УДК 004.056+511.176

Ю. Є. Яремчук[1]

АВТЕНТИФІКАЦІЯ СТОРІН ВЗАЄМОДІЇ З ОБМЕЖЕНОЮ РАНДОМІЗАЦІЄЮ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

[1]Вінницький національний технічний університет

Розглянуто можливість автентифікації сторін взаємодії з обмеженою рандомізацією на основі математичного апарату рекурентних V_k- та U_k-послідовностей. Показано можливість зменшення (у декілька разів) обчислювальної та комунікаційної складності під час виконання криптографічних перетворень, що особливо важливо для систем типу «свій–чужий», де зменшення часу життя ключа через відсутність сеансового ключа рандомізації з боку претендента не є критичним.

Ключові слова: захист інформації, криптографія, автентифікація сторін взаємодії, рекурентні послідовності.

Вступ

Задача забезпечення цілісності на сьогодні є не менш актуальною задачею, ніж забезпечення конфіденційності інформації. Ця задача може розв'язуватись за допомогою криптографічних протоколів автентифікації та цифрового підписування [1]. Автентифікація сторін взаємодії [1] — це процес криптографічних перетворень, під час якого одна зі сторін переконується в ідентичності другої сторони, а також у тому, що друга сторона активна у часі або безпосередньо перед моментом підтвердження доказів.

Найвідомішими методами автентифікації є методи Фейге–Фіата–Шаміра, Гіллоу–Куіскуотера та Шнорра [1, 2]. Ці методи базуються на операції піднесення до степеня, яка вимагає виконання досить складних обчислень, що впливає на швидкість роботи методу у його практичній реалізації.

При цьому існують задачі, в яких автентифікація відбувається у якийсь певний важливий момент часу, зокрема це стосується так званих систем ідентифікацій «свій–чужий», де забезпечення доведення з нульовим розголошенням не є критичним, тому рандомізація з використанням сеансового ключа з боку учасника взаємодії може не використовуватись. Причому у таких системах найважливішим є забезпечення максимальної швидкості, оскільки уповільнення передавання інформації між учасниками може створювати середовище передавання — вода, повітря тощо.

У зв'язку з цим звертаємо увагу на математичний апарат рекурентних послідовностей, зокрема V_k- та U_k-послідовностей [3], який дозволяє за певних умов спрощувати обчислення під час виконання криптографічних перетворень.

Таким чином, актуальним є дослідження можливості здійснення автентифікації сторін взаємодії на основі рекурентних послідовностей, який би забезпечував спрощення обчислень для систем автентифікації з обмеженою рандомізацією.

Здійснення автентифікації сторін взаємодії з обмеженою рандомізацією

Автентифікація сторін взаємодії з обмеженою рандомізацією може бути реалізована на основі математичного апарату рекурентних U_k- та V_k-послідовностей. Розглянемо можливість автентифікації сторін взаємодії на основі цього математичного апарату. Суть ідеї автентифікації [4] базується на аналітичній залежності U_k-послідовності обчислення елемента $u_{n+m,k}$, яка дозволяє визначати цей елемент, або використовуючи елементи $v_{m+i,k}$, $i=\overline{-1,k-2}$, та $u_{n-i,k}$, $i=\overline{0,k-1}$, або використовуючи елементи $v_{n+i,k}$, $i=\overline{-1,k-2}$, та $u_{m-i,k}$, $i=\overline{0,k-1}$. Це дає можливість створення такого методу автентифікації сторін взаємодії.

Спочатку претендент, який має довести свою автентичність, виконує попередню процедуру обчислення ключів. Для цього він випадковим чином вибирає секретний ключ a, після чого обчис-

© Ю. Є. Яремчук, 2014

лює і передає перевіряльнику відкритий ключ $u_{a-i,k}$, $i=\overline{0,k-1}$.

Коли перевіряльник бажає перевірити автентичність претендента, він вибирає випадкове число b, обчислює $u_{b-i,k}$, $i=\overline{0,k-1}$, і передає отриманий набір елементів претенденту. Претендент, прийнявши цей набір елементів, здійснює на їх основі обчислення $u_{b+a,k}$. Одночасно перевіряльник обчислює $u_{a+b,k}$. Потім претендент передає отримане значення $u_{b+a,k}$ перевіряльнику, який звіряє його зі значенням $u_{a+b,k}$, ідентифікуючи таким чином претендента.

Схема автентифікації сторін взаємодії за цим методом показана на рис. 1.

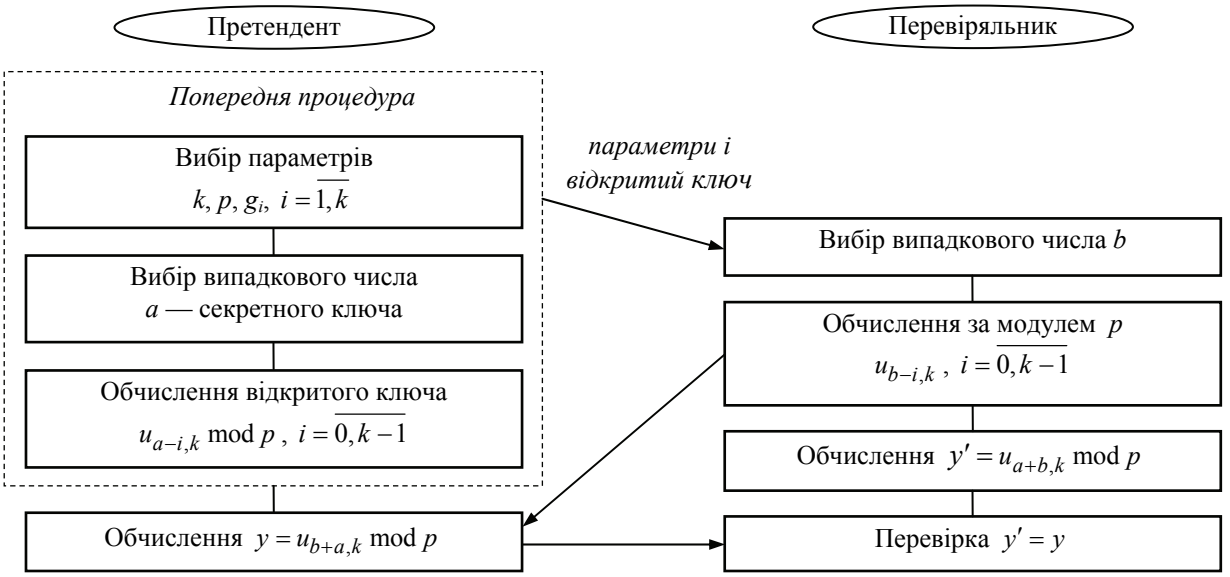

Рис. 1. Схема автентифікації сторін взаємодії на основі елементів U_k-послідовності

Слід зазначити, що претендент та перевіряльник можуть вибирати, відповідно, секретні числа a і b та обчислювати за модулем p елементи $u_{a-i,k}$ і $u_{b-i,k}$ для $i=\overline{0,k-1}$ попередньо, заздалегідь до безпосереднього процесу автентифікації.

Не важко пересвідчитись, що претендент та перевіряльник згідно із запропонованим методом автентифікації будуть виконувати приблизно ті ж обчислення, що і, відповідно, користувачі A та B у запропонованому в [3] методі розподілу секретних ключів на основі U_k-послідовностей. Враховуючи це, складність виконання запропонованого протоколу автентифікації з боку як претендента, так і перевіряльника, буде складати приблизно $H^2q\left[6H\left(k^2+k\right)+3\left(3k^2+k\right)\right]$ операцій над машинними одиницями інформації.

Порівнюючи запропонований метод автентифікації з відомими методами Фейге–Фіата–Шаміра, Гіллоу–Куіскуотера та Шнорра відносно складності виконання автентифікації, слід зазначити, що у запропонованому методі претенденту та перевіряльнику необхідно виконувати обчислення певного елементу U_k-послідовності по одному разу, в той час як за відомими методами їм необхідно виконувати піднесення до степеня по два рази. Враховуючи те, що складність обчислення певного елемента V_k- або U_k-послідовності для малих значень k має приблизно той самий порядок, що і складність піднесення до заданого степеня, то можна стверджувати, що описаний метод має приблизно вдвічі меншу складність обчислень, ніж відомі методи автентифікації. Крім того, запропонований метод має значно простішу процедуру завдання параметрів, оскільки їх вибір не потребує проведення складних обчислень над великими числами.

Слід також зазначити, що у відомих методах автентифікації, окрім передавання параметрів, необхідно виконувати три передачі інформації: дві від претендента до перевіряльника і одну — від перевіряльника до претендента, в той час як за запропонованим методом достатнім є лише два передавання: по одному з кожного боку.

Проведемо тепер дослідження криптографічної стійкості запропонованого методу автентифікації сторін взаємодії. Під час здійснення криптоаналізу запропонованого методу автентифікації

зловмиснику відомі ті ж дані, що й у методі розподілу секретних ключів на основі U_k-послідовностей, дослідження криптостійкості якого на математичному рівні проведено у [5]. Однак, окрім цих даних, у запропонованому методі автентифікації зловмиснику додатково, після першого сеансу автентифікації, стає відомим значення $y = u_{b+a,k} \bmod p$, яке передається на завершальному етапі автентифікації від претендента до перевіряльника. У подальших сеансах автентифікації для заданого секретного ключа це призведе до зменшення рівня стійкості, оскільки у зловмисника з'являється додаткова можливість спроби зламу методу шляхом знаходження секретного ключа a з елементів $u_{b+a,k}$, а також $u_{a-i,k}$ та $u_{b-i,k}$, $i = \overline{0,k-1}$, обчислених за модулем p.

Така спроба може бути реалізована шляхом побудови системи з k рівнянь та з k невідомими на основі аналітичних залежностей обчислення елемента $u_{n,k}$ через елементи V_k-послідовності та властивості обчислення елемента $u_{n+m,k}$ через елементи V_k- або U_k-послідовностей, виразивши відповідно елементи $u_{a-i,k}$, $i = \overline{0,k-1}$, та $u_{b+a,k}$ через елементи V_k- або U_k-послідовностей. На прикладі для $k = 2$ система рівнянь в такому випадку буде мати вигляд

$$\begin{cases} u_{a+1,2} = g_2 v_{a,2} + g_1^2 v_{a-1,2}; \\ u_{b+a,2} = v_{a,2} u_{b,2} + g_1 v_{a-1,2} u_{b-1,2}. \end{cases}$$

Таким чином, описаний варіант методу автентифікації сторін взаємодії на основі U_k- та V_k^+-послідовностей забезпечує достатній рівень стійкості лише для одноразового секретного ключа a. Це обмежує використання методу, однак і в такому поданні він може мати доволі широке застосування в системах різного призначення, особливо в тих, де ідентифікація «свій–чужий» повинна відбуватись лише в один певний важливий або критичний момент часу, причому саме в цей момент часу важливим також може бути якомога швидке здійснення ідентифікації.

Підвищити стійкість запропонованого методу автентифікації на основі U_k-послідовностей можна шляхом ускладнення на завершальному етапі автентифікації обчислення елемента рекурентної послідовності, використовуючи складніший спосіб зміни його індексу. Для цього для побудови методу автентифікції можна використовувати математичний апарат виключно на основі рекурентних V_k^+-послідовностей, що дасть можливість обчислювати елемент послідовності на завершальному етапі автентифікації за мультиплікативним, а не адитивним способом зміни індексу.

Таким чином, метод автентифікації сторін взаємодії може бути створений на основі властивості обчислення елемента $v_{n+m,k}$ V_k^+-послідовності [6], завдяки якій забезпечується можливість реалізації процедур прискореного обчислення елементів $v_{n,k}$ та $v_{n\cdot m,k}$ для великих значень індексів.

Згідно з методом, спочатку претендент (або центр довіри) виконує попередню процедуру вибору параметрів та обчислення ключів. Для цього він вибирає і відкрито публікує параметри — ціле додатне число p $(p > 2)$ та цілі числа g_1, g_k. Після цього він випадковим чином вибирає секретний ключ a, $1 < a < p$, та обчислює за модулем p і передає перевіряльнику відкритий ключ $v_{a+i,k}$, $i = \overline{0,k-1}$. Перевіряльник на своєму боці розширює набір елементів відкритого ключа, обчислюючи за модулем p елементи $v_{a+i,k}$, $i = \overline{0,k-1}$, за формулою обчислення $v_{n,k}$, що визначає V_k^+-послідовність.

Коли претендент хоче довести свою автентичність, він повідомляє про це перевіряльника, який вибирає випадкове число b, $1 < b < p$, обчислює за модулем p $v_{b+i,k}$, $i = \overline{0,k-1}$, і передає ці елементи претенденту. Претендент, прийнявши цей набір елементів, спочатку розширює його, обчислюючи за модулем p елементи $v_{b+i,k}$, $i = \overline{0,k-1}$, за формулою обчислення $v_{n,k}$, що визначає V_k^+-послідовність, а потім здійснює на основі всього набору елементів $v_{b+i,k} \bmod p$, $i = \overline{-(k-1),k-1}$ обчислення коду автентифікації $v_{b\cdot a,k} \bmod p$, використовуючи свій секретний ключ a, та передає отриманий код автентифікації перевіряльнику. Одночасно перевіряльник обчислює значення $v_{a\cdot b,k} \bmod p$ на основі отриманого ним раніше набору елементів $v_{a+i,k} \bmod p$, $i = \overline{-(k-1),k-1}$, та

свого секретного значення b. На завершення, перевіряльник звіряє обчислене значення з отриманим від претендента кодом автентифікації, ідентифікуючи тим самим претендента.

Схема автентифікації сторін взаємодії за цим методом показана на рис. 2.

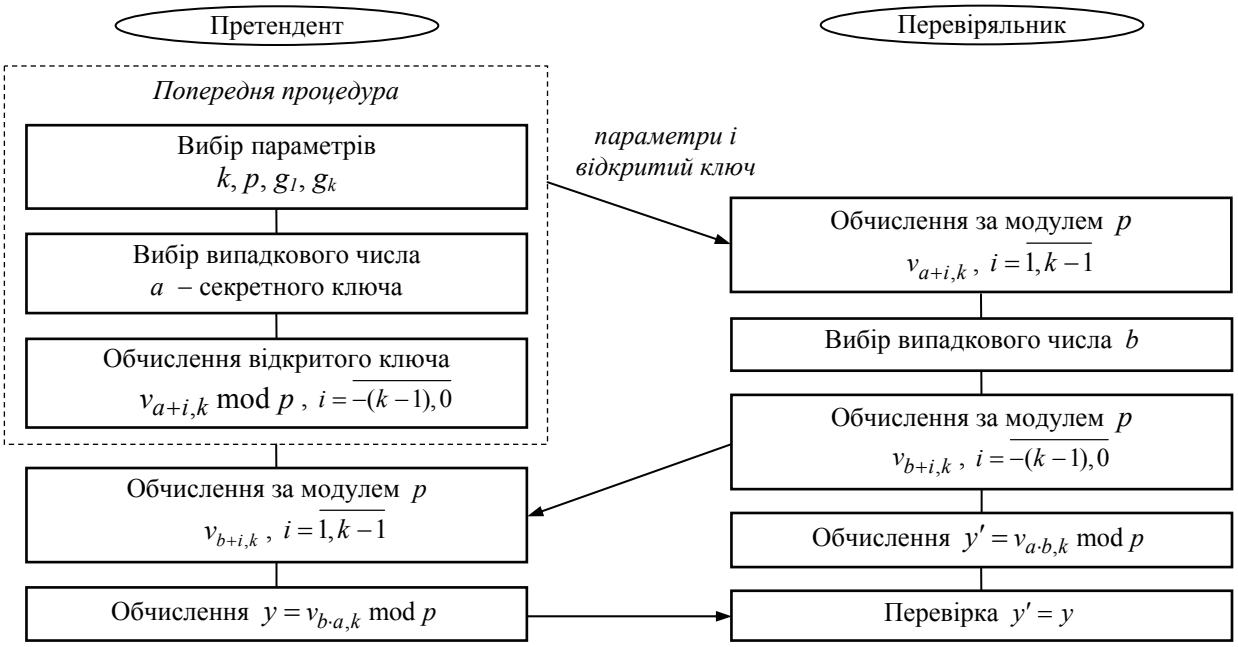

Рис. 2. Схема автентифікації сторін взаємодії на основі елементів V_k^+-послідовності

Вибір числа b та обчислення за модулем p елементів $v_{b+i,k}$, $i = \overline{-(k-1),0}$, можуть бути виконані перевіряльником попередньо, заздалегідь до безпосередньої автентифікації. Так само попередньо перевіряльник обчислює за модулем p елементи $v_{a+i,k}$, $i = \overline{1,k-1}$, за формулою обчислення $v_{n,k}$, що визначає V_k^+-послідовність, розширюючи набір елементів відкритого ключа. Можливість попередніх обчислень з боку перевіряльника дає можливість зменшити майже у два рази обчислювальну складність процедури перевірки автентичності безпосередньо під час автентифікації.

У запропонованому методі автентифікації сторін взаємодії основні обчислення виконуються згідно з залежністю $v_{n+m,k}$. Визначення цього елемента здійснюється на основі елементів $v_{n+i,k}$, $i = \overline{-(k-1),0}$, та елементів $v_{m+i,k}$, $i = \overline{-1,k-2}$.

Порівнюючи запропонований метод автентифікації сторін взаємодії на основі V_k^+-послідовностей за методом автентифікації на основі U_k-послідовностей, який було описано вище, слід зазначити, що запропонований метод на основі V_k^+-послідовностей має вищу, майже у два рази, складність обчислень, однак при цьому він забезпечує вищу криптографічну стійкість процесу автентифікації, оскільки в ньому код автентифікації отримується як результат обчислень елемента $v_{n\cdot m,k}$ V_k^+-послідовності, тобто за мультиплікативним способом зміни індексу, а не за адитивним способом зміни індексу при обчисленні елемента $u_{n+m,k}$ U_k-послідовності за відповідним методом автентифікації.

Проведемо детальніший аналіз криптографічної стійкості запропонованого методу автентифікації на основі V_k-послідовностей. Для здійснення криптоаналізу цього методу криптоаналітику під час кожного сеансу автентифікації відомі елементи відкритого ключа $v_{a+i,k} \bmod p$ та сеансові значення елементів $v_{b+i,k} \bmod p$, $i = \overline{-(k-1),0}$, а також значення y, яке визначається елементом $y = v_{b\cdot a,k} \bmod p$, що також залежіть від сеансу автентифікації.

Таким чином, криптоаналітик може здійснювати статистичний аналіз, використовуючи для цього певний метод математичної статистики, оскільки в нього з кожним сеансом є можливість розширювати для різних значень b набір елементів $v_{b+i,k} \bmod p$, $i = \overline{-(k-1),0}$, та $v_{b\cdot a,k} \bmod p$ для

статистики з метою розкриття секретного ключа a з елементів $v_{a+i,k} \bmod p$, $i = \overline{-(k-1),0}$, які є незмінними під час сеансів в межах часу життя ключа.

Причому, збирати статистичні дані і виконувати статистичний аналіз може як зловмисник, так і перевіряльник, який може виконувати криптоаналіз для отримання секретного ключа a, порушуючи доведення з нульовим розголошенням. Для цього перевіряльник може навмисно так вибирати своє сеансове секретне значення b, щоб за найменшу кількість сеансів отримати необхідну інформацію для знаходження секретного ключа.

Висновки

Розглянуто можливість автентифікації сторін взаємодії на основі математичного апарату рекурентних U_k- та V_k^+-послідовностей. У порівнянні з відомими методами Фіата–Шаміра, Фейге–Фіата–Шаміра, Гіллоу–Куіскуотера та Шнорра метод має простішу процедуру задання параметрів та приблизно удвічі меншу складність обчислень для малих значень k-порядку послідовності. Крім того, у відомих методах, окрім передавання параметрів, безпосередньо під час автентифікації необхідно виконувати три етапи передавання інформації, в той час як за представленим методом лише два. Аналіз криптографічної стійкості розглянутого методу автентифікації сторін взаємодії на основі U_k- та V_k^+-послідовностей показав, що метод забезпечує достатній рівень стійкості лише для одноразового секретного ключа. Це обмежує його використання, однак і у такому представлені метод має своє застосування, особливо у системах, де має відбуватись ідентифікація «свій–чужий» лише в один певний важливий момент часу, причому з максимальною швидкістю.

Розглянуто можливість автентифікації сторін взаємодії на основі рекурентних V_k^+-послідовностей. Метод має приблизно самий рівень складності обчислень, що й відомі аналоги. У порівнянні з представленим методом автентифікації на основі U_k-послідовностей метод на основі V_k^+-послідовностей хоч і має вищу, майже у два рази, складність обчислень, однак при цьому він забезпечує вищу криптографічну стійкість, оскільки у ньому код автентифікації отримується як результат обчислень елемента V_k^+-послідовності за мультиплікативним, а не адитивним, способом зміни індексу. Проведено також аналіз криптографічної стійкості методу автентифікації на основі V_k^+-послідовностей, який показав можливість, на відміну від методу на основі U_k-послідовностей, багаторазового використання секретного ключа. Однак час життя ключа в методі на основі V_k^+-послідовностей не може бути довгим, оскільки в ньому відсутня сеансова ключова рандомізація з боку претендента. Це певним чином обмежує використання методу, але й у такому представлені забезпечує запропонованому методу доволі широке застосування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Menezes, A. J. Handbook of Applied Cryptography [Текст] / A. J. Menezes, P. C. van Oorschot, S. A. Vanstone. — CRC Press, 2001. — 816 p.

2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си [Текст] / Б. Шнайер. — М. : Триумф, 2002. — 816 с.

3. Яремчук Ю. Є. Використання рекурентних послідовностей для побудови криптографічних методів з відкритим ключем [Текст] / Ю. Є. Яремчук // Захист інформації. — 2012. — № 4.— С. 120—127.

4. Яремчук Ю. Є. Метод автентифікації сторін взаємодії на основі рекурентних послідовностей [Текст] / Ю. Є. Яремчук // Сучасний захист інформації. — 2013. — № 1. — С. 4—10.

5. Яремчук Ю. Є. Оцінювання криптостійкості методів шифрування інформації на основі рекурентних послідовностей [Текст] / Ю. Є. Яремчук // Східно-Європейський журнал передових технологій. — 2013. — № 2/10(62). — С. 35—38.

6. Яремчук Ю. Є. Можливість автентифікації сторін взаємодії на основі рекурентних послідовностей [Текст] / Ю. Є. Яремчук // Захист інформації. — 2013. — Т. 15, № 4. — С. 394—398.

Рекомендована кафедрою менеджменту та безпеки інформаційних систем ВНТУ

Стаття надійшла до редакції 18.11.2014

Яремчук Юрій Євгенович — канд. техн. наук, доцент, професор кафедри менеджменту та безпеки інформаційних систем, e-mail: yurevyar@vntu.net.

Вінницький національний технічний університет, Вінниця

Yu. Ye. Yaremchuk[1]

Authentication of the parties interaction with limited randomization based on recurrent sequences

[1]Vinnytsia National Technical University

The possibility of authentication of the parties interaction with limited randomization based on the mathematical apparatus of recurrence of V_k- and U_k-sequences is considered in the paper. Demonstrated the possibility of reducing (in several times) the computing and communication difficulties during the execution of cryptographic transformations is demonstrated, which is particularly important for systems of the type of "friend or foe", where the reduction of the lifetime of the key due to the lack of randomization of the session key by the applicant is not critical.

Keywords: informational security, cryptography, authentication of parties interaction, recurrent sequences.

Yaremchuk Yurii Ye. — Cand. Sc. (Eng), Assistant Professor, Professor of the Chair of Management and Information Systems Security, e-mail: yurevyar@vntu.net

Ю. Е. Яремчук[1]

Аутентификация сторон взаимодействия с ограниченной рандомизацией на основе рекуррентных последовательностей

[1]Винницкий национальный технический университет

Рассмотрена возможность аутентификаци сторон взаимодействия с ограниченной рандомизацией на основе математического аппарата рекуррентных V_k- и U_k-последовательностей. Показана возможность уменьшения (в несколько раз) вычислительной и коммуникационной сложности во время выполнения криптографических преобразований, что особенно важно для систем типа «свой–чужой», где уменьшение времени жизни ключа за счёт отсутствия сеансового ключа рандомизации со стороны претендента не является критичным.

Ключевые слова: защита информации, криптография, аутентификация сторон взаимодействия, рекуррентные последовательности.

Яремчук Юрий Евгениевич — канд. техн. наук, доцент, профессор кафедры менеджмента и безопасности информационных систем, e-mail: yurevyar@vntu.net