УДК 004.056.55 **DOI:10.30837/rt.2020.3.202.07**

Ю.І. ГОРБЕНКО, канд. техн. наук, М.В. ЄСІНА, канд. техн. наук,
В.В. ОНОПРІЄНКО, канд. техн. наук, Г.А. МАЛЄЄВА

МОДЕЛІ ЗАГРОЗ ЩОДО АСИМЕТРИЧНИХ КРИПТОПЕРЕТВОРЕНЬ ПЕРСПЕКТИВНОГО ЕЛЕКТРОННОГО ПІДПИСУ

Вступ

Модель загроз ЕП (далі – Модель загроз) повинна бути документом, яким закріплено найбільш повний перелік загроз щодо існуючих та перспективних ЕП, що може застосовуватись в постквантовий період. Відповідно до Законів України "Про захист інформації в інформаційно-телекомунікаційних системах", "Про електронні довірчі послуги" та "Про захист персональних даних", інформація в основних інформаційних ресурсах поділяється на відкриту і конфіденційну. Інформація у підтримуючих інформаційних ресурсах є технологічною інформацією [1 – 4].

При застосуванні ЕП, незалежно від видів додатків, використовуються асиметричні пари ключів, для кожної пари особистий та відкритий [1, 3 – 5]. В подальшому при реальному застосуванні ЕП відкритий ключ, як правило, є сертифікатом відкритого ключа та є доступним усім користувачам інфраструктури відкритого ключа (ІВК).

Оскільки сертифікат відкритого ключа є відкритою інформацією, то під час обробки згідно з [2, 5] він повинен зберігати цілісність, справжність, доступність, неспростовність та бути захищеним від несанкціонованих дій, які можуть привести до випадкової чи умисної модифікації, нав’язування хибного чи знищення. Усім користувачам, наприклад ІВК, повинен бути забезпечений доступ до ознайомлення з відкритою інформацією, в даному випадку у вигляді сертифіката відкритого ключа [1, 3, 4].

Під час обробки (застосування) конфіденційної інформації, в нашому випадку особистого ключа, вона повинна зберігати цілісність, справжність, доступність, неспростовність та бути захищеною від несанкціонованих дій, а також практично повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання та поширення. Тобто, безумовно повинна бути забезпечена конфіденційність особистого ключа кожного користувача. Також, згідно з [1 – 3] технологічна інформація повинна бути відома тільки авторизованим на це особам та зберігати цілісність.

Таким чином, в усіх відомих додатках, у яких використовується ЕП, стосовно відкритого ключа ЕП повинна бути можливість забезпечення його цілісності, справжності, доступності, неспростовності та захист від несанкціонованих дій, які можуть привести до випадкової чи умисної модифікації, нав’язування хибного чи знищення. Стосовно особистого ключа повинна забезпечуватись його цілісність, справжність, доступність, неспростовність та захист від несанкціонованих дій, а також його захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання та поширення, тобто конфіденційність.

Тобто як існуючі ЕП, так і перспективні ЕП повинні дозволяти гарантовано захищати їх асиметричні пари ключів у відповідності із вказаними вище вимогами, незалежно від їх подання при використанні в апаратному, програмному чи апаратно-програмному вигляді. Причому, незалежно від виду їх обробки, реалізація загроз, що спрямовані на вказані ресурси, може призводити до порушення вимог безпеки первинних інформаційних ресурсів, вплинути на інше програмне забезпечення (ПЗ), що підписується, та, в окремих випадках, на функціонування апаратних ресурсів.

Метою цієї статі є обґрунтування та розробка пропозицій щодо побудування моделі загроз стосовно асиметричних криптоперетворень типу перспективний ЕП, що може застосовуватись в постквантовий період.

Загальні загрози щодо перспективних ЕП та їх оцінка

На наш погляд повний перелік можливих загроз безпеці застосування існуючих та перспективних ЕП, що сформований з числа загроз, наявних у IT-Grundschutz Catalogues з урахуванням апаратних, програмних та апаратно-програмних ресурсів, технологій обробки даних та механізмів криптографічного захисту при застосуванні ЕП, в тому числі з урахуванням вимог та умов синтезу перспективних ЕП та застосуванні ЕП в постквантовий період, може бути прийнятий таким, що наведений нижче.

Загрози, пов'язані з апаратним, програмним забезпеченням та технологіями обробки, що використовуються в ІВК та системі Блокчейн (БЧ), мають розглядатись додатково [4, 8].

У цілому за результатами аналізу щодо методів синтезу та застосування відомих та перспективних ЕП визначено такі загрози:

- закладення вразливостей в алгоритми синтезу та застосування ЕП;
- застосування криптоаналітичних систем щодо аналізу чутливих даних ЕП;
- викрадення чутливих даних ЕП за допомогою мобільних носіїв інформації;
- викрадення пристроїв, носіїв чутливої інформації та документів з чутливими даними ЕП;
- витік чутливих даних ЕП каналами побічних електромагнітних випромінювань і наведень;
- відмова від дій проти загроз щодо чутливих даних ЕП;
- відмова криптомодулю з чутливими даними ЕП;
- відсутнє або недостатнє оповіщення при виникненні інцидентів компрометації чутливих даних ЕП;
- відсутність прозорості для особи, що зацікавлена та уповноважена контролювати захист чутливих даних ЕП;
- відсутня або неповна документація щодо чутливих даних ЕП;
- втрата цілісності інформації, яка повинна бути захищена (чутливих даних та програмного забезпечення ЕП);
- старіння чутливих даних та криптографічних методів ЕП;
- зловживання повноваженнями щодо чутливих даних ЕП;
- зловживання правами адміністратора щодо чутливих даних ЕП;
- зловживання правами користувачів щодо чутливих даних ЕП;
- компрометація асиметричних пар криптографічних ключів ЕП;
- крадіжка чутливих даних ЕП;
- не виявлені інциденти інформаційної безпеки щодо чутливих даних ЕП;
- невірне тлумачення події інформаційної безпеки щодо чутливих даних ЕП;
- недооцінення актуальності виправлень і змін щодо чутливих даних ЕП;
- неналежне зберігання носіїв інформації з чутливими даними в разі виникнення надзвичайної ситуації ЕП;
- неправильне використання криптомодулів з чутливими даними ЕП;
- несанкціоноване використання криптомодулів ЕП;
- несанкціоноване використання прав адміністраторів та користувачів ЕП;
- нестійкі криптографічні алгоритми ЕП;
- неякісна або відсутня автентифікація щодо чутливих даних ЕП;
- підробні сертифікати відкритих ключів ЕП;
- порушення законів або правил щодо чутливих даних при синтезі та застосуванні ЕП;
- проблеми при автоматизації поширення виправлень і змін щодо ЕП;
- розголошення чутливої інформації щодо синтезу та застосування ЕП;
- систематичний перебір паролів доступу до ЕП;
- троянський кінь щодо чутливих даних ЕП при синтезі та застосуванні ЕП;
- уразливості або помилки ПЗ щодо ЕП;

- атака "Людина посередині";
- атака Clickjacking (буквально – натискання);
- шкідливе програмне забезпечення при синтезі та застосуванні ЕП.

Безумовно, що щодо обґрунтованої та вибраної на основі IT-Grundschutz Catalogues бази Германії моделі загроз, при синтезі та застосуванні існуючих стандартизованих та перспективних ЕП, повинне бути зроблено перекриття названих загроз з необхідною якістю. Для цього, у залежності від механізмів та засобів, що застосовуються для протидії, повинні бути розроблені відповідні нормативно-правові документи.

Моделі загроз щодо ЕП при застосуванні методів та засобів класичного криптоаналізу

Детально загрози щодо застосування класичного криптоаналізу при синтезі та застосуванні ЕП повинні бути визначеними безумовно. Їх перекриття повинне бути зроблене на всіх етапах синтезу та застосування перспективних ЕП. Вказані загрози з точки зору застосування математичних методів синтезу та застосування перспективних методів ЕП залежить від математичних методів, що застосовуються, та умов їх функціонування. Детально ці особливості розглянуті в [3-5], наприклад, для математичних методів, що визначені в якості кандидатів на постквантові стандарти ЕП.

Основними загрозами (методами) класичного криптоаналізу, що повинні бути врахованими, є наступні:

- атаки типу «повне розкриття», загальною можливістю яких є компрометація чутливих параметрів та ключів при відомих відкритих даних;
- атаки «повне розкриття» на основі підписаних даних, призначенням яких є спроба компрометації ключових даних при наявності множини підписаних даних;
- атаки типу «екзистенційна підробка», що можуть бути застосованими за наявності слабкостей у функції гешування, яка використовується при виробленні ЕП;
- атак типу «селективна підробка», яка полягає в тому, що при невідомому особистому ключі для заздалегідь обраних даних можна обчислити ЕП;
- атаки щодо ЕП на «зв'язаних» ключах, особливістю яких є те, що при генеруванні асиметричних пар ключів закладається вразливість;
- атаки на програмну реалізацію ЕП, особливістю яких є те, що при генеруванні асиметричних пар ключів закладається вразливість тощо.

Моделі загроз при синтезі та застосуванні ЕП сторонніми каналами

Загрози (атаки) сторонніми каналами є виділеним класом атак, основною особливістю яких є спрямованість на вразливості практичної реалізації криптосистем, тобто, на відміну від теоретичного криптоаналізу. Загрозливістю такого класу атак над традиційними є менша потужність та більш висока дієвість [4].

Атаки сторонніми каналами націлені на використання інформації про фізичні процеси у технічних пристроях, в тому числі на основі таких:

1) Час виконання операцій вироблення та перевірки ЕП та управління ключами;
2) Спожита енергія (потужність) під час вироблення та перевірки ЕП та управління ключами;
3) Акустичні звуки та сигнали під час вироблення та перевірки ЕП та управління ключами;
4) Електромагнітні випромінювання під час синтезу та застосування ЕП тощо;

Основними видами атак сторонніми каналами є такі [4]:

- атаки за часом (timing attack) – найбільш відомий вид атак стосовно ЕП;
- атаки зондування (probing attack) – один з різновидів простої пасивної атаки;
- атаки на основі помилок обчислень (fault-induction attack) – різновид активної атаки;

Загрози сторонніми каналами можуть бути реалізовані такими методами:

- впливи змінним магнітним полем або лазерними променями;
- порушення контактів у засобі криптографічного перетворення або зміна його тактової частоти;
- зміна напруги живлення системи (сильно перевищені значення норм можуть призвести до помилок на деяких етапах);
- переміщення пристрою до локації з сильним електромагнітним полем;
- підвищення температури усієї системи або ж лише криптографічної частини тощо.

Атаки сторонніми каналами є надзвичайно небезпечними, якщо їх не перекривати. Концепція цих атак існує вже доволі тривалий час, але реалізація захищеності від них вимагає знань не лише у сфері криптографії, а й у сферах технічного характеру. Тому переважна більшість перспективних ЕП розрахована на використання у пристроях, які не можуть захистити від сторонніх атак, бо не мають відповідних програмних рішень щодо захисту від витоку сторонніми каналами.

Моделі загроз при синтезі та застосуванні ЕП при використанні квантових комп'ютерів та оцінки при їх застосуванні

Основними загрозами (атаками) із застосуванням квантових математичних методів, які можуть бути реалізовані на квантовому комп'ютері (звичайно, якщо він буде побудований), є такі [4, 6 – 8, 10 – 12]:

- квантовий алгоритм факторизації Шора;
- квантовий алгоритм Гровера;
- квантовий алгоритм Шора вирішення дискретного логарифму в полі;
- квантовий алгоритм Шора вирішення дискретного логарифму в групі точок еліптичної кривої;
- квантовий алгоритм криптоаналізу для перетворень в фактор кільці тощо.

Порівняльний аналіз складності факторизації для класичного та квантового алгоритмів наведено у табл. 1 [4].

Таблиця 1

Порівняльний аналіз класичного та квантового алгоритмів факторизації (RSA)

Розмір модуля N, бітів	Кількість необхідних кубітів $2n$	Складність квантового алгоритму $4n^3$	Складність класичного алгоритму
512	1024	$0.54 \cdot 10^9$	$1.6 \cdot 10^{19}$
3072	6144	$12 \cdot 10^{10}$	$5 \cdot 10^{41}$
15360	30720	$1.5 \cdot 10^{13}$	$9.2 \cdot 10^{80}$

Порівняльний аналіз складності алгоритму дискретного логарифмування в скінченому полі на основі решета числового поля та алгоритму Шора наведено в табл. 2.

Таблиця 2

Порівняльний аналіз класичного і квантового алгоритму дискретного логарифмування в скінченому полі

Розмір модуля перетворення (бітів)	Кількість необхідних кубітів $\approx 3n$	Час квантового алгоритму $\approx n^3$	Час класичного алгоритму
1024	3072	$0.1 \cdot 10^{10}$	$3.3 \cdot 10^{20}$
3072	9216	$2.9 \cdot 10^{10}$	$1.4 \cdot 10^{31}$
15360	46080	$3.6 \cdot 10^{12}$	$5.9 \cdot 10^{56}$

Деякі оцінки та результати порівняльного аналізу класичних алгоритмів та квантового алгоритму Шора наведений у табл. 3.

Таблиця 3

Порівняльний аналіз складності класичного і квантового алгоритмів дискретного логарифмування групі точок еліптичної кривої (ECC)

Алгоритм розв'язку дискретного логарифмічного рівняння			
Розмір порядку базової точки, бітів	Кількість необхідних кубітів $f(n) = 7n + 4\log_2 n + 10$	Складність квантового алгоритму $360n^3$	Складність класичного алгоритму
163	1210	$1.6 \cdot 10^9$	$3.4 \cdot 10^{24}$
256	1834	$6 \cdot 10^9$	$3.4 \cdot 10^{38}$
571	4016	$6.7 \cdot 10^{10}$	$8.8 \cdot 10^{85}$
1024	7218	$3.8 \cdot 10^{11}$	$1.3 \cdot 10^{154}$

Аналіз даних табл. 1 – 3 дозволяє зробити висновок, що збільшення розміру порядку базової точки при криптоаналізі з використанням квантового алгоритму не дає суттєвого збільшення криптографічної стійкості криптографічної системи на еліптичних кривих. Також видно, що при збільшенні модуля складність дискретного логарифмування класичними методами в групі точок еліптичної кривої зі збільшенням порядку базової точки збільшується суттєво. Але потрібно взяти до уваги, що реалізація квантового алгоритму пов'язана зі застосуванням регістрів з великою кількістю кубітів, яка необхідна для проведення квантової атаки. Наприклад, для базової точки з порядком 2^{571} необхідно використовувати реєстр з довжиною 4016 кубітів. Вважається, що така велика кількість кубітів, ще певний час буде не реалізованою.

Моделі загроз при синтезі та застосуванні ЕП постквантового періоду

У залежності від математичних методів, що застосовуються для синтезу та застосування ЕП, можуть застосовуватись різні методи, системи та засоби.

Розглянемо загрози (атаки) на прикладі проблеми стійкості криптоперетворень на основі навчання з помилками (LWE) [6, 7].

Наразі в постквантовій криптології актуальними є завданнями забезпечення криптографічної стійкості щодо квантових атак.

Стосовно атак на LWE можливо виділити та необхідно розглядати наступні атаки (загрози) [6 – 8, 12]:

1. Атака грубої сили, тобто повного перебору.
2. Традиційної атаки зустріч посередині.
3. Атака на основі алгоритму Arora-Ge.
4. BKW, коли LWE зводиться до SIS атаки.
5. Primal attack (Search-LWE зводиться до BDD атаки).
6. Dual attack (Decision-LWE зводиться до SIS).
7. Зведення до uSVP атаки пошуку короткого вектора.
8. Диференційні атаки.

У цілому атаки на LWE можливо розділити на два великі класи – атаки, що ґрунтуються на переборі, та атаки, що ґрунтуються на редукції решіток. До першого класу належать атаки повного перебору, зустріч посередині та Arora-Ge. Підхід, що використаний в атаці Arora-Ge, є цікавим та перспективним, але він поки що поступається атакам на решітках.

Попередній аналіз дозволяє зробити висновок, що сучасні варіанти механізмів LWE ґрунтуються на поліноміальних кільцях, зокрема на $R_q = \mathbf{Z}_q[X]/(x^{2^n}+1)$. Властивості полі-

номів кільця дозволяють довести ряд теоретичних тверджень щодо стійкості криптосистеми і розробляти ефективні програмні реалізації. Проте, такі кільця мають нетривіальні підполя, що теоретично може використовуватися для криптоаналізу, проте на практиці атак, що застосовують ці додаткові структури, не було знайдено, або ці атаки знаходяться в незавершеному вигляді досліджень.

Проблеми криптоаналізу RLWE та MLWE по суті зводяться до LWE проблеми. Таке зведення можливо для $R_q = \mathbf{Z}_q[X]/(x^{2^n}+1)$, оскільки доведено, що RLWE є не менш стійким, ніж LWE. Проте, при такому підході внутрішня структура кільця ігнорується.

Атаки на решітках, що полягають у зведенні проблеми LWE, відносяться до достатньо вивчених теоретичних проблем в теорії решіток. Існують три основні підходи: зведення LWE до BDD, зведення LWE до SIS, зведення LWE до uSVP. Кожен з цих підходів в кінцевому випадку зводиться до задачі пошуку достатньо малого вектора на решітці, для чого використовується алгоритм BKZ та його варіації.

Точні оцінки для BKZ та його варіацій невідомі. При практичній оцінці використовується ряд евристичних підходів та екстраполяція результатів, що отримані на решітках меншої розмірності. Це становить основну проблему при оцінці криптостійкості систем подібних Dilithium, оскільки немає гарантії, що не з'явиться кращого способу редукції решіток, або оцінка виявиться недопустимо неточною.

Висновки

1. Модель загроз щодо криптоперетворення ЕП повинна бути документом, яким закріплено найбільш повний перелік загроз щодо існуючих та перспективних ЕП.
2. Відповідно до Законів України інформація у основних інформаційних ресурсах поділяється на відкриту і конфіденційну. Інформація у підтримуючих інформаційних ресурсах є технологічною інформацією.
3. При застосуванні ЕП, незалежно від видів додатків, використовуються асиметричні пари ключів, для кожної пари особистий та відкритий. В подальшому при реальному застосуванні ЕП відкритий ключ, як правило, є сертифікатом відкритого ключа та є доступним усім користувачам ІВК.
4. Стосовно відкритого ключа ЕП повинна бути можливість забезпечення його цілісності, справжності, доступності, неспростовності та захист від несанкціонованих дій, які можуть привести до випадкової чи умисної модифікації, нав'язування хибного чи знищення.
5. Стосовно особистого ключа повинна забезпечуватись його цілісність, справжність, доступність, неспростовність та захист від несанкціонованих дій, а також його захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання та поширення, тобто конфіденційність.
6. Перелік можливих загроз безпеці застосування існуючих та перспективних ЕП сформований з числа загроз, що визначені у IT-Grundschutz Catalogues Германії з урахуванням апаратних, програмних та апаратно-програмних ресурсів, технологій обробки даних та механізмів криптографічного захисту при застосуванні ЕП, в тому числі з урахуванням вимог та умов синтезу перспективних та застосуванні ЕП в постквантовий період.
7. Безумовно, що щодо обґрунтованої та вибраної на основі IT-Grundschutz Catalogues бази Германії моделі загроз, при синтезі та застосуванні існуючих стандартизованих та перспективних ЕП повинне бути зроблено перекриття названих загроз з необхідною якістю. Для цього, у залежності від механізмів та засобів, що застосовуються для протидії, повинні бути розробленими відповідні нормативно-правові документи.
8. Загрози (атаки) сторонніми каналами є виділеним класом атак, основною особливістю яких є спрямованість на вразливості практичної реалізації криптосистем, тобто, на відміну від теоретичного криптоаналізу. Загрозою такого класу атак над традиційними є менша потужність та більш висока дієвість.

9. Загрози (атаки) сторонніми каналами є надзвичайно небезпечними, якщо їх не перекривати. Концепція цих атак існує вже доволі тривалий час, але реалізація захищеності від них вимагає знань не лише у сфері криптографії, а й у сферах технічного характеру. Тому переважна більшість перспективних ЕП розрахована на використання у пристроях, які не можуть захистити від сторонніх атак, бо не мають відповідних програмних рішень щодо захисту від витоку сторонніми каналами.

10. Основними загрозами (атаками) з застосуванням квантових математичних методів, які можуть бути реалізованими на квантовому комп'ютері (звичайно, якщо він буде побудований), є такі:

- квантовий алгоритм факторизації Шора;
- квантовий алгоритм Гровера;
- квантовий алгоритм Шора вирішення дискретного логарифму в полі;
- квантовий алгоритм Шора вирішення дискретного логарифму в групі точок еліптичної кривої;
- квантовий алгоритм криптоаналізу для перетворень в фактор кільці.

Список літератури:

1. Наказ від 20.07.2007 №141 «Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної та відкритої інформації з використанням електронного цифрового підпису» № 862/14129.
2. Закон України «Про основні засади забезпечення кібербезпеки України» // Відомості Верховної Ради (ВВР). 2017. № 45, ст. 403.
3. Закон України «Про електронні довірчі послуги» // Відомості Верховної Ради (ВВР). 2017. № 45, ст. 400.
4. Горбенко Ю. І. Методи побудування та аналізу криптографічних систем. Харків : Форт, 2015. 959 с.
5. Горбенко І. Д. Прикладна криптологія : монографія / І. Д. Горбенко, Ю. І. Горбенко. 2-ге вид. Харків : Форт, 2012. 868 с.
6. Gorjan Alagic Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. NISTIR 8309 / Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone // 22 July 2020.Режим доступу: https://doi.org/10.6028/NIST.IR.8309.
7. ЕП Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler and Damien Stehlé CRYSTALS-Dilithium: Algorithm Specifications and Supporting Documentation.Access mode: https://pq-crystals.org/dilithium/data/dilithium-specification.pdf.
8. Горбенко І. Д. Особливості побудування та аналіз електронних підписів 5 рівня безпеки для постквантового періоду на основі алгебраїчних решіток / І. Д. Горбенко, О. Г. Качко, А. М. Олексійчук, Ю. І. Горбенко, В. П. Звєрєв, М. В. Єсіна, В. А. Пономар // Прикладная радиоэлектроника. Харьков : ХНУРЭ, 2019.Т. 18, № 3, 4. С. 123–136.
9. Горбенко Ю. І. Аналіз можливостей квантових комп'ютерів та квантових обчислень для криптоаналізу сучасних криптосистем / Ю. І. Горбенко, Р. С. Ганзя. // Східно-європейський журнал передових технологій. 2014. № 1/9 (67). С. 8–15.
10. Квантовые компьютеры. [Електронний ресурс].Режим доступу: http://www.nkj.ru/archive/articles/5309/.
11. Горбенко І. Д., Постквантова криптографія та механізми її реалізації / І. Д. Горбенко, О. О. Кузнецов, О. В. Потій, Ю. І. Горбенко, Р. Ганзя, В. А. Пономар // Радиотехника. 2017. Вып. 186.С. 32–52.
12. Yesina Maryna Comparative Analysis of Key Encapsulation Mechanisms / Maryna Yesina, Mikolaj Karpinski, Volodymyr Ponomar, Yurij Gorbenko, Tomasz Gancarczyk, Uliana Iatsykovska // Proceedings of the 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). September 18-21.

Надійшла до редколегії 10.09.2020

Відомості про авторів:

Горбенко Юрій Іванович – канд. техн. наук, АТ «інститут інформаційних технологій», перший заступник головного конструктора, Україна, e-mail: gorbenkou@iit.kharkov.ua, ORCID: https://orcid.org/0000-0003-0073-9107

Єсіна Марина Віталіївна – канд. техн. наук, Харківський національний університет імені В. Н. Каразіна, доцент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Україна, e-mail: rinayes20@gmail.com, ORCID: https://orcid.org/0000-0002-1252-7606

Онопрієнко Віктор Васильович – канд. техн. наук, генеральний директор АТ «Інститут інформаційних технологій», Україна.

Малєєва Ганна Андріївна – Харківський національний університет радіоелектроніки, аспірант кафедри безпеки інформаційних технологій, Україна, e-mail: hanna.malieieva@nure.ua