Міністерство освіти і науки України
Вінницький національний технічний університет

В. В. Ковтун

МОДЕЛІ АТРИБУТІВ ГАРАНТОЗДАТНОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ КРИТИЧНОГО ЗАСТОСУВАННЯ ІЗ АВТЕНТИФІКАЦІЄЮ СУБ'ЄКТА ЗА ГОЛОСОМ

Монографія

Вінниця
ВНТУ
2020

УДК 004.93:159.95
К65

Рекомендовано до друку Вченою радою Вінницького національного технічного університету Міністерства освіти і науки України (протокол № 4 від 28 листопада 2019 р.)

Рецензенти:
д. т. н., професор Лужецький В. А.
к. т. н, доцент Сажок М. М.
д. т. н., професор Харченко В. С.

Ковтун, В. В.

К65 Моделі атрибутів гарантоздатності інформаційної системи критичного застосування із автентифікацією суб'єкта за голосом : монографія / В. В. Ковтун. – Вінниця : ВНТУ, 2020. – 412 с.

ISBN 978-966-641-785-8

В монографії розглянуто теоретичні основи оцінювання атрибутів гарантоздатності інформаційних систем критичного застосування із автентифікацією суб'єкта за голосом. Представлено моделі індивідуальності голосу в мовленнєвому сигналі із шумом для конфіденційної автентифікації суб'єкта. Формалізовано моделі конфіденційності, доступності, цілісності, безвідмовність, готовність, обслуговуваність, інтенсивність відмов і напрацювань на відмову такого класу інформаційних систем. Запропонований комплекс моделей дозволяє об'єктивно оцінити довільний екземпляр класу інформаційних систем критичного застосування у метриці атрибутів гарантоздатності.

УДК 004.93:159.95

ISBN 978-966-641-785-8

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ І ПОЗНАЧЕНЬ 5

ПЕРЕДМОВА 7

1 НАЛІЗ ТЕОРЕТИЧНОЇ ЗАБЕЗПЕЧЕНОСТІ ПРОЦЕСУ ОЦІНЮВАННЯ ГАРАНТОЗДАТНОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ КРИТИЧНОГО ЗАСТОСУВАННЯ ІЗ АВТЕНТИФІКАЦІЄЮ СУБ'ЄКТА ЗА ГОЛОСОМ 11

1.1 Аналіз теоретичної забезпеченості процесу оцінювання гарантоздатності інформаційних систем 11

1.2 Аналіз теоретичної забезпеченості процесу синтезу інформаційної системи критичного застосування 21

1.3 Аналіз теоретичної забезпеченості процесу автентифікації суб'єкта за голосом 39

2 ДЕТЕРМІНОВАНІ І СТОХАСТИЧНІ МОДЕЛІ ІНДИВІДУАЛЬНОСТІ ГОЛОСУ В МОВЛЕННЄВОМУ СИГНАЛІ 57

2.1 Моделювання мовленнєвих сигналів у контексті задачі автентифікації суб'єкта за голосом 57

2.2 Базова детермінована модель індивідуальності голосу в мовленнєвому сигналі 72

2.3 Уточнена детермінована модель індивідуальності голосу в мовленнєвому сигналі 81

2.4 Стохастична інтерпретація базової і уточненої моделей індивідуальності голосу в мовленнєвому сигналі 88

2.5 Спектральні компоненти уточненої детермінованої моделі індивідуальності голосу в мовленнєвому сигналі 100

2.6 Опис шумних фрагментів у стохастичній моделі індивідуальності голосу в мовленнєвому сигналі 108

2.7 Синтез і аналіз бікомпонентної моделі індивідуальності голосу в мовленнєвому сигналі 117

3 ОЦІНЮВАННЯ АДЕКВАТНОСТІ МАТЕМАТИЧНИХ МОДЕЛЕЙ ІНДИВІДУАЛЬНОСТІ ГОЛОСУ В МОВЛЕННЄВОМУ СИГНАЛІ 129
3.1 Оцінювання адекватності математичних моделей індивідуальності голосу в мовленнєвому сигналі емпіричним даним 121
3.2 Попереднє оцінювання порогу прийняття рішень в задачі автентифікації суб'єкта за голосом 137
3.3 Емпіричне оцінювання адекватності запропонованих моделей індивідуальності голосу в мовленнєвому сигналі 153
4 МОДЕЛІ ПРОЦЕСУ АВТЕНТИФІКАЦІЇ СУБ'ЄКТА ЗА МОВЛЕННЄВИМ СИГНАЛОМ ІЗ ШУМОМ 180
4.1 Компенсація шумів у фонограмі мовленнєвого сигналу в контексті задачі автентифікації суб'єкта за голосом 180
4.2 Імовірнісні моделі процесу автентифікації суб'єкта за мовленнєвим матеріалом із шумом 201
4.3 Моделі процесу класифікації в задачі автентифікації суб'єкта за мовленнєвим матеріалом із шумом 238
5 МОДЕЛІ АТРИБУТІВ ГАРАНТОЗДАТНОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ КРИТИЧНОГО ЗАСТОСУВАННЯ ІЗ АВТЕНТИФІКАЦІЄЮ СУБ'ЄКТА ЗА ГОЛОСОМ 265
5.1 Концепції і модель забезпечення конфіденційності сеансу суб'єкт-системної інформаційної взаємодії 265
5.2 Модель політики безпеки інформаційної системи критичного застосування 387
5.3 Модель доступності інформаційної системи критичного застосування 315
5.4 Модель залежності конфіденційності процесу автентифікації і доступності в інформаційній системі критичного застосування 334
5.5 Напівмарковська модель гарантоздатності інформаційної системи критичного застосування 346
ПІСЛЯМОВА 368
ЛІТЕРАТУРА 374
ДОДАТОК А Тексти спеціалізованих програмних процедур 397

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ І ПОЗНАЧЕНЬ

АС – суб’єкт автентифікації
АСГ – автентифікація суб’єкта за голосом
АСММШ – автентифікація суб’єкта за мовленнєвим матеріалом із шумом
БОД – блок оброблювання даних
БРД – блок розмежування доступу
ВМ – віртуальна машина
ВМП – відновлюваний марковський процес
ІГМС – індивідуальність голосу в мовленнєвому сигналі
ІС – інформаційна система
ІСКЗ – інформаційна система критичного застосування
ІнР – інформаційні ресурси
ІнС – інформаційне середовище
ІП – інформаційний процес
КНМП – керований напівмарковський процес
КП – критична помилка
КФР – кумулятивна функція розподілу
НМП – напівмарковський процес
НФ – негативний фактор
ОМП – оцінна мережа Петрі
ПА – процес автентифікації
ПБ – політика безпеки
ПБІС – підсистема безпеки інформаційної системи
ПЗНД – підсистема захисту від несанкціонованого доступу
ПКЦІ – підсистема контролю цілісності інформації
ПММ – прихована марковська модель
ПП – підозра на помилку
ПРД – підсистема розмежування доступу
СГР – суміш гаусівських розподілів
СД – сервер даних
СІБ – система інформаційної безпеки
СК – системний контур
СПБ – системна політика безпеки
СТРП – спектрально-темпоральні рецептивні поля
СУБД – система управління базами даних
СРЦ – сервер-реєстраційний центр

AA – додаток для автентифікації
DET-крива – крива компромісного визначення похибки
EER-коефіцієнт – точка рівності похибок α і β
EM-метод – метод максимізації правдоподібності
ERB – еквівалент-прямокутна шкала пропускання
FAR, β – імовірність хибного допуску
FRR, α – імовірність хибного недопуску
MAP-метод – метод максимальної апостеріорної адаптації
MFCC – Мел-частотні кепстральні коефіцієнти
PNC – перцептивні коефіцієнти лінійного передбачення
PNCC – нормовані за потужністю кепстральні коефіцієнти
SNR – рівень відношення «сигнал»/«шум»

ПЕРЕДМОВА

Ступінь інтеграції інформаційних систем у всі сегменти сучасного суспільства зростає експансивно. Властивостями споживати, виробляти, накопичувати і узагальнювати інформацію зараз наділені не тільки передові комп'ютерні системи, а й звичайні побутові речі. Втім, велике значення має об'єкт у який інтегрується інформаційна система. Серед існуючих класів автоматизованих систем окреме місце займають так звані критичні системи [1–10], які функціонують із високою надійністю та функціональною безпекою, зберігаючи прогнозований рівень цих атрибутів під час життєвого циклу експлуатації за рахунок закладених на етапі проектування механізмів протидії впливу визначених класів негативних факторів. Якщо із критичною системою трапляється надзвичайна ситуація, це може завдати значних матеріальних, репутаційних, а головне, людських втрат.

Зв'язок критичних систем із інформаційним простором забезпечують відповідні програмні засоби – інформаційні системи критичного застосування, основною характеристикою яких можна вважати прогнозованість результатів функціонування в умовах впливу як відомих, так і не відомих негативних факторів. Втім, прогнозованість не є достатньо наукомістким терміном. У актуальних вітчизняних і закордонних наукових роботах [11–28] і нормативних документах [29] залежно від галузі, якій належить критична система, вводиться відповідна таксономія якісних показників функціонування цільових систем із введенням, зокрема, метрик для оцінювання інформаційних системних компонентів. Все частіше при цьому вживається термін «гарантоздатність» (англ. dependability). У своєму вихідному варіанті, гарантоздатність утворилося як результат синтезу елементів теорії надійності та теорії безпеки і ризику в прикладному їх застосування для оцінювання функціональної якості досліджуваних систем. Серед атрибутів гарантоздатності виділяють безвідмовність, ремонтопридатність, обслуговуваність, готовність, довговічність, збереженість, живучість, функціональну безпечність, цілісність, конфіденційність, достовірність тощо. Втім, хоча ці властивості давно відомі, одностайності що-

до їх застосування для оцінювання інформаційних систем загалом та інформаційних систем критичного застосування зокрема немає. Навіть на рівні термінології у міжнародних стандартах, зокрема, IEC61508, ITU E800, IEEE 982.1, IEEE 1332, IEEE 1413, IEEE 1624, IEEE 1633,, ECSS-Q-80-3, ECSS-Q-30A, IAEA NS-G-1.3, немає однозначності. Отже, актуальним є застосування строго наукового підходу для адаптації відповідних положень теорії надійності і теорії інформаційної безпеки з метою синтезу достовірних математичних моделей оцінювання атрибутів гарантоздатності інформаційних систем критичного застосування. Також актуальним є отримання моделей і методів, які б сприяли позитивній динаміці значень цих атрибутів для цільового підкласу інформаційних систем.

Монографія, матеріал якої ґрунтується на роботах [30–60], складається з п’яти розділів. У першому з них наведено результати аналізу теоретичної забезпеченості процесу оцінювання гарантоздатності інформаційної системи критичного застосування із автентифікацією суб’єкта за голосом як комплексного явища. Здійснено огляд теоретичних розробок з оцінювання гарантоздатності інформаційних систем. Представлено описову таксономію та проаналізовано структуру інформаційних систем критичного застосування як підкласу інформаційних систем, призначених для забезпечення інформаційної підтримки критичних систем. Проведено огляд технологій підвищення конфіденційності інформаційних систем методами біометричної автентифікації, зокрема, за голосом.

Як виявилось, найпомітніше на конфіденційність інформаційної системи критичного застосування впливає надійність процесу розмежування доступу, що зумовило доцільність досліджень, спрямованих на підвищення надійності двофакторної схеми верифікації для доступу до цільової інформаційної системи за рахунок інтеграції процесу біометричної автентифікації суб’єкта-користувача за голосом. Це зумовило відповідну орієнтацію наступних розділів монографії.

У другому розділі, спираючись на результати аналізу відомих підходів до опису мовленнєвих сигналів, пропонуються моделі індивідуальності голосу в мовленнєвому сигналі для розв’язання задачі автен-

тифікації суб'єкта за голосом. Формалізовано базову й уточнену детерміновані моделі індивідуальності голосу в мовленнєвому сигналі. Пропонуються стохастичні інтерпретації синтезованих детермінованих моделей. Описуються ефективні методи представлення характеристичних параметрів моделей індивідуальності голосу в мовленнєвому сигналі у часовому і частотному вимірах у контексті вирішуваної задачі. Формалізується бікомпонентна модель класифікації фрагментів мовленнєвих сигналів відповідно до їх інформативності для автентифікації суб'єкта за голосом.

В третьому розділі систематизується процес встановлення адекватності емпіричних мовленнєвих сигналів і їх опис математичними моделями, представленими у другому розділі монографії, в контексті задачі автентифікації суб'єкта за голосом. Синтезовано методику верифікації математичних моделей індивідуальності голосу в мовленнєвому сигналі за значенням обраного критерію. Формалізовано процес оцінювання порогу прийняття рішень в задачі автентифікації суб'єкта за голосом відповідно до рівня відношення «сигнал»/«шум» у аналізованому мовленнєвому сигналі. Здійснено емпіричну верифікацію отриманих теоретичних результатів моделювання індивідуальності голосу в мовленнєвому сигналі із узагальненням результатів та їх аналізом.

В четвертому розділі оцінюється вплив шумів акустичного оточення приймачів мовленнєвого сигналу на конфіденційність процесу автентифікації суб'єкта за голосом. Запропоновано моделі компенсування шумів у мовленнєвих сигналах, які стали основою для синтезу імовірнісних моделей процесу автентифікації суб'єкта за мовленнєвим матеріалом із шумом, практичним наслідком яких стало удосконалення відповідних методів прийняття рішень. Враховуючи значну ресурсозатратність процесу класифікації як неодмінної складової процесу автентифікації суб'єкта за голосом, проведено дослідження з оптимізації методів прийняття рішень щодо особи суб'єкта, зокрема, методами машинного навчання.

У п'ятому розділі відображено структурні і функціональні особливості інформаційної системи критичного застосування із автентифі-

кацією суб'єкта за голосом у адекватні моделі гарантоздатності як інтегральної характеристики, яка дає можливість оцінити конфіденційність, доступність, цілісність, безвідмовність, готовність, обслуговуваність, інтенсивність відмов і напрацювань на відмову таких інформаційних систем. В отриманих моделях атрибутів гарантоздатності враховано архітектурні особливості інформаційного середовища цільової системи, важливість її інформаційних ресурсів, специфіку процесу автентифікації та формування системної політики безпеки тощо. Зважаючи на конкуруючу суть атрибутів конфіденційність і доступність та цілісність і функціональність, представлено відповідні моделі взаємозалежності цих інтегральних складових гарантоздатності із утворенням відповідних критеріїв.

Представлені у монографії теоретичні і прикладні результати отримано автором у рамках кафедральної науково-дослідної роботи №46К4 «Методи моделювання та оптимізації складних систем на основі інтелектуальних технологій» на кафедрі комп'ютерних систем управління Вінницького національного технічного університету за підтримки колективів рідної кафедри і спорідненої кафедри автоматизації та інтелектуальних інформаційних технологій.

Автор буде щиро вдячний за відгуки на цю книгу, які можна надсилати на E-mail: kovtun_v_v@gmail.com.

РОЗДІЛ 1
АНАЛІЗ ТЕОРЕТИЧНОЇ ЗАБЕЗПЕЧЕНОСТІ ПРОЦЕСУ ОЦІНЮВАННЯ ГАРАНТОЗДАТНОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ КРИТИЧНОГО ЗАСТОСУВАННЯ ІЗ АВТЕНТИФІКАЦІЄЮ СУБ'ЄКТА ЗА ГОЛОСОМ

У розділі наведено результати аналізу теоретичної забезпеченості процесу оцінювання гарантоздатності інформаційної системи критичного застосування із автентифікацією суб'єкта за голосом як комплексного явища. Проведено огляд теоретичних розробок з оцінювання гарантоздатності інформаційних систем. Представлено описову таксономію та проаналізовано структуру інформаційних систем критичного застосування як підкласу інформаційних систем, призначених для забезпечення інформаційної підтримки критичних систем. Проведено огляд технологій підвищення конфіденційності інформаційних систем методами біометричної автентифікації, зокрема за голосом. Наведені у розділі результати дозволили обґрунтувати вміст і рівень формалізації теоретичних результатів, представлених у наступних розділах монографії.

1.1 Аналіз теоретичної забезпеченості процесу оцінювання гарантоздатності інформаційних систем

У своєму вихідному варіанті [26] гарантоздатність (англ. dependability) [60] утворилася як результат синтезу елементів теорії надійність [61–78] і теорії безпеки і ризику [79–86] у прикладному їх застосування для оцінювання функціональної якості досліджуваної системи. Декомпозицією поняття гарантоздатність є ідентифікація для досліджуваної системи елементів множин атрибутів, загроз і засобів. Множина атрибутів включає методи оцінювання надійності, ремонтопридатності, конфіденційності, доступності і цілісності досліджуваної системи. Ідентифікація множини загроз передбачає визначення типів несправностей, помилок і збоїв, які можуть виникнути під час життєвого циклу досліджуваної системи. Множина засобів включає методи: – запобігання загрозам; – забезпечення відмовостійкості; – усунення наслідків, спричинених впливом загроз; – прогнозування впливу загроз тощо.

Інтегральними характеристиками елементів цих множин є:

– безвідмовність [87], як властивість досліджуваної системи зберігати функціональний стан протягом обмеженого, неперервного інтервалу часу;

– готовність [88, 89] як здатність досліджуваної системи, забезпеченої необхідними зовнішніми ресурсами, у заданий момент та протягом фіксованого інтервалу часу виконувати передбачені специфікацією функції при дотриманні визначених умов експлуатації і регламенту технічного обслуговування;

– живучість [90–94], як властивість досліджуваної системи зберігати або відновлювати функціональний стан у визначеному обсязі при санкціонованій або несанкціонованій зміні умов експлуатації або структури апаратної чи інформаційної складових;

– обслуговуваність [21, 95], як властивість досліджуваної системи підлягати регламентованим процесам технічного обслуговування та ремонту;

– цілісність [96–109], як властивість досліджуваної системи зберігати визначений рівень структурної сталості при функціонуванні в умовах зовнішніх випадкових або детермінованих спотворень або руйнівних впливів;

– конфіденційність [96–109], як властивість досліджуваної системи самоубезпечуватися від несанкціонованого використання або структурних змін;

– функціональна безпека [110–112], як здатність досліджуваної системи не завдавати небезпечних (катастрофічних) впливів на людину або навколишнє середовище у відповідь на дію факторів із визначеної на етапі проектування множини загроз.

Оцінювання ***безвідмовності*** досліджуваної системи передбачає визначення таких параметрів як:

– імовірність безвідмовного функціонування $R(t)$ – імовірність того, що до настання моменту часу t досліджувана система не перейде у нефункціональний стан;

– середня тривалість безвідмовного функціонування $\overline{T}$ – математичне сподівання тривалості часу перебування системи у функціональному стані аж до моменту її першого переходу у нефункціональний стан;

– коефіцієнт потоку відмов $\omega(t)$ – добуток кількості переходів досліджуваної системи у нефункціональний стан із поверненням у функціональний стан за часовий інтервал тривалістю t і оберненого значення t^{-1}.

Методики розрахунку цих параметрів змінюються, якщо досліджуваній системі властива ***відмовостійкість***. Так імовірність безвідмовного функціонування відмовостійкої досліджуваної системи оцінюватиметься виразом

$$R_{ts} = c^s\left(1 - F\left(f, q, s\right)\right), \tag{1.1}$$

де $F\left(f, q, s\right)$ – функція імовірності переходу системи в нефункціональний стан; s – кількість резервних модулів, які можна ввімкнути для переведення системи із нефункціонального стану у функціональний (потребує витрат на резервування на етапі проектування); q – кількість однотипних модулів, які функціонують паралельно для запобігання переходу системи у нефункціональний стан (потребує витрат на резервування як на етапі проектування, так і на етапі експлуатації); c – ступінь компенсування наслідків відмови (імовірність того, що система зможе із нефункціонального стану відновити функціональний стан у повному або обмеженому обсязі); f – гранично допустима для модуля кількість переходів із функціонального стану у нефункціональний і навпаки.

Якщо досліджувана система – електротехнічна, то, відповідно до актуальних міжнародних стандартів [29, 113], імовірнісна функція $F\left(f, q, s\right)$ з виразу (1.1) є дифузійним монотонним (DN) розподілом:

$$\begin{aligned} F\left(f, q, s\right) = DN\left(x, \nu, f, q, s\right) = \Phi\left(\left(\nu\sqrt{x}\right)^{-1}\left(x - 1\right)\right) + \\ + \exp\left(2\nu^{-2}\right)\Phi\left(\left(\nu\sqrt{x}\right)^{-1}\left(-x - 1\right)\right), \end{aligned} \tag{1.2}$$

де x – відносна тривалість безвідмовного функціонування: $x = \overline{T}^{-1}$; ν – коефіцієнт варіації розподілу; Φ – функція нормованого нормального розподілу тощо. Згідно з тими ж стандартами, значення елементів множини $P_{ts} = \{q, c, f, s\}$ за замовчуванням визначено як $\{1,1,0,0\}$, від-

повідно. Зростання значень елементів множини P_{ts} спричиняє зростання імовірності R_{ts} та зростання витрат на експлуатацію досліджуваної системи.

Якщо в архітектурі досліджуваної системи виділено підсистеми, то підсумкову кількість функціональних конфігурацій системи можна встановити за виразом $U_s = \prod_{i=1}^{n} U_i^{ss}$, де U_i^{ss} – кількість функціональних конфігурацій i-ї підсистеми.

Також вклад апаратної складової у безвідмовність досліджуваної системи враховують параметром N_s – обсяг апаратних ресурсів, які необхідно акумулювати у досліджуваній системі для досягнення останньою заданого рівня безвідмовності. Відповідно, якщо на етапі проектування є різні варіанти реалізації досліджуваної системи, то їх варто порівняти, визначивши для кожного із них вартість, яку необхідно витратити для досягнення вибраного порогового значення характеристики R_{ts}.

Множина параметрів такої вкрай важливої для систем критичного застосування інтегральної характеристики як ***готовність*** включає коефіцієнт готовності і коефіцієнт оперативної готовності тощо.

Коефіцієнт готовності характеризує імовірність перебування досліджуваної системи в функціональному стані:

$$K_f = T_f \left(T_f + T_{rf}\right)^{-1}, \tag{1.3}$$

де T_f – середня тривалість перебування системи в функціональному стані; T_{rf} – тривалість відновлення системою функціонального стану після переходів у нефункціональний стан, спричинених впливом НФ.

Коефіцієнт оперативної готовності характеризує імовірність перебування досліджуваної системи у функціональному стані у конкретний момент часу:

$$K_{of} = K_f R_t, \tag{1.4}$$

де R_t – імовірність перебування досліджуваної системи у функціональному стані у момент часу t.

До параметрів ***живучості***, як властивості досліджуваної системи зберігати повну або часткову функціональність при експлуатації в умовах, які не передбачено на етапі проектування, відносять виживаність, запас живучості і коефіцієнти живучості та деградації.

Коефіцієнт живучості показує співвідношення кількості функціональних станів до всієї можливої кількості станів, у яких може перебувати досліджувана система,

$$K_G = M\left(C_l^i\right)^{-1} = M\left((l-i)!i!(l!)^{-1}\right), \tag{1.5}$$

де M – кількість функціональних станів; i – кратність відмови; l – кількість функціональних одиниць живучості досліджуваної системи.

Коефіцієнт деградації показує співвідношення кількості нефункціональних станів до всієї можливої кількості станів, у яких може перебувати досліджувана система,

$$K_D = N\left(C_l^i\right)^{-1} = N\left((l-i)!i!(l!)^{-1}\right), \tag{1.6}$$

де N – кількість нефункціональних станів досліджуваної системи.

Виживаність – це властивість досліджуваної системи перебувати у функціональному стані під впливом n-кратного НФ:

$$R(n) = 1 - Q(n) = P\left(F = A_n^{-1}\right), \tag{1.7}$$

де F – бінарна функція роботоздатності рівна одиниці, якщо система роботоздатна, або нулю – у протилежному випадку; A_n – подія, яка відбувається у наслідок впливу n-кратного НФ.

Запас живучості $d = C - 1$ є зменшеною на одиницю критичною кількістю дефектів C, яка характеризує граничну кількість дефектів, по перевищенню якої досліджувана система перейде у нефункціональний стан.

Також інтегральною характеристикою гарантоздатності є ***обслуговуваність***, яка узагальнено описує складність регламентного обслуговування досліджуваної системи для підтримки її у функціональному стані. До параметрів обслуговуваності відносять:

– тривалість технічного обслуговування T_{to} – середній час, що має витрачатися на обслуговування досліджуваної системи згідно з технічною документацією;

– трудомісткість технічного обслуговування $T_{tz}(i)$ – середні трудовитрати на проведення i-го типу технічного обслуговування досліджуваної системи;

– вартість технічного обслуговування $C_{to}(i)$ – середня вартість проведення i-го типу технічного обслуговування досліджуваної системи;

– тривалість відновлення T_{rn} – середня тривалість часу, яка витрачається на переведення досліджуваної системи з нефункціонального стану у функціональний;

– обчислюваний за певний визначений період експлуатації досліджуваної системи коефіцієнт технічного використання $K_{tu} = T_u(T_u + T_r + T_{to})^{-1}$, де T_u – тривалість перебування системи у функціональному стані; T_r – тривалість перебування системи у нефункціональному стані з причини ремонту; T_{to} – тривалість перебування системи у нефункціональному стані з причини технічного обслуговування.

Функціональна безпека як інтегральна характеристика гарантоздатності досліджуваної системи описується:

– імовірністю безпечного функціонування $R_{op}(t) = 1 - F_{op}(t)$ – імовірність того, що за час функціонування досліджуваної системи, рівний t, не трапиться критично небезпечна ситуація, тобто випадок, наслідки якого є критично небезпечними для навколишнього середовища, інфраструктури, життя людей тощо. Визначена імовірнісна функція $F_{op}(t)$ описує розподіл тривалості функціонування системи до настання критично небезпечної ситуації;

– імовірність критично небезпечної ситуації $Q_{op}(t) = 1 - R_{op}(t)$ – імовірність того, що за період функціонування досліджуваної системи, рівний t, трапиться критично небезпечна ситуація;

– відносна середня тривалість функціонування із урахуванням настання критично небезпечних ситуацій T_{cs} – відношення тривалості функціонування досліджуваної системи до математичного сподівання

кількості зафіксованих за цей часовий період випадків настання критично небезпечних ситуацій;

– коефіцієнт безпечності $K_{fs} = T_{cs}\left(T_{cs} + T_{rcs}\right)$ – імовірність того, що у довільний момент часу функціонування досліджуваної системи не станеться критично небезпечна ситуація, якщо у цей час система використовується за призначенням. Параметр T_{rcs} описує середню тривалість відновлення функціонального стану досліджуваної системи після настання критично небезпечної ситуації.

Цілісність є властивістю досліджуваної системи зберігати структурну сталість незважаючи на вплив випадкових чи навмисних спотворювальних чи руйнівних факторів. Параметрами цієї інтегральної характеристики є рівні цілісності апаратної й інформаційної системних складових.

Рівень цілісності апаратної складової L_a це властивість досліджуваної системи унеможливити несанкціоновані структурні зміни своєї апаратної складової.

Рівень цілісності інформаційного середовища L_{is} – властивість досліджуваної системи унеможливити несанкціоновані структурні зміни свого ІнС.

Рівень цілісності інформаційних ресурсів L_{is} – властивість досліджуваної системи унеможливити несанкціоновані структурні зміни своїх ІнР.

Конфіденційність, як властивість досліджуваної системи запобігати несанкціонованому використанню власних апаратних і інформаційних ресурсів, параметризується імовірністю загроз, рівнем доступності, рівнем секретності тощо.

Імовірність загроз P_{th} – це імовірність виникнення ситуації порушення конфіденційності досліджуваної системи.

Рівень доступності L_d – це властивість досліджуваної системи нейтралізувати за відповідний проміжок часу формалізовані типи загроз, спрямовані на отримання несанкціонованого доступу до власного ІнС.

Рівень секретності L_s – це властивість досліджуваної системи протидіяти формалізованим типам загроз, спрямованим на отримання несанкціонованого доступу до власних ІнР.

Якщо досліджувана система – інформаційна, то в актуальних стандартах [29, 104–106] параметри її цілісності оцінюються узагальненням значень бінарних критеріїв, які репрезентують відповідні параметри інтегральної складової.

Зокрема, такий параметр як рівень цілісності ІнС L_{is} декомпозується на два параметри – цілісність обчислювальних ресурсів L_{CR} і цілісність програмних ресурсів L_{PR}.

Цілісність обчислювальних ресурсів L_{CR} репрезентується такими бінарними критеріями: правильність експлуатації; безпека експлуатації; здатність перевіряти і зберігати дані; здатність захисту від суттєвих втрат конфіденційності в разі успішної реалізації загроз; здатність відновлювати конфіденційність після успішної реалізації збоїв і загроз; наявність захисту від порушень авторського права; наявність функцій відновлення конфіденційності; наявність функцій контролю конфіденційності; наявність захисту конфіденційності при функціонуванні у локальній мережі; наявність захисту конфіденційності при функціонуванні в середовищі мережі Internet; наявність функцій ідентифікації і автентифікації; наявність сервісів моніторингу та оповіщення; наявність сервісів оброблювання помилок. Як видно, більша частина критеріїв орієнтована на оцінювання конфіденційності. На оцінювання цілісності і доступності орієнтовано приблизно однакову кількість критеріїв.

Такий параметр як цілісність програмних ресурсів L_{PR} репрезентується такими бінарними критеріями: наявність функцій відновлення виконуваного процесу в разі збою операційної системи, процесора, зовнішніх пристроїв; наявність сервісів відновлення процесу в разі збоїв обладнання; наявність можливості повторного старту процесу з точки зупину; наявність автоматичного резервування ресурсів для збереження поточного стану процесу; наявність сервісів забезпечення стійкості при: виявленні помилок у вхідних даних, виявленні помилок користувача, відсутності необхідних даних; наявність сервісів забезпечення сумісності із апаратними засобами; наявність сервісів забезпечення сумісності із системними програмними засобами; наявність сервісів забезпечення сумісності із іншими програмними засобами, включаючи обмін даними; наявність сервісів оброблювання помилкових ситуацій.

Параметр рівень цілісності ІнР L_{is} репрезентується такими бінарними критеріями: достовірність; точність; якість; своєчасність; правильність; наявність сервісу контролю правильності введеної / виведеної інформації; наявність інформації про сервіси зберігання даних; наявність тестів для контролю допустимих значень вхідних / вихідних даних; наявність сервісів контролю повноти вхідних / вихідних даних; наявність сервісів контролю коректності вхідних / вихідних даних; наявність сервісів контролю несуперечливості вхідних / вихідних даних; наявність сервісів контролю дотримання діапазонів даними і адресами; наявність сервісів оброблювання граничних значень; наявність інформації про здатність відновлювання після помилок.

Як вже зазначалося наведені критерії – бінарні, що спрощує облік відповідних характеристик, але суттєво нівелює їх інформативність.

Окрім цілісності, процес оцінювання конфіденційності також репрезентується множинами бінарних критеріїв, які узагальнюють оцінки відповідних параметрів.

Параметр конфіденційності – імовірність загроз P_{th} репрезентується такими бінарними критеріями: правильність експлуатації обчислювальних ресурсів; безпека експлуатації обчислювальних ресурсів; здатність перевіряти і зберігати дані; здатність запобігати суттєвих наслідків для конфіденційності з причини виникнення помилок; здатність відновлювати конфіденційність після збоїв і помилок; наявність захисту від порушень авторського права; наявність функцій відновлення конфіденційності; наявність функцій контролю конфіденційності; наявність захисту конфіденційності при роботі у локальній мережі; наявність захисту конфіденційності при роботі у середовищі Internet; наявність функцій ідентифікації і автентифікації; наявність сервісів моніторингу та оповіщення; наявність сервісів оброблювання помилок.

Рівень доступності L_d, як параметр конфіденційності, репрезентується такими бінарними критеріями: наявність документа, що регламентує доступ до секретної інформації; наявність документа, що регламентує доступ до технічних засобів; наявність паролів доступу до ІнР; наявність фізичного захисту технічних ресурсів; наявність захисту технічних ресурсів програмними засобами; наявність у персоналу дозволу на роботу із секретними технічними і / або ІнР; наявність сервісів відновлення виконуваного процесу після збоїв операційної системи, процесора, зовнішніх пристроїв; наявність сервісів забезпечення

стійкості функціонування при наявності помилок у вхідних даних, помилок користувача, відсутності необхідних даних; наявність сервісів забезпечення сумісності із апаратними засобами; наявність сервісів забезпечення сумісності із системними програмними засобами; наявність сервісів забезпечення сумісності з іншими програмними засобами, включаючи обмін даними; наявність сервісів опрацювання помилкових ситуацій. Можна помітити, що майже половина критеріїв тотожна введеним для регламентування цілісності програмних ресурсів L_{PR}. Таке дублювання характеризує неточність у семантичній інтерпретації термінів «цілісність» і «конфіденційність».

Рівень секретності L_s, як параметр конфіденційності, репрезентується такими бінарними критеріями: наявність документа, що регламентує доступ до секретної інформації за рівнями секретності; наявність документа, що регламентує доступ до технічних засобів за рівнями секретності; наявність паролів доступу до ІнР; наявність фізичного захисту технічних ресурсів; наявність захисту технічних ресурсів програмними засобами; наявність у персоналу дозволу на роботу із секретними технічними і / або інформаційними ресурсами; наявність сервісів контролю правильність введеної / виведеної інформації; наявність сервісів контролю процесів збереження даних; наявність тестів контролю допустимих значень вхідних / вихідних даних; наявність сервісів контролю повноти вхідних / вихідних даних; наявність сервісів контролю коректності вхідних / вихідних даних; наявність сервісів контролю несуперечності вхідних / вихідних даних; наявність сервісів контролю дотримання діапазонів даними і адресами; наявність сервісів оброблювання граничних значень; наявність сервісів для відновлення інформації після помилок. Видно, що більше половини критеріїв тотожна введеним для регламентування рівня цілісності ІнР L_{is}.

Узагальнюючи наведені результати слід відзначити, що таксономії гарантоздатності властива суттєва надлишковість, спричинена відсутністю єдиного цільового міжнародного стандарту. Ця обставина зумовлює неоднозначність у параметризації інтегральних характеристик гарантоздатності. Також слід відмітити загальність критеріїв оцінювання гарантоздатності ІС. Враховуючи темпи розвитку галузі інформаційних технологій такі вади можуть стати причинами значних втрат, що обумовлює актуальність наукової формалізації процесу оцінювання атрибутів гарантоздатності ІСКЗ у парадигмі класичної теорії надійності, ризиків та інформаційної безпеки.

ЛІТЕРАТУРА

1. L. F. Robert, R. A. R Norma, *Critical Systems Thinking: Current Research and Practice.* Germany: Springer Science & Business Media, 2007.
2. V. P. Nandish, *Critical Systems Analysis and Design: A Personal Framework Approach.* USA, NY: Psychology Press, 2005.
3. C. Dale, T. Anderson, "Safety-Critical Systems: Problems, Process and Practice," in *Proceedings of the Seventeenth Safety-Critical Systems Symposium*, Brighton, UK, 3–5 February 2009. Springer Science & Business Media, 2009.
4. M. Bozzano and A. Villafiorita, *Design and Safety Assessment of Critical Systems*. Boca Raton, USA: CRC Press, 2010.
5. M. Rausand, *Reliability of Safety-Critical Systems: Theory and Applications.* Hoboken, USA: John Wiley & Sons, 2014.
6. S. Gnesi and T. Margaria, *Formal Methods for Industrial Critical Systems: A Survey of Applications*. Hoboken, USA: John Wiley & Sons, 2012.
7. P. Millot, *Risk Management in Life-Critical Systems.* Hoboken, USA: John Wiley & Sons, 2014.
8. Ding W. Using Model Checking to Generate Test Cases for Critical Systems. George Mason University, 2000.
9. C. Brooke, *Critical Management Perspectives on Information Systems*. London, UK: Routledge, 2009.
10. R. Wallace, *Information Theory Models of Instabilities in Critical Systems.* World Scientific, 2016.
11. В. С. Харченко, «Гарантоздатність комп'ютерних систем: проблеми і результати,» *Авіаційнокосмічна техніка і технологія*, № 7(23), с. 352–376, 2005.
12. В. С. Харченко, «Гарантоспособность и гарантоспособные системы: элементы методологии,» *Радіоелектронні і комп'ютерні системи*, № 5(17), с. 7–19, 2006.
13. В. С. Харченко, «Гарантоздатність комп'ютерних систем: проблеми, напрямки досліджень, результати,» *Радіоелектронні і комп'ютерні системи*, № 5(17), с. 105–109, 2006.
14. В. С. Харченко, «Гарантоздатність комп'ютерних систем: межа універсальності в контексті інформаційно-технічного стану,» *Радіоелектронні і комп'ютерні системи*, № 8, с. 8–16, 2007.
15. В. Глухов, «Оцінювання гарантоздатності криптографічних комп'ютерних систем,» *Вісник Національного університету "Львівська політехніка"*, № 616: *Комп'ютерні науки та інформаційні технології*, с. 66–72, 2008.

16. А. В. Федухин і В. П. Пасько, «К вопросу о количественных характеристиках безотказности избыточных компьютерных систем,» *Математические машины и системы*, № 1, с. 180–188, 2012.

17. А. В. Федухин и Г. Н. В. Сеспедес, «Атрибуты и метрики гарантоспособных компьютерных систем,» *Математические машины и системы*, № 2, с. 195–201, 2013.

18. А. В. Федухин и Б. Г. Мудла, «Гарантоспособность компьютерных систем – мода или объективная необходимость,» *Математические машины и системы*, № 4, с. 179–188, 2014.

19. В. Г. Сербін і А. І. Сухомлин, «Визначення і формалізація основних показників гарантоздатності живучих комп'ютерних систем керування на основі ймовірнісно-фізичного підходу для їх проектної оцінки і прогнозування,» *Математические машины и системы*, № 4, с. 182–189, 2012.

20. Г. С. Теслер, «Концепция построения гарантоспособных вычислительных систем,» *Математические машины и системы*, № 1, с. 134–145, 2006.

21. Г. С. Теслер, «Решение проблемы гарантоспособности компьютерных систем в аспекте базисов компьютерной науки,» *Математические машины и системы*, № 4, с. 171–189, 2008.

22. Б. Г. Мудла, Т. І .Єфімова і Р. М. Рудько, «Гарантоздатність як фундаментальний узагальнюючий та інтегруючий підхід,» *Математические машины и системы*, № 2, с. 148–165, 2010.

23. Р. Ю. Царев, Д. В. Капулин, Д. В. Машурова, Я. А. Тынченко и Д. Н. Ковтанюк, «Многоатрибутивное формирование гарантоспособных систем управления и обработки информации,» С*ибирский журнал науки и технологий*, № 5(45), с. 106–110, 2012.

24. И. Б. Шубинский, А. М. Замышляев, Л. Р. Папич, «Адаптивная гарантоспособность информационных систем управления,» *Надежность*, № 4(18). с. 3–9. doi:10.21683/1729-2646-2018-18-4-3-9.

25. W. Hasselbring, *Dependability Engineering*. Berlin, Germany: GITO mbH Verlag, 2006.

26. F. J. Redmill, *Dependability of Critical Computer Systems*. USA, NY: Springer Science & Business Media, 1989.

27. S. Bernardi, J. Merseguer, D. Corina Petriu, *Model-Driven Dependability Assessment of Software Systems*. USA, NY: Springer Science & Business Media, 2013.

28. M. Tokoro, *Open Systems Dependability: Dependability Engineering for Ever-Changing Systems*. USA, NY: CRC Press, 2012.

29. IEC-TC56: Dependability Standards and Supporting Standards [Online]. Available: http://www2.fiu.edu/~revellk/pad3003/Neave.pdf. Accessed on: August 26, 2019.

30. В. В. Ковтун, М. М. Биков, Н. Г. Савінова. Надійний метод виділення складових сегментів у мовленнєвому сигналі. *Наукові праці Вінницького національного технічного університету*, №1, 2007. [Електронний ресурс]. Режим доступу: https://trudy.vntu.edu.ua/index.php/trudy/article/view/19/19. Дата звернення: Серпень 26, 2019.

31. В. В. Ковтун, М. М. Биков, Н. Г. Савінова. Оцінювання впливу завад на достовірність роботи інформаційно-вимірювальної системи розпізнавання голосу. *Наукові праці Вінницького національного технічного університету*, № 3, 2009. [Електронний ресурс]. Режим доступу: https://trudy.vntu.edu.ua/index.php/trudy/article/view/149/148. Дата звернення: Серпень 26, 2019.

32. В. В. Ковтун, М. М. Биков, А. Раїмі, «Метод виділення основного тону на основі модифікованої математичної моделі слухової системи людини,» *Вісник Вінницького політехнічного інституту,* № 5, с. 130–135, 2011.

33. В. В. Ковтун, М. М. Биков, Н. Г. Савінова, «Оцінювання метрологічних характеристик інформаційно-вимірювальної системи автоматизованого розпізнавання голосів,» *Вісник Вінницького політехнічного інституту*, № 6, с. 189–193, 2011.

34. В. В. Ковтун, М. М. Биков, Н. Г. Савінова, «Аналіз стану проблеми розробки ефективних систем пошуку ключових слів,» *Вісник Вінницького політехнічного інституту*, № 1. с. 179–181, 2012.

35. В. В. Ковтун, М. М. Биков, К. Конате, «Метод підвищення ефективності роботи пам’яті в системах пошуку ключових слів у мовленнєвому сигналі,» *Вісник Вінницького політехнічного інституту*, № 2, с. 159–162, 2012.

36. В. В. Ковтун, М. М. Биков, «Оцінювання надійності автоматизованих систем розпізнавання мовців критичного застосування,» *Вісник Вінницького політехнічного інституту*, № 2, с. 70–76, 2017.

37. В. В. Ковтун, М. М. Биков. «Використання множини мікрофонів у автоматизованій системі розпізнавання мовця критичного застосування,» *Вісник Вінницького політехнічного інституту*, № 3, с. 84–91, 2017.

38. В. В. Ковтун, М. М. Биков, А. Д. Гафурова, «Дослідження комітету нейромереж у автоматизованій системі розпізнавання мовців критичного застосування,» *Вісник Хмельницького національного університету, серія: Технічні науки*, № 2(247), с. 144–150, 2017.

39. В. В. Ковтун, М. М. Биков, А. О. Береза, А. Д. Гафурова, «Оптимізація алфавіту інформативних ознак для автоматизованої системи розпізнавання мовців критичного застосування,» *Вісник Хмельницького національного університету, серія: Технічні науки*, № 3(249), с. 222–228, 2017.

40. В. В. Ковтун, М. М. Биков, «Метод представлення ознак у автоматизованій системі розпізнавання мовця критичного застосування,» *Вісник Хмельницького національного університету, серія: Технічні науки*, № 5(253), с. 112–120, 2017.

41. В. В. Ковтун, М. М. Биков, «Дослідження ефективності ознак розпізнавання мовців при використанні згортальних нейромереж,» *Оптико-електронні інформаційно-енергетичні технології*, № 2(32), с. 22–28, 2016.

42. В. В. Ковтун, М. М. Биков, О. О. Максимов. Детектування мовленнєвої активності в автоматизованій системі розпізнавання мовця критичного застосування. *Журнал інженерних наук*, Т. 4, № 1, 2017. [Електронний ресурс]. Режим доступу: http://jes.sumdu.edu.ua/wp-content/uploads/2017/11/JES_2017_01_H14-H20.pdf Дата звернення: Серпень 26, 2019.

43. V. V. Kovtun et al. “Research of neural network classifier in speaker recognition module for automated system of critical use,” *Proc. SPIE Photonics Applications in Astronomy, Communications, Industry, and High Energy Physics Experiments*, 1044521, August 7, 2017. doi:10.1117/12.2280930.

44. В. В. Ковтун, Т. В. Грищук, «Підвищення шумостійкості автоматизованої системи розпізнавання мовця критичного застосування,» *Вісник Вінницького політехнічного інституту*, № 1, с. 98–111, 2018.

45. В. В. Ковтун В.В., О. В. Бісікало, Т. В. Грищук, «Оптимізація класифікатора автоматизованої системи розпізнавання мовця критичного застосування,» *Радіоелектроніка, інформатика, управління*, № 2, с. 30–43, 2018. doi:10.15588/1607-3274-2018-2-4.

46. В. В. Ковтун, М. М. Биков, «Підвищення інформативності основного тону для розпізнаванні мовців згортальними нейромережами,» *Оптико-електронні інформаційно-енергетичні технології*, № 2(34). с. 44–51, 2017.

47. В. В. Ковтун, «Оцінювання основного тону у автоматизованій системі розпізнавання мовця критичного застосування,» *Вісник Вінницького політехнічного інституту*, №4. с. 61-73, 2018.

48. V. V. Kovtun et al. “Neural network modelling by rank configurations,” *Proc. SPIE Photonics Applications in Astronomy, Communications, Industry, and High Energy Physics Experiments*, 1080821, 2018. doi: 10.1117/12.2501521.

49. V. V. Kovtun, I. D. Ivasyuk, A. Kotyra, A. Mussabekova, “The automated speaker recognition system of critical use,” *Proc. SPIE Photonics Applications in Astronomy, Communications, Industry, and High Energy Physics Experiments*, 108082V, 2018. doi: 10.1117/12.2501688.

50. В. В. Ковтун, «Концепція впровадження автоматизованої системи розпізнавання мовця у процес автентифікації для доступу до критичної системи,» *Вісник Вінницького політехнічного інституту*, № 5, с. 41–52, 2018. doi:10.31649/1997-9266-2018-140-5-41-52.

51. V. V. Kovtun, O. V. Bisikalo, M. S. Yukhimchuk, I. F. Voytyuk, “Analysis of the automated speaker recognition system of critical use operation results,” *Radio Electronics, Computer Science, Control*, № 4, pp. 71–84, 2018. doi:10.15588/1607-3274-2018-4-7.

52. В. В. Ковтун, Т. В. Грищук, А. О. Береза, «Оцінювання надійності сеансу розпізнавання особи автоматизованою системою розпізнавання мовця критичного застосування,» *Вісник Хмельницького національного університету, серія: Технічні науки*, № 6(267, Т.1), с. 143–150, 2018. doi:10.31891/2307-5732-2018-267-6(1)-143-150.

53. В. В. Ковтун, А. Д. Гафурова, «Нейромережева адаптація PLDA для використання у автоматизованій системі розпізнавання мовця критичного застосування,» *Вісник Хмельницького національного університету, серія: Технічні науки*, № 1(269, Т.1), с. 172–178, 2019. doi:10.31891/2307-5732-2019-269-1-172-177.

54. V. V. Kovtun, O. V. Bisikalo, M. S. Yukhimchuk, “Modeling the security policy of the information system for critical use,” *Radio Electronics, Computer Science, Control*, № 1, pp. 132–149, 2019. doi:10.15588/1607-3274-2019-1-13.

55. В. В. Ковтун, «Моделювання залежності конфіденційності автентифікації і доступності у інформаційній системі критичного застосування,» *Вісник Вінницького політехнічного інституту*, № 6, с. 77–89, 2018. doi: 10.31649/1997-9266-2018-141-6-77-89.

56. В. В. Ковтун, «Моделювання доступності інформаційної системи критичного застосування,» *Вісник Вінницького політехнічного інституту*, № 1, с. 41–57, 2019. doi:10.31649/1997-9266-2019-142-1-41-57.

57. V. V. Kovtun, M. S. Yukhimchuk, P. Kisała, A. Abisheva, S. Rakhmetullina, “Integration of hidden markov models in the automated

speaker recognition system for critical use," *Przeglad Elektrotechniczny*, № 1, pp. 178–182, 2019. doi:10.15199/48.2019.04.32.

58. В. В. Ковтун, «Напівмарковське оцінювання гарантоспроможності інформаційної системи критичного застосування,» *Вісник Вінницького політехнічного інституту*, № 2, с. 61–77, 2019. doi:10.31649/1997-9266-2019-143-2-61-77.

59. V. V. Kovtun, O. V. Bisikalo, V. V. Sholota, "The Information System for Critical Use Access Process Dependability Modeling," *Proc. 9th International Conference on Advanced Computer Information Technologies (ACIT)*, 5–7 June 2019. doi:10.1109/ACITT.2019.8780013.

60. A. Avizienis, J.-C. Laprie, B. Randell, C. Landweh, "Basic Concepts and Taxonomy of Dependable and Secure Computing," *IEEE Transactions on Dependable and Secure Computing*, Vol. 1, №1, pp. 11-33, 2004. doi: 10.1109/TDSC.2004.2.

61. Н. А. Северцев, В. Г. Шолкин, Г. А. Ярыгин, В. И. Никишин, *Статистическая теория подобия: надежность технических систем*. М: Наука, 1986.

62. В. А. Острейковский, *Теория надежности*. М.: Высшая школа, 2003.

63. R. E. Barlow, *Engineering Reliability. American Statistical Association and the Society for Industrial and Applied Mathematics*. USA: ASA-SIAM Series on Statistics and Applied Probability, 1998.

64. I. B Frenkel et al., *Applied Reliability Engineering and Risk Analysis: Probabilistic Models and Statistical Inference*. USA, NY: Wiley, 2013, 2014.

65. Л. Н. Александровская, И. З. Аронов, А. И. Елизаров и др., *Статистические методы анализа безопасности сложных технических систем*. М.: Логос, 2001.

66. E. Bauer, *Design for reliability: information and computer-based systems*. USA: IEEE Press + Wiley, 2010.

67. H. Pham, *System Software Reliability*. USA, NY: Springer, 2006.

68. О. Г. Додонов, М. Г. Кузнєцова, О. С. Горбачик, *Живучість складних систем: аналіз та моделювання*. К.: НТУУ КПІ, 2009.

69. Р. Лонгботтом, *Надежность вычислительных систем*. М.: Энергоатомиздат, 1985.

70. В. П. Тарасенко, А. Ю. Маламан, Ю. П. Черніченко, В. І. Корнійчук, *Надійність комп'ютерних систем*. К.: Корнійчук, 2007.

71. Н. Я. Яхьяев, А. В. Кораблин, *Основы теории надежности и диагностика*. М.: Академия, 2009.

72. В. М. Дубовой, *Моделювання систем контролю та керування*. Вінниця: ВНТУ, 2005.
73. А. А. Червоный, В. И. Лукьященко, Л. В. Котин, *Надежность сложных систем*. М.: Машиностроение, 1976.
74. С. А. Тимашев, *Инфраструктуры. Том 1. Надежность и долговечность*. Екатеринбург: Изд-во НИСО УрО РАН, 2016.
75. Е. Сугак, *Надёжность техники. Часть 1. Теоретические основы*. Germany: LAP Lambert Academic Publishing GmbH & Co, 2014.
76. И. А. Рябинин, *Надежность и безопасность структурно-сложных систем*. СПб: Политехника, 2000.
77. А. М. Половко, С. В. Гуров, *Основы теории надежности*. СПб: БХВ-Петербург, 2006.
78. А. М. Половко, С. В. Гуров. *Основы теории надежности. Практикум*. СПб: БХВ-Петербург, 2006.
79. Э. Дж. Хенли, Х. Кумамото, *Надежность технических систем и оценка риска*. М.: Машиностроение, 1984.
80. С. П. Тимошенков, Б. М. Симонов, В. Н. Горошко, *Надежность технических систем и техногенный риск*. М.: Юрайт, 2018.
81. Н. А. Северцев, В. Н. Темнов, *Метрологическое обеспечение безопасности сложных технических систем*. М.: Курс: Инфра-М, 2015.
82. V. V. Kovtun et al. “Improvement of the learning process of the automated speaker recognition system for critical use with HMM-DNN component,” Proc. SPIE, 11176, 1117620, November 6, 2019. doi: 10.1117/12.2536888.
83. Н. Н. Рахимова, *Управление риском, системный анализ и моделирование*. *Практикум.* Оренбург: ОГУ, 2017.
84. В. В. Костерев, *Надежность технических систем и управление риском*. М.: МИФИ, 2008.
85. В. А. Зорин, *Основы работоспособности технических систем*. М.: Академия, 2009.
86. А. В. Гуськов, К. Е. Милевский, *Надежность технических систем и техногенный риск*. Новосибирск: НГТУ, 2007.
87. Л. Н. Александровская, А. П. Афанасьев, А. А. Лисов, *Современные методы обеспечения безотказности сложных технических систем*. М.: Логос, 2001.
88. Д. К. Потресов, Д. В. Скоморохов, «Факторы надежности информационных систем высокой готовности,» *Горный*

информационно-аналитический бюллетень (научно-технический журнал), № 5, с. 134–139, 2013.

89. В. В. Гришин, «Модель готовности сложной технической системы управления,» *Информационно-управляющие системы*, № 6, с. 8–11, 2004.

90. А. О. Недосекин, В. В. Виноградов, З. И. Абдулаева, *Методы и модели оценки функциональной живучести структурно-сложных технических систем*. СпБ: Изд-во Политехнического университета, 2018.

91. А. Г. Додонов, Д. В. Флейтман, «Технологические аспекты обеспечения живучести информационных систем,» *Известия Южного федерального университета. Технические науки*, № 4(48), с. 5–7, 2005.

92. А. И. Елисеев, Ю. В. Минин, Г. Г. Ягудаев, «Графовая модель показателей частных характеристик живучести сетевых информационных структур,» *Вестник Воронежского института МВД России*, № 1, с. 73–78, 2013.

93. А. Г. Додонов, Е. С. Горбачик, М. Г. Кузнецова, «Живучесть компьютерных систем и безопасность информационной инфраструктуры,» *Известия Южного федерального университета. Технические науки*, № 1(76), с. 203–207, 2007.

94. Д. К. Потресов, Д. В. Скоморохов, «Факторы надежности информационных систем высокой готовности,» *Горный информационно-аналитический бюллетень (научно-технический журнал)*, № 5, с. 134–139, 2013.

95. G. B. Digo, N. B. Digo, “Approximation of domains of serviceability and attainability of control system on the basis of the inductive approach,” *Reliability: Theory & Applications*, vol. 6, no. 2(21), pp. 41-46, 2011.

96. A. I. Awad, M. Fairhurst, *Information Security. Foundations, technologies and applications*. USA: The Institution of Engineering and Technology, 2018.

97. M. Bishop, *Computer Security: Art and Science*. 2nd ed. USA: Addison-Wesley Professional, 2018.

98. В. В. Бондарев, *Введение в информационную безопасность автоматизированных систем*. М.: МГТУ им. Н. Э. Баумана, 2016.

99. В. И. Ярочкин, *Информационная безопасность*. Учебник для вузов. 2-е издание. М.: Академический Проект, Гаудеамус, 2004.

100. В. Ф. Шаньгин, *Информационная безопасность*. М.: ДМК Пресс, 2014.

101. С. А. Филин, *Информационная безопасность*. М.: Альфа-Пресс, 2006.
102. О. О. Шумейко, *Інформаційна безпека*. Дніпродзержинськ: Дніпродзержинський державний технічний університет, 2012.
103. О. Б. Проценко, К. В. Меркулова, *Кібербезпека у системі національної безпеки України: пріоритетні напрями розвитку*. Маріуполь: Маріупольський державний університет, 2018.
104. Ю. Н. Сычев, *Стандарты информационной безопасности. Защита и обработка конфиденциальных документов*. М.: РЭУ им. Г. В. Плеханова, 2017.
105. А. А. Парошин, *Информационная безопасность: стандартизированные термины и понятия*. Владивосток: Дальневосточный университет, 2010.
106. В. П. Кириленко, Г. В. Алексеев, *Международное право и информационная безопасность государства*. СПб: СПбГИКиТ, 2016.
107. А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов и др., *Аутентификация. Теория и практика. Обеспечение безопасного доступа к информационным ресурсам*. М.: Горячая линия-Телеком, 2009.
108. О. Р. Лапонина, *Криптографические основы безопасности*, 2-е изд. М.: Национальный Открытый Университет ИНТУИТ, 2016.
109. С. Бармен, *Разработка правил информационной безопасности*. М.: Вильямс, 2002.
110. M. Rausand, *Reliability of Safety-Critical Systems: Theory and Applications*. New Jersey: Wiley, Hoboken, 2014.
111. E. Griffor, *Handbook of System Safety and Security. Cyber Risk and Risk Management, Cyber Security, Threat Analysis, Functional Safety, Software Systems, and Cyber Physical Systems*. Amsterdam: Syngress, 2017.
112. В. В. Липаев, *Надежность и функциональная безопасность комплексов программ реального времени*. Саратов: Вузовское образование, 2015.
113. В. В. Белозеров, А. Ю. Любавский, С. Н. Олейников, *Модели диагностики надежности и безопасности СВТ и АСУ объектов техносферы*. М.: Издательский дом Академия Естествознания, 2015. doi:10.17513/np.133.
114. H. Pham, *Safety and Risk Modeling and Its Applications*. USA: Springer, 2011.
115. D. Antonucci, *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*. USA: Wiley, 2017.

116. А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой, *Управление рисками информационной безопасности*, 2-е изд., испр. М.: Горячая линия-Телеком, 2014.

117. G. C. Wilshusen, *Cybersecurity: Continued Efforts Are Needed to Protect Information Systems Form Evolving Threats: Congressional Statement for the Record*. USA: DIANE Publishing, 2010.

118. K. A. Wager, F. W. Lee, J. P. Glaser, *Managing Health Care Information Systems: A Practical Approach for Health Care Executives*. USA: John Wiley & Sons, 2005.

119. Rainbow Books. *Wikipedia* : web-site. [Online]. Available: https://en.wikipedia.org/wiki/Rainbow_Books Accessed on: August 26, 2019.

120. S. Sumathi, S. Esakkirajan, *Fundamentals of Relational Database Management Systems*. USA: Springer Science & Business Media, 2007.

121. В. А. Сердюк, *Организация и технологии защиты информации : обнаружение и предотвращение информационных атак в автоматизированных системах предприятий*. М.: Издательский дом Высшей школы экономики, 2011.

122. Ю. Н. Загинайлов, *Теория информационной безопасности и методология защиты информации*. Барнаул: Directmedia, 2015.

123. Н. В. Скабцов, *Аудит безопасности информационных систем*. СПб: Питер, 2017.

124. T. R. Peltier, *Information Security Policies and Procedures: A Practitioner's Reference, Second Edition*. USA: CRC Press, 2004.

125. J. L. Bayuk, J. Healey, P. Rohmeyer, *Cyber Security Policy Guidebook*. USA: Wiley, 2012.

126. В И. Шестухина, *Теоретические основы компьютерной безопасности*. Учебное пособие. Хабаровск: ДВГУПС, 2008.

127. А. В. Овчинников, В. Г. Семин, *Обеспечение информационной безопасности автоматизированных систем транснациональных корпораций (АСТК)*. Учеб. пособие. М.: РУДН, 2008.

128. А. Ю. Щеглов, *Модели, методы и средства контроля доступа к ресурсам вычислительных систем*. СПб: Университет ИТМО, 2014.

129. С. В. Белим, С. В. Усов, «Объектно-ориентированный подход в построении дискреционной политики безопасности,» *Математические структуры и моделирование*, № 2(20), с. 153–159, 2009.

130. В. Ю. Мельников, Е. К. Пугачев, *Методы защиты операционных систем и данных*. М.: МГТУ им. Баумана, 2017.

131. В. В. Гуренко, Б. И. Бычков, «Анализ структур данных для представления базовых моделей конечных автоматов,» *Машиностроение и компьютерные технологии*, № 2, с. 150–168, 2015.

132. И. А. Гудкова, Н. Д. Масловская, «Вероятностная модель для анализа задержки доступа к инфраструктуре облачных вычислений с системой мониторинга,» *T-Comm - Телекоммуникации и Транспорт*, № 6, с. 13–15, 2014.

133. Е. А. Рогозин, А. Д. Попов, «Модель функционирования типовой системы защиты информации от несанкционированного доступа в автоматизированных информационных системах ОВД,» *Вестник Воронежского института МВД России*, № 4, с. 122–131, 2016.

134. A. Acquisti, S. Gritzalis, C. Lambrinoudakis, S. Di Vimercati at al., *Digital Privacy. Theory, Technologies, and Practices*. Germany: Auerbach Publications, 2008.

135. В. Ф. Шаньгин, *Защита компьютерной информации. Эффективные методы и средства*. М.: ДМК Пресс, 2010.

136. В. А. Хорошко, А. А. Чекатков, *Методы и средства защиты информации*. К.: Юниор, 2003.

137. В. И. Петренко, *Теоретические основы защиты информации*. Ставрополь: СКФУ, 2015.

138. С. Е. Остапов, С. П. Євсеєв, О. Г. Король, *Технології захисту інформації*. Харків: ХНЕУ, 2013.

139. А. А. Малюк, *Теория защиты информации*. М.: Горячая линия – Телеком, 2012.

140. С. В. Ленков, Д. А. Перегудов, В. А. Хорошко, *Методы и средства защиты информации*. Том 2. Информационная безопасность. К.: Арий, 2008.

141. С. В. Войцеховский, А. С. Марковский, В. А. Палагушин, *Защита информации в автоматизированных системах*. СПб.: Питер, 2005.

142. Б. Ю. Анин, *Защита компьютерной информации*. СПб: БХВ-Петербург, 2000.

143. R. Zeidman, *The Software IP Detective's Handbook: Measurement, Comparison, and Infringement Detection*. UK: Pearson Education, 2011.

144. А. Ю. Зубов, *Математика кодов аутентификации*. М.: Гелиос АРВ, 2007.

145. Основная теорема безопасности Белла-Лападулы. *Википедия* [Электронный ресурс]. Режим доступа::

https://ru.wikipedia.org/wiki/Модель_Белла_—_Лападулы Дата обращения: Авг. 26, 2019.

146. В. С. Симанков, Е. В. Луценко, *Адаптивное управление сложными системами на основе теории распознавания образов*. Краснодар: ТУ КубГТУ, 1999.

147. И. В. Мирошник, *Теория автоматического управления. Линейные системы*. СПб: Питер, 2005.

148. В. Н. Афанасьев, *Управление неопределенными системами*. М.: РУДН, 2008.

149. И. В. Мирошник, В. О. Никифоров, А. Л. Фрадков, *Нелинейное и адаптивное управление сложными динамическими системами*. СПб: Наука, 2000.

150. Y. Haimes, *Modeling and Managing Interdependent Complex Systems of Systems*. USA: Wiley-IEEE Press, 2019.

151. E. E. N. Macau, *A Mathematical Modeling Approach from Nonlinear Dynamics to Complex Systems*. USA: Springer, 2019.

152. Q. Zhu, A. T. Taher Azar, *Complex System Modelling and Control Through Intelligent Soft Computations*. USA: Springer, 2015.

153. A. Ioannou Petros, A. Pitsillides, *Modeling and Control of Complex Systems*. USA: CRC Press, Taylor & Francis Group, 2008.

154. J. Lü, X. Yu, G. Chen, W. Yu, *Complex Systems and Networks: Dynamics, Controls and Applications*. Berlin, Heidelberg: Springer-Verlag, 2016.

155. T. R. J. Bossomaier, D. G. Green, *Complex Systems*. UK: Cambridge University Press, 2000.

156. M. Davoodi, N. Meskin, K. Khorasani, *Integrated Fault Diagnosis and Control Design of Linear Complex Systems*. New York: The Institution of Engineering and Technology, 2017.

157. G. G. Schulmeyer at al., *Handbook of Software Quality Assurance*. Fourth Edition. USA: Artech House, 2007.

158. D. Galin, *Software Quality: Concepts and Practice*. USA: Wiley, 2018.

159. Б В. Черников, *Управление качеством программного обеспечения*. М.: Форум, 2012

160. Б В. Черников, *Управление качеством программного обеспечения*. М.: Форум, 2012.

161. J. A. Anderson, *Automata Theory with Modern Applications*. UK: Cambridge University Press, 2006.

162. J. E. Hopcroft, R. Motwani, J. D. Ullman, *Introduction to Automata Theory, Languages, and Computation*. 2nd Edition. UK: Pearson Publication, 2000.

163. J.-É. Pin, *Mathematical Foundations of Automata Theory*. Paris: Jean-Eric Pin, 2016.

164. Д. Хопкрофт, Р. Мотвани, Дж. Ульман, *Введение в теорию автоматов, языков и вычислений*. 2-е изд. М.: Вильямс, 2002.

165. A. Bondy, U. S. R. Murty, *Graph Theory*. USA: Springer, 2008.

166. L. Novak, A. Gibbons, *Hybrid Graph Theory and Network Analysis*. UK: Cambridge University Press, 1999.

167. Д. В. Карпов, *Теория графов*. СПБ: Санкт-Петербургское отделение Мат. института им. В. А. Стеклова РАН, 2017.

168. Н. П. Хоменко, *Топологические аспекты теории графов*. К.: Издание Института математики АН УССР, 1971.

169. А. Е. Пентус, М. Р. Пентус, *Математическая теория формальных языков*. М.: Интернет-университет информационных технологий; БИНОМ. Лаборатория знаний, 2006.

170. G. Bel-Enguix, M. D. Jiménez-López, *New Developments in Formal Languages and Applications*. USA: Springer, 2008.

171. S. C. Reghizzi, *Formal Languages and Compilation*. USA: Springer, 2009.

172. D. H. Greene, D. E. Knuth, *Mathematics for the Analysis of Algorithms*. Germany: Birkhauser, 2008.

173. L. Parida, *Pattern Discovery in Bioinformatics. Theory & Algorithms*. USA: Chapman & Hall / CRC Press, 2008.

174. В. Н. Крупский, В. Е. Плиско, *Теория алгоритмов*. М.: Академия, 2009.

175. В. И. Игошин, *Математическая логика и теория алгоритмов*. 2-е изд. М.: Академия, 2008.

176. P. Gatti, *Probability theory and mathematical statistics for engineers*. Londonand New-York: Spon Press. 2005.

177. A. A. Borovkov, *Probability Theory*. USA: Springer, 2013.

178. W. Linde, *Probability Theory: A First Course in Probability Theory and Statistics*. Germany: Walter de Gruyter GmbH, 2016.

179. Н. Г. Тактаров, *Теория вероятностей и математическая статистика: Краткий курс с примерами и решениями*. М.: УРСС, 2010.

180. В. Н. Тарасов, Н. Ф. Бахарева, *Теория вероятностей, математическая статистика и случайные процессы*. 3-е изд. Самара: Изд-во ПГУТИ, 2017.

181. W. Penczek, A. Półrola, *Advances in Verification of Time Petri Nets and Timed Automata. A Temporal Logic Approach*. USA: Springer, 2006.

182. N. Wu, M. Zhou, *System Modeling and Control with Resource-Oriented Petri Nets*. USA: CRC Press, 2006.

183. K. Jensen, *Coloured Petri Nets*. USA: Springer, 2009.

184. T. Aized, *Advances in Petri Net: Theory and Applications*. Pakistan: InTechOpen, 2010.

185. Дж. Питерсон, *Теория сетей Петри и моделирование систем*. М.: Мир, 1984.

186. MengChu Zhou, *Petri Nets in Flexible and Agile Automation*. USA: Springer Science & Business Media, 2012.

187. E. Badouel, L. Bernardinello, P. Darondeau, *Petri Net Synthesis*. USA: Springer, 2015.

188. E. Best, R. Devillers, M. Koutny, *Petri Net Algebra*. USA: Springer Science & Business Media, 2001.

189. J. Janssen, *Semi-Markov Models: Theory and Applications*. USA: Springer, 2013.

190. B. Harlamov, *Continuous Semi-Markov Processes*. USA: Wiley, 2008.

191. V. S. Barbu, N. Limnios, *Semi-Markov Chains and Hidden Semi-Markov Models toward Applications: Their use in Reliability and DNA Analysis*. USA: Springer, 2008.

192. S.-Z. Yu, *Hidden Semi-Markov Models: Theory, Algorithms and Applications*. Amsterdam: Elsevier, 2016.

193. Теорема Радона-Нікодима *Вікіпедія* [Електронний ресурс]. Режим доступу: https://uk.wikipedia.org/wiki/Теорема_Радона_—_Нікодима Дата звернення: серпень, 26, 2019.

194. О. Ю. Мєшков, О. О. Новіков, В. О Новіков, *Аналіз голосових сигналів людини та аутентифікація особистості за голосом*. Херсон: ФОП Вишемирський В. С., 2018.

195. М. Н. Григорьев, С. А. Уваров, *Логистика*. 4-е изд. М.: Юрайт, 2019.

196. Кардинг *Вікіпедія* [Електронний ресурс]. Режим доступу: https://uk.wikipedia.org/wiki/Кардинг Дата звернення: серпень, 26, 2019.

197. Корпус української мови MOVA.info [Електронний ресурс]. Режим доступу: http://www.mova.info/carticle.aspx?l1=210&DID=5347 Дата звернення: серпень, 26, 2019.

198. Генеральний регіонально анотований корпус української мови [Электронный ресурс]. Режим доступу: http://uacorpus.org/ Дата звернення: серпень, 26, 2019..

199. А. Н. Продеус, «Речевые корпуса: создание и проблемы,» *Электротехнические и компьютерные системы*, № 9(85), с. 118–126, 2013.

200. A. Bouziane, H. Kadi, S. Hourri, J Kharroubi, "An open and free speech corpus for speaker recognition: The FSCSR speech corpus," *Proc. 11th International Conference on Intelligent Systems: Theories and Applications (SITA)*, pp. 1–5, 2016. doi: 10.1109/SITA.2016.7772320.

201. J. P. Campbell, D. A. Reynolds, "Corpora for the evaluation of speaker recognition systems," *IEEE International Conference on Acoustics, Speech, and Signal Processing. Proceedings. ICASSP99 (Cat. No.99CH36258)*, pp. 829–832, 1999. doi:10.1109/icassp.1999.759799.

202. M. Tatham, K. Morton, *Speech Production and Perception*. UK: Palgrave, 2006.

203. W. J. Hardcastle, A. Marchal, *Speech Production and Speech Modelling*. Netherlands: Kluwer, 1990.

204. S. E. Levinson, *Mathematical Models for Speech Technology*. USA: John Wiley & Sons, 2005.

205. Jay Timothy, *Why We Curse: A Neuro-Psycho-Social Theory of Speech*. Netherlands: John Benjamins Publishing, 2000.

206. L. Deng, *Dynamic Speech Models. Theory, Algorithms, and Applications*. California: Morgan & Claypool, 2006.

207. W. Hess, *Pitch Determination of Speech Signals. Algorithms and Devices*. USA: Springer, 1983.

208. S. Seneff, *Pitch and Spectral Analysis of Speech Based on an Auditory Synchrony Model*. Barcelona: Universitat Politècnica de Catalunya, 1985.

209. D. M. Howard, J. A. S. Angus, *Acoustics and Psychoacoustics. Fourth edition*. Massachusetts: Focal Press, 2010.

210. H. Fastl, E. Zwicker, *Psychoacoustics. Facts and Models*. Germany: Springer-Verlag, 2007.

211. Я. А. Альтман и др., *Слуховая система. Основы современной физиологии*. Л.: Наука, 1990.

212. А. Б. Сергиенко, *Цифровая обработка сигналов*. СПБ: БХВ-Петербург, 2011.

213. А. И. Солонина, *Цифровая обработка сигналов. Моделирование в MATLAB*. СПб: БХВ-Петербург, 2008.

214. F. E. Theunissen, K. Sen, A. J. Doupe, “Spectral-Temporal Receptive Fields of Nonlinear Auditory Neurons Obtained Using Natural Sounds,” *Journal of Neuroscience*, № 20(6), pp. 2315–2331, 2000. doi:10.1523/JNEUROSCI.20-06-02315.2000.

215. S. Handel, *Perceptual Coherence: Hearing and Seeing*. UK: Oxford University Press, 2006.

216. M. S. Malmierca, D. R. F. Irvine, *Auditory Spectral Processing*. Texas: Gulf Professional Publishing, 2005.

217. L. Zhao, L. Zhaoping, “Understanding Auditory Spectro-Temporal Receptive Fields and Their Changes with Input Statistics by Efficient Coding Principles,” *PLoS Computational Biology*, № 7(8), e1002123, 2011. doi:10.1371/journal.pcbi.1002123.

218. J. Benesty, M. M. Sondhi, Y. Huang, *Springer Handbook of Speech Processing*. USA: Springer, 2008.

219. Р. Габасов, Ф. М. Кириллова, *Основы динамического программирования*. Минск: Изд-во БГУ, 1975.

220. Р. Арис, *Дискретное динамическое программирование*. М.: Мир, 1969.

221. Дж. Хедли, *Нелинейное и динамическое программирование*. М.: Мир, 1967.

222. Х. Бринк, Дж. Ричардс, М. Феверолф, *Машинное обучение*. СПБ: Питер, 2017.

223. В. В. Вьюгин, *Математические основы теории машинного обучения и прогнозирования*. М.: МЦНМО, 2013.

224. Гифт Ной, *Прагматичный ИИ. Машинное обучение и облачные технологии*. СПБ: Питер, 2019.

225. Ф. Шолле, *Глубокое обучение на Python*. СПБ: Питер, 2018.

226. Э. Траск, *Грокаем глубокое обучение*. СПБ: Питер, 2019.

227. Л. Р. Рабинер, Р. В. Шафер, *Цифровая обработка речевых сигналов*. М.: Радио и связь, 1981.

228. М. А. Сапожков, В. Г. Михайлов, *Вокодерная связь*. М.: Радио и связь, 1983.

229. К. Фукунага, *Введение в статистическую теорию распознавания образов*. М.: Наука, 1979.

230. Э. А. Патрик, *Основы теории распознавания образов*. М.: Советское радио, 1980.

231. Дж. Ту, Р. Гонсалес, *Принципы распознавания образов*. М.: Мир, 1978.

232. Р. Дуда, П. Харт, *Распознавание образов и анализ сцен*. М.: Мир, 1976.

233. Т. К. Вінцюк, М. М. Сажок, Р. А. Селюх, Д. Я. Федорин, О. А. Юхименко, В. В. Робейко, «Автоматичне розпізнавання, розуміння та синтез мовленнєвих сигналів в Україні,» *Управляющие системы и машины*, № 6. с. 7–24, 2018.

234. В. В. Булатов, *Введение в математические методы моделирования сложных систем*. М.: ОнтоПринт, 2018.

235. И. В. Кузьмин, *Основы моделирования сложных систем*. К.: Вища школа, 1980.

236. В. П. Тарасик, *Математическое моделирование технических систем*. Минск: Дизайн-ПРО, 2004.

237. А. А. Харкевич, *Основы радиотехники*. 3-е издание, стереотипное. М.: Физматлит, 2007.

238. М. В. Амалицкий, *Основы радиотехники*. 3-е издание. М.: Связьиздат, 1959.

239. В. И. Тихонов, *Статистическая радиотехника*. М.: Рипол Классик, 2013.

240. Л. Е. Варакин, *Теория сложных сигналов*. М.: Рипол Классик, 1970.

241. T. Herbig, F. Gerl, W. Minker, *Self-Learning Speaker Identification. A System for Enhanced Speech Recognition*. USA: Springer, 2011.

242. F. E. El-Samie, *Information Security for Automatic Speaker Identification*. USA: Springer, 2011.

243. T. B. Alderman, *Forensic Speaker Identification: A Likelihood Ratio-based Approach Using Vowel Formants*. EU: Lincom Europa, 2005.

244. L. F. Gallardo, *Human and Automatic Speaker Recognition over Telecommunication Channels*. USA: Springer, 2014.

245. J. Keshet, S. Bengio, *Automatic Speech and Speaker Recognition. Large Margin and Kernel Methods*. USA: Wiley, 2009.

246. D. D. Zhang, *Automated Biometrics. Technologies and Systems*. Netherlands: Kluwer, 2000.

247. P. Rose, *Forensic Speaker Identification*. UK: Taylor & Francis, 2002.

248. A. Neustein, H. A. Patil, *Forensic Speaker Recognition. Law Enforcement and Counter-Terrorism*. USA: Springer, 2012.

249. H. Beigi, *Fundamentals of Speaker Recognition*. USA: Springer, 2011.

250. В. В. Волгин, Р. Н. Каримов, *Оценка корреляционных функций в промышленных системах управления*. М.: Энергия, 1979.

251. Е. Н. Львовский, *Статистические методы построения эмпирических функций*. М.: Высшая школа, 1988.
252. Ю. И. Алимов, *Измерение спектров и статистических вероятностей*. Свердловск: Изд-во Уральского политехнического ин-та, 1986.
253. Г. Дженкинс, *Спектральный анализ и его приложения*. М.: Мир,1971.
254. К. Раушер, Ф. Йанссен, Р. Минихольд, *Основы спектрального анализа*. М.: Горячая линия-Телеком, 2006.
255. А. М. Крот, Е. Б. Минервина, *Быстрые алгоритмы и программы спектральной обработки сигналов и изображений*. Минск: Навука і тэхніка, 1995.
256. М. В. Назаров, Ю. Н. Прохоров, *Методы цифровой обработки и передачи речевых сигналов*. М.: Радио и связь, 1985.
257. Д. Маркел, А. Х. Грей, *Линейное предсказание речи*. М.: Связь, 1980.
258. О. И. Шелухин, Н. Ф. Лукьянцев, *Цифровая обработка и передача речи*. М.: Радио и связь, 2000.
259. Н. К. Обжелян, В. Н. Трунин-Донской, *Машины, которые говорят и слушают*. Кишинёв: Штиинца, 1987.
260. Дж. Бокс, Г. Дженкинс, *Анализ временных рядов прогноз и управление*. Кн.1. М.: Мир, 1974.
261. С. Малла, *Вейвлеты в обработке сигналов*. М.: Мир, 2005.
262. А. В. Фролов, Г. В. Фролов, *Синтез и распознавание речи. Современные решения*. М.: Связь, 2003.
263. Ю. Ю. Громов, О. Г. Иванова, В. О. Драчев, В. В. Алексеев, *Фрактальный анализ и процессы в компьютерных сетях*. Тамбов: ТГТУ, 2012.
264. В. Н. Сорокин, *Синтез речи*. М.: Наука, 1992.
265. Дж. Л. Фланаган, *Анализ, синтез и восприятие речи*. М.: Связь, 1968.
266. N. R. Shabtai, *Advances in Speech Recognition*. Pakistan: InTech, 2010.
267. A. J. Rubio Ayuso, J. M. Lopez Soler, *Speech Recognition and Coding. New Advances and Trends*. USA: Springer, 1995.
268. F. Mihelič, J. Žibert, *Speech Recognition. Technologies and Applications*. Pakistan: InTech, 2008.
269. Z.-H. Tan, B. Lindberg, *Automatic Speech Recognition on Mobile Devices and over Communication Networks*. USA: Springer, 2008.

270. С. Е. Фалькович, Э. И. Хомяков, *Статистическая теория измерительных радиосистем*. М.: Радио и связь, 1981.

271. А. Н. Лукин, *Радиофизические методы измерения параметров сложных источников излучения* : дис. докт. физ.-мат. наук : 01.04.03 / Воронеж, 1998.

272. Г. Корн, *Справочник по математике для научных работников и инженеров*. М.: Наука, 1973.

273. И. Н. Бронштейн, К. А. Семендяев, *Справочник по математике для инженеров и учащихся втузов*. 10-е издание. М.: Наука, 1964.

274. В. И. Тихонов, Н. К. Кульман, *Нелинейная фильтрация и квазикогерентный прием сигналов*. М.: Советское радио, 1975.

275. Э. С. Айфичер, Б. У. Джервис, *Цифровая обработка сигналов: практический подход*. М.: Вильямс, 2004.

276. Преобразование Гильберта *Википедия* [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/Преобразование _Гильберта Дата обращения: Авг. 26, 2019.

277. Критерий Бартлетта *Википедия* [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/Критерий_Бартлетта Дата обращения: Авг. 26, 2019..

278. Ю. Н. Прохоров, *Статистические модели и рекуррентное предсказание речевых сигналов*. М.: Радио и связь, 1984.

279. Ю. Г. Сосулин, *Теория обнаружения и оценивания стохастических сигналов*. М.: Сов. радио, 1978.

280. И. Д. Мандель, *Кластерный анализ*. М.: Финансы и статистика, 1988.

281. М. Кендалл, А. Стьюарт, *Статистические выводы и связи*. М.: Наука, 1973.

282. NOIZEUS: Noisy speech corpus – Univ. Texas-Dallas [Online]. Available: https://ecs.utdallas.edu/loizou/speech/noizeus/ Accessed on: August 26, 2019.

283. Ф. Р. Гантмахер, *Теория матриц*. М.: ФИЗМАТЛИТ, 2004. 560 с.

284. В. Н. Тарасов, Н. Ф. Бахарева, *Математическое программирование. Теория, алгоритмы, программы*. Самара: Гольфстрим, 2007.

285. А. М. Загребаев и др., *Методы математического программирования в задачах оптимизации сложных технических систем*. М.: МИФИ, 2007.

286. А. В. Кузнецов, В. А. Сакович, Н. И. Холод, *Высшая математика. Математическое программирование*. 4-е изд., стер. СПб: Лань, 2013.

287. Е. Янке, Ф. Эмде, Ф. Лёш, *Специальные функции*. М.: Наука, 1977.

288. В. Ю. Королёв, *EM-алгоритм, его модификации и применение к задаче разделения смесей вероятностных распределений*. М.: ИПИ РАН, 2007.

289. Р. Н. Вадзинский, *Справочник по вероятностным распределениям*. М.: Наука, 2001.

290. M. N. Stuttle, *A Gaussian Mixture Model Spectral Representation for Speech Recognition*. UK: Cambridge University, 2003.

291. A. Salazar, *On Statistical Pattern Recognition in Independent Component Analysis Mixture Modelling*. USA: Springer, 2013.

292. Unsupervised Machine Learning in Python. Master Data Science and Machine Learning with Cluster Analysis, Gaussian Mixture Models, and Principal Components Analysis. LazyProgrammer, 2016. 66 p. [Online]. Available: https://lazyprogrammer.me/ Accessed on: August 26, 2019.

293. А. В. Аграновский, Д. А. Леднов, *Теоретические аспекты алгоритмов обработки и классификации речевых сигналов*. М.: Радио и связь, 2004.

294. M. R. Gupta, Y. Chen, *Theory and Use of the EM Algorithm*. Boston: NOWPress, 2011.

295. Ch. D. Manning, P. Raghavan, H. Schütze, *Introduction to Information Retrieval*. UK: Cambridge University Press, 2008.

296. Р. В. Шамин, *Практическое руководство по методам машинного обучения*. М.: Lector.ru, 2019.

297. S. J. Godsill, P. J. W. Rayner, *Digital Audio Restoration - a Statistical Model Based Approach*. USA: Springer, 1998.

298. B. Xiang, *Acoustic modeling for efficient speaker verification*. UK: Cornell University, 2003.

299. M. A. Pathak, *Privacy-Preserving Machine Learning for Speech Processing*. USA: Springer Science & Business Media, 2012.

300. В. М. Буре, Е. М. Парилина, А. А Седаков, *Теория вероятностей и вероятностные модели*. СПб: Лань, 2018.

301. А. Б. Мерков, *Распознавание образов. Построение и обучение вероятностных моделей*. М.: Ленанд, 2014.

302. В. Г. Лисиенко, О. Г. Трофимова, С. П. Трофимов, Н. Г. Дружинина, П. А. Дюгай, *Моделирование сложных вероятностных систем*. Екатеринбург: УРФУ, 2011.
303. В. В. Губарев, *Вероятностные модели*. Часть 1. Новосибирск: Новосибирский электротехн. ин-т, 1992.
304. В. В. Губарев, *Вероятностные модели*. Часть 2. Новосибирск: Новосибирский электротехн. ин-т, 1992.
305. М. А. Федоткин, *Построение вероятностных моделей*. Нижний Новгород: Нижегородский госуниверситет, 2012.
306. Р. Е. Саркисян, *Системный анализ и принятие решений*. Часть 3. Вероятностные модели и методы. Неформальные правила решения. Диалоговые модели многокритериальной оптимизации. М.: МИИТ, 2009.
307. П. И. Тутубалин, В. С. Моисеев, *Вероятностные модели обеспечения информационной безопасности автоматизированных систем обработки информации и управления*. Казань: РИЦ Школа, 2008.
308. Т. Сегаран, *Программируем коллективный разум*. СПб: Символ-Плюс, 2008.
309. S. Abe, *Support Vector Machines for Pattern Classification*. USA: Springer, 2010.
310. I. Steinwart, A. Christmann, *Support Vector Machines*. USA: Springer, 2008.
311. Y. Ma, G. Guo, *Support Vector Machines Applications*. USA: Springer, 2014.
312. C. Campbell, Y. Ying, *Learning with Support Vector Machines*. California: Morgan & Claypool, 2011.
313. Теорема Мерсера *MachineLearning.ru* [Электронный ресурс]. Режим доступа: http://www.machinelearning.ru/wiki/index.php?title=Теорема_Мерсера Дата обращения: Авг. 26, 2019.
314. Розходження Кульбака-Лейблера *Вікіпедія* [Електронний ресурс]. Режим доступу: https://uk.wikipedia.org/wiki/Розходження_Кульбака_—_Лейблера Дата звернення: серпень, 26, 2019.
315. Бхаттачариа расстояние - Bhattacharyya distance *qwerty.wiki* [Электронный ресурс]. Режим доступа: https://ru.qwerty.wiki/wiki/Bhattacharyya_distance Дата обращения: Авг. 26, 2019.
316. N. Dehak, R. Dehak, P. Kenny, N. Brummer, P. Ouellet, P. Dumouchel, “Support Vector Machines versus Fast Scoring in the Low-Dimensional Total Variability Space for Speaker Verication,” *InterSpeech*, pp. 1559–1562, 2009.

317. Алгоритм Баума-Велша *Википедия* [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/Алгоритм_Баума_—_Велша Дата обращения: Авг. 26, 2019.

318. The Microsoft Cognitive Toolkit - Cognitive Toolkit - CNTK Microsoft Azure [Электронный ресурс]. Режим доступа: https://docs.microsoft.com/en-us/cognitive-toolkit/ Дата обращения: Авг. 26, 2019.

319. L. Lu, Y. Zheng, G. Carneiro, L. Yang, *Deep Learning and Convolutional Neural Networks for Medical Image Computing: Precision Medicine, High Performance and Large-Scale Datasets*. USA: Springer International Publishing, 2017.

320. M. Sewak, Md. R. Karim, P. Pujari. Practical Convolutional Neural Networks. Packt Publishing, 2018.

321. A. Menshawy, *Deep Learning By Example: A Hands-on Guide to Implementing Advanced Machine Learning Algorithms and Neural Networks*. UK: Packt, 2018.

322. H. Zou, T. Hastie, R. Tibshirani, "Sparse Principal Component Analysis," *Journal of Computational and Graphical Statistics*, № 15(2), pp. 265–286, 2006. doi:10.1198/106186006x113430.

323. U. Khan, P. Safari, J. Hernando, "Restricted Boltzmann Machine Vectors for Speaker Clustering and Tracking Tasks in TV Broadcast Shows," *Applied Sciences*, № 9(13). pp. 2761, 2019. doi:10.3390/app9132761.

324. N. Zhang, S Ding., J. Zhang, Y. Xue. An overview on Restricted Boltzmann *Machines. Neurocomputing*. no. 275, pp. 1186–1199, 2018. doi:10.1016/j.neucom.2017.09.065.

325. Y. Zhang, X. Gao, X. Peng, J. Ye, X. Li, "Attention-Based Recurrent Temporal Restricted Boltzmann Machine for Radar High Resolution Range Profile Sequence Recognition," *Sensors*, no. 18(5), pp. 1585, 2018. doi:10.3390/s18051585.

326. S. K. Kim, L. C. McAfee, P. L. McMahon, K. A. Olukotun, "A highly scalable Restricted Boltzmann Machine FPGA implementation," *2009 International Conference on Field Programmable Logic and Applications*, pp. 367–372, 2009. doi:10.1109/fpl.2009.5272262.

327. C. Vielhauer, *Biometric User Authentication for IT Security. From Fundamentals to Handwriting*. USA: Springer, 2006.

328. D. R. Kisku, P. Gupta, J. K. Sing, *Advances in Biometrics for Secure Human Authentication and Recognition*. USA: CRC Press, 2014.

329. S. O. Thian, C. Tee, S. M. Shohel, *Security and Authentication*. USA, NY: Nova Science Publishers, Inc., 2017.

330. I. F. Blake, G. Seroussi, N. P. Smart, *Advances in Elliptic Curve Cryptography*. UK: Cambridge University Press, 2005.

331. J. H. Silverman, *The Arithmetic of Elliptic Curves*. 2nd Edition. USA: Springer Science & Business Media, 2009.
332. Darrel R. Hankerson, Alfred J. Menezes, Scott A. Vanstone, *Guide to Elliptic Curve Cryptography*. USA: Springer, 2004.
333. К. Хоггер, *Введение в логическое программирование*. М.: Мир, 1988.
334. K. Scarfone, D. Benigni, T. Grance. Cyber Security Standards. [Online]. Available: https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=152153 Accessed on: August 26, 2019.
335. M. M. Alani, *Guide to OSI and TCP/IP Models*. USA: Springer, 2014.
336. McM. Troy, *Cisco Networking Essentials. Textbook*, Second Edition. USA: Wiley, 2015.
337. P. Bernus, K. Mertins, G. Schmidt, *Handbook on Architectures of Information Systems*. USA: Springer, 2006.
338. Á. Rocha et al., *Advances in Information Systems and Technologies*. USA: Springer, 2013.
339. Christos Kalloniatis, *Modern Information Systems*. Pakistan: InTech, 2012.
340. K. Klinger, Enterprise Information Systems: Concepts, Methodologies, Tools and Applications. France: Information Science Reference, 2011.
341. R. Pooley et al., *Information Systems Development: Reflections, Challenges and New Directions*. USA: Springer, 2013.
342. A. Gunasekaran, *Modeling and Analysis of Enterprise Information Systems*. France: IGI Global, 2007.
343. B. S. Dhillon, *Robot System Reliability and Safety: A Modern Approach*. USA: CRC Press, 2015.
344. А. П. Кирпичников, *Методы прикладной теории массового обслуживания*. М.: УРСС, 2018.
345. В. Ф. Матвеев, В. Г. Ушаков, *Системы массового обслуживания*. М.: Изд-во МГУ, 1984.
346. А. А. Назаров, А. Ф. Терпугов, *Теория массового обслуживания*. Томск: Изд-во НТЛ, 2004.
347. Л. Клейнрок, *Теория массового обслуживания*. М.: Машиностроение, 1979.
348. Р. Г. Асадуллаев, *Нечеткая логика и нейронные сети*. Белгород: БелГУ, 2017.
349. В. В. Круглов, М. И. Дли, Р. Ю. Голунов, *Нечеткая логика и искусственные нейронные сети*. М.: ФИЗМАТЛИТ, 2001.

Наукове видання

Ковтун В'ячеслав Васильович

МОДЕЛІ АТРИБУТІВ ГАРАНТОЗДАТНОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ КРИТИЧНОГО ЗАСТОСУВАННЯ ІЗ АВТЕНТИФІКАЦІЄЮ СУБ'ЄКТА ЗА ГОЛОСОМ

Монографія

Редактор С. Малішевська

Оригінал-макет підготовлено В. Ковтуном

Підписано до друку 4.02.2020 р.
Формат 29,7×42¼. Папір офсетний.
Гарнітура Times New Roman.
Друк різографічний. Ум. др. арк. 23,79.
Наклад 300 (1-й запуск 1–75) пр. Зам № В2020-01

Вінницький національний технічний університет,
ІРВЦ ВНТУ,
21021, м. Вінниця, Хмельницьке шосе, 95,
ВНТУ, ГНК, к. 114.
Тел. (0432) 59-85-32.
press.vntu.edu.ua; *email*: kivc.vntu@gmail.com.
Свідоцтво суб'єкта видавничої справи
серія ДК № 3516 від 01.07.2009 р.

Віддруковано ФОП Барановська Т. П.
21021, м. Вінниця, вул. Порика, 7.
Свідоцтво суб'єкта видавничої справи
серія ДК № 4377 від 31.07.2012 р.