2. *Нормативний документ Системи технічного захисту інформації "Критерії оцінки захищеності інформації в комп'ютерних системах від НСД" (НД ТЗІ 2.5 – 004 – 99).* ***3.*** *Нормативний документ Системи технічного захисту інформації "Класифікація автоматизованих систем та стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу" (НД ТЗІ 2.5.–005 –99).* ***4.*** *Нормативний документ Системи технічного захисту інформації "Типове положення про службу захисту інформації в автоматизованій системі" (НД ТЗІ 1.4–001–2000).*

УДК 004.43(031):681.3.01(02)

ВИЗНАЧЕННЯ УРАЗЛИВОСТІ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ЯК СКЛАДОВА ПОРЯДКУ РОЗРОБКИ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Володимир Луценко, Валерій Худяков
НТУУ «КПІ»

Анотація: **Розглядається проблема аналізу властивостей методів та засобів підтримки прийняття рішень для створення проектів систем захисту інформації. Визначено основні властивості таких проектів. Запропоновано підхід до створення нової методики проектування системи захисту інформації від несанкціонованого доступу.**

Summary: **The paper considers problem of analyzing of property of means of support of acceptance of decisions for information security systems projects. The basic properties of such projects are given.The technique of complex system designing for non-authorized access protection is developed on the basis of means of support of acceptance of decisions.**

Ключові слова: **Захист інформації; комплексна система захисту; асоціативна пам'ять; нейроподібна сітка.**

I Вступ

Складні системи найчастіше тому складні, що передбачають необхідність прийняття рішень при протирічних або неповних даних і загалом є напрямком, котрий має тенденцію до розвитку. Це стосується і технічного захисту інформації (ТЗІ), а особливо комплексних систем захисту інформації (КСЗІ) для інформаційно-комунікаційних систем (ІКС) та об'єктів інформаційної діяльності (ОІД) [1, 2], у тому числі таких, котрі не мають у своєму складі засобів інформаційних комунікацій, або мають, але без виходу за межі контрольованої зони (КЗ).

Реальні проекти захисту за якісними показниками мають об'єктивно відтворювати умови життєдіяльності об'єктів, але реально мають тенденцію до відставання від життєвих вимог. Для подолання такого відставання мають відтворюватися вимоги щодо життєдіяльності системи проектування окремо для кожного об'єкту в повному обсязі. Такі вимоги передбачають необхідність використання системи захисту, що базується на базі принципово об'єктивного проектування, тобто такого, котре не залежить від якісних показників проектанта. Крім того, створювана система захисту має бути динамічною в часі, тобто відкритою щодо можливості змін у часі складових методів та засобів захисту або умов існування об'єкту, а такий чинник залежить від методологічних властивостей системи проектування, котра створювала систему захисту. І, насамкінець, майже завжди є відкритим питання необхідної та достатньої завершеності проекту системи захисту. Складність визначення завершеності проекту полягає у відсутності критерію завершеності. Таким реальним критерієм може стати правило, згідно з яким система захисту є достатньо завершеною, якщо за визначений термін часу повторне незалежне проектування дає однаковий результат. Наразі ні один з зазначених чинників не приймається до уваги, а найголовнішою умовою завершеності проектів є формальна за нормативними документами дієздатність системи захисту на даний час та відповідність реалізації спроектованої системи захисту фінансовим можливостям користувача.

Початком більш об'єктивного проектування має бути напрацювання методів та засобів отримання максимально повної та об'єктивної інформації про об'єкт на етапі дослідження об'єкту, а також інженерний аналіз для виявлення місць уразливості об'єкту, тобто визначення ступеня стійкості об'єкта до загроз. Найбільш суб'єктивним фрагментом зазначеного етапу є експертна оцінка при визначенні ризиків і характеристик можливих каналів витоку інформації. Причому, математична або логіко-статистична обробка отриманих від експертів даних є більш досконалою, ніж сама процедура експертизи обмеженою кількістю

експертів з різною кваліфікацією, вподобаннями щодо підходів до захисту, досвідом роботи з об'єктами різної складності, тощо.

Саме на цей етап проектування зроблено головний наголос у даній статті.

II Порядок розробки систем захисту інформації

Ближній розгляд послідовності процедури розробки системи захисту інформації на ОІД хоч і здійснюється під супроводом низки документів, але все одно вимагає деякого творчого початку. Загалом таку процедуру можна ілюструвати згідно з рис.1.

Перш за все зауважимо, що в наведеній послідовності етапи робіт базуються на документах, призначених для регламентування дій як на ОІД (без урахування наявності ІКС на об'єкті) так і в ІКС, хоча частина об'єктів може і не мати у своєму складі ІКС як таких, наприклад, виділені приміщення (ВП) для проведення конфіденційних переговорів. Такі приміщення можуть взагалі не мати у своєму складі будь-яких технічних засобів. Головними елементами техніки у ВП найчастіше є акустичні підсилювачі з гучномовцями (великі кімнати для нарад і конференцзали) або засоби відображення відеоінформації. В обох випадках про ІКС, у тому числі такі, котрі мають вихід за межі КЗ, мова не йде.

Загалом, з урахуванням визначених вище зауважень, картина щодо методологічного забезпечення та забезпечення з боку системи стандартизації виглядає незавершеною. Перегляд списку документації від НікС вказує на наголос у проектуванні КСЗІ на ІКС загального користування, користування з використанням мережі Internet, автоматизованих систем та комп'ютерних систем, що складають ІКС.

При таких умовах найважливішим етапом проектування систем захисту очевидно є початковий етап – отримання інформації від замовника та обстеження об'єкту з метою отримання даних про його уразливі місця, недоліки проведення котрого накладає відбиток на будь-який етап послідовності дій.

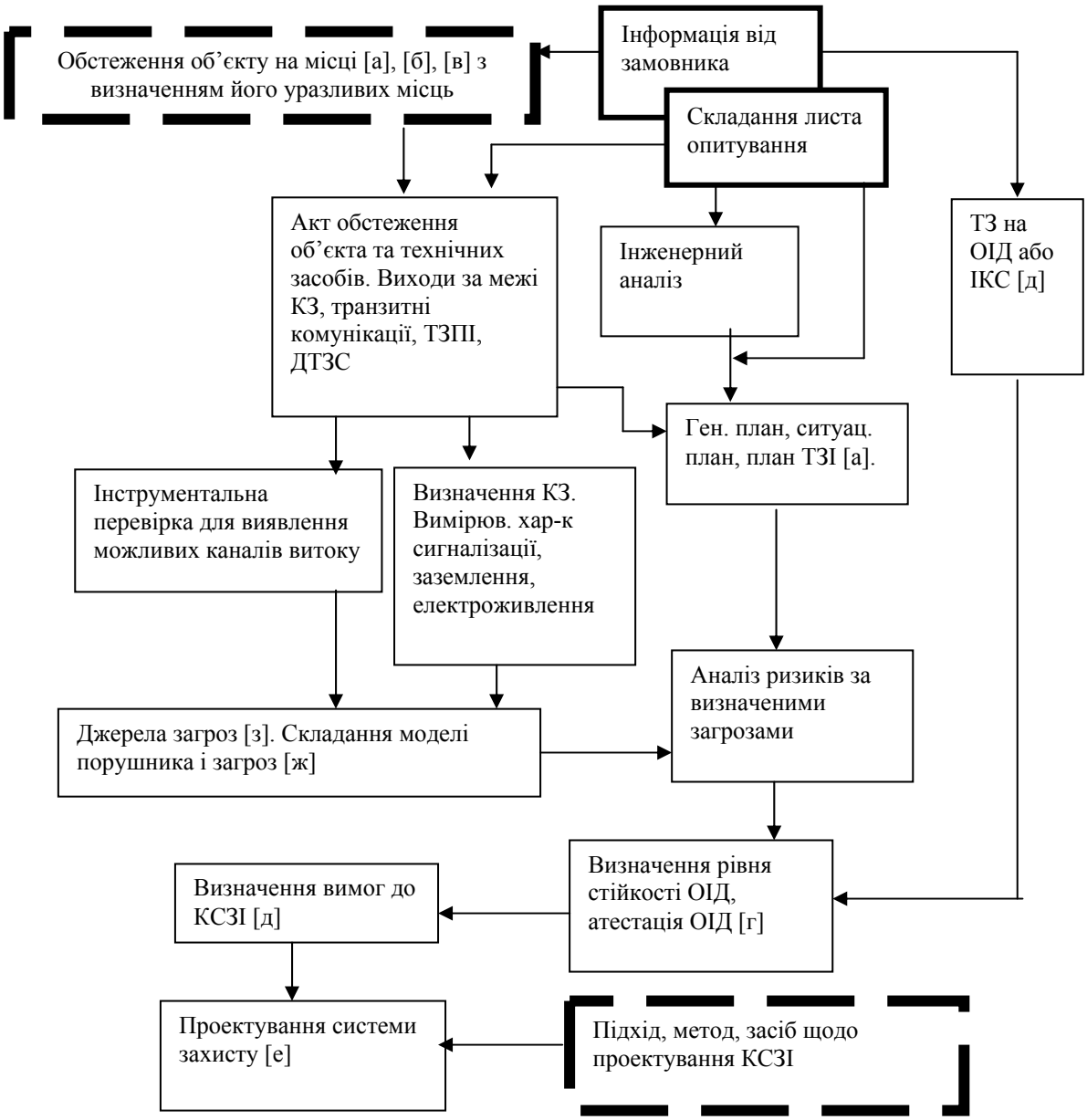
Відносно нечіткою процедурою на початковому етапі є отримання інформації від замовника (рис.1). Загалом складання листа опитування взагалі є не обов'язковою процедурою. Якщо лист опитування складається, тоді не зрозуміло, чи має він складатися з урахуванням інтересів виконання технічного завдання, котре на початку формує замовник, а надалі доповнює виконавець. Якщо такий лист надається виконавцю тільки для визначення приблизного об'єму та кошторису робіт, тоді він може звузити рамки об'єктивності інженерного аналізу і складання акту обстеження. Напрошується висновок про те, що формалізація (розробка єдиного підходу до процедури) складання листа опитування та введення його як складової в обстеження об'єкту на місці має забезпечити більшу визначеність, об'єктивність та уніфікацію щодо пошуку уразливих місць на об'єкті. Але тоді сама процедура обстеження та складання акту обстеження має також виконуватися за жорсткими правилами з єдиною метою – визначення уразливих місць не зважаючи на об'єми робіт та кошторис майбутнього проекту. Тільки за цих умов при подальшому порівнянні отриманих даних щодо уразливості об'єкту з ТЗ на систему захисту можна по-перше, визначити шляхи оптимізації майбутнього проекту захисту, а по-друге, визначитися з підходом, методом та засобом самого проектування КСЗІ. Тобто, впорядкований початковий етап розробки системи захисту прямим чином впливає на загальний результат робіт.

III Обстеження об'єкту

Загалом обстеження об'єкту на місці з визначенням його уразливих місць фактично здійснюється експертною оцінкою, в [3] при створенні комплексу захисту інформації (зазначимо, що це не є КСЗІ) – комісією.

Для невеликих об'єктів (ВП, серверне приміщення, комп'ютерна кімната, тощо) немає потреби в залученні великої кількості експертів. Зазвичай достатньо одного експерта з ТЗІ і представника від замовника. У цьому випадку особливих труднощів не виникає.

Для великих, складних об'єктів, що вміщують на одній території підрозділи різного функціонального призначення і складну структуру з засобами зовнішнього зв'язку та зовнішніми комунікаціями (електроживленням, транспортуванням, газовим, тепловим і водопостачанням), або ІКС загального користування та різними типами зв'язку (телефонні лінії, виділені лінії, супутниковий та сотовий зв'язок, підключенням до магістралей волокняно-оптичних каналів, тощо), виникає необхідність залучення експертів різних технологічних напрямків та спеціалістів-представників замовника разом з представниками адміністрації об'єкту. Якщо в перспективі мова піде про створення КСЗІ регіонально-територіального масштабу, в рамках району, міста, області, тощо, з залученням даних щодо інфраструктури об'єкту, структури його ІКС, тоді зазначена експертиза ще більше ускладнюється. Дані від експертів вміщують різне спрямування, – технічне, технологічне, економічне, психологічне, політичне, тощо. Складовими КСЗІ складних об'єктів є також комплекси, головними з яких можна визначити ті, що представлені на рис. 2.



а. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.

б. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.

в. НД ТЗІ 3.7-003-2005. Порядок проведення робіт із створення КСЗІ в інформаційно-телекомунікаційних системах.

г. НД ТЗІ 2.1-001-2001. Атестація об'єктів інформаційної діяльності.

д. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. З доповненням №1 за наказом ДСТСЗІ СБУ №37 від 18.06.02.

е. НД ТЗІ 1.6-003-04. Створення комплексів ТЗІ на ОІД. Правила розробки, побудови викладення та оформлення моделі загроз для інформації.

ж. НД ТЗІ 1.1-002, НД ТЗІ 1.4-001 та НД ТЗІ 1.6-003 (для ІКС).

з. ДСТУ 3396.0 -96. Захист інформації. Технічний захист інформації. Основні положення. Розд. 4.

ТЗПІ – технічні засоби перетворення інформації; ДТЗС – допоміжні технічні засоби та системи; ТЗ – технічне завдання.

Рисунок 1 – Процедура розробки системи захисту інформації на ОІД

Рисунок 2 – Складові КСЗІ

Навіть отримавши експертні оцінки для кожної складової у вигляді масиву даних, а в нашому випадку – з різними формами представлення, незрозуміло, яким чином підготувати їх до загального взаємопов'язаного виду, котрий дозволить визначити хоча б підхід до методики сукупної обробки таких даних. Тобто, такі елементи, як «Проектування системи захисту» та «Підхід, метод, засіб щодо проектування КСЗІ» (рис. 1. нижній рядок) залишаються невизначеними і наразі традиційні методи проведення та обробки результатів експертиз (як, наприклад, при проведенні аудиту безпеки) навряд чи є результативними. Подальше нарощування кількості ДСТУ, НД, методик, тимчасових рекомендацій, тощо, здатне тільки ускладнити ситуацію щодо їх сумісного використання.

Таким чином, діючі наразі та перспективні складні об'єкти, в плані оптимальності або дієздатності їх КСЗІ викликають сумнів.

Підхід до можливого розв'язання зазначеної проблеми може полягати у залученні радикально нового підходу, наприклад, у використанні інформаційних технологій, що базуються на використанні засобів інтелектуальної підтримки прийняття рішень. Очевидно, що користування засобами проектування, для котрих залучені технології інтелектуальної підтримки прийняття рішень, не може проводитись у ручному режимі, а вимагає розробки та залучення спеціалізованих автоматизованих систем проектування.

IV Використання методів моделювання з залученням засобів інтелектуальної підтримки прийняття рішень

Усе частіш з'являються роботи, в яких автори намагаються активізувати залучення інтелектуалізованих технологій моделювання складних процесів до напрямків проектування складних систем. Відомо підхід, що базується на еволюційній архітектурі системи захисту інформації [4]. Підхід базується на представленні методу створення опису об'єкту захисту та моделі управління подіями (поточна поведінка у загальній послідовності) у вигляді деякого образу. При цьому набір моделей можливих поведінок (бібліотека можливих образів поведінки) представлений також у вигляді образів поведінки. Образами можуть бути гістограми станів або у часовій послідовності, або у послідовності можливих станів, які можуть створюватися або одночасно, або в часовій послідовності. При такому підході створення методології проектування зводиться до створення формалізованих, тобто математичних інструментів, що забезпечують зв'язок між образами станів та образами поведінки.

Відомим є також підхід, при якому до розробки залучаються онтологічні моделі властивостей зрілості процесів захисту інформації [5], де, за визначенням авторів цього підходу, під зрілістю розуміють сукупність

спеціальних властивостей процесу захисту інформації, які обумовлюють та характеризують його здатність досягти запланованої мети та результатів відповідно до його призначення. Підхід дозволяє вирішити завдання стратегічного планування складних процесів і технологій при виключенні з результату проектування вербальності та інтуїтивності рішень, що отримуються. При цьому кінцевою метою є створення універсальної методології проектування, при якій процес захисту інформації здатний досягти запланованої мети та результатів відповідно виключно до його призначення.

Такі підходи мають свої переваги і недоліки і не є єдиними можливими напрямками вирішення проблеми, що обговорюється.

Як можливий підхід до створення системи автоматизованого проектування КСЗІ є використання асоціативної пам'яті (АП) на базі моделі нейроподібної ансамблевої сітки з навчанням. Завданням такої сітки є виконання функцій пам'яті з вибіркою за змістом запиту та подальшим прийняттям квазіоптимальних рішень, наприклад, за методологією, реалізованою у сітках Хопфілда [6]. Щодо принципової необхідності розробки нових підходів до проектування КСЗІ сумнівів немає [7], та відкритим є питання тактики використання автоматизованого проектування. Мається на увазі, що необхідно вирішити питання, – чи необхідно використовувати нейромоделі АП як загальну систему проектування КСЗІ від початкового етапу і до отримання проекту захисту, чи підхід, при якому АП використовується тільки на окремих етапах створення проекту КСЗІ, а ті етапи, що піддаються жорсткій алгоритмізації, можуть обслуговуватися традиційними методами. Наразі питання є відкритим. Але напрацювання з використанням сітьового моделювання на окремих етапах створює передумову до прогресивного розвитку нових напрямків при проектування КСЗІ на різних його етапах.

Рамки даної статті обмежуються розглядом початкового етапу проектування КСЗІ, метою якого є визначення уразливості об'єкту, що захищається. Оскільки вище визначено, що цей етап вимагає залучення методики експертної оцінки, отриманої від спеціалістів-експертів, логічним є підміна, повна або часткова, людей-експертів. Найпривабливішим здається підхід, коли статистичні дані щодо результатів аналізу уразливості діючих об'єктів (наприклад, у межах України) складають як базу даних (БД). Шляхом аналізу структури об'єктів, їх складу, призначення, умов існування (далі параметрів), формується бібліотека вхідних для БД (вхідна БД) образів об'єктів. Таким чином, визначений набір параметрів відповідає декотрому образу об'єкту. Параметри заповнюють вхідну БД у вигляді кінцевого набору з n1 текстів (слів, фраз, словосполучень). Такий кінцевий набір має регламентуватися документом ТЗІ. Складність у тому, щоб створити такий набір (фактично, набір параметрів), котрий задовольняє опису образу будь-якого об'єкту. Принципових проблем при цьому не має виникнути, якщо створювати БД достатнього розміру.

Далі, для кожного вхідного образу об'єкту (вхідної БД), визначається образ захищеності у вихідній БД, аналогічно складений (також у текстовій формі) у вигляді списку вразливостей розміром n2. Цей текстовий набір і формує вихідну БД. Так формується структура послідовності дій, подібна до персептронної, де присутні рецептори як вхідні збудники (параметри образу об'єкту), та ефектори (як вихідний перелік уразливостей) (рис. 3.).

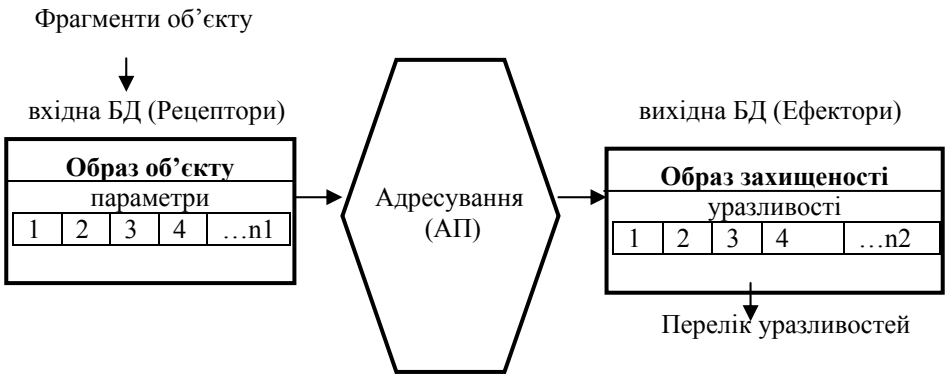


Рисунок 3 – Структура адресування даних від вхідної до вихідної БД

Після заповнення обох баз даних, аналогічно тому, як робить АП у вигляді моделі персептрона або нейроподібної сітки, при складанні опису фрагментів нового, «незнайомого» об'єкту та пред'явленні цих фрагментів до вхідної БД, з неї вилучається вже занесений до вхідної БД відповідний (найбільш близький за змістом) перелік фрагментів «образу об'єкту». Цей образ є вибіркою адресування до вихідної БД, за якою з вихідної БД вилучається образ захищеності у вигляді переліку вразливостей. На цьому етапі завдання

полягає в тому, щоб реалізувати адресування від вхідної БД до вихідної за асоціативним принципом, тобто за змістом запиту, а не за числовою адресою осередку пам'яті. Таким чином, можна реалізувати методику роботи АП. Тут і може допомогти визначена вище умова скінченності списку параметрів, а в результаті і образів об'єкту. При цьому, перелік уразливостей також має бути скінченним, хоча його розмір n2 може бути довільним і складатися з комбінації образів об'єкту. В термінології персептронів та нейроподібних сіток функціонально заповнення обох БД є аналогом процесу навчання. Формування переліку вразливостей при «пред'явленні» «незнайомого» об'єкту є аналогом процедури впізнавання.

Використання такої системи дозволяє вилучити з процедури визначення вразливостей об'єкту людський фактор. Експерт-людина залишається тільки на етапі збору даних про об'єкт і призначений для складання (бажано якнайбільш об'єктивних) даних, що описують його за фрагментами: властивості інформації що циркулюють на об'єкті, опис поверхового плану, структуру системи заземлення та електроживлення, опис прилеглої території, тощо [2].

Звісно, рис. 3. ілюструє не структуру АП, а лише сенс алгоритму процедури користування БД як АП.

Існує декілька алгоритмів навчання. Наприклад, закон навчання Кохонена, алгоритм Гросберга, просторово-часове навчання Коско-Клопфа та ін. Але інтуїтивно намагання вилучити обмеження щодо скінченності списку параметрів та уразливостей є природним. Якщо формувати не персептронну структуру, де таке обмеження є обов'язковим, а використати парадигму нейросітьового моделювання (наприклад, за рахунок Хопфілдовських сіток [6] з так званою ансамблевою структурою образів [8]), тоді можна формувати сітки з необмеженою кількістю образів (обмеженням є тільки розмір фізичної пам'яті, яка використовується для зберігання величини вагових коефіцієнтів зв'язку між нейроподібними елементами). Якщо ж залучити ці сітки з доповненням системою підсилення-гальмування [9], запропонованою академіком Амосовим Н. М. [10], то реалізується тактика «забування», згідно з якою накопичення усе більшої кількості нових пред'явлень об'єктів для навчання до БД трансформує БД та взагалі АП так, що старі образи, тобто такі, що зустрічаються усе рідше, поступово зникають. Процедурно це виглядає як повільне зменшення ваги зв'язків між вхідною та вихідною БД для окремих комбінацій параметрів об'єкту (образів об'єкту). Сітки (система проектування) набуває властивості поступової автоматичної адаптації до нових видів об'єктів, нових умов їх існування, нових видів уразливостей. Тобто в процесі життєдіяльності такий автоматизований проектант залишається відкритим до подальшого «донавчання», тобто розвитку. Він «пам'ятає» історію великої кількості діючих об'єктів і доповнюється властивостями нових об'єктів, котрі він проектує.

V Висновки

Процес розвитку технології проектування КСЗІ поступово набуває властивості «переповнення», при якому подальший розвиток цього напрямку вимагає нових підходів, з вищим рівнем технологічності. Практично, такі підходи існують, але обслуговують технологічні напрямки, не пов'язані з напрямком захисту інформації. Однак факт наявності таких високотехнологічних підходів дозволяє оптимістично дивитися в майбутнє напрямку ТЗІ і не створює ситуації глухого кута. Розвиток напрямку проектування КСЗІ можна характеризувати як такий, що вимагає розвитку і вдосконалення за рахунок залучення відомих технологій і не вимагає радикального перегляду в підході до загальної методології КСЗІ.

*Література: **1**. ДСТУ ISO/IEC TR 13335:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 1: Концепції та моделі безпеки інформаційних технологій. Частина 2: Керування та планування безпеки інформаційних технологій. Частина 3: Методи керування безпекою інформаційних технологій. **2**. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт. **3**. НД ТЗІ 3.1-001-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Перед проектні роботи. **4**. Ayaz Isazadeh. Behavioral Views for Software Requirements Engineering. A thesis submitted to the Department of Computing and Information Science in conformity with the requirements for the degree of Doctor of Philosophy Queen's University Kingston, Ontario, Canada, September 1996. (Досяжні в Інтернет www.sciencedirect.com). **5**. Потій О. В. Онтологічні моделі властивостей зрілості процесів захисту інформації.// Харьков. Прикладная радиоэлектроника. ISSN 1727-1290. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. 2009 г., т. 8, № 3, с. 388-395. **6**. Hopfield J. J., Tank D.W. Neural Computation of Decisions in Optimization Problems.// Biological Cybernetics – 1985. – 52, No. 3. – p. 141–152. **7**. Луценко В. М. Системи інтелектуальної підтримки прийняття рішень при проектуванні комплексних систем захисту інформації. Наук. вісті. НТУУ «КПІ». № 5, 2010, с. 68–74. **8**. D. O. Hebb. The Organization of Behavior. John Wiley, New York, 1949, 323 p. **9**. Куссуль Э. М., Федосеева Т. В. О распознавании звуковых сигналов в нейроподобных ансамблевых структурах. Киев: 1989. 21 с. – Препр./ АН УССР Ин-т киберн. им. В. М. Глушкова, 87–28. **10**. Амосов Н. М.,*

Касаткин А. М., Касаткина Л. М., Талаев С. А. Автоматы и разумное поведение. –Киев: Наук думка, 1973. – 370 с.

УДК 681.3.06:519.248.681

ТЕСТ НА ПРОФІЛЬ ЛІНІЙНОЇ СКЛАДНОСТІ

Людмила Завадська, Максим Семибаламут
ФТІ НТУУ «КПІ»

Анотація: **Наведено новий тест для оцінки якості випадкових послідовностей, який базується на профілі лінійної складності. Тест оперує кількістю стрибків лінійної складності і працює у певних випадках значно ефективніше за відповідний тест з набору NIST.**
Summary: **A new randomness test, based on linear complexity profile is proposed. It takes into account the number of linear complexity jumps and shows in some cases much better results than the NIST linear complexity test does.**
Ключові слова: **Криптографія, випадкові послідовності, тести оцінки якості, лінійна складність, профіль лінійної складності.**

I Вступ

Задача оцінки якості випадкових та псевдовипадкових послідовностей посідає важливе місце у сучасній теоретичній та прикладній криптографії. Висока якість вихідної послідовності є необхідною умовою стійкості потокових систем шифрування; якісні випадкові послідовності потрібні для генерування ключів і різноманітних випадкових параметрів симетричних та асиметричних криптосистем тощо.

Під якісною бінарною послідовністю розуміють послідовність бітів, близьку за своїми характеристиками до чисто випадкової послідовності – послідовності незалежних бітів з рівними ймовірностями 0 та 1. Існують набори тестів для оцінки якості послідовностей, найвідомішим серед яких є набір статистичних тестів NIST (National Institute of Standards and Technology) [1]. Проте задача побудови нових, більш ефективних критеріїв для виявлення відхилень від випадковості залишається актуальною.

Важливою характеристикою бінарної випадкової послідовності є лінійна складність – довжина найкоротшого регістра зсуву з лінійним зворотним зв'язком, що може згенерувати дану послідовність. Однак високої лінійної складності ще недостатньо для того, аби послідовність була якісною з точки зору випадковості. Вона, наприклад, може бути звичайною рекурентою, до якої в кінці додано коротку послідовність випадкових бітів, і попри все це мати високу лінійну складність. Зокрема набір тестів NIST містить і тест на лінійну складність, який не враховує усіх нюансів її поведінки і тому пропускає певні типи неякісних послідовностей. Вхідна послідовність розбивається на відносно короткі відрізки, для кожного з яких за допомогою алгоритму Берлекемпа-Мессі [2, 3] підраховується значення лінійної складності без урахування специфіки її зміни на цьому відрізку. Отримані значення перевіряються за χ^2-критерієм на відповідність певному розподілу. У даній статті пропонується побудова та обґрунтування нового тесту, який враховує кількість стрибків лінійної складності на відрізках, і у певних випадках працює краще за тест на лінійну складність з набору NIST.

Під час роботи над матеріалом авторами було виявлено в Інтернеті анонс роботи [4]. На жаль, в нас немає доступу до тексту статті, тому нам невідомо, яку статистику використовували її автори. Можна лише констатувати, що тест LP було розроблено незалежно від [4].

II LP-тест

Профіль лінійної складності випадкової послідовності являє собою графік зміни лінійної складності L_n залежно від довжини послідовності n. Для чисто випадкової послідовності профіль стрибкоподібно зростає, коливаючись певним чином навколо прямої

$$L_n = n/2, \tag{1}$$

причому великі стрибки L_n малоймовірні внаслідок обмеженості дисперсії лінійної складності [5]. На рисунку 1, запозиченому з [5], зображено типовий вид профілю лінійної складності якісної випадкової, а також лінійної рекурентної послідовностей. Якщо в послідовності присутні достатньо довгі відрізки лінійної рекуренти, які чергуються з відрізками якісної послідовності, або лінійна рекурента зрідка спотворюється, це має призводити до великих стрибків профілю лінійної складності. В свою чергу, наявність великих стрибків лінійної складності спричиняє зменшення їх кількості. Тож авторами пропонується як основну