УДК 004.056.53 +530.145

АНАЛІЗ ПОСЛІДОВНОЇ АТАКИ ПАСИВНОГО ПЕРЕХОПЛЕННЯ ДЕКІЛЬКОХ ЗЛОВМИСНИКІВ НА ПІНГ-ПОНГ ПРОТОКОЛ З ПЕРЕПЛУТАНИМИ ПАРАМИ КУБІТІВ

Євген Василіу, Сергій Ніколаєнко

У статті проаналізовано послідовну атаку пасивного перехоплення двох і більшого числа зловмисників на оригінальний пінг-понг протокол з парами переплутаних кубітів. Отримано загальний рекурсивний вираз для імовірності d виявлення атаки довільної кількості n зловмисників, що дозволяє обчислити цю імовірність через відповідну імовірність при атаці n – 1 зловмисників. Показано, що збільшення кількості атакуючих у квантовому каналі призводить до збільшення ймовірності виявлення їх атаки легітимними користувачами. Отримано вирази для максимальної кількості інформації зловмисників при послідовній атаці двох і трьох зловмисників. Показано, що максимальна кількість інформації зловмисників визначається тим же виразом, що й у випадку атаки одного зловмисника, змінюється тільки величина d. Показано, що пінг-понг протокол з парами переплутаних кубітів вразливий до атаки пасивного перехоплення декількох зловмисників не більше, ніж до атаки одного.

Ключові слова: *квантова криптографія, пінг-понг протокол, атака пасивного перехоплення декількох зловмисників, імовірність виявлення атаки, кількість інформації зловмисників.*

Вступ. Захист інформації є однією з найважливіших проблем сучасного інформаційного суспільства. В останнє десятиріччя активно розвивається новий напрямок захисту інформації – квантова криптографія, яка є найбільш зрілою технологією в новітній науково-технічній галузі квантової інформатики. На відміну від криптографічних методів, безпека яких ґрунтується на недоведених математичних твердженнях, безпека квантової криптографії ґрунтується на законах квантової фізики. Цей напрямок розвивається з перспективою на майбутнє.

Одним із напрямків квантової криптографії є протоколи квантового прямого безпечного зв'язку (КПБЗ), які дозволяють передавати конфіденційні повідомлення безпосередньо через квантовий канал, тобто без використання шифрування. На цей час запропонована значна кількість різних за призначенням протоколів КПБЗ [1–7]. Одним з таких протоколів, що не потребує квантової пам'яті великого обсягу, є пінг-понг протокол з парами переплутаних кубітів і без використання квантового надщільного кодування, який дозволяє передати один біт класичної інформації за один цикл протоколу [1].

Пінг-понг протокол є простим протоколом КПБЗ, який може бути реалізований практично з використанням сучасних технологій квантової інформатики [8]. На цей час запропоновано багато варіантів цього протоколу [1–4,7], досліджено їх стійкість до різних видів атак. Але питання про стійкість цих протоколів до атаки пасивного перехоплення, що виконується послідовно декількома зловмисниками в одному квантовому каналі, раніше не розглядалось.

Метою цієї роботи є аналіз атаки декількох зловмисників на пінг-понг протокол з переплутаними парами кубітів за умови, що зловмисники не знають про атаки один одного.

Загальна схема пінг-понг протоколу з парами переплутаних кубітів і без квантового надщільного кодування. Пінг-понг протокол є двостороннім протоколом квантового безпечного зв'язку – для передавання повідомлення від одного абонента (Аліси) до іншого абонента (Боба) кубіт пересилається спочатку від Боба до Аліси, а потім назад від Аліси до Боба. В пінг-понг протоколі застосовуються два режими – режим передавання самого повідомлення і режим контролю підслуховування, необхідний для виявлення атаки пасивного перехоплення. Аліса і Боб чергують ці режими випадковим чином. Атака виявляється з деякою імовірністю в режимі контролю підслуховування.

Схема режиму передавання повідомлення для оригінального пінг-понг протоколу, в якому використовуються два стани Бела і відповідно не використовується квантове надщільне кодування, показана на рис. 1 [1]. Боб готує повністю переплутаний стан пари кубітів $\left|\psi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle\left|1\right\rangle + \left|1\right\rangle\left|0\right\rangle\right)$. Він оставляє в себе один з кубітів ("домашній") і посилає другий ("передаваний") Алісі квантовим каналом зв'язку. Аліса виконує кодувальну операцію й повертає кубіт назад Бобові. Кодувальні операції, відповідні двійковим "0" і "1", мають вигляд:

$$U_0 = I\,;\;\; U_1 = \sigma_z\,, \qquad (1)$$

де $I = |0\rangle\langle 0| + |1\rangle\langle 1|$ – тотожний оператор,

$\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$ – один з операторів Паулі.

Боб після отримання кубіту від Аліси виконує вимірювання в базисі Бела над обома кубітами і при відсутності атаки і природного шуму в каналі зв'язку отримує стан $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle)$ або $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle)$ в залежності від того, яка кодувальна операція виконана Алісою. Таким чином, цей варіант пінг-понг протоколу дозволяє передати один біт класичної інформації за один раунд режиму передавання повідомлень і є найпростішим з пінг-понг протоколів з найменшою інформаційною місткістю.

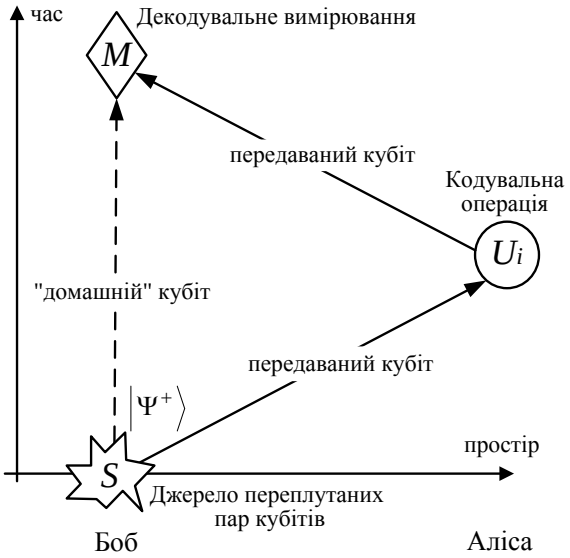


Рис. 1. Схема режиму передавання повідомлення

Режим контролю підслуховування в пінг-понг протоколі при послідовній атаці пасивного перехоплення двох зловмисників. Загальна схема послідовної атаки пасивного перехоплення двох зловмисників показана на рис. 3. Для здійснення такої атаки зловмисники повинні мати можливість, крім виконання операцій над окремими кубітами, також прослуховувати звичайний канал зв'язку між легітимними користувачами.

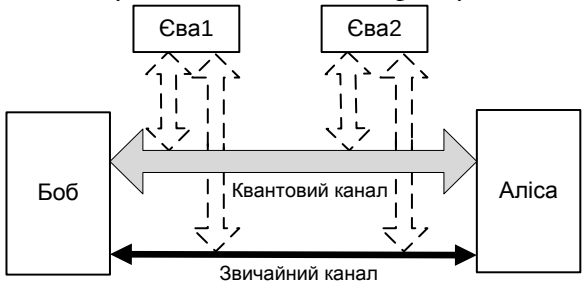


Рис. 3. Загальна схема атаки двох зловмисників на пінг-понг протокол

В режимі контролю підслуховування (рис. 2) Аліса і Боб виконують однокубітне вимірювання в одному з двох випадково обраних базисів: вертикально-горизонтальному $B_z = \{|0\rangle, |1\rangle\}$ або діагональному $B_x = \{|+\rangle, |-\rangle\}$. Ці вимірювання дозволяють їм визначити, чи було втручання зловмисника (Єви) на лінії Боб $\rightarrow$ Аліса.

Для сповіщення один одного про зміну режимів у протоколі, для обміну результатами вимірювань в режимі контролю підслуховування, а також при необхідності для корекції помилок Аліса і Боб передають повідомлення звичайним (не квантовим) аутентифікованим каналом зв'язку.

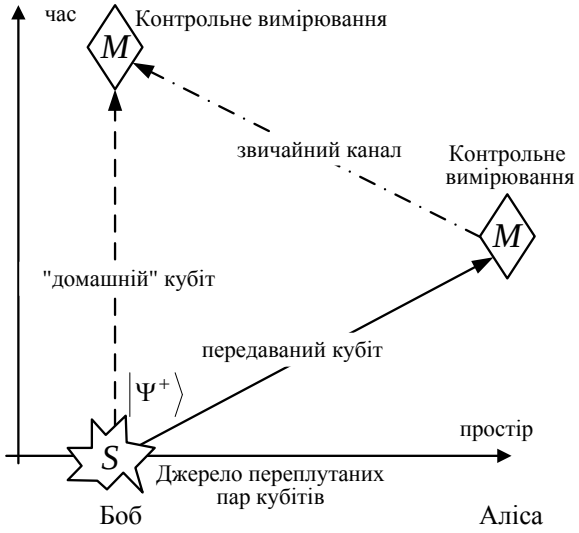


Рис. 2. Схема режиму контролю підслуховування

Розглянемо детально алгоритм режиму контролю підслуховування в пінг-понг протоколі при послідовній атаці двох зловмисників (рис. 4).

Крок 1. Аліса готує повідомлення у вигляді двійкової послідовності $x^N = (x_1 \ldots, x_N)$, де $x_i \in \{0,1\}$.

Крок 2. Боб приготовляє двохкубітний переплутаний стан $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$.

Крок 3. Боб зберігає один кубіт (домашній кубіт) у себе в квантової пам'яті і посилає інший кубіт (передаваний кубіт) Алісі через квантовий канал.

Крок 4. Єва$_1$ переплутує передаваний кубіт зі своєю допоміжної квантової системою (пробою) і відправляє його далі квантовим каналом.

Крок 5. Єва$_2$ отримує передаваний кубіт (що вже знаходиться в переплутаному стані з пробою

Єви$_1$) і переплутує його зі своєю пробою, а потім відправляє далі каналом.

Крок 6. Аліса отримує передаваний кубіт і перемикається в режим контролю підслуховування. Вона випадковим чином вибирає однокубітний вимірювальний базис: B_z або B_x і виконує вимірювання. Використовуючи звичайний канал зв'язку, вона посилає Бобу результат вимірювання та використаний нею базис.

Крок 7. Боб вимірює стан свого домашнього кубіту в тому ж базисі, в якому вимірювала стан переданого кубіту Аліса. Потім він порівнює результат свого вимірювання з тим, що повідомила Аліса. Оскільки початковий стан $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ не повинен змінитися при відсутності атаки (і природного шуму), то результати вимірювань Аліси і Боба завжди повинні бути антикорельовані. У разі атаки така антикореляція буде спостерігатися тільки з деякою імовірністю, що й дозволяє, зрештою, виявити атаку (вплив природного шуму в каналі на імовірність виявлення атаки в даній статті не розглядається).

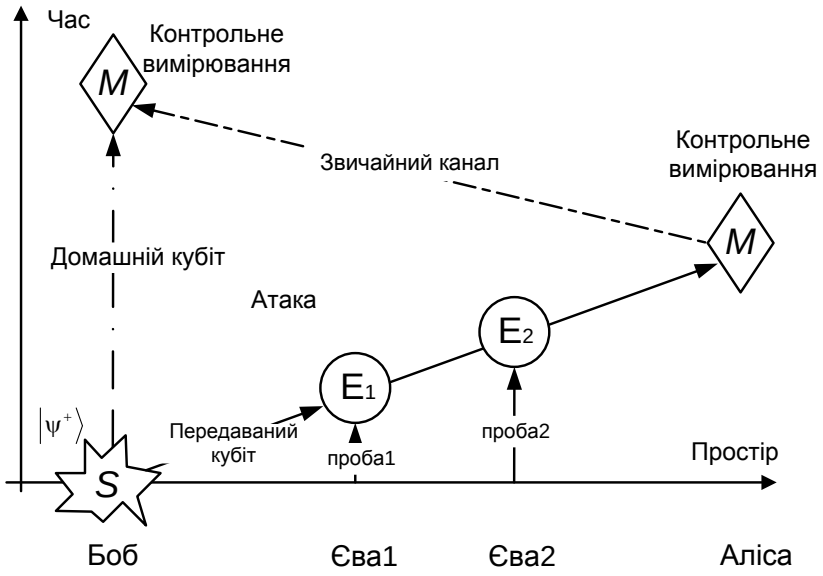


Рис. 4. Режим контролю підслуховування при послідовній атаці двох зловмисників

Максимальна інформація двох зловмисників при їх послідовній атаці пасивного перехоплення на пінг-понг протокол. Розглянемо послідовні атаки пасивного перехоплення двох зловмисників (див. рис. 4) і обчислимо максимальну кількість інформації, яку вони можуть отримати в режимі передавання повідомлення в залежності від імовірності їх виявлення в режимі контролю підслуховування. Будемо дотримуватись схеми аналізу атаки пасивного перехоплення на пінг-понг протокол, вперше запропонованої в [1] для одиночної атаки.

Так як для Єви$_1$ стан переданого Бобом кубіту не можна відрізнити від повністю змішаного стану, то це відповідає ситуації, якщо б Боб посилав передаваний кубіт в станах $|0\rangle$ або $|1\rangle$ з однаковою імовірністю 1/2. Тоді стани складеної квантової системи "передаваний фотон – проба Єви$_1$" після атаки записуються у вигляді:

$$|\psi_0\rangle = \hat{E}_1(|0\rangle \otimes |\chi\rangle) = \alpha_0 |0\rangle \otimes |\chi_{00}\rangle + \beta_0 |1\rangle \otimes |\chi_{01}\rangle,$$

$$|\psi_1\rangle = \hat{E}_1(|1\rangle \otimes |\chi\rangle) = \alpha_1 |0\rangle \otimes |\chi_{10}\rangle + \beta_1 |1\rangle \otimes |\chi_{11}\rangle, \qquad (2)$$

де $\{|\chi_{ik}\rangle\}$- множина станів проби Єви$_1$; $|\alpha_0|^2 + |\beta_0|^2 = 1$ та $|\alpha_1|^2 + |\beta_1|^2 = 1$. З унітарності операції $\hat{E}_1$ також слідують співвідношення: $|\alpha_0|^2 = |\beta_1|^2$ та $|\alpha_1|^2 = |\beta_0|^2$.

Імовірність виявити атаку Єви$_1$ за один раунд контролю підслуховування за відсутності Єви$_2$:

$$d_1 = |\beta_0|^2 = |\alpha_1|^2 = 1 - |\alpha_0|^2 = 1 - |\beta_1|^2. \qquad (3)$$

Будемо вважати, що Єва$_2$ не знає про присутність Єви$_1$ і виконує таку ж операцію переплутування переданого фотона зі своєю пробою, що і Єва$_1$, вважаючи, що кубіт прийшов безпосередньо від Боба. Тоді після операції Єви$_2$ стани системи "передаваний фотон – проби зловмисників" стануть

$$|\psi_0'\rangle = \hat{E}_2\left(|\psi_0\rangle \otimes |\varphi\rangle\right) = \left(a_0\alpha_0 + a_1\beta_0\right)|0\rangle \otimes |\chi_{00}\rangle \otimes |\varphi_{00}\rangle + \left(b_0\alpha_0 + b_1\beta_0\right)|1\rangle \otimes |\chi_{01}\rangle \otimes |\varphi_{01}\rangle;$$
$$|\psi_1'\rangle = \hat{E}_2\left(|\psi_1\rangle \otimes |\varphi\rangle\right) = \left(a_0\alpha_1 + a_1\beta_1\right)|0\rangle \otimes |\chi_{10}\rangle \otimes |\varphi_{10}\rangle + \left(b_0\alpha_1 + b_1\beta_1\right)|1\rangle \otimes |\chi_{11}\rangle \otimes |\varphi_{11}\rangle, \quad (4)$$

де $\{|\varphi_{ik}\rangle\}$ – множина станів проби Єви$_2$; $|a_0|^2 + |b_0|^2 = 1$, $|a_1|^2 + |b_1|^2 = 1$, а також з унітарності операції $\hat{E}_2$ випливає: $|a_0|^2 = |b_1|^2$ та $|a_1|^2 = |b_0|^2$. Відзначимо, що хвильові функції (4) не нормовані.

Імовірність виявити атаку Єви$_2$ за один раунд контролю підслуховування за відсутності Єви$_1$, аналогічно (3), визначається рівностями:

$$d_2 = |b_0|^2 = |a_1|^2 = 1 - |a_0|^2 = 1 - |b_1|^2. \quad (5)$$

Хвильові функції (4) необхідно нормувати для виконання умови рівності одиниці повної імовірності, тобто виконання умов $|a_0\alpha_0 + a_1\beta_0|^2 + |b_0\alpha_0 + b_1\beta_0|^2 = 1$ для $|\psi_0'\rangle$ і $|a_0\alpha_1 + a_1\beta_1|^2 + |b_0\alpha_1 + b_1\beta_1|^2 = 1$ для $|\psi_1'\rangle$. Таким чином,

$$|\psi'_{0(norm)}\rangle = \frac{a_0\alpha_0 + a_1\beta_0}{\sqrt{|a_0\alpha_0 + a_1\beta_0|^2 + |b_0\alpha_0 + b_1\beta_0|^2}}|0\rangle \otimes |\chi_{00}\rangle \otimes |\phi_{00}\rangle + \frac{b_0\alpha_0 + b_1\beta_0}{\sqrt{|a_0\alpha_0 + a_1\beta_0|^2 + |b_0\alpha_0 + b_1\beta_0|^2}}|1\rangle \otimes |\chi_{01}\rangle \otimes |\phi_{01}\rangle;$$
$$|\psi'_{1(norm)}\rangle = \frac{a_0\alpha_1 + a_1\beta_1}{\sqrt{|a_0\alpha_1 + a_1\beta_1|^2 + |b_0\alpha_1 + b_1\beta_1|^2}}|0\rangle \otimes |\chi_{10}\rangle \otimes |\phi_{10}\rangle + \frac{b_0\alpha_1 + b_1\beta_1}{\sqrt{|a_0\alpha_1 + a_1\beta_1|^2 + |b_0\alpha_1 + b_1\beta_1|^2}}|1\rangle \otimes |\chi_{11}\rangle \otimes |\phi_{11}\rangle. \quad (6)$$

Розглянемо випадок, коли Боб спочатку "посилає 0". Тоді стан після атаки Єви$_2$ стає $|\psi'_{0(norm)}\rangle$ (6). Відповідна матриця щільності має вигляд:

$$\rho_0' = |\psi_0'\rangle\langle\psi_0'| = \frac{1}{norm} \cdot \begin{pmatrix} |a_0\alpha_0 + a_1\beta_0|^2 & (b_0\alpha_0 + b_1\beta_0)^*(a_0\alpha_0 + a_1\beta_0) \\ (a_0\alpha_0 + a_1\beta_0)^*(b_0\alpha_0 + b_1\beta_0) & |b_0\alpha_0 + b_1\beta_0|^2 \end{pmatrix}, \quad (7)$$

де введено позначення $norm = |a_0\alpha_0 + a_1\beta_0|^2 + |b_0\alpha_0 + b_1\beta_0|^2$.

Використовуючи (7), а також співвідношення (3) і (5), можна отримати вираз для величини d – імовірності виявити спільну послідовну атаку двох зловмисників за один раунд контролю підслуховування:

$$d = \frac{|b_0\alpha_0 + b_1\beta_0|^2}{norm} = \frac{\left(\sqrt{(1-d_1)\cdot d_2} + \sqrt{(1-d_2)\cdot d_1}\right)^2}{\left(\sqrt{(1-d_1)\cdot d_2} + \sqrt{(1-d_2)\cdot d_1}\right)^2 + \left(\sqrt{(1-d_1)\cdot(1-d_2)} + \sqrt{d_1\cdot d_2}\right)^2}. \quad (8)$$

Обчислимо тепер максимальні кількості інформації, які можуть отримати зловмисники Єва$_1$ та Єва$_2$, виконуючи свої атаки в режимі передавання повідомлення (рис. 5).

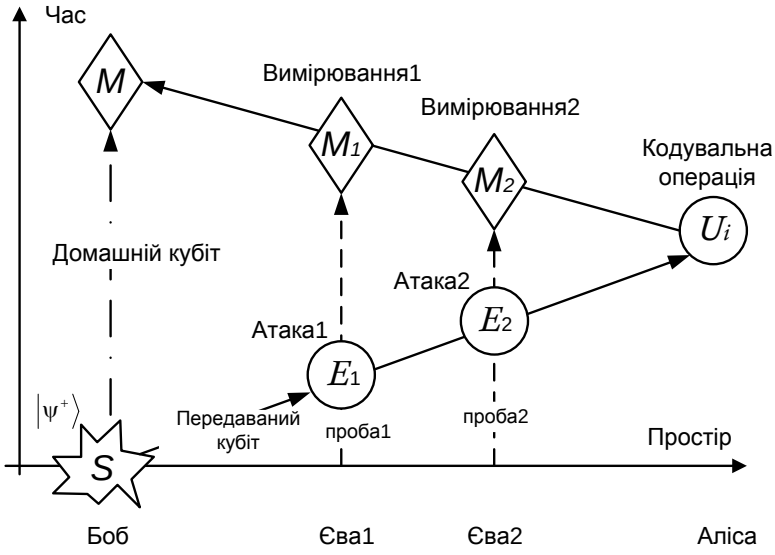


Рис. 5. Режим передавання повідомлення при послідовній атаці двох зловмисників

Після виконання Алісою кодувальних операцій I та σ_z, що відповідають передаванню "0" і "1", з ймовірностями p_0 та p_1 відповідно, матриця щільності системи буде мати вид:

$$\rho_0'' = \frac{1}{norm}\cdot\begin{pmatrix} |a_0\alpha_0 + a_1\beta_0|^2 & (p_0 - p_1)(b_0\alpha_0 + b_1\beta_0)^*(a_0\alpha_0 + a_1\beta_0) \\ (p_0 - p_1)(a_0\alpha_0 + a_1\beta_0)^*(b_0\alpha_0 + b_1\beta_0) & |b_0\alpha_0 + b_1\beta_0|^2 \end{pmatrix}, \quad (9)$$

Максимальна кількість класичної інформації I_0, яка може бути отримана шляхом вимірювання квантового стану, визначається величиною Холево:

$$I_0 = S(\rho_0'') - \sum_{i=0}^{1} p_i S(\rho_0^i) = S(\rho_0''), \quad (10)$$

де $S(\rho)$ – ентропія фон Неймана; ρ_0^i – матриці щільності станів після виконання Алісою кодувальних операцій I та σ_z з ймовірностями p_0 та p_1 відповідно, і обидва $S(\rho_0^i) = 0$, оскільки ці стани – чисті.

Таким чином, максимальна кількість інформації, яку може отримати Єва$_2$, визначається виразом (10). Оскільки

$$I_0 = S(\rho_0'') \equiv -Tr[\rho_0'' \log_2 \rho_0''] = -\sum_i \lambda_i \log_2 \lambda_i, \quad (11)$$

то для знаходження I_0 необхідно знайти власні значення матриці щільності (9).

Обчислення, виконані з використанням пакету символьних математичних обчислень Wolfram Mathematica 8, призводять до наступних виразів:

$$\lambda_1 = 0{,}5(p_1 + p_2) + 0{,}5\sqrt{(p_1 + p_2)^2 - 16 p_1 p_2 \cdot d(1-d)},$$
$$\lambda_2 = 0{,}5(p_1 + p_2) - 0{,}5\sqrt{(p_1 + p_2)^2 - 16 p_1 p_2 \cdot d(1-d)}, \quad (12)$$

де d визначено в (8).

Розглядаючи тепер випадок, коли Боб "посилає" $|1\rangle$, тобто стан після атаки Єви$_2$ стає $|\psi'_{1(norm)}\rangle$ (6), можна показати, що вирази (8) і (12) залишаються незмінними. Таким чином, у цьому випадку максимальна кількість інформації Єви$_2$ задається тим же виразом (11), де λ_0 та λ_1 визначені в (12) і d визначено в (8).

Порівняння цих виразів з отриманими в [1] для атаки пасивного перехоплення одного зловмисника показує, що ці вирази мають однаковий вигляд, з тією лише різницею, що вирази для d – імовірності виявлення атаки за один раунд контролю підслуховування – різні в цих випадках. При атаці одного зловмисника d визначається формулою (3), а при послідовній атаці двох зловмисників – формулою (8). Максимальна імовірність виявлення атаки як одного зловмисника, так і двох для даного варіанту пінг-понг протоколу дорівнює 0,5.

На рис. 6 представлені залежності $d(d_1,d_2)$ при заданих значеннях d_2. Видно, що другий зловмисник збільшує імовірність виявлення атаки легітимними користувачами, причому тим сильніше, чим більше інформації він хоче отримати. Також видно, що при d_2 = 0,5 величина d також дорівнює 0,5 і не залежить від d_1 (і навпаки). Це означає, що якщо другий зловмисник хоче отримати повну інформацію (що відповідає d_2 = 0,5), то перший зловмисник не може регулювати свою атаку (і навпаки).

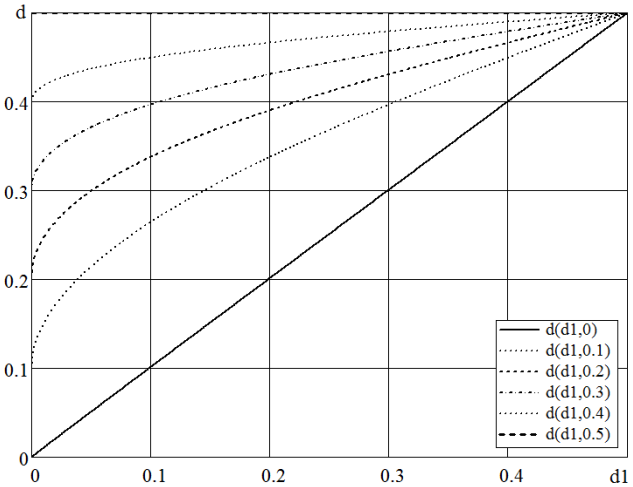


Рис. 6. Залежності ймовірності d виявлення атаки двох зловмисників від ймовірностей d_1 і d_2 виявлення їх атак окремо

На рис. 7 представлено залежність максимальної кількості інформації I_0 Єви$_2$ при послідовних атаках двох зловмисників. Видно, що I_0 монотонно зростає із збільшенням як d_1, так і d_2. Видно також, що перший зловмисник як би "допомагає" другому, тобто другий може отримати

більше інформації, ніж він очікує при заданому ним d_2. Однак величина d при цьому перевищує d_2 (див. рис. 6), тобто другий зловмисник, не знаючи про атаку першого, створить більшу імовірність виявлення його атаки, ніж він планував, задаючи d_2 шляхом регулювання параметрів своїх допоміжних квантових систем. Оскільки вираз (8) для d є симетричним відносно d_1 і d_2, то і перший зловмисник, не знаючи про атаку другого, створить більшу імовірність виявлення атаки, ніж, якби він був один.

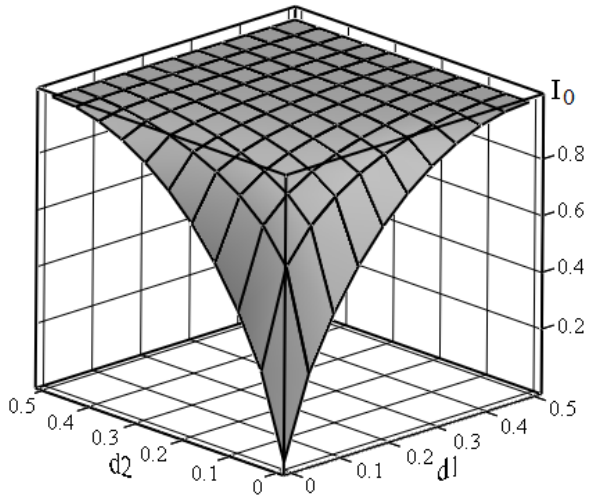


Рис. 7. Максимальна кількість інформації другого зловмисника

Відзначимо також, що внаслідок вимірювання, що виконується Євою$_2$ над складеною квантовою системою "передаваний кубіт – проба" на шляху Аліса → Боб (див. рис. 5), стан цієї системи буде збурений, і відповідно максимальна кількість інформації Єви$_1$ буде не більше максимальної кількості інформації Єви$_2$, тобто Єва$_1$ в результаті атаки отримає не більше інформації, ніж її отримає Єва$_2$. При цьому, як випливає з (11) і (12), ця кількість інформації визначається єдиною величиною – ймовірністю d виявлення атаки легітимними користувачами за один раунд контролю підслуховування, яка залежить від параметрів допоміжних квантових систем обох зловмисників згідно з (8).

Імовірність виявлення атаки пасивного перехоплення *n* зловмисників і їх максимальна кількість інформації. Розглянемо тепер випадок трьох зловмисників, які послідовно здійснюють атаку пасивного перехоплення на пінг-понг протокол з парами переплутаних кубітів [1] і не знають один про одного.

Обчислення, виконані за допомогою Wolfram Mathematica 8, деталі яких ми опускаємо зважаючи на їх громіздкість, показують, що імовірність d виявити атаку в цьому випадку визначається формулою

$$d=\frac{\left[\left(\sqrt{(1-d_1)\cdot d_2}+\sqrt{(1-d_2)\cdot d_1}\right)\cdot\sqrt{1-d_3}+\left(\sqrt{(1-d_1)\cdot(1-d_2)}+\sqrt{d_1\cdot d_2}\right)\cdot\sqrt{d_3}\right]^2}{norm(d_1,d_2,d_3)}, \quad (13)$$

де

$$norm(d_1,d_2,d_3)=\left[\left(\sqrt{(1-d_1)\cdot d_2}+\sqrt{(1-d_2)\cdot d_1}\right)\cdot\sqrt{1-d_3}+\left(\sqrt{(1-d_1)\cdot(1-d_2)}+\sqrt{d_1\cdot d_2}\right)\cdot\sqrt{d_3}\right]^2+$$
$$+\left[\left(\sqrt{(1-d_1)\cdot d_2}+\sqrt{(1-d_2)\cdot d_1}\right)\cdot\sqrt{d_3}+\left(\sqrt{(1-d_1)\cdot(1-d_2)}+\sqrt{d_1\cdot d_2}\right)\cdot\sqrt{1-d_3}\right]^2. \quad (14)$$

Третій зловмисник ще більше збільшує імовірність виявлення атаки легітимними користувачами (в порівнянні з випадком атаки двох зловмисників), причому природно тим сильніше, чим більше інформації він хоче отримати. Відзначимо, що максимальне значення величини d (13) дорівнює 0,5, як і у випадку атак одного чи двох зловмисників.

У роботі [9] була досліджена атака пасивного перехоплення n зловмисників на протокол квантового розподілення ключів BB84, коли всі зловмисники використовують некогерентну та оптимальну для себе стратегію. Досліджувана в цій статті атака на пінг-понг протокол є аналогом розглянутої в [9] атаки на протокол BB84. Тому цікаво порівняти вирази для d, отримані тут для пінг-понг протоколу: (8) і (14), з відповідними виразами, виведеними в [9] для BB84. Порівняння показує, що ці вирази не збігаються повністю, але мають дуже схожу структуру. Так, для атаки трьох зловмисників на протокол BB84 в [9] отримано наступний вираз:

$$d=\left[(1-d_1)\cdot d_2+(1-d_2)\cdot d_1\right]\cdot(1-d_3)+$$
$$+\left[(1-d_1)\cdot(1-d_2)+d_1\cdot d_2\right]\cdot d_3 \quad . \quad (15)$$

Така подібність структури формул для d, отриманих нами для пінг-понг протоколу і в [9] для протоколу BB84, є непрямим свідченням на користь правильності отриманих нами формул (внаслідок подібності самих стратегій атак), а також дозволяє вивести вираз для ймовірності виявлення атаки в пінг-понг протоколі для загального випадку n зловмисників, так як відповідний вираз для BB84 отримано в [9]. Таким

чином, використовуючи формули (8) і (14), а також результати роботи [9], можна отримати наступний рекурсивний вираз для ймовірності d виявлення атаки пасивного перехоплення за один раунд контролю підслуховування при наявності n зловмисників:

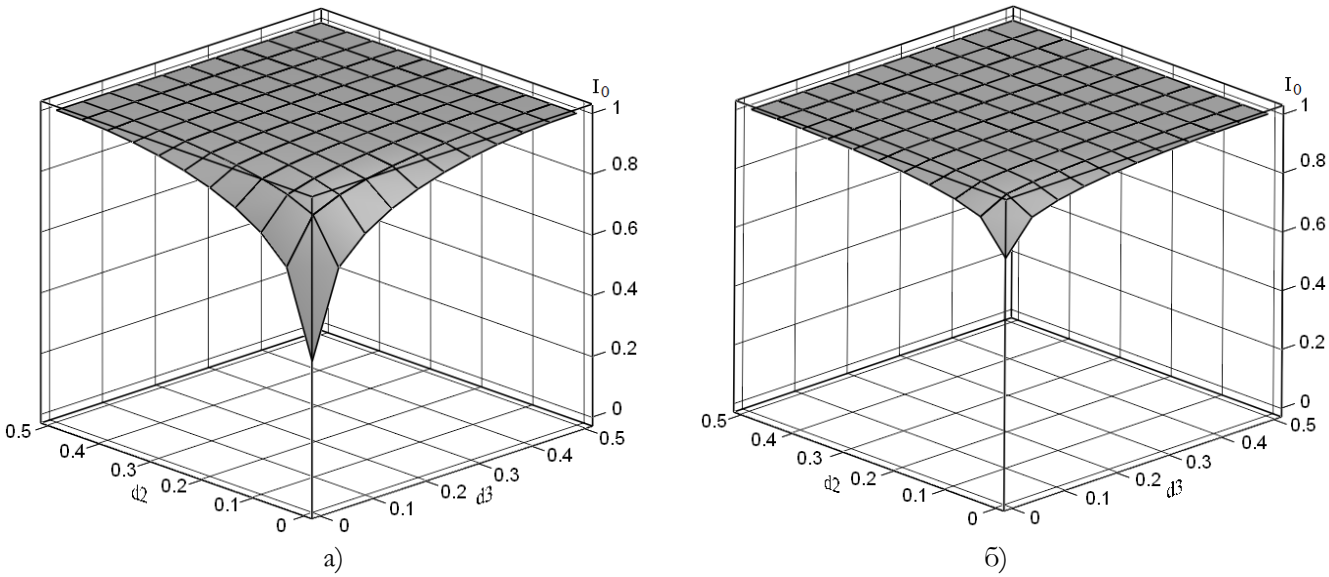
$$d^{(n)} = \frac{\left[\sqrt{d^{(n-1)}}\cdot\sqrt{(1-d_n)} + \sqrt{d^{(n-1)}\big|_{d_{n-1}\to 1-d_{n-1}}}\cdot\sqrt{d_n}\right]^2}{\left[\sqrt{norm_{1st-term}^{(n-1)}}\cdot\sqrt{(1-d_n)} + \sqrt{norm_{2nd-term}^{(n-1)}}\cdot\sqrt{d_n}\right]^2 + \left[\sqrt{norm_{1st-term}^{(n-1)}}\cdot\sqrt{d_n} + \sqrt{norm_{2nd-term}^{(n-1)}}\cdot\sqrt{(1-d_n)}\right]^2} \quad (n \geq 3), \quad (16)$$

де індекс зверху позначає кількість зловмисників, які проводять атаку, не знаючи один про одного, а індекс внизу – імовірність виявлення атаки i-го зловмисника у випадку, якщо б він був один; індекс внизу біля *norm* позначає перший або другий доданок цієї величини для попереднього значення n (тобто для $n-1$).

Оскільки значення $d^{(2)}$ відомо (вираз (8)), то всі наступні значення $d^{(n)}$ можуть бути рекурсивно обчислені за формулою (16).

Що стосується кількості інформації зловмисників, то в разі атаки трьох зловмисників кількість інформації останнього може бути обчислена за тією ж схемою, що викладена вище для випадку атаки двох. Як показують розрахунки, виконані з використанням Wolfram Mathematica 8, власні значення матриці щільності квантової системи "проби трьох зловмисників – передаваний кубіт" після виконання кодувальної операції Аліси визначаються тими ж виразами (12), де в якості d тепер потрібно підставляти (13) і (14). Таким чином, максимальна кількість інформації третього зловмисника розраховується за формулами (11) і (12) з d, визначеним у (13), (14). Максимальна кількість інформації решти зловмисників буде не більше кількості інформації останнього (третього).

На рис. 8 представлені залежності максимальної кількості інформації третього зловмисника ($Єви_3$) при послідовних атаках трьох зловмисників на пінг-понг протокол з парами переплутаних кубітів. Рисунок *а* відповідає $d_1 = 0{,}1$, рисунок *б* – $d_1 = 0{,}25$.



а) б)

Рис. 8. Максимальна кількість інформації третього зловмисника у залежності від ймовірностей виявлення атаки d_2 та d_3

З порівняння з рис. 7 видно, що оскільки три зловмисника створюють більше збурення стану передаваного кубіта, і відповідно більше значення $d^{(3)}$, ніж два зловмисника, то й інформація, що її отримує третій зловмисник, збільшується. Звідси можна зробити висновок, що зі збільшенням кількості атакуючих останній з них буде отримувати суттєво більше інформації, ніж він розраховував, вибираючи своє значення d_n, але і сумарне значення $d^{(n)}$ при цьому буде значно більше, ніж він хотів би. Також відзначимо, що у випадку, якщо будь-який з n зловмисників вибирає $d_i = 0{,}5$, тобто максимальне значення, при якому він може отримати повну інформацію, то всі інші зловми-

сники позбавляються можливості регулювати атаку, тобто незалежно від значень d_i, які вони виберуть, $d^{(n)} = 0{,}5$.

Висновки. У статті проаналізовано атаку пасивного перехоплення двох і більшого числа зловмисників на пінг-понг протокол з переплутаними парами кубітів, коли зловмисники послідовно один за одним виконують операції над передаваними кубітами в квантовому каналі й не знають один про одного. Виведено вирази для імовірності виявлення атаки легітимними користувачами при атаці двох і трьох зловмисників в залежності від ймовірностей виявлення їх атак окремо (тобто якщо б перший проводив атаку за відсутності другого або навпаки і т.д.). Отримано загальний рекурсивний вираз для імовірності виявлення атаки довільної кількості n зловмисників, що дозволяє обчислити цю імовірність через відповідну імовірність при атаці $n-1$ зловмисників. Показано, що збільшення кількості атакуючих в квантовому каналі призводить до збільшення імовірності виявлення їх атаки легітимними користувачами.

Отримано вирази для максимальної кількості інформації зловмисників при послідовній атаці двох і трьох зловмисників в каналі зв'язку. Показано, що максимальна кількість інформації зловмисників визначається тим же виразом, що й у випадку атаки одного зловмисника, змінюється тільки величина d – імовірність виявлення атаки легітимними користувачами. Оскільки при атаці декількох зловмисників кожен з них, виконуючи операцію переплутування передаваного кубіта зі своєю допоміжної квантової системою, "робить внесок" у імовірність d виявлення атаки, то ця імовірність збільшується. У відповідності з вищесказаним збільшується і максимальна кількість інформації, яку можуть отримати зловмисники. Однак при цьому імовірність виявлення атаки буде більше, ніж планував кожен із зловмисників, вибираючи параметри своєї операції переплутування.

Максимальне значення імовірності d виявлення атаки на пінг-понг протокол з парами переплутаних кубітів у разі послідовної атаки будь-якого числа зловмисників дорівнює 0,5, як і у випадку атаки одного. При цьому, якщо хоча б один із зловмисників вибирає параметри своєї операції переплутування так, що імовірність d_i виявлення його одноосібної атаки (у відсутність інших зловмисників) дорівнює 0,5, то цієї величині буде дорівнювати і загальна імовірність d виявлення атаки при будь-якій кількості атакуючих. У цьому випадку всі інші зловмисники позбавляються можливості регулювати свою атаку. Однак і максимальна кількість інформації, яку вони можуть отримати, дорівнює 1 біт на раунд протоколу, тобто повної інформації.

Таким чином, отримані результати свідчать про те, що пінг-понг протокол з парами переплутаних кубітів вразливий до атаки пасивного перехоплення декількох зловмисників не більше, ніж до атаки одного. Декілька зловмисників не отримують жодних переваг, проводячи послідовно спочатку операції переплутування своїх проб з передаваним кубітом на шляху Боб $\rightarrow$ Аліса, а потім проводячи вимірювання над складеною системою "передаваний кубіт – проби" на зворотному шляху. Звідси випливає, що у випадку, якщо зловмисники можуть домовитися між собою, найкращою стратегією для них буде проводити одну атаку, а потім ділитися отриманою інформацією. Звідси випливає також, що розроблений раніше в роботах авторів метод підсилення стійкості пінг-понг протоколів [10] дозволить підсилити стійкість протоколу з парами переплутаних кубітів не тільки в разі атаки одного зловмисника, але й у випадку атаки довільної їх кількості.

ЛІТЕРАТУРА

[1]. Boström K. Deterministic secure direct communication using entanglement / K. Boström, T. Felbinger // Physical Review Letters. – 2002. – Vol. 89, issue 18. – 187902.

[2]. Cai Q.-Y. Improving the capacity of the Boström – Felbinger protocol / Q.-Y. Cai, B.-W. Li // Physical Review A. – 2004. – V. 69, issue 5. – 054301.

[3]. Василиу Е.В. Анализ безопасности пинг-понг протокола с квантовым плотным кодированием / Е.В. Василиу // Наукові праці ОНАЗ ім. О.С. Попова. – 2007. – № 1. – С. 32–38.

[4]. Vasiliu E.V. Non-coherent attack on the ping-pong protocol with completely entangled pairs of qutrits / Eugene V. Vasiliu // Quantum Information Processing. – 2011. – V. 10, num. 2. – P. 189–202.

[5]. Li X.-H. Multiparty Quantum Remote Secret Conference / X.-H. Li, C.-Y. Li, F.-G. Deng et al // Chinese Physics Letters. – 2007. – V. 24, № 1. – P. 23–26.

[6]. Jin X.-R. Three-party quantum secure direct communication based on GHZ states / X.-R. Jin, X. Ji, Y.-Q. Zhang et al // Physics Letters A. – 2006. – V. 354, № 1-2. – P. 67–70.

[7]. Василиу Е.В. Пинг – понг протокол с трех– и четырехкубитными состояниями Гринбергера – Хорна – Цайлингера / Е.В. Василиу, Л.Н. Василиу // Труды Одесского политехнического университета. – 2008. – Вып. 1(29). – С. 171–176.

[8]. Ostermeyer, M. On the implementation of a deterministic secure coding protocol using polarization entangled photons / M. Ostermeyer, N. Walenta // Optics Communications. – 2008. – V. 281, issue 17. – P. 4540–4544.
[9]. Jung E. Attack of many eavesdroppers via optimal strategy in quantum cryptography / E. Jung, M.-R. Hwang, D.K. Park [et al.] // Physical Review A. – 2009. – V. 79, issue 3. – 032339.
[10]. Василиу Е.В. Синтез основанной на пинг-понг протоколе квантовой связи безопасной системы прямой передачи сообщений / Е.В. Василиу, С.В. Николаенко // Наукові праці ОНАЗ ім. О.С. Попова. – 2009, № 1. – С. 83–91.

REFERENCES

[1]. Boström K. Deterministic secure direct communication using entanglement / K. Boström, T. Felbinger // Physical Review Letters, 2002, Vol. 89, issue 18. – 187902.
[2]. Cai Q.-Y. Improving the capacity of the Boström – Felbinger protocol / Q.-Y. Cai, B.-W. Li // Physical Review A., 2004, V. 69, issue 5. – 054301.
[3]. Vasiliu Ye.V. Security analysis of ping-pong protocol with quantum thick coding / Ye.V.Vasiliu // Science works of ONAZ n.a. O.S.Popov, 2007, № 1, P. 32–38.
[4]. Vasiliu E.V. Non-coherent attack on the ping-pong protocol with completely entangled pairs of qutrits / Eugene V. Vasiliu // Quantum Information Processing, 2011, V. 10, num. 2, P. 189–202.
[5]. Li X.-H. Multiparty Quantum Remote Secret Conference / X.-H. Li, C.-Y. Li, F.-G. Deng et al // Chinese Physics Letters, 2007, V. 24, № 1, P. 23–26.
[6]. Jin X.-R. Three-party quantum secure direct communication based on GHZ states / X.-R. Jin, X. Ji, Y.-Q. Zhang et al // Physics Letters A, 2006, V. 354, № 1-2, P. 67–70.
[7]. Vasiliu Ye.V. Ping-pong protocol with 3- and 4-qubits Greenberger-Horne-Zeilinger states / Ye.V.Vasiliu, L.N.Vasiliu // Works of Odessa polytechnic university, 2008, Vol. 1(29), P. 171–176.
[8]. Ostermeyer, M. On the implementation of a deterministic secure coding protocol using polarization entangled photons / M. Ostermeyer, N. Walenta // Optics Communications., 2008, V. 281, issue 17. – P. 4540–4544.
[9]. Jung E. Attack of many eavesdroppers via optimal strategy in quantum cryptography / E. Jung, M.-R. Hwang, D.K. Park [et al.] // Physical Review A. – 2009. – V. 79, issue 3. – 032339.
[10]. Vasiliu Ye.V. Synthesis of safety system direct message transferring based on ping-pong protocol of quantum communications / Ye.V.Vasiliu, S.V.Nikolaenko // Science works of ONAZ n.a. O.S.Popov, 2009, № 1, P. 83–91.

АНАЛИЗ ПОСЛЕДОВАТЕЛЬНОЙ АТАКИ ПАССИВНОГО ПЕРЕХВАТА НЕСКОЛЬКИХ ЗЛОУМЫШЛЕННИКОВ НА ПИНГ-ПОНГ ПРОТОКОЛ С ПАРАМИ ПЕРЕПУТАННЫХ КУБИТОВ

В статье проанализирована последовательная атака пассивного перехвата двух и большего числа злоумышленников на оригинальный пинг-понг протокол с парами перепутанных кубитов. Получено общее рекурсивное выражение для вероятности d обнаружения атаки произвольного количества n злоумышленников, позволяющее вычислить эту вероятность через соответствующую вероятность при атаке n – 1 злоумышленников. Показано, что увеличение количества атакующих в квантовом канале приводит к увеличению вероятности обнаружения их атаки легитимными пользователями. Получены выражения для максимального количества информации злоумышленников при последовательной атаке двух и трех злоумышленников. Показано, что максимальное количество информации злоумышленников определяется тем же выражением, что и в случае атаки одного злоумышленника, изменяется только величина d. Показано что пинг-понг протокол с парами перепутанных кубитов уязвим к атаке пассивного перехвата нескольких злоумышленников не более, чем к атаке одного.

Ключевые слова: квантовая криптография, пинг-понг протокол, атака пассивного перехвата нескольких злоумышленников, вероятность обнаружения атаки, количество информации злоумышленников.

ANALYSES OF THE CONSISTENT EAVESDROPPING ATTACK OF SEVERAL EAVESDROPPERS ON THE PING-PONG PROTOCOL WITH ENTANGLED PAIRS OF QUBITS

In this paper the analyses of the eavesdropping attack of two or more eavesdroppers on the original ping-pong protocol with entangled pairs of qubits is carried out. General recursive expression for probability d of attack detection for any number n of eavesdroppers that allows to calculate this probability through the corresponding probability when n – 1 eavesdroppers attack is obtained. It is shown that an increase in the number of attackers in the quantum channel leads to an increase in the probability of detecting these attacks by legitimate users. The expressions for the maximum eavesdroppers' amount of information during a consistent attack of two and three eavesdroppers are obtained. It is indicated that the maximum eavesdroppers' amount of information determined by the same expression as in the case of one eavesdropper's attack, only the value of d is varying. It is shown that the ping-pong protocol with pairs of entangled qubits is vulnerable to eavesdropping attack of several eavesdroppers not more than to one eavesdropper's attack.

Keywords: quantum cryptography, a ping-pong protocol, eavesdropping attack of several eavesdroppers, the prob-

ability of eavesdroppers' detection, eavesdroppers' amount of information.

Василіу Євген Вікторович, доктор технічних наук, доцент, директор навчально-наукового інституту радіо, телебачення та електроніки Одеської національної академії зв'язку ім. О.С. Попова.
E-mail: vasiliu@ua.fm
Василиу Евгений Викторович, доктор технических наук, доцент, директор учебно-научного института радио, телевидения, электроники Одесской национальной академии связи им. А.С. Попова.
Vasiliu Yevhen, Doctor of Science in Eng., Full Professor, Director of Educational and research institute of radio, television, electronics Odessa national academy of telecommunications named after O.S.Popov.
Ніколаєнко Сергій Вадимович, викладач Одеської національної академії телекомунікацій ім. Попова О.С.
E-mail: serezhanik@gmail.com
Николаенко Сергей Вадимович, преподаватель Одесской национальной академии связи им. А.С. Попова.
Nikolayenko Sergiy, Lecturer at IT Dept, Odessa National Academy of Telecommunications named after O.S. Popov.

УДК 004.056; 681.58

ДІЛОВІ ІГРИ ЯК МЕТОД ПІДГОТОВКИ ФАХІВЦІВ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Наталія Шиліна, Юрій Копитін

Забезпечення належного рівня інформаційної безпеки напряму залежить від якісної професійної підготовки майбутніх фахівців, рівня впровадження та використання інноваційних педагогічних, інформаційно-комунікаційних технологій та формування інформаційної культури. Проаналізований сучасний стан підготовки фахівців з інформаційної безпеки свідчить, що поточні вимоги до вмінь та навичок студентів не відповідають тим, які необхідні для побудови ефективної системи управління інформаційною безпекою організації. У роботі розкрито методику проведення ділових ігор для підготовки фахівців з інформаційної безпеки. Описаний метод підготовки фахівців дозволить студентам краще осмислити матеріал, розвинути свої творчі здібності в розв'язанні проблеми захисту інформації, розбиратися в тих чи інших питаннях інформаційної безпеки та вчитися працювати в колективі. Ділові ігри допоможуть забезпечити майбутніх фахівців з інформаційної безпеки необхідними теоретичними знаннями та практичними навиками у сфері сучасних методів та засобів захисту інформації.

***Ключові слова**: інформаційна безпека; модель вищої професійної освіти; технічний захист; ділові ігри; професійна підготовка.*

1. ВСТУП. Стрімкі темпи впровадження нових інноваційних та інформаційно-комунікаційних технологій (ІКТ), зростання обсягів цифрової інформації і підвищення її значимості несуть у собі ризики, що можуть призвести до порушення цілісності, конфіденційності, доступності інформації та заподіяння шкоди.

Саме тому власники, розпорядники і користувачі інформаційних ресурсів повинні розуміти, що надійний захист інформації та гарантоване покриття ризиків можливі тільки за умови забезпечення належного рівня інформаційної безпеки (ІБ), яка є невід'ємною складовою кожної зі сфер національної безпеки і водночас важливою самостійною сферою забезпечення національної безпеки держави [1].

Забезпечення належного рівня ІБ напряму залежить від якісної професійної підготовки майбутніх фахівців, рівня впровадження та використання інноваційних педагогічних, інформаційно-комунікаційних технологій та формування інформаційної культури. В сучасних умовах переходу від когнітивної до компетентнісної моделі побудови змісту освіти це особливо важливо для України, яка модернізується як європейська держава та інтегрується в світове інформаційне співтовариство.

У зв'язку з цим зростає потреба у кваліфікованих фахівцях у галузі інформації безпеки, оскільки рівень захищеності інформації безпосередньо залежить від рівня підготовки кадрів у національній системі освіти.