., проф., департамент систем і промислового виробництва Технологічного університету Монтеррея, Монтеррей, Мексика. E-mail: kalash@itesm.mx

Поступила: Квітень 2020.

**Автори:**
Ольга Мелкозьорова, к.т.н., доцент кафедри Безпеки інформаційних систем і технологій, Харківський національний університет імені В. Н. Каразіна, Харків, Україна. E-mail: olja.mex@gmail.com
Сергій Малахов, к.т.н., с.н.с., доцент кафедри Безпеки інформаційних систем і технологій, Харківський національний університет імені В. Н. Каразіна, Харків, Україна. E-mail: mailgate@meta.ua

**Верифікація відбитків пальців методом декомпозиції мінуцій.**

**Анотація.** У теперішній час здійснюється спроба впровадження біометричних технологій у різні сфери суспільного і державного життя: криміналістика, системи контролю доступу, додатки на мобільних пристроях, банківське діло і т.п. Проблема точності при цьому залишається відкритим питанням для обговорення, тому що при вирішенні задачі верифікації біометричних зразків виникають проблеми дописування або зникнення опорних точок, деформація відстаней між ними, лінійні та кутові зміщення всього зразку. Також розроблені біометричні системи не відповідають всім вимогам інформаційної безпеки, а саме цілісності, доступності, автентичності, незаперечності, спостережливості та конфіденційності. У статті наведено аналіз методу декомпозиції околиць міну цій при верифікації відбитків пальців, описано його переваги та недоліки у порівнянні з іншими методами. Він базується на створенні локальних структур для кожної мінуції відбитку, тому що саме локальні структурі мають стійкість до змішування, кутового та лінійного зміщення точок. Побудова глобальних структур найчастіше не призводить до гарних показників точності, так як виникає проблема центрування всього зразку. Проведено повний перебір випробувань зразків бази даних відбитків пальців при їх верифікації цим методом. Описано алгоритм побудови коду для довільної мінуції та алгоритм порівняння двох шаблонів зразку. У результатах статті наведено значення парних порівнянь двох шаблонів для істинних та хибних випробувань. Досліджено показники хибної відмови (*FRR – False Rejection Rate*), хибного доступу (*FAR – False Acceptance Rate*), єдиної еквівалентної помилки (*EER – Equal Error Rate*).

**Ключові слова:** відбитки пальців; метод декомпозиції околиці мінуції; мінуція.

УДК 004.056.5 DOI: 10.26565/2519-2310-2020-1-05

# УДОСКОНАЛЕНА СХЕМА ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ НА ОСНОВІ КОДІВ

Олександр Кузнецов[1,2], Анастасія Кіян[2], Тетяна Кузнецова[1]

[1] Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, Харків, 61022, Україна
[2] ПАТ «Інститут інформаційних технологій», вул. Бакуліна, 12, Харків, 61166, Україна
kuznetsov@karazin.ua, nastyak931@gmail.com, kuznetsova.tatiana17@gmail.com

**Рецензент**: Сергій Кавун, доктор економічних наук, к.т.н., проф., Харківський технологічний університет "Шаг", вул. Малом'ясницька, 9/11, Харків, 61010, Україна.
kavserg@gmail.com

Надійшло: Квітень 2020.

***Анотація***. *Стаття присвячена вивченню та дослідженню властивостей криптосистем на основі кодів. Вони забезпечують високий рівень безпеки навіть в умовах квантового криптографічного аналізу, тобто відносяться до криптосистем нового покоління, до так званих, криптосистем для пост-квантового застосування. Головним недоліком відомих схем цифрового підпису із застосуванням кодів є великий час на формування підпису. Це пов'язано із великою кількістю спроб декодування випадково сформованого вектору (який інтерпретується як синдромний вектор). Висока складність такої процедури вимагає пошуку нових механізмів та алгоритмів, які б прискорили формування електронного підпису за допомогою кодів. У статті представлено результати за двома векторами досліджень. По-перше, ми пропонуємо нову кодову схему цифрового підпису, що базується на використанні однонаправленої функції із класичної криптосистеми Мак-Еліса і не тільки дозволяє забезпечити належний рівень стійкості до класичного криптоаналізу та криптоаналізу із застосуванням квантових компютерів, але і, порівняно із відомими альтернативами,надає захист від атак особливого типу, таких як атака одночасної підробки. Також наводяться кількісні оцінки надійності та швидкості нового криптографічного алгоритму, які отримано шляхом експериментальної перевірки на кодах БЧХ. Другий вектор досліджень стосується дослідження нового напряму, який пов'язаний із модифікацією роботи декодеру шляхом штучного збільшення виправляючої здатності коду. Завдяки вдосконаленій схемі декодування ми можемо значно скоротити час генерації підписів. У роботі підтверджено ефективність застосуванння запропонованої модифікації декодеру алгебраїчних блокових кодів при реалізації нової схеми цифрового підпису у порівнянні із класичним декодером Пітерсона-Горенстейна-Цирлера у контексті порівняння швидкості формування підпису та кількості необхідних спроб декодування.*

***Ключові слова***: *криптосистеми на кодах; пост-квантова криптографія; електронний підпис; алгебраїчне декодування.*

## 1 Вступ

У сучасному інформаційному суспільстві важко переоцінити значимість електронного цифрового підпису, що застосовується як для ідентифікації особистості автора, так і для підтвердження цілісності та справжності підписаного ним документа. Це дозволяє надійно використовувати електронний документообіг та отримувати доступ до критично важливих ресурсів [1–3].

На сьогодні у комп'ютерних системах застосовується набір перевірених та стандартизованих на світовому чи державному рівні криптоалгоритмів [4–6]. Однак більшість з подібних схем втратять свою надійність із застосуванням криптоаналізу на повномасштабних квантових комп'ютерах [7–9], розробкою яких займаються ряд компаній зі світовим ім'ям (IBM®, Google® та інші), оскільки подібні методи криптоаналізу здатні вирішувати поширені математичні задачі такі, як дискретне логарифмування чи факторизація, за поліноміальний час. Цей факт призведе до потенційної вразливості не тільки окремих громадян, але і державної електронної документації в цілому [10].

З цієї причини необхідним є всебічне дослідження та аналіз нових методів для формування електронного цифрового підпису, що базуються на принципово інших математичних основах [11]. Подібним перспективним напрямком досліджень пост-квантової криптографії є криптографія, заснована на кодах [12]. Прийнято вважати, що кодова криптографія є ефективною для побудови схем направленого шифрування та інкапсуляції ключів, тоді як для фор-

мування та перевірки цифрового підпису вона не є раціональним рішенням через високу обчислювальну складність [12].

У цілому ряді попередніх робіт [13–15] ми вже розглядали нову кодову схему електронного цифрового підпису (ЕЦП) та довели її ефективності, порівняно з поширеною альтернативою - схемою CFS [16]. Мета цієї роботи полягає в короткому огляді запропонованої схеми та представленню її модифікації із новим декодером, якій дозволяє відчутно знизити обчислювальні затрати на формування підпису, що є вагомим практичним кроком для подолання основного недоліку кодових схем ЕЦП.

## 2 Кодові схеми ЕЦП

Схема функціонування запропонованої схеми розглядається у якості прикладу роботи кодових схем електронного цифрового підпису, оскільки спільною рисою цих схем є циклічне декодування синдрому задля отримання вектору, що потім стане складовою кінцевого підпису. Повторне декодування є найбільш витратною частиною алгоритму, оскільки зі збільшення кодових параметрів збільшується стійкість схеми, але одночасним є збільшення необхідної кількості спроб для успішного декодування [16].

Запропонована у [13–15] схема цифрового підпису базується на використанні односторонньої функції з класичної криптосистеми Мак-Еліса [17]. Її сутність полягає у інтерпретації гешованого повідомлення у якості кодового слова з помилками, що обчислено згідно двох векторів $I$ та $e$, які разом зі значенням лічильника складають вихідний підпис.

Розглянемо функціонування схеми, у вигляді чотирьох етапів.

*Eman 1*. Генерація поля $GF(p^m)$, параметрів коду $m,t \in \mathbb{N}$ та обрання конкретного типу коду, що буде використовуватися.

*Eman 2*. Формування секретних ключів, що представляють собою матриці $X, P, G$, які є випадковою невиродженою, переставною та породжуючою матрицею відповідно. Формування відкритого ключа $H_X = X \cdot G \cdot P$.

*Eman 3*. Формування підпису.

Вхід: повідомлення $M$, геш-функція $h$, параметри $m,t$.

Вихід: підпис у форматі $Y = (I, e, i)$.

1) Обчислюємо геш-значення $h(M)$, згідно обраної на етапі ініціалізації геш-функції. Результатом роботи такої функції є вектор довжини $n$;

2) Встановлюємо значення лічильника $i = 1$;

3) Знаходимо геш-значення повідомлення $h(M)$, а потім геш-значення $h(h(M) \| i)$, де $\|$ позначає конкатенацію лічильника та геш-значення повідомлення;

4) Тлумачимо $h(h(M) \| i)$ у вигляді кодового слова з помилками $c'_x = (c_0, c_1, ..., c_{n-1})$, на значення якого впливають три фактори: секретний ключ, інформаційне повідомлення $I = (I_0, I_1, ..., I_{k-1})$ та вектор помилок $e = (e_0, e_1, ..., e_{n-1})$, а саме

$$c'_x = I \cdot G_x + e = I \cdot X \cdot G \cdot P + e \ ;$$

5) Множимо знайдене кодове слово на обернену переставну матрицю:

$$c'_x \cdot P^{-1} = I \cdot X \cdot G \cdot P \cdot P^{-1} + e \cdot P^{-1} = I \cdot X \cdot G + e \cdot P^{-1} \ .$$

Отриманий результат представляє з собою кодове слово, що викривлене не більше, ніж в $t$ розрядах. По відношенню до нього можна застосувати алгоритм швидкого декодування для отримання необхідних векторів $I$ та $e$.

6) Декодуємо отримане кодове слово $c'_x = (c_0, c_1, ..., c_{n-1})$:

- Якщо декодування вдале, продовжуємо обчислення;
- Якщо декодування невдале, збільшуємо значення лічильника на 1, та повторюємо кроки №№ 3-6;

7) Декодування дозволило отримати вектори $I' = I \cdot X$ та $e' = e \cdot P^{-1}$;

8) Обчислюємо вектори $I' \cdot X^{-1} = I$ та $e' \cdot P = e$;

9) Формуємо підпис: $Y=(I,e,i)$.

Декодування кодового слова для уповноваженого користувача, як і декодування синдромної послідовності, є задачею поліноміальної складності. Для неуповноваженого користувача напроти *NP*–складною задачею, розв'язання якої обчислювально недосяжне за нормальних умов.

*Етап 4*. Перевірка підпису.

Вхід: повідомлення $M$, підпис $Y=(I,e,i)$, геш-функція $h$, відкритий ключ $G_x$.

Вихід: висновок про коректність підпису.

Сутність перевірки підпису полягає у перевірці факту, чи інтерпретація геш-функції у якості кодового слова з помилками обчислена за переданим у підписі вектором помилок $e=(e_0,e_1,...,e_{n-1})$ та вектором $I=(I_0,I_1,...,I_{k-1})$. Для того, щоб здійснити подібну перевірку, необхідно:

1. Знайти геш-значення $s'_x=h(h(M)\|i)$;
2. Обчислити вектору $s''_x=I\cdot G_x+e$;
3. Порівняти отримані $s'_x$ та $s''_x$. Якщо вектори збігаються, то можливо зробити висновок про коректність підпису. В іншому випадку-підпис відхиляється.

Очевидним є той факт, що найбільше часу серед представленого алгоритму формування підпису, вимагає саме крок повторного декодування синдрому. І ефективність процедури декодування напряму залежить від типу використовуваного декодеру. Нижче розглянемо типовий декодер, що використовує схеми кодового цифрового підпису, а також нову - модифіковану схему декодеру, яка дозволяє суттєво оптимізувати процес.

## 3 Удосконалена схема електронного підпису на кодах

На сьогодні найбільш поширеними кодами, що застосовуються при реалізації кодових схем ЕЦП є коди Гоппа та коди БЧХ [12,16,18]. Нижче розглянемо останню модифікацію відповідних схем. Відомо, що коди БЧХ відносять до класу циклічних кодів і з цієї причини вони можуть бути декодовані методами, що застосовуються до декодування циклічних кодів, а також із застосуванням спеціально розроблених методів, зокрема метод на основі рішення ключового рівняння [19–21]. Сутність цього методу полягає у знаходженні многочлену локаторів помилок. З цією метою можуть бути застосовані лише три метода: алгоритм Пітерсона, алгоритм Евкліда та алгоритм Берлекемпа-Мессі [19, 20].

Найбільш універсальним при цьому є алгоритм Пітерсона, що дозволяє виконати декодування, як у двійковому, так і у недвійковому випадку, на відміну від своїх альтернатив, які потребують для недвійкового випадку проведення додаткових етапів. Докладно алгоритм Пітерсона представлено у роботах [19–21]. Спираючись на такі міркування, вважаємо за можливе запропонувати власну, модифіковану конфігурацію декодера, яка може бути застосована для оптимізації обчислень кодових схем цифрового підпису.

Як відомо, для коректного формування підпису важливим є сам факт правильності декодування синдромної послідовності, а не те, у який вектор вона декодується. З цієї причини сутність запропонованої схеми декодера полягає у штучному збільшенні виправляючої здатності коду $t$, без зміни інших кодових параметрів. Цей факт дозволить збільшити кількість дозволених комбінацій, у які може декодуватися синдромна послідовність.

Припустимо, що задано код $(n,k,d=2t+1)$. На вхід декодеру подається послідовність довжини $n-k$. У полі $GF(2^m)$ кількість можливих послідовностей дорівнює $2^{n-k}$. На виході декодеру має бути отримано послідовність довжини $n$, при чому кількість помилок має не перевищувати виправлячу здатність коду $t$. Всього можливих конфігурацій помилок $C_n^t$. Таким чином ймовірність успішного декодування можна визначити як відношення кількості можливих наборів помилок до загальної кількості вхідних синдромів:

$$P = \frac{C_n^t}{2^{n-k}} .$$

Узагальнений алгоритм декодера можна представити у вигляді наступних кроків:

1. На вхід декодеру поступає значення виправляючої здатності коду $t$, коефіцієнт штучного збільшення виправляючої здатності $\eta$ та кодова комбінація $c'(x) = c(x) + e(x)$, де $c(x)$ - це передана комбінація, у якій під час передачі виникли помилки, що представлені у вигляді многочлену $e(x) = e_{i_1} x^{i_1} + e_{i_2} x^{i_2} + ... + e_{i_v} x^{i_v}$, де $0 \le v \le t$ представляє собою кількість помилок, $e_{i_k}$ -значення помилки, $i_k$ - номер позиції, в якій відбулася помилка. Для того, щоб виправити помилку, необхідно визначити $e_{i_k}$ та $i_k$;

2. Встановити кількість рівнянь $v = t$ рівною значенню виправляючої здатності коду;

3. Обчислити синдроми $s(x) = s_1 x^0 + s_2 x^l + ... + s_{n-k} x^{n-k-l}$, де коефіцієнти $s_i$ визначаються підстановкою у $c(x)$ коренів $\alpha^i$ породжуючого многочлена коду;

4. Інтерпретувати обчислені синдроми у вигляді матриці при $\mu = v$

$$M = \begin{bmatrix} s_1 & s_2 & s_\mu \\ s_2 & s_3 & s_{\mu+1} \\ \dots & \dots & \dots \\ s_\mu & s_{\mu+1} & s_{2\mu-1} \end{bmatrix}.$$

Матриця є невиродженою, якщо виникло рівно $t$ помилок, у іншому випадку матриця є виродженою і у цьому випадку детермінант матриці дорівнює 0, та необхідно повторити кроки №№ 2-4 для $v = v - 1$;

5. Синтезувати многочлен локаторів помилок $\lambda(x)$ згідно із знайденими попередньо коефіцієнтами. Визначення коефіцієнтів многочлена локаторів помилок в алгоритмі Пітерсона зводиться до рішення $v$ лінійних рівнянь з $v$ невідомими коефіцієнтами $\lambda_k$;

6. Обчислити локатори $x_i$ многочлена $\lambda(x)$ за допомогою процедури Ченя: послідовне обчислення $\lambda(\alpha^j)$ для кожного можливого $j$ та перевірка отриманих значень на нуль. Якщо $\lambda(\alpha^{-k})$ дорівнює нулю, то $\alpha^k$ є локатором помилки;

7. Знайти синдроми $s'_x$ згідно многочлену локаторів помилок;

8. Перевірити рівність векторів $s_x = s'_x$:
   - Якщо вектори рівні, то декодування вдале і декодування завершується;
   - Якщо вектори відрізняються, то збільшуємо значення виправляючої здатності коду $t = t + 1$ та повторюємо кроки №№ 1-7 до тих пір, поки декодування не буде вдалим, або поки значення виправляючої здатності не досягне значення, заданого коефіцієнтом збільшення.

## 4 Експериментальні дослідження

З метою дослідження особливостей функціонування запропонованого декодеру було синтезовано відповідні реалізації схеми CFS [16] та розглянутої вище схеми, з урахуванням декодеру Пітерсона і запропонованого нами декодеру на мові програмування Java. Проведене моделювання підтвердило теоретичні твердження [13–15], а саме, що практичні результати експериментів для схеми CFS та запропонованої схеми є еквівалентними. Враховуючи цю обставину наведемо результати експериментів лише для запропонованої схеми.

*Експеримент №1*.

Вхідні дані: код $(n, k, d = 2t + 1)$, $n = 255$, параметр $t$ змінюється від 1 до 11 з кроком 1. У залежності від параметра $t$ відповідно змінюється і параметр $k$. Використовується зви-

чайний (відомий) декодер. Результати наведено у таблиці 1.

Таблиця 1 – Результати експерименту №1

| n | k | t | Час підпису, mc | Кількість спроб для успішного декодування |
|---|---|---|---|---|
| 255 | 247 | 1 | 196 | 1 |
| 255 | 239 | 2 | 43 | 1 |
| 255 | 231 | 3 | 30 | 4 |
| 255 | 223 | 4 | 160 | 42 |
| 255 | 215 | 5 | 460 | 213 |
| 255 | 207 | 6 | 2043 | 1356 |
| 255 | 199 | 7 | 739 | 417 |
| 255 | 191 | 8 | 432499 | 262670 |
| 255 | 187 | 9 | 15874 | 8355 |
| 255 | 179 | 10 | 1681908 | 781048 |

Вихідні дані: кількість спроб для успішного декодування та значення швидкості формування підпису.

*Експеримент №2*.

Вхідні дані: код $(n,k,d=2t+1)$, $n=255$, параметр $t$ змінюється від 1 до 11 з кроком 1. У залежності від параметра $t$ відповідно змінюється і параметр $k$. Використовується новий декодер зі збільшенням $t$ на 2 та коефіцієнтом $\eta=0.7$. Результати наведено у таблиці 2.

Таблиця 2 – Результати експерименту №2

| n | k | t | Час підпису, mc | Кількість спроб для успішного декодування |
|---|---|---|---|---|
| 255 | 247 | 1 | 147 | 1 |
| 255 | 239 | 2 | 50 | 2 |
| 255 | 231 | 3 | 32 | 1 |
| 255 | 223 | 4 | 122 | 11 |
| 255 | 215 | 5 | 75 | 8 |
| 255 | 207 | 6 | 2241 | 732 |
| 255 | 199 | 7 | 8624 | 2615 |
| 255 | 191 | 8 | 14922 | 4128 |
| 255 | 187 | 9 | 139732 | 30101 |
| 255 | 179 | 10 | 147717 | 31476 |

Вихідні дані: кількість спроб для успішного декодування та значення швидкості формування підпису.

*Експеримент №3*.

Вхідні дані: код $(n,k,d=2t+1)$, $n=255$, параметр $t$ змінюється від 1 до 11 з кроком 1. У залежності від параметра $t$ відповідно змінюється і параметр $k$. Використовується новий декодер зі збільшенням $t$ на 4 та коефіцієнтом $\eta=0.7$. Результати наведено у таблиці 3.

Вихідні дані: кількість спроб для успішного декодування та значення швидкості формування підпису.

Відобразимо отримані дані моделювання у вигляді відповідних залежностей часу підпису від коректуючої здатності коду та кількості спроб для успішного декодування (див. Рис. 1-2). Отримані залежності представлені у логарифмічному масштабі за віссю ординат. Розрахунок логарифмічного значення здійснено згідно з формулою: $y=\lfloor \log_{10} y' \rfloor$, де символ $\lfloor\ \rfloor$ - позначає округлення значення до найменшого цілого.

Таблиця 3 – Результати експерименту №3

| n | k | t | Час підпису, mc | Кількість спроб для успішного декодування |
|---|---|---|---|---|
| 255 | 247 | 1 | 197 | 1 |
| 255 | 239 | 2 | 60 | 1 |
| 255 | 231 | 3 | 46 | 3 |
| 255 | 223 | 4 | 78 | 5 |
| 255 | 215 | 5 | 741 | 121 |
| 255 | 207 | 6 | 1717 | 368 |
| 255 | 199 | 7 | 16513 | 3373 |
| 255 | 191 | 8 | 63055 | 11262 |
| 255 | 187 | 9 | 138325 | 24848 |
| 255 | 179 | 10 | 1532886 | 197837 |

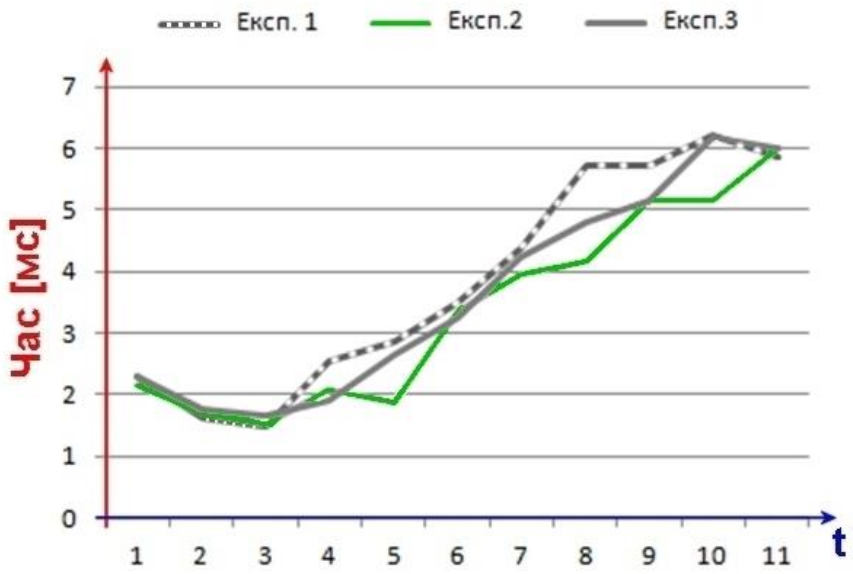



Рис. 1 – Швидкість формування підпису з використанням різних декодерів

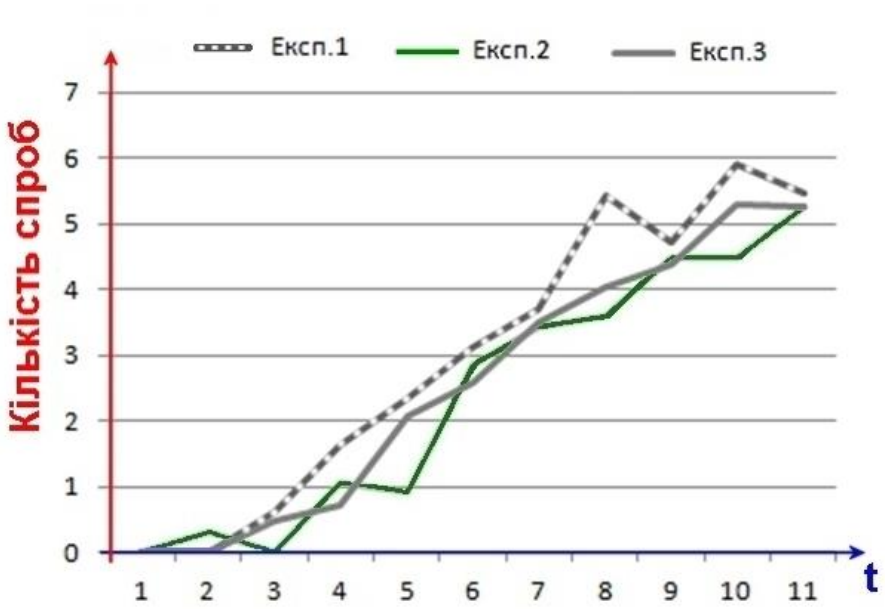



Рис. 2 – Кількість спроб для успішного декодування
з використанням різних декодерів

Змінний характер графіків швидкості пояснюється залежністю швидкості від кількості спроб, які необхідні для успішного декодування, а також завантаженістю обчислювальної платформи, яка вносить похибку. Більш об'єктивним є показник кількості спроб декодування. Так, якщо ми збільшимо параметр $t$ на 1, то це автоматично збільшить кількість можливих конфігурацій помилок у

$$\frac{C_n^{t+1}}{C_n^t} = \frac{n!t!(n-t)!}{(t+1)!\cdot(n-t-1)!n!} = \frac{n-t}{t+1}$$

разів. Звідси, збільшення загальної ймовірності декодування буде відбуватися поки $n-t > t+1$, тобто $t < \frac{n+1}{2}$. Для обмеження даної величини в роботу декодеру було введено додатковий параметр, коефіцієнт збільшення t, аби запобігти випадкам нераціонального виконання алгоритму.

Спираючись на аналіз отриманих результатів моделювання, можна зробити висновок, що застосування запропонованого декодеру дозволяє зменшити час, якій необхідний для формування підпису. Цей ефект досягається за рахунок того, що дообчислення додаткових синдромів та повторне декодування потребують меншої кількості обчислень, ніж збільшення лічильника і виконання усіх кроків: - від гешування значень до декодування.

## 5 Висновки

Кодова криптографія є одним з найбільш перспективних напрямків розвитку пост-квантової криптографії, особливо у контексті реалізації схем направленого шифрування та інкапсуляції ключів. Однак, цей напрямок криптографії рідко розглядають як альтернативу для реалізації пост-квантового цифрового підпису через високу обчислювальну складність алгоритму формування ЕЦП. Ця складність, перш за все, обумовлена складністю циклічного декодування синдрому, оскільки етап декодування в алгоритмах формування цифрового підпису вимагає найбільшу кількість обчислень. При цьому ефективність декодування напряму залежить від використовуваного декодеру.

В даній роботі авторами запропоновано та досліджено принципово новий тип декодеру, що реалізує штучне збільшення значення виправляючої здатності після невдалого декодування та повторному декодуванні синдрому. Такий принцип роботи дозволяє збільшити ймовірність успішного декодування через збільшення кількості можливих наборів помилок по відношенню до загальної кількості вхідних синдромів.

Проведені практичні дослідження довели, що застосування запропонованої схеми роботи декодеру, порівняно із типовим декодером циклічних кодів Пітерсона, дозволяє значно зменшити кількість спроб, необхідних для декодування синдрому, і таким чином зменшити час, що вимагає алгоритм формування цифрового підпису. Зменшення часових витрат обумовлюється тим, що дообчислення додаткових синдромів і повторне декодування потребують меншої кількості обчислень, ніж збільшення значення лічильника та повторне виконання усіх кроків від гешування значень до декодування.

Подібна, удосконалена схема декодеру може бути застосована не тільки до розглянутого конкретного прикладу запропонованої кодової схеми підпису, але і для усіх схем цифрового підпису, що базуються на використанні циклічних кодів.

Подальшим напрямком досліджень є вивчення можливостей застосування запропонованого підходу до інших класів кодів, зокрема, до кодів Гоппи, на яких будується більшість надійних та безпечних кодових криптосистем [12, 22].

## Посилання

[1] Padhye S. et al. Digital Signature [Electronic resource] // Introduction to Cryptography. CRC Press, 2018. P. 205–222. URL: https://www.taylorfrancis.com/ (accessed: 16.07.2020).

[2] Priyadarshini S.B.B. et al. Digital Signature and Its Pivotal Role in Affording Security Services [Electronic resource] // Handbook of e-Business Security. Auerbach Publications, 2018. P. 365–384. URL: https://www.taylorfrancis.com/ (accessed: 16.07.2020).

[3] Martin K.M. Digital Signature Schemes. Oxford University Press, 2017. Vol. 1.
[4] Rubinstein-Salzedo S. Cryptography. Cham: Springer International Publishing, 2018.
[5] Klima R.E. et al. Cryptology : Classical and Modern. Chapman and Hall/CRC, 2018.
[6] Martin K. Everyday Cryptography. Oxford University Press, 2017. Vol. 1.
[7] National Academies of Sciences E. Quantum Computing: Progress and Prospects. 2018.
[8] Aaronson S. Quantum computing and hidden variables // Phys. Rev. A. 2005. Vol. 71, № 3. P. 032325.
[9] Preskill J. Quantum Computing in the NISQ era and beyond // Quantum. 2018. Vol. 2. P. 79.
[10] Post-Quantum Cryptography: 11th International Conference, PQCrypto 2020, Paris, France, April 15–17, 2020, Proceedings / ed. Ding J., Tillich J.-P. Cham: Springer International Publishing, 2020. Vol. 12100.
[11] Computer Security Division I.T.L. Post-Quantum Cryptography | CSRC | CSRC [Electronic resource] // CSRC | NIST. 2017. URL: https://content.csrc.e1c.nist.gov/Projects/Post-Quantum-Cryptography/faqs (accessed: 16.07.2020).
[12] Overbeck R., Sendrier N. Code-based cryptography // Post-Quantum Cryptography / ed. Bernstein D.J., Buchmann J., Dahmen E. Berlin, Heidelberg: Springer, 2009. P. 95–145.
[13] Kuznetsov A. et al. Code-based electronic digital signature // 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). 2018. P. 331–336.
[14] Kuznetsov A. et al. New Approach to the Implementation of Post-Quantum Digital Signature Scheme // 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT). 2020. P. 166–171.
[15] Kuznetsov A. et al. Code-Based Schemes for Post-Quantum Digital Signatures // 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). 2019. Vol. 2. P. 707–712.
[16] Courtois N.T., Finiasz M., Sendrier N. How to Achieve a McEliece-Based Digital Signature Scheme // Advances in Cryptology — ASIACRYPT 2001 / ed. Boyd C. Berlin, Heidelberg: Springer, 2001. P. 157–174.
[17] McEliece R.J. A Public-Key Cryptosystem Based On Algebraic Coding Theory // Deep Space Netw. Prog. Rep. 1978. Vol. 44. P. 114–116.
[18] Finiasz M. Parallel-CFS // Selected Areas in Cryptography / ed. Biryukov A., Gong G., Stinson D.R. Berlin, Heidelberg: Springer, 2011. P. 159–170.
[19] Blahut R.E. Theory and Practice of Error Control Codes. Reprint. with corr edition. Reading, MA: Addison-Wesley, 1983. 500 p.
[20] The Theory of Error-Correcting Codes. Elsevier, 1977. Vol. 16.
[21] Clark G.C., Cain J.B. Error-Correction Coding for Digital Communications. Boston, MA: Springer US, 1981.
[22] Kuznetsov A. et al. Code-based public-key cryptosystems for the post-quantum period // 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T). 2017. P. 125–130.

**Рецензент:** Сергей Кавун, доктор экономических наук, к.т.н., проф., Харьковский технологический университет "ШАГ", ул. Маломясницкая, 9/11, Харьков, 61010, Украина.
E-mail: kavserg@gmail.com

Поступила: Апрель 2020.

**Авторы:**

Александр Кузнецов, д.т.н., проф., ХНУ имени В.Н. Каразина, Харьков, 61022, Украина.
E-mail: kuznetsov@karazin.ua

Анастасия Киян, аналитик по системам защиты информации, АО "Институт информационных технологий", ул. Бакулина, 12, Харьков, 61166, Украина.
E-mail: nastyak931@gmail.com

Татьна Кузнецова, научный сотрудник, ХНУ имени В.Н. Каразина, Харьков, 61022, Украина.
E-mail: kuznetsova.tatiana17@gmail.com

**Усовершенствованная схема электронной цифровой подписи на основе кодов.**

**Аннотация.** Статья посвящена изучению и исследованию свойств криптосистем на основе использования кодов. Они обеспечивают высокий уровень безопасности даже в условиях квантового криптографического анализа, то есть относяться к криптосистем нового поколения, к так называемым, криптосистемам для пост-квантового применения. Главным недостатком известных схем цифровой подписи с использованием кодов является большое время, требуемое для формирования подписи. Это связано с большим количеством попыток декодирования случайно сформированного вектора (который интерпретируется как синдромный вектор). Высокая сложность такой процедуры требует поиска новых механизмов и алгоритмов, которые способны ускорить формирование электронной подписи. В статье представлены результаты согласно двух векторов исследований. Во-первых, мы предлагаем новую кодовую схему цифровой подписи, которая основана на использовании однонаправленной функции из классической криптосистемы Мак-Элиса и не только позволяет обеспечить надлежащий уровень устойчивости к классическому криптоанализу и криптоанализу с применением квантовых компьютеров, но и по сравнению с известными альтернативами, предоставляет защиту от атак особого типа, таких как атака одновременной подделки. Также приводятся количественные оценки надежности и скорости нового криптографического алгоритма, полученные путем экспериментальной проверки реализаций на кодах БЧХ. Второй вектор исследований касается исследования нового направления, связанного с модификацией работы декодера алгебраических блоковых кодов путем искусственного увеличения исправляющей способности кода. Благодаря усовершенствованной схеме декодирования мы можем значительно сократить время генерации подписей. В работе подтверждена эффективность применения предлагаемой модификации декодера при реализации новой схемы цифровой подписи по сравнению с классическим декодером Питерсона-Горенстейна-Цирлера в контексте сравнения скорости формирования подписи и количества необходимых попыток декодирования.

**Ключевые слова**: криптосистемы на кодах; пост-квантовая криптография; электронная подпись; алгебраическое декодирование.

**Reviewer**: Serhii Kavun, Doctor of Sciences (Economics), Ph.D. (Engineering), Full Prof., Kharkiv University of Technology "STEP", Malom'yasnitska St. 9/11, Kharkiv, 61010, Ukraine. Ï
E-mail: kavserg@gmail.com

Received on April 2020.

**Authors**:
Alexandr Kuznetsov, Doctor of Sciences (Eng.), Full Prof., V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: kuznetsov@karazin.ua
Anastasiia Kiian, information security analyst, JSC "Institute of Information Technologies", Kharkiv, 61166, Ukraine
E-mail: nastyak931@gmail.com
Tatyana Kuznetsova, Researcher, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: kuznetsova.tatiana17@gmail.com

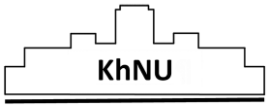
**Advanced code-based electronic digital signature scheme.**

***Annotation.*** The article is devoted to the study and research of the properties of code-based cryptosystems. They provide a high level of security even in the conditions of quantum cryptographic analysis, i.e. belong to the new generation of cryptosystems for post-quantum application. The main disadvantage of the known code-based digital signature schemes is the long time to generate a signature. This is due to the large number of attempts to decode a randomly generated vector (which is interpreted as a syndrome vector). The high complexity of such a procedure requires the search for new mechanisms and algorithms that would accelerate the formation of code-base electronic signatures. The article presents the results of two research vectors. First, we propose a new code-based digital signature scheme on the use of a one-way function from the classical McEliece cryptosystem and not only provides a proper level of resistance to classical cryptanalysis and cryptanalysis using quantum computers, but also, compared to known alternatives, provides protection against special types of attacks, such as simultaneous counterfeit attacks. Quantitative estimates of the reliability and speed of the new cryptographic algorithm, which were obtained by experimental verification on the BCH codes, are also given. The second vector of research concerns the study of a new direction, which is associated with the modification of the decoder by artificially increasing the corrective code ability. Thanks to the improved decoder scheme, we can significantly reduce the generation time of signatures. The paper confirms the effectiveness of the proposed decoder modification in the implementation of a new digital signature scheme in comparison with the classic Peterson-Gorenstein-Zierler decoder in the context of comparing the speed of signature formation and the number of required decoding attempts.

**Key words:** Cryptosystems on codes; Post-quantum cryptography; Electronic signature; Algebraic decoding.

ISSN 2519-2310 DOI: 10.26565/2519-2310-2020-1





Наукове видання

# КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА

**Випуск 1(17) 2020**

Міжнародний електронний науково-теоретичний журнал

Англійською, українською, російською мовами

Комп'ютерне верстання – Федоренко В.В., Єсіна М.В.

61022, Харків, майдан Свободи, 6
Харківський національний університет імені В.Н. Каразіна

V. N. Karazin Kharkiv National University Publishing

CS&CS

2020