prediction // Complexity 9(2) (ISSN: 1076-2787): 15-18 (2003). 3. Грушо А. А., Тімоніна Є. Є. Теоретичні основи захисту інформації. – М.: Видавництво Агентства "Яхтсмен", 1996. – 192 с. 4. Новіков О., Тимошенко А. Побудова логіко-ймовірнісної моделі захищеної комп'ютерної системи // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2001. – Вип. 3. – С. 101–105. 5. Новіков О. М., Родіонов А. М. Логіко-імовірнісна модель захищеності компонентів інформаційно-комунікаційних систем // Інформаційні технології та комп'ютерна інженерія. – 2008. – № 1(11). – С. 170–175. 6. Яциковська У. О. Модель захищеної архітектури клієнт-сервер [Текст] / У. О.°Яциковська, І. В. Васильцов, М. П. Карпінський // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2010. – № 9 (151). – С. 74–79. 7. Яциковська У. О. Дослідження реалізації розподілених атак в комп'ютерній мережі [Текст] / У. О. Яциковська, І. В. Васильцов, М. П. Карпінський // Сучасна спеціальна техніка. – 2011. – № 2 (25). – С. 124–127. 8. Яциковська У. О. Моделювання мережного трафіка комп'ютерної мережі під час реалізації атак типу DoS/DDoS [Текст] / У. О. Яциковська, М. П. Карпінський // Інформаційна безпека. – 2011. – № 1 (5). – С. 142–145.

УДК 004.056.5:004.7

В. О. Кононова, О. В. Харкянен, С. В. Грибков
Національний університет харчових технологій,
кафедра інформаційних систем

ОЦІНКА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Розглянуто особливості захисту інформаційних ресурсів у корпоративних мережах та системах, а також описано підхід щодо їх оцінки. Розглянутий підхід щодо оцінки засобів захисту дає змогу знизити витрати на їх впровадження, він легко адаптується до конкретних потреб будь-якої організації з урахуванням специфіки її діяльності та бізнесу. Такий підхід дозволяє точніше описувати інформаційні ресурси через характерні для них вразливості, вартість самих ресурсів, а також ранжувати ризики та відповідно інформаційні ресурси за ступенем критичності для діяльності організації.

Ключові слова: захист інформації, оцінка захисту, інформаційний ресурс, комп'ютерна мережа, інформаційна безпека.

ASSESSING PROTECTION MEANS OF INFORMATION RESOURCES

The paper considers specifics of information resources protection in corporate networks and systems. An approach to assessing protection means is described which allows to reduce their deployment cost and adapts easily to specific needs of any organization with an allowance for specifics of its activities and business. Such an approach makes it possible to describe information resources more precisely through their characteristic vulnerabilities and resources cost. It also helps to rank the risks and information resources according to their criticality for organization activities.

Key words: information protection, protection assessment, information resource, computer network, information security.

Вступ

Сучасна організація режиму інформаційної безпеки стає критично важливим стратегічним чинником розвитку будь-якої вітчизняної компанії. При цьому, як правило, основну увагу звертають на вимоги і рекомендації нормативно-методичної бази в галузі захисту інформації. Разом

з тим, багато провідних вітчизняних компаній сьогодні використовують деякі додаткові засоби, спрямовані на забезпечення стійкості та стабільності функціонування корпоративних інформаційних систем для підтримки своїх бізнес-процесів. Ціль захисту будь-якого інформаційного ресурсу зрозуміла кожному, а реалізація захисту потребує серйозних ресурсів. Проте що більші вимоги ставлять до системи захисту інформації, то важча і складніша реалізація поставленої задачі. Сьогодні захист кожного окремого елемента втрачає значущість, а постає проблема створення комплексу надійного захисту всієї інформаційної інфраструктури компанії. Під час реалізації системи захисту необхідно враховувати не тільки властивості кожного окремого елемента, а й їх взаємодію, що зумовлює наявність специфічних властивостей, що притаманні саме пов'язаним між собою елементам.

Все частіше в інформаційних джерелах використовують поняття "системний підхід" під час побудови системи захисту інформації. Поняття системності полягає не просто у створенні відповідних механізмів захисту, а являє собою регулярний процес, що здійснюється на усіх етапах життєвого циклу інформаційної системи. Всі засоби, методи і заходи, що використовуються для захисту інформації, об'єднуються в єдиний, цілісний механізм – систему захисту. На жаль, необхідність системного підходу до питань забезпечення безпеки інформаційних технологій поки що належно не усвідомили користувачі сучасних інформаційних систем [1].

Фахівці з різноманітних галузей знань, так чи інакше, змушені займатися питаннями забезпечення інформаційної безпеки. Особливо гостро ця проблема постає в організаціях, де користувачі мають різні права та розподілений доступ до різноманітних інформаційних ресурсів. Завдання системних адміністраторів – захист усіх інформаційних ресурсів компанії від несанкціонованого доступу. Для ресурсів забезпечення надійного захисту сьогодні й на найближче майбутнє у системі інформаційної безпеки повинні бути реалізовані сучасні прогресивні й перспективні технології інформаційної безпеки. На сучасному ринку інформаційних технологій представлено багато різних систем захисту різноманітної складності та структури. Основна проблема полягає у виборі системи захисту для конкретної задачі, а тому необхідно коректно та правильно оцінювати системи захисту: ті що експлуатуються, та ті, що бажають впровадити.

Аналіз досліджень та публікацій

Оцінкою інформаційної безпеки займаються з початку появи інформаційних технологій. З цієї тематики є багато праць, але найбільш актуальними та фундаментальними працями є нормативні документи, що зробили вагомий теоретичний та практичний внесок у розв'язання задач забезпечення інформаційної безпеки, а саме: "Помаранчева книга" [2], у якій викладені та систематизовані критерії оцінки захисту комп'ютерних систем; Європейські критерії оцінки безпеки інформаційних технологій [3], що врахували усі недоліки та обмеження, викладені у "Помаранчевій книзі"; Канадські критерії оцінки безпеки надійності комп'ютерних систем [4]; Федеральні критерії США [5], розроблені на замовлення уряду США і спрямовані на усунення обмежень, незручностей практичного застосування і недоліків "Помаранчевої книги"; Міжнародний стандарт ISO/IEC 15408 – "Критерії оцінки безпеки інформаційних технологій" [6–8]; Стандарт CEM-97/017 – "Загальна методологія оцінки безпеки інформаційних технологій" [9]. Окремо необхідно відзначити публікацію [10], в якій розглянуто використання коефіцієнта емерджентності для визначення рівня захисту інформаційних потоків для певного класу архітектури комп'ютерної мережі.

Розглянуті нормативні документи є основою єдиної міжнародної науково-методологічної бази вирішення проблем забезпечення інформаційної безпеки в інформаційних ресурсах, системах та технологіях. Для вирішення завдань досягнення інформаційної безпеки, поряд з формальними методами моделювання процесів та оцінки ефективності функціонування систем, необхідно використовувати методи декомпозиції та структуризації компонентів систем і процесів, неформальні методи оцінки ефективності функціонування та прийняття рішень.

Формулювання цілі статті

Використання сучасних систем інформаційної безпеки вимагає, з одного боку, відстеження швидких змін в інформаційних технологіях і загрозах, що з'являються, а з іншого боку – врахування реальних характеристик апаратного й програмного забезпечення корпоративних мереж і систем. Процедура придбання пристроїв інформаційної безпеки нескладна. Істотно складнішим є вирішення проблеми – як захищати і які засоби безпеки застосовувати з урахуванням мінімізації витрат. Упроваджуючи різні засоби захисту, необхідно визначити баланс між можливим збитком від несанкціонованого витоку інформації та розміром вкладень, які витрачені для забезпечення захищеності інформаційних ресурсів. Щоб підвищити ефективність захисту інформаційних ресурсів, необхідно дослідити підходи щодо оцінки рівня їх захисту та систем захисту. Така оцінка для кожного окремого випадку є індивідуальною та залежить від багатьох факторів (вартість інформації, статусу організації, важливості інформації, рівня апаратного та програмного забезпечення тощо).

Особливості захисту інформаційних ресурсів у корпоративних мережах

Захист інформаційних ресурсів корпорації залежить від рівня програмних та апаратних засобів, що використовуються. Упроваджуючи інформаційні системи, кожна організація очікує максимально корисної функціональності для підтримки її бізнес-процесів. Захист даних в інформаційних системах будується заради захисту важливої інформації, втрата чи пошкодження якої призведе до значних грошових втрат. Забезпечення захисту вимагає використання сучасних апаратних та програмних засобів для захисту інформаційних ресурсів компанії, що повинно забезпечувати цілісність, доступність та певний режим доступу до кожного з ресурсів. Цілісність передбачає незмінність інформації у будь-який час від моменту її створення, тобто вона повинна бути достовірною та містити сенс, що заклав її власник. Інформаційний ресурс зберігає цілісність за умов дотримання прав доступу до нього.

Існування інформаційного ресурсу неможливе в автономному режимі без віддаленого доступу до нього, тому доступність інформації зумовлена нормальною взаємодією між її носієм та користувачем. Інформація зберігає доступність, якщо не втрачається взаємодія між носієм та користувачем інформації. Встановлення розподіленого режиму доступу забезпечує конфіденційність інформації на певному ресурсу. Конфіденційність розуміють як недоступність інформації для користувачів, яким не надана можливість її використання. Конфіденційність інформації зберігається, якщо дотримується режимна адекватність під час ознайомлення з нею.

Говорячи про інформаційні ресурси, необхідно зазначити, що їх функціонування неможливе без корпоративних мереж, тому доцільно висвітлити деякі їхні особливості. Корпоративна мережа, як правило, є територіально розподіленою, тобто об'єднує офіси, підрозділи та інші структури, значно віддалені один від одного. Часто вузли корпоративної мережі виявляються розташованими в різних містах, а іноді й країнах. Принципи, за якими будується така мережа, доволі сильно відрізняються від тих, що використовуються під час створення локальної мережі, навіть якщо вона охоплює декілька будівель. Відповідно зростає складність системи захисту.

Одним з принципів, покладених в основу створення мережі, є максимальне використання типових рішень, стандартних уніфікованих компонентів. Конкретизуючи цей принцип стосовно до прикладного програмного забезпечення, можна виділити універсальні сервіси, які доцільно зробити базовими компонентами захисту.

Діяльність будь-якої сучасної організації багато в чому залежить від мережі Internet і тих сервісів, які вона надає, тому питання про доцільність використання Internet виникає дуже рідко. Водночас дуже гостро ставиться питання про можливість використання всіх привілеїв та переваг, що надає мережа Internet, з мінімальним ризиком для діяльності організації. Тому сьогодні на перший план виходить проблема забезпечення безпеки в комп'ютерних інформаційних систем з боку мережевого впливу [1]. Цей сегмент удосконалюється і постійно розвивається, причому дуже динамічно.

Основними засобами захисту комп'ютерних інформаційних систем були, є і залишаються мережеві екрани (брандмауер, firewall, фільтрувальні маршрутизатори тощо). Мережеві екрани є лише інструментом системи безпеки. Вони надають певний рівень захисту і є засобом реалізації політики безпеки на мережевому рівні. Рівень безпеки, що надає мережевий екран, може варіюватися залежно від вимог безпеки. Існує традиційний компроміс між безпекою, простотою використання, вартістю, складністю тощо. Мережевий екран є одним з декількох механізмів, що використовують для управління і спостереження за доступом до мережі з метою її захисту [11].

Сьогодні ніхто не заперечуватиме важливості системи антивірусної безпеки в інформаційній інфраструктурі будь-якої організації – це здебільшого найактуальніша система зі всього ряду розгорнутих систем забезпечення інформаційної безпеки. Звичайно, така ситуація виникла не сама по собі, а зумовлена передусім обвальним зростанням кількості нових комп'ютерних вірусів.

Поширення глобальних мереж передавання даних надає можливість об'єднувати територіально віддалені локальні мережі організацій для створення так званих приватних віртуальних мереж (VPN). Глобальні мережі в цьому випадку виступають як транспортний компонент, що об'єднує локальні мережі в єдину інформаційно-обчислювальну систему. Створення віртуальних мереж зумовило стрімке зростання глобальних мереж, однак для їх об'єднання використовуються виділені канали передавання даних, що призвело до: високої вартості оренди виділених каналів зв'язку; жорсткої прив'язки до розташування. Наприклад, у разі переїзду офісу одного з відділів організації з розгорнутим сегментом локальної мережі, що пов'язаний виділеним каналом із загальною мережею організації, виникають додаткові проблеми з подальшим під'єднанням локальної та загальної мережі.

Для вирішення проблеми передавання інформації через відкриті канали Інтернету використовують VPN рішення. VPN – це об'єднання декількох локальних мереж, підключених до мережі загального призначення, в єдину віртуальну (логічно виділену) мережу. VPN кошти організовують захищений тунель між двома точками засобами криптографії, надаючи широкі можливості з виборів алгоритмів аутентифікації, шифрування та перевірки цілісності потоку даних [12].

Оцінки рівня захисту інформаційних ресурсів

Як правило, для оцінки рівня захисту необхідно спочатку визначити поточний стан інформаційної безпеки. Сьогодні існують два підходи щодо оцінки поточного стану інформаційної безпеки, а саме "дослідження знизу догори " та "дослідження згори донизу".

Використання першого підходу полягає у тому, що адміністратори починають перевіряти систему захисту на усі відомі їм види атак. Отже, адміністратори виступають в ролі зловмисників, які роблять спроби порушити захист інформаційного ресурсу. Але відразу стає зрозуміло, що найталановитіші адміністратори не можуть знати усі можливі методи злому, а також усі програмно-апаратні засоби зловмисників.

Підхід "згори донизу" ґрунтується на детальному аналізі усіх відомих схем зберігання та обробки даних. Спочатку визначають інформаційні об'єкти та потоки захисту, а потім досліджують сучасний стан систем інформаційного захисту з метою визначення реалізованих методик захисту інформаційних ресурсів, а також їх стан та рівень. Далі проводиться класифікація всіх інформаційних об'єктів за класами відповідно до їх конфіденційності, вимог до доступності та цілісності.

Останнім кроком є "оцінка ризику" що полягає у визначенні розміру збитків фірми через порушення захисту кожного конкретного інформаційного ресурсу. Наближеним ризиком називається добуток "можливого збитку від атаки" на "ймовірність цієї атаки". Як правило, оцінка ризику складається з аналізу ризиків та оцінювання збитку.

Під час аналізу ризиків проводиться інвентаризація та впорядкування інформаційних ресурсів, з'ясовуються нормативні, технічні, договірні вимоги до ресурсів у сфері інформаційної безпеки, після чого з урахуванням цих вимог визначають вартість ресурсів. У вартість входять усі потенційні витрати, пов'язані з можливим несанкціонованим доступом до інформаційних ресурсів,

що захищаються. Наступним етапом аналізу ризиків є складання переліку переважних загроз та перелік вразливостей до них кожного інформаційного ресурсу, а потім обчислюється ймовірність реалізації можливих загроз чи атак. За стандартом [13] загрози інформаційної безпеки мають подвійне тлумачення, а саме: умова реалізації вразливості ресурсу (в цьому випадку вразливості та погрози ідентифікуються окремо); загальна потенційна подія, здатна призвести до несанкціонованого доступу до інформаційного ресурсу (коли наявність можливості реалізації вразливості і є загрозою).

Оцінюють ризик, обчислюючи його й зіставляючи із заданою шкалою. Величину ризику обчислюють множенням ймовірності виникнення несанкціонованого доступу до інформації чи ресурсу на значення збитку компанії від цього. Встановлене значення ризику дає змогу визначити важливість для компанії кожного інформаційного ресурсу.

Усі сучасні стандарти в сфері безпеки відображають сформований у міжнародній практиці загальний підхід до організації управління ризиками. Управління ризиками розглядається як базова частина системи менеджменту якості організації. Стандарти мають відверто концептуальний характер, що дозволяє експертам з інформаційної безпеки реалізувати будь-які методи, засоби і технології оцінки, відпрацювання та управління ризиками. В різних стандартах допускається використання кількісних та якісних методів оцінки ризику інформаційної безпеки, але немає обґрунтування та рекомендацій щодо вибору математичного та методологічного апарату. У додатку до стандарту [13] наводиться приклад якісного методу оцінювання, а саме використання три- та п’ятибальної оцінних шкал. За п’ятибальною шкалою рівні вартості ідентифікованого ресурсу оцінюють як: “незначний”, “низький”, “середній”, “високий”, “дуже високий”. За трибальною шкалою – як “низький”, “середній”, “високий”.

Загальні критерії оцінки безпеки повинні застосовуватись на єдиній загальній методологічній основі, що ґрунтується на синтезі заходів, засобів та сервісів безпеки для мінімізації інформаційних ризиків. Використовують загальну методологію оцінки інформаційної безпеки експерти, розробники та замовники для оцінки й контролю інформаційної безпеки ресурсів [9].

З погляду розробника профілю захисту застосування загальної методології дає змогу виконати його незалежну і послідовну оцінку та обґрунтування.

Розробникові застосування загальної методології дасть змогу:

- незалежно обґрунтувати та перевірити задокументовані у профілі та проекті показники захисту безпеки кожного інформаційного ресурсу;
- переконати споживача у тому, що об’єкт оцінки відповідає необхідним показникам безпеки;
- ефективно використати отримані під час оцінки інших продуктів і систем результати для побудови систем безпеки;
- зменшити витрати часових та матеріальних ресурсів у процесі оцінки безпеки системи.

За загальною методологією оцінки інформаційної безпеки вона повинна здійснюватися за три етапи: підготовчий, основний, заключний.

На підготовчому етапі основними дійовими особами є замовник оцінки та експерт. Замовник інформує всі сторони щодо необхідності оцінки профілю захисту або об’єкта оцінки, забезпечує експерта необхідною документацією, матеріалами за профілем захисту й об’єкта оцінки. Завдання експерта – визначити можливість успішного здійснення оцінки на основі отриманих матеріалів, а за необхідності вимагати додаткових матеріалів у замовника або розробника. Підсумком підготовчого етапу є укладання між замовником і експертом угоди на виконання робіт з оцінки об’єкта або профілю захисту.

Результатом основного етапу є розроблення та надання експертом технічного звіту оцінки, що містить обґрунтування прийнятого рішення. На основному етапі експерт досліджує подані йому матеріали, профіль захисту або об’єкт оцінки. Експерт складає цілу низку звітів з вимогами надання пояснень за вимогами органу контролю, виявленими недоліками та іншою інформацією про хід оцінки. Контролюючий орган здійснює безперервний моніторинг процесу оцінки відповідно до схеми оцінки.

На заключному етапі здійснюється всебічний аналіз технічного звіту оцінки органом контролю на предмет його відповідності загальним критеріям загальної методології та вимогам схем оцінки безпеки. На основі технічного звіту формується підсумковий звіт з оцінювання з рішенням про відповідність необхідним вимогам. Усі залучені в процес оцінювання сторони вивчають підсумковий звіт та мають право вимагати відповідних пояснень.

Більшість організацій з різних причин не мають можливості здійснити повну оцінку захисту інформаційних ресурсів, тому пропонується використовувати кількісну оцінку рівня захищеності. Її використання можливе на стадії впровадження. У результаті застосування кількісної оцінки є можливість точніше порівняти декілька варіантів захисту, що дає змогу вибрати найефективніший. Для її застосування визначають ймовірність виникнення загроз та вразливості інформаційних ресурсів, вартість ресурсів, що захищаються (оцінка втрати в разі виходу з ладу інформаційного ресурсу) та частоту загроз кожного виду в загальному потоці загроз. Обов'язковим є визначення обмежень на вартість системи захисту інформації та зниження рівня продуктивності системи.

Для здійснення оцінки захищеності пропонується виконати наведені нижче кроки:

- на першому кроці складають список загроз з позиції забезпечення інформаційної безпеки, визначають ймовірності виникнення загроз та ймовірності їх відображення системою захисту, вартість інформаційних ресурсів;
- на другому кроці вводять обмеження на вартість системи захисту інформації та на зниження рівня продуктивності комп'ютерної інформаційної системи;
- на третьому кроці проводиться оцінка за математичними формулами загального рівня захисту комп'ютерної інформаційної системи вибраними засобами;
- на четвертому кроці з розглянутих та оцінених варіантів вибирають той, що максимально відповідає вимогам і не виходить за задані обмеження.

Фактично рівень захисту визначається як відношення ризиків у захищеній системі до ризиків у незахищеній системі. Такий підхід дає змогу точніше описувати інформаційні ресурси через характерні для них вразливості, вартість самих ресурсів, ранжувати ризики та відповідно інформаційні ресурси за ступенем критичності для діяльності організації.

Висновок

Розглянутий підхід щодо оцінки рівня захищеності інформаційних ресурсів можна застосувати на усіх етапах проектування та супроводження інформаційних систем організацій будь-якої сфери діяльності. Застосовуючи його, інформаційну систему чи мережу розглядають з погляду можливої вразливості її засобів безпеки, а також відбувається адаптація підходу під конкретні потреби організації з урахуванням специфіки її функціонування та ведення бізнесу. Точність результату залежить передусім від повноти списку загроз і уражень як основних складових ризику, точності оцінки інформаційних ресурсів, а також точності оцінки ймовірнісних характеристик реалізації загроз. Перевагами такого підходу є нескладна реалізація, поширений математичний апарат, доступність для розуміння. Як недоліки можна зазначити, що цей підхід не забезпечує врахування особливостей функціональної взаємодії засобів захисту.

Застосування розглянутого підходу щодо оцінки захисту інформаційних ресурсів зменшить витрати організації та забезпечить вибір найкращого засобу захисту.

1 Форристал Д. Защита от хакеров WEB-приложений. – ДМК. 2004. – 496 с. 2. Trusted Computer Systems Evaluation criteria, US DoD 5200.28-STD, 1985. 3. Information Tecnhology Security Evaluation Criteria, v. 1.2. – Office for Official ublications of the European Communities, 1991. 4. Canadian Tusted Computer Product Evaluation Criteria, v. 3.0. Canadian System Security Centre, Communications Security Establishment, Government of Canada, 1993. 5. Federal Criteria for Information Technology security. – NIST, NSA, US Government, 1993. 6. ISO/IEC 15408-1:1999 – Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model. 7. ISO/IEC 15408-2:1999 – Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements. 8. ISO/IEC 15408-3:1999 – Information

technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements. 9. CEM-97/017. Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model. 10. Якименко І. З. Критерії оцінки рівня захисту комп'ютерних мереж з врахуванням їх архітектури // Інформатика та математичні методи в моделюванні, 2013. – Т. 3 – №1 – С. 82–90. 11. Защита сетевого периметра: наиболее полное руководство по брандмауэрам, виртуальным частным сетям, маршрутизаторам и системам обнаружения вторжений [Текст] / С. Норткатт [и др.]; науч. ред. Н. И. Алишов. – К.; М.; СПб.: DiaSoft, 2004. – 664 с. 12. Петров А. А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. – 445 с. 13. ISO/IEC 15408-2:1999 – Information technology – Security techniques – Code of practice for information security management.

УДК 621.319.5+004.3

Ю. М. Костів[1], В. М. Максимович[1], О. І. Гарасимчук[2], М. М. Мандрона[1,3]
Національний університет "Львівська політехніка",
[1]кафедра безпеки інформаційних технологій,
[2]кафедра захисту інформації;
Львівський державний університет безпеки життєдіяльності,
[3]кафедра управління інформаційною безпекою

ФОРМУВАННЯ ПУАССОНІВСЬКОЇ ІМПУЛЬСНОЇ ПОСЛІДОВНОСТІ НА ОСНОВІ ГЕНЕРАТОРА ГОЛЛМАННА

Показано можливість формування пуассонівської імпульсної послідовності на основі псевдовипадкової бітової послідовності. Для формування останньої використано генератор Голлманна. Якість бітової послідовності досліджували за допомогою статистичних тестів NIST. Для оцінки якості пуассонівської послідовності використано методику, що ґрунтується на критерії Пірсона.

Ключові слова: псевдовипадкові імпульсні послідовності, генератори псевдовипадкових чисел, статистичні характеристики, критерій Пірсона.

FORMING OF POISSON PULSE SEQUENCE BASED ON GOLLMAN GENERATOR

The possibility of forming Poisson pulse sequence on the base of pseudorandom bit sequence is shown. Gollman generator is used for forming the last of these sequences. Estimation of bit sequence quality was conducted with the help of NIST statistic tests. For estimation of Poisson sequence quality the methodology that based on Pearson criterion is used.

Key words: pseudorandom pulse sequences, pseudorandom number generators, statistic characteristics, Pearson criterion.

Вступ

Широке застосування розподілу Пуассона зумовлене тим, що він описує виникнення рідкісних подій з незмінною, або такою, що змінюється порівняно повільно, середньою частотою. Тому серед усього різноманіття генераторів випадкових та псевдовипадкових чисел або послідовностей важливе місце займають генератори пуассонівських імпульсних послідовностей (ГПІП).