ризиками без застосування заходів та засобів захисту.

4. В разі неприйнятності деяких із підходів визначеної стратегії управління ризиками, для подальшого зменшення можливості реалізації загроз необхідним є **застосування заходів та засобів захисту**. Зрозуміло, що відтепер розмову слід вести про захист лише від тих загроз, від яких не можна ухилитися, змінити їх характер чи сприйняти допустимість їх реалізації з певним рівнем залишкового ризику і, відповідно, певним рівнем збитків. Тобто слід внести відповідні зміни в модель загроз шляхом необхідної корекції таблиці.

Після вибору конфігурації можливої системи захисту та визначення параметрів її елементів (відповідних ймовірностей подолання засобів захисту певними загрозами, чи, навпаки, ймовірностей протистояти цим загрозам) слід зробити оцінку залишкового ризику (методика такої оцінки розглядається нижче), який забезпечується при застосуванні засобів забезпечення кожної з властивостей захищеності відповідних ресурсів, і повторити етапи 3 та 4 даної методики (аналіз можливостей сприйняття допустимості реалізації певних загроз з певним рівнем залишкового ризику і застосування заходів та засобів захисту). При цьому будуть виявленими загрози, для яких уже застосовані заходи та засоби не дали бажаного ефекту. Тому проти таких загроз слід розробляти (чи вибирати) більш ефективні, а отже більш витратні заходи чи засоби захисту. Ці етапи слід повторювати доти, поки не буде прийнятим рішення щодо сприйняття допустимості реалізації усіх загроз з тим рівнем залишкового ризику, який вдалося досягти при прийнятних витратах.

Таким чином, наведені методики надають змогу здійснення досить глибокого і достовірного аналізу можливих порушників, загроз ресурсам автоматизованих систем з боку цих порушників, визначення можливих контрзаходів для протидії цим загрозам, в тому числі, складу необхідних засобів захисту з метою забезпечення припустимої захищеності АС.

Література: ***1.*** *Астахов А. Актуальные вопросы выявления сетевых атак. JetInf0 № 3 (106), 2002. На сайті http://www.jetinfo.ru/2002/3/1/article1.3.2002.html;* ***2.*** *Астахов А. Анализ защищенности корпоративных систем. // Открытые системы, № 07-08/2002. На сайті http://www.osp.ru/os;* ***3.*** *Будько М. М. Визначення залишкового ризику при оцінці захищеності інформації в інформаційно – обчислювальних системах // К.: НТУ "КПІ" //Правове, нормативне та метрологічне забезпечення Системи захисту інформації в Україні. Випуск 8 // 2004, с. 20-26;* ***4.*** *Будько М. М., Василенко В. С., Проскурін В. М. Методика оцінки захищеності інформації в ЛОМ // К.: Військовий інститут інформатизації та телекомунікацій НТУУ "КПІ" Збірка доповідей на II НТК інституту "Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення";* ***5.*** *Василенко В. С., Будько М. М. Методики визначення вихідних даних для оцінки залишкових ризиків у ЛОМ // К.: НТУ "КПІ" // Правове, нормативне та метрологічне забезпечення Системи захисту інформації в Україні. Випуск 9 // 2004, с. 110-120.*

УДК 681.3.06

АНАЛІЗ СКЛАДУ ПРОФІЛІВ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ

Анатолій Антонюк, Денис Берестов, Сергій Пустовіт

Національний науково-дослідний центр оборонних технологій і воєнної безпеки України

Анотація: **Вивчається основне поняття нормативних документів системи технічного захисту інформації – стандартний функціональний профіль захищеності. Розглядаються питання його формалізації та пропонується підхід щодо оцінки рівня захищеності автоматизованих систем та вартості реалізації профілів.**

Summary: **It's studied basic conception normative system document technical protection to information - standard functional profile protectability. They are considered question to it's formalizations and is offered approach for estimations level protectability computer-based systems and cost to realization of the profiles.**

Ключові слова: **нормативні документи, автоматизована система**

Вступ

В нормативних документах із захисту інформації в автоматизованих системах (АС) [1 - 4] визначено важливе поняття стандартного функціонального профілю захищеності, причому для кожного з класів введеної в [3] класифікації АС визначена певна їх кількість. В поданому списку вони розміщені за певним ієрархічним принципом і фактично складають затверджений довідник для практичного застосування. Проте, навіть зважаючи на їх ієрархічність, виникає проблема вибору найбільш придатного профілю,

оскільки в [4] подаються лише загальні рекомендації щодо вибору профілів для різних АС (призначених для автоматизації діяльності органів державної влади, банківської діяльності, керування технологічними процесами і довідково-пошукових). Зазначається також, що для найповнішої відповідності характеристикам і вимогам до конкретної АС необхідно проведення в повному обсязі аналізу загроз і оцінки ризиків.

При практичному застосуванні профілів постійно виникає питання, які саме властивості повинна мати конкретна АС для застосування в ній того чи іншого профілю. Крім того виявилося, що для різних класів АС визначені семантично ідентичні профілі на практиці принципово не можуть бути ідентичними внаслідок суттєвої різниці як за механізмами, так і можливостями реалізації. Дійсно, реалізувати один і той же профіль для окремої ПЕОМ (1-ий клас АС) і для локальної обчислювальної мережі (2-ий клас АС) – дві цілком різні проблеми. Тобто, крім якісного їх порівняння за довідником, необхідно мати можливість їх кількісного порівняння, яке було б дуже корисним для полегшення вибору переліку функцій для захищених АС, мінімізації витрат на початкових етапах створення АС, при визначенні рівня захищеності АС, а також у задачах визначення можливих витрат на побудову систем захисту інформації (СЗІ). Відповіді на поставлені питання мають бути змістом відповідних нормативних документів, яких поки що немає.

Питання моделювання профілів розглядалося в [5]. Відзначимо також, що в [6] розглянута одна з наведених проблем, а саме задача оцінки рівня захищеності АС. На основі ймовірносного підходу там, зокрема, пропонується аналізувати можливі канали несанкціонованого доступу (НСД) з подальшим урахуванням конкретної моделі порушника. Потім за допомогою ймовірностей блокування несанкціонованих дій порушника, відмови системи та обходу порушником низки перешкод обчислюється інтегральна ймовірність вразливості даного каналу НСД. Подаються також деякі міркування щодо обчислення цих ймовірностей. Проте, слід зазначити, що наведені ймовірності дуже важко знайти, а також важко ідентифікувати всі канали НСД. Крім того, такий підхід запропоновано без прив'язки до нормативних документів і він не дає можливості оцінювати вартість розробки та побудови СЗІ.

Проте, як показує аналіз складу профілів, навіть за загальними рекомендаціями з [4] можна отримати досить важливі висновки щодо їх подальшого застосування в конкретних АС. Отже, метою даної роботи є аналіз складу та властивостей профілів, розробка математичної моделі профілю, розробка моделі шкали, яка дозволила б певним чином порівнювати різні профілі і, можливо, різні СЗІ.

Для аналізу складу та властивостей профілів зручно спочатку розглянути основні складові профілю – послуги. Як відомо, спроможність АС забезпечувати певний рівень захисту оброблюваної інформації визначається функціональними критеріями [3], розбитими на чотири групи: конфіденційності, цілісності, доступності і спостереженості. Кожна з груп критеріїв описує послуги, що забезпечують захист відповідно від загроз одного з чотирьох основних груп. Так, для критеріїв конфіденційності визначено 5 послуг, для цілісності – 4, для доступності – 4, для спостереженості – 9 (отже, всього – 22). Схема критеріїв, а також назва і зміст кожної послуги приведені в [3]. В свою чергу, кожна послуга набір функцій [3], що дозволяють протистояти певній множині загроз.

Послуга може включати декілька рівнів [3]. Чим вище рівень послуги, тим більш повно вона забезпечує захист від певного виду загроз. Рівні послуг мають ієрархію за повнотою захисту, хоча зовсім не обов'язково являють собою точні підмножини один одного. Вони починаються з першого і зростають до значення n, де n – унікальне для кожного виду послуг. Якщо, як приклад, узяти таку послугу, як довірча конфіденційність, то її ранжування за рівнями виглядає у такий спосіб: мінімальна довірча конфіденційність, базова довірча конфіденційність, повна довірча конфіденційність і абсолютна довірча конфіденційність. Отже, в даному випадку $n = 4$, причому усі наступні рівні включають попередні, тобто, наприклад, можливості забезпечення абсолютної довірчої конфіденційності автоматично покривають можливості забезпечення і повної, і базової, і мінімальної.

Далі в [3] наводиться перелік необхідних вимог щодо механізмів і засобів захисту для забезпечення кожної з функцій, що входять до складу кожної з послуг усіх рівнів. Наприклад, для забезпечення абсолютної довірчої конфіденційності необхідно виконання таких умов як наявність відповідної політики безпеки, певних правил розмежування доступу, певних вимог по спостереженості і т. д. Зазначимо, що вибір способів реалізації умов (апаратний, програмний і т. д.) залишається за розробником АС.

Послуги різних видів та рівнів певним чином групуються в структури, які отримали назву стандартних функціональних профілів захищеності АС (далі просто профіль). Згідно з [4] профіль – це мінімально необхідний перелік послуг, який може забезпечити СЗІ, щоб задовольнити певним вимогам щодо рівня захищеності інформації в АС. Порядок переліку не має значення. Всього визначено 90 профілів і вони є ієрархічними в тому сенсі, що їх реалізація забезпечує дедалі більшу захищеність від загроз відповідного типу. Підвищення ступеня захищеності може досягатися як підсиленням певних послуг, тобто включенням

до профілю більш високого їх рівня, так і безпосереднім включенням до профілю нових послуг.

Семантичний опис профілю складається з трьох частин, які відокремлюються один від одного крапкою: літерно-числового ідентифікатора, знака рівності і переліку послуг певних рівнів, взятого в фігурні дужки. Ідентифікатор включає: позначення класу АС (1, 2 або 3), літерну частину, що характеризує види загроз, від яких забезпечується захист (К, і/або Ц, і/або Д) і номер профілю. Отже, виділяється 7 груп профілів, що забезпечують: К – конфіденційність, Ц – цілісність, Д – доступність, КЦ – конфіденційність і цілісність, КД – конфіденційність і доступність, ЦД – цілісність і доступність, КЦД – конфіденційність, цілісність і доступність. Наприклад, 2.КЦ.3 – функціональний профіль для АС класу 2, в яких основною вимогою до захисту інформації є забезпечення її конфіденційності та цілісності, номер три в своїй групі. Зазначимо, що з точки зору практичного застосування профілів навіть з поданого прикладу видно досить загальний характер такого визначення.

Формальний опис профілю можна здійснити наступним чином. Як було відзначено, профіль має включати ідентифікатор і перелік послуг різних рівнів, який фактично являє собою набір множин, до складу кожної з яких входить ряд послуг певних рівнів. Наприклад, для конфіденційності визначено п'ять видів послуг і кожна з них має декілька рівнів, тому множина послуг з конфіденційності може містити до п'яти видів послуг різних рівнів. Отже, вираз для запису профілю може бути записано в такій формі

$$CIA = \{\{C_{ij}\},\{I_{ij}\},\{A_{ij}\},\{S_{ij}\}\}, \qquad (1)$$

де *CIA* – ідентифікатор профілю, *C* – означає конфіденційність, *I* – цілісність, *A* – доступність, *S* – спостереженість, *i, j* – індекси послуг і рівнів відповідно конфіденційності, цілісності, доступності і спостереженості, причому для кожної з властивостей захищеної інформації визначаються відповідні множини індексів.

Звернемо увагу на те, що в лівій і правій частинах (1) можуть бути присутніми не всі види послуг. Наприклад, можливий профіль

$$I = \{\{C_{ij}\},\{I_{ij}\},\{A_{ij}\},\{S_{ij}\}\},$$

який реалізується в системі, що призначена для обробки інформації, основною вимогою з захисту якої є забезпечення тільки цілісності. Зазначимо також те, що в правій частині скрізь обов'язково мають бути присутніми послуги властивості *S* (спостереженості). Змістовно це означає, що для забезпечення кожної послуги на кожному рівні мають бути присутніми деякі послуги спостереженості в усіх профілях без винятку, тобто має бути контроль в більшому чи меншому ступені певних подій, що відбуваються в АС. Перелік таких подій визначається конкретною політикою безпеки в АС. Можливі також і інші ідентифікатори профілів, наприклад, *CI, IA* і т. д., тобто не скрізь і не завжди необхідно протистояти одразу всім відомим типам загроз – іноді досить мати на увазі лише деякі з них залежно від конкретної мети і задач захисту.

Зберігаючи порядок набору множин в формулі (1), визначимо самі множини наступним чином. Кожну з них зручно ототожнювати з послідовністю цифр, порядок розміщення яких аналогічний порядку опису послуг в [3], а самі цифри відповідають рівню послуги. Однак в багатьох профілях використовуються не всі послуги, а отже, за таким описом різні профілі будуть мати різні послідовності цифр. Тому для узагальнення опису в подальшому замість (1) зручно скористатися наступною формалізацією.

Як раніше було зазначено, всього визначено 22 послуги. Тоді кожному профілю поставимо у відповідність 22-компонентний вектор-стовпчик p_i, за значення компонент якого можна взяти номери рівнів відповідних послуг. Якщо ж якась послуга в профілі взагалі відсутня, то відповідна компонента вектора просто дорівнюватиме нулю. Нижче для прикладу подано частину таблиці з профілями лише для АС 1-го та 2-го класів. В лівому стовпчику таблиці стоять види критеріїв і кількість послуг (*C* – 5, *I* – 4, *A* – 4, *S* – 9); кожен стовпчик містить нулі (відсутність послуги) або цифри (номер відповідної послуги); кількість стовпчиків в кожній графі – кількість профілів у відповідній групі.

	1	1	1	1	1	1	1	2	2	2	2	2	2	2
	C	I	A	CI	CA	IA	CIA	C	I	A	CI	CA	IA	CIA
C	00	00	00	00	0000	0000	0000	00	00	00	00	0000	0000	0000
	01	00	00	01	1000	0000	1111	01	00	00	01	1000	0000	1111
	01	00	00	01	1000	0000	1111	01	00	00	01	1000	0000	1111
	00	00	00	00	0000	0000	0000	00	00	00	00	0000	0000	0000
	00	00	00	00	0000	0000	0000	00	00	00	00	0000	0000	0000

	1	1	1	1	1	1	1	2	2	2	2	2	2	2
	C	I	A	CI	CA	IA	CIA	C	I	A	CI	CA	IA	CIA
I	00	00	00	00	0000	0000	0000	00	00	00	00	0000	0000	0000
	00	02	00	02	0000	1111	1111	00	02	00	02	0000	1111	1111
	00	01	00	01	0000	1111	1111	00	01	00	01	0000	1111	1111
	00	00	00	00	0000	0000	0000	00	00	00	00	0000	0000	0000
A	00	00	12	00	1222	1222	1222	00	00	12	00	1222	1222	1222
	00	00	01	00	0123	0123	0123	00	00	01	00	0123	0123	0123
	00	00	01	00	0123	0123	0123	00	00	01	00	0123	0123	0123
	00	00	12	00	1223	1223	1223	00	00	12	00	1223	1223	1223
S	12	12	22	12	2234	2234	2234	12	12	22	12	2234	2234	2234
	11	11	11	11	1111	1111	1111	11	11	11	11	1111	1111	1111
	11	11	11	11	1122	1122	1122	11	11	11	11	1122	1122	1122
	11	11	12	11	1222	1222	1222	11	11	12	11	1222	1222	1222
	00	00	00	00	0000	0000	0000	00	00	00	00	0000	0000	0000
	12	12	22	12	2222	2222	2222	12	12	22	12	2222	2222	2222
	11	11	11	11	1111	1111	1111	11	11	11	11	1111	1111	1111
	00	00	00	00	0000	0000	0000	00	00	00	00	0000	0000	0000
	00	00	00	00	0000	0000	0000	00	00	00	00	0000	0000	0000

Таким чином, всі профілі описуються однаково і таку таблицю, тобто всю множину профілів, зручно представити у вигляді матриці *P*(22X90), кожний зі стовпців якої є деякий профіль. Тоді операція формального виділення будь-якого p_i профілю (вектора) з такої матриці буде простим множенням її на одиничний вектор e_i, тобто

$$p_i = Pe_i,\ p_i \in E^{22},\ e_i \in E^{90},$$

де через E^{22} та E^{90} позначені векторні множини відповідних розмірностей. Проте, за такою моделлю фактично можна визначити лише наявність певних послуг певних рівнів для даного профілю, тобто ідентифікувати їх. В практичних задачах більш важливим є визначення не тільки їх наявності, а також оцінки повноти (або якості) та вартості (звичайно, в деяких умовних одиницях) їх реалізації.

Розглянемо деякі міркування щодо першого чинника. Детальний аналіз складу всієї множини профілів з довідника [4] дає можливість стверджувати, що оцінку повноти реалізації послуг зручно робити в термінах ймовірностей, тобто величина ймовірності може характеризувати певний рівень реалізації послуги. Однак "в лоб" для послуги таку оцінку отримати дуже важко, оскільки практично для реалізації послуги залучається багато різних механізмів та засобів. Дійсно, як визначено в [4], профіль – це набір послуг, кожна з яких є набором функцій, що дозволяють протистояти певній множині загроз. Це дає можливість для кожної функції визначити ймовірність її реалізації p_{ijk}, де: *i* – номер профілю, *i*=1,…,90; *j* – номер послуги в даному профілі, *j*=1,…,22; *k*-– номер функції для даної послуги, *k*=1,…, n_{ij}. Неважко помітити, що оцінки таких ймовірностей отримати уже набагато легше, ніж для послуги в цілому, оскільки поняття функції є більш конкретним та наглядним порівняно з поняттям послуги. З великим ступенем достовірності можна вважати, що всі функції в основному є незалежними. Тоді їх відповідні ймовірності будуть також незалежними, а це дозволяє обчислювати ймовірності p_{ij} для кожної з послуг в цілому за формулою:

$$p_{ij} = 1 - \prod_{k=1}^{n_{ij}} (1 - p_{ijk}).$$

Більше того, виникає можливість обчислення ймовірності p_i реалізації всього профілю. Тобто, вважаючи незалежними і самі послуги, що, зокрема, відзначено в [4], можна записати

$$p_i = 1 - \prod_{j=1}^{22} (1 - p_{ij}) = 1 - \prod_{j=1}^{22} \prod_{k=1}^{n_{ij}} (1 - p_{ijk}) \,. \quad (3)$$

Фактично ця ймовірність може слугувати оцінкою рівня захищеності конкретної АС.

Зазначимо дуже важливу обставину щодо такого підходу. Вона полягає в тому, що в деяких випадках процес реалізації самої функції можна представити ще більш детально, а саме, у вигляді послідовності деяких незалежних і ще більш конкретних та наглядних дій чи операцій, для яких ймовірності їх реалізації можуть оцінюватися ще більш просто. Тоді ймовірність реалізації самої функції (а в подальшому послуг і всього профілю) визначатиметься аналогічно (3). Як неважко помітити, запропонований процес деталізації можна поглибити ще на одну чи навіть більше ступенів, що суттєво може полегшити процес їх оцінки. Проте, навіть подібні деталізації не можуть розв'язати до кінця задачу отримання оцінок відповідних ймовірностей – вона залишається складною задачею, яка розв'язується в основному за допомогою експертних оцінок, і лише в деяких випадках – за допомогою методів моделювання. Деякі міркування щодо вирішення такої задачі розглядаються в [6].

Тепер розглянемо питання оцінки вартості реалізації профілю. Можна сформулювати наступні твердження.

- З точки зору витрат, очевидно, що профілі з групи КЦД повинні бути більш вагомими (більш витратними з точки зору їх практичної реалізації) порівняно з профілями з груп КЦ, КД, чи ЦД і, природньо, ще більш вагомими порівняно з групами К, Ц, Д. З цих же міркувань профілі з груп КЦ, КД, ЦД більш вагомі, ніж К, Ц, Д. Такий висновок ґрунтується на простому міркуванні: перші групи профілів мають забезпечувати більше послуг, ніж наступні, а отже, вимагають більших витрат.
- Очевидно, що витрати на реалізацію профілів для різних класів АС будуть зростати з ростом класу АС, оскільки, наприклад, для профілів для АС 3-го класу потрібно забезпечувати набагато більше послуг і більш високих рівнів, ніж для аналогічних профілів для АС 2-го чи 1-го класів, а для 2-го класу, природньо, більш, ніж для 1-го.
- Очевидно, також, що витрати для послуг різних рівнів будуть зростати з ростом рівнів, оскільки ясно, що для реалізації більш високого рівня послуги необхідні більш складні, а отже, більш витратні функції.
- Як неважко впевнитись, деталізація профілів на послуги та функції суттєво полегшує проведення оцінок значень витрат для реалізації окремих функцій, ніж для послуг і, тим більше, для профілю в цілому, причому об'єктивніше і точніше.
- Для кожної функції визначимо величину витрат c_{ijk} щодо її реалізації, де: i – номер профілю, i=1,…,90; j – номер послуги в даному профілі, j=1,…,22; k-– номер функції для даної послуги, k=1,…, n_{ij} .

Тоді з наведених міркувань випливає можливість легко оцінювати вартість реалізації будь-якого профілю в цілому – простим сумуванням витрат (з певними ваговими коефіцієнтами a_{ijk}) спочатку за кількістю функцій, що визначають деяку послугу (це буде оцінка для даної послуги), а в подальшому – за послугами:

$$c_i = \sum_{j=1}^{22} \sum^{n_{ij}} a_{ijk} c_{ijk} \,. \quad (4)$$

Практично ця величина може слугувати базою для отримання більш точних оцінок вартості створення всієї СЗІ. Вагові коефіцієнти характеризують певну залежність між різними функціями при їх реалізації. Їх значення, а також значення відповідних вартостей є предметом експертних оцінок. Додамо, що тут також можливий процес подальшої деталізації.

Введені таким чином ймовірності та витрати фактично є критеріями, що дозволяють розв'язувати важливу практичну проблему – проблему порівняння різних профілів, причому не тільки якісно, а навіть кількісно. Це, зокрема, відноситься до профілів, що належать до різних класів АС, але за своїми наборами послуг є ідентичними.

З запропонованого підходу виникає досить проста схема його можливої комп'ютерної реалізації. Вона є практично аналогічною змісту критеріїв [3], в яких у формі таблиць детально описані як самі послуги за рівнями, так і відповідні їм функції. Для отримання кількісних оцінок застосовуються формули (3) та (4). Якщо необхідно введення ще одного (чи більше) ступеню деталізації, то це проводиться цілком аналогічно. Розробка такої системи є предметом подальших досліджень.

Висновки

Таким чином, в роботі проведено аналіз довідника стандартних профілів захищеності на предмет їх складу та властивостей. Здійснено математичний опис профілю, а також визначено важливий підхід щодо проведення процесу порівняння профілів за певною шкалою. Саме завдяки сформульованому підходу виявилася можливість отримати загальні оцінки рівня захищеності конкретних АС в термінах ймовірностей, а також оцінки трудомісткості побудови СЗІ. Причому слід підкреслити, що запропонований формалізм базується на основі лише детального аналізу існуючих нормативних документів і досить загальних міркувань.

В подальшому отримані результати дозволять розглянути важливу задачу формального опису процесу вибору найбільш придатного профілю для конкретних АС, а також суттєво полегшити розв'язок проблеми формального опису вимог щодо критеріїв гарантії [3].

Література: ***1.*** *Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. – НД ТЗІ 1.1-002-99, ДСТСЗІ СБ України, Київ, 1999.* ***2.*** *Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. – НД ТЗІ 1.1-003-99, ДСТСЗІ СБ України, Київ, 1999.* ***3.*** *Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. – НД ТЗІ 2.5-004-99, ДСТСЗІ СБ України, Київ, 1999.* ***4.*** *Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. – НД ТЗІ 2.5.-005 -99, ДСТСЗІ СБ України, Київ, 1999.* ***5.*** *Антонюк А. О. Про деякі важливі поняття захисту інформації в автоматизованих системах // Наукові записки НаУКМА. – 2002. – № 2. – 8 с.* ***6.*** *Мельников В. В. Защита информации в компьютерных системах. – М.: Финансы и статистика, 1997.*

УДК681.391

АНАЛИЗ ВЛИЯНИЯ ЧАСТОТЫ ДИСКРЕТИЗАЦИИ НА ТОЧНОСТЬ ЦИФРОВОЙ ОБРАБОТКИ РЕЧЕВЫХ СИГНАЛОВ В СИСТЕМАХ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ

Владимир Журавлев

Запорожский национальный технический университет

Аннотация: **Проведен анализ критериев выбора оптимальной частоты дискретизации при создании эталона идентификации речевых сигналов. Теоретически обоснована и экспериментально подтверждена точность алгоритма расчета частоты дискретизации, основанная на критерии заданной максимальной дисперсии и интервальной вероятности аппроксимации автокорреляционной функции сигнала на интервале корреляции.**

Summary: **The analysis of optimal discretization frequency during speech signals identification standard creating is given in present article. The precision of sampling frequency calculation algorithm, based on criteria of established maximum dispersion and interval approximation probability of signal autocorrelation function on correlation window is theoretically based and experimentally confirmed.**

Ключевые слова: **Идентификация, речевой сигнал, частота дискретизации, максимально допустимая дисперсия.**

I Введение

Традиционные методы идентификации абонента точки доступа сети связи, в основе которых применяются различные идентификационные карты, ключи или уникальные данные, такие как, например, пароль, не являются надежными в той степени, которая требуется на сегодняшний день. Естественным направлением в повышении надежности систем разграничения доступа стало внедрение в системы безопасности биометрических технологий.

Биометрическая система аутентификации по характеристикам и параметрам речи включает в себя технологический этап создания эталонов идентификации, которые должны отражать индивидуальные особенности речеобразующего тракта разрешенных абонентов точки доступа.

В связи с тем, что речевой сигнал в общем случае представляет собой нестационарный стохастический процесс, создание эталона идентификации с определенными статистическими параметрами является сложной научно технической задачей, не решенной до настоящего времени, что определяется невысокой