https://doi.org/10.31649/1997-9266-2018-141-6-77-89

УДК 681.327.12

В. В. Ковтун[1]

МОДЕЛЮВАННЯ ЗАЛЕЖНОСТІ КОНФІДЕНЦІЙНОСТІ АВТЕНТИФІКАЦІЇ І ДОСТУПНОСТІ У ІНФОРМАЦІЙНІЙ СИСТЕМІ КРИТИЧНОГО ЗАСТОСУВАННЯ

[1]Вінницький національний технічний університет

Сучасні тенденції до організації процесу автентифікації у інформаційних системах критичного застосування орієнтовані перш за все на підвищення його надійності, втім, такий підхід входить у суперечність з домінуючою у сфері інформаційної безпеки тріадою CIA, зокрема, у суперечність входять, перший і третій компоненти тріади. Отже, виникає потреба у формалізації математичного апарату який би дозволив описати залежність між конфіденційністю комплексної ступінчастої процедури автентифікації та доступністю ресурсів інформаційної системи критичного застосування, що б дозволило гнучкіше налаштовувати роботу підсистеми розмежування доступу відповідно до умов експлуатації інформаційної системи. У статті вперше запропоновано модель залежності втрат конфіденційності процесу автентифікації і показника доступності інформаційної системи критичного застосування, яка на відміну від існуючих формалізує як задачу математичного програмування процес синтезу оптимальної напівмарковської стратегії управління прийняттям рішень у марковському процесі автентифікації суб'єктів, що бажають отримати доступ до ресурсів інформаційної системи критичного застосування, що дозволяє мінімізувати втрати доступності процесу автентифікації, конфіденційність якого не повинна знизитися нижче заданого адміністратором порогового значення. Сформульовано методику застосування вищеописаної моделі, вважаючи, що у системній політиці безпеки описано ситуації «критична помилка» і «підозра на помилку», які можуть ідентифікуватися підсистемою розмежування доступу під час перебігу процесу автентифікації. Згадані ситуації визначено з урахуванням того, що підсистема розмежування доступу має ступінчасту, комплексну, послідовно з'єднану блочну структуру, а кожен блок-ступінь підсистеми включає відповідні підблоки виділення інформативних ознак і класифікації, об'єднані у ансамбль. Проведені з використанням створеної моделі експерименти показали, що зі зменшенням вимог щодо строгості процесу автентифікації доступність інформаційної системи критичного застосування зростає, але після досягнення пороговим значенням втрат конфіденційності рівня $\alpha \approx 10 \cdot 10^{-2}$ зростання доступності припиняється. Це можна пояснити остаточним завершенням процесу адаптації підсистеми розмежування доступу до індивідуальних особливостей суб'єктів, на розпізнавання яких навчали систему. Виявилося, що за малих значень α доступність інформаційної системи критичного застосування є порівняно низькою, що зумовлено реєстрацією великої кількості ситуацій «критична помилка» і «підозра на помилку», на опрацювання яких витрачається час. Підсистеми розмежування доступу, основані на найпростіших (персептронних) і найскладніших (GMM-HMM) класифікаторах, забезпечують найнижчі показники доступності за малих значень α, що зумовлено реєстрацією великої кількості ситуацій «критична помилка» у першому і великої кількості ситуацій «підозра на помилку» у другому випадках. Нарешті, найкращі показники щодо доступності за будь-яких значень α показали підсистеми розмежування доступу, основані на глибоких і глибоких згортальних нейромережах, ефективність яких у задачах біометричної ідентифікації суб'єктів за індивідуальними особливостями їх голосів виявилася найвищою.

Ключові слова: інформаційна система критичного застосування, процес автентифікації, підсистема розмежування доступу, системна політика безпеки, конфіденційність, доступність.

Вступ

Практичне впровадження інформаційних систем у прикладні галузі підтримки функціонування суспільних інститутів держави, сферу зберігання конфіденційної інформації призвело до поступового виділення похідного класу інформаційних систем — інформаційних систем критичного застосування (ІСКЗ). На сьогодні вичерпного, математично формалізованого, загальновизнаного

визначення ІСКЗ немає. Зокрема, зараз розглядаються проекти внесення змін у Закон України «Про основи національної безпеки України» з метою формулювання положень критичної інформаційної інфраструктури України та заходів її убезпечення. У наукових публікаціях в залежності від масштабу аналізу до ІСКЗ відносять моделі автоматизованих систем управління критично важливих об'єктів, моделі критичної інформаційної інфраструктуру держави, моделі прикладних інформаційних систем, ресурси яких являють значну цінність для визначеного кола зацікавлених суб'єктів.

У роботі [1] автор формалізував поняття автоматизованої системи розпізнавання мовця критичного застосування (АСРМКЗ), як системи біометричної ідентифікації, яка гарантує обмовлену у системній політиці безпеки достовірність розпізнавання особи мовця за дотримання умов експлуатації. Критичне застосування інформаційної системи обумовлює жорсткі вимоги до забезпечення її інформаційної безпеки. В широкому сенсі під інформаційною безпекою розуміють систему заходів щодо запобігання несанкціонованому доступу, використання, розкриття, спотворення, зміні або знищення інформації. Конкретніше визначення інформаційної безпеки втілено у домінуючу на сьогодні тріаду CIA [2]: «конфіденційність», «цілісність», «доступність», що розуміють як збалансований захист конфіденційності, цілісності і доступності даних без шкоди продуктивності роботи підприємства, де захист впроваджується. Під конфіденційністю розуміють чітку відповідність рівня інформаційного доступу встановленій в результаті процедури автентифікації ролі суб'єкта, що авторизується. Під цілісністю розуміють постійне гарантування достовірності інформаційного простору і даних підприємства. Під доступністю розуміють забезпечення безперешкодного доступу до інформації суб'єкт, автентичність якого доведено результатами авторизації, відповідно до присвоєній йому адміністратором ролі.

Зазвичай інформаційну безпеку представляють як багатоетапний процес управління ризиками, який ідентифікує структуру організації інформаційного простору підприємства, джерела загроз, вразливості, потенційні ступені впливу і можливості управління ризиками. Актуальні методики оцінювання ризиків інформаційної безпеки можна умовно розділити на стандартизовані та наукові. Перші, здебільшого, базуються на якісному підході до управління ризиками із застосуванням різноманітних таблиць зі шкалами значень ризику. У світовій практиці найуживанішими є методики, наведені у стандартах ISO/IEC 27005:2011 [3], NIST SP800-30 [4], OCTAVE [5], EBIOS [5]. Наприклад, у міжнародному стандарті ISO/IEC 31010 [7] наведено понад 30 підходів до аналізу та оцінки ризиків. До недоліків зазначених підходів можна віднести їх жорсткість, надмірну комплексність і швидке старіння. Наукові методики здебільшого, базуються на різноманітних методах кількісного аналізу із застосуванням відповідного математичного апарату, а саме: теорії імовірності [8], мереж Петрі [8], теорії нечіткої логіки [8], нейронних мереж [8] тощо. Втім, спільним для всіх цих методів є універсальність, що приводить до необхідності їх адаптації при спробах застосування для опису специфічних класів інформаційних систем, до яких відноситься і інформаційна система критичного застосування (ІСКЗ) [9]. При чому часто адаптація можлива лише після створення проміжної моделі-інтерфейсу, яка може виявитися складнішою за саму модель оцінювання ризику. Також ці підходи розглядають процеси оцінювання ризиків конфіденційності і доступності як незалежні задачі. Отже, враховуючи вищезгадані обставини, можна констатувати відсутність моделі оцінювання залежності конфіденційності і доступності у ІСКЗ, а актуальність цієї задачі обумовлює доцільність досліджень для її ідентифікації.

Постановка задачі дослідження

Нехай у рамках тріади CIA безпека інформаційної системи визначається, зокрема такими характеристиками як конфіденційність і доступність. Ці показники значною мірою антогонічні — збільшення одного приводить до зменшення іншого, а убезпечення інформаційної системи досягається оптимальним їх балансуванням. Звузимо об'єкт дослідження до класу інформаційних систем критичного застосування [9]. У таких системах забезпечення конфіденційності покладається на підсистему розмежування доступу, яка управляє процесом автентифікації. Доступність таких систем визначається здебільшого тривалістю та коректністю процесу автентифікації, який оцінюється відповідно до положень системної політики безпеки. Отже, *метою статті* є математична формалізація оптимальної залежності характеристик конфіденційності і доступності інформаційної системи критичного застосування у контексті парадигми CIA. Для досягнення поставленої мети пропонується параметризувати ці характеристики і представити їх залежність у формі класичної зада-

чі однопараметричної оптимізації, ввівши одну з характеристик у цільову функцію, а іншу — у систему обмежень. Також, враховуючи специфіку структури та застосування ІСКЗ, у системі обмежень задачі оптимізації необхідно відобразити керований підсистемою розмежування доступу процес автентифікації інформаційної системи критичного застосування. Далі, класифікувавши отриману задачу оптимізації, необхідно обрати метод її розв'язання, сформулювати методику його застосування, дослідити динаміку зміни вищезгаданих характеристик у реальній інформаційній системі критичного застосування та порівняти їх з результатами моделювання, на основі чого пересвідчитися у коректності отриманих наукових результатів.

Моделювання залежності конфіденційності автентифікації і доступності у ІСКЗ

Описана у роботах [8], [9] ІСКЗ, враховуючи орієнтацію на критичне застосування, має ступінчасту, комплексну процедуру автентифікації, у якій задіяні об'єднані у мережу термінали користувачів сервера даних і сервер-реєстраційний центр. Процедура автентифікації, види користувачів, їх ролі і привілеї, питання убезпечення інформаційних процесів та реакція ІСКЗ на несанкціоновані дії описано у системній політиці безпеки (СПБ), модель якої наведено у [9]. Описана у [10] процедура автентифікації для доступу до ІСКЗ підтримується підсистемою розмежування доступу (ПРД), яка здійснює розпізнавання суб'єкта за даними ідентифікаційної карти, за паролем, за біометричними характеристиками голосу. Для прийняття рішення за кожною із вищезгаданих індивідуальних ознак у ПРД реалізовано ансамбль класифікаторів з можливістю ранжування генерованих ними рішень відповідно до обраної адміністратором стратегії управління. Узагальнюючи ранжовані результати розпізнавання від кожного з класифікаторів ансамблю, ПРД приймає остаточне рішення щодо автентифікації аналізованого суб'єкта. Такий підхід до організації процесу автентифікації (ПА) робить його вкрай надійним, але входить у суперечність з домінуючою у сфері інформаційної безпеки тріадою CIA [2]. Зокрема, у суперечність входять, насамперед, перший і третій компоненти тріади, адже, підвищення конфіденційності приводить до ускладнення процедури автентифікації і робить її все тривалішою, що, відповідно, знижує доступність системи, прямою характеристикою, для визначення якої є час, за який суб'єкт отримує доступ до інформаційних ресурсів системи відповідно до його особи і ролі. Отже, виникає потреба у формалізації математичного апарату, який би дозволив ідентифікувати залежність між конфіденційністю комплексної ступінчастої процедури автентифікації, керованої ПРД, та доступністю інформаційних ресурсів ІСКЗ. Для отримання базової моделі під управлінням конфіденційністю розумітимемо можливість активації/деактивації окремих класифікаторів у ансамблі ПРД, а поняття доступності ототожнимо з тривалістю процедури автентифікації суб'єкту. Зрештою, необхідно мінімізувати втрати доступності ПА, конфіденційність якого не повинна знизитися нижче заданого адміністратором порогового значення.

Враховуючи ступінчастий характер процедури автентифікації у ІСКЗ, яка включає каскад послідовно реалізовуваних процедур ідентифікації суб'єкта за даними його ідентифікаційної карти, секретним паролем і, нарешті, за індивідуальними параметрами його голосу, в якості базового математичного апарату для моделювання її надійності використаємо напівмарковську модель прийняття рішень для керованого марковського ПА у неперервному часі з дискретною тривалістю окремих його етапів. Такий вибір базового математичного апарату походить з визначення напівмарковського процесу як випадкового процесу, що переходить з одного стану в інший відповідно із заданими розподілами імовірностей, а тривалість перебування процесу в будь-якому стані є випадковою величиною, розподіл якої залежить як від поточного стану, так і від стану, у який буде здійснено подальший перехід процесу. Це визначення органічно корелює з вищеописаним процесом автентифікації у ІСКЗ.

В рамках вищеописаної концепції створювана модель має дозволити обрати оптимальну стратегію роботи ПРД з активації/деактивації окремих класифікаторів у ансамблях, для чого планується застосувати методи бульового програмування. Нехай існує множина станів $i \in S = \{0,1,\ldots,N\}$, кожному з яких відповідає етап ПА, під час якого ПРД приймає одне зі скінченної множини описаних у СПБ рішень $R_i = \{1,2,\ldots,r_i\}$. Імовірнісний закон

$$Y_{ij}^{r}(t) = P_{ij}^{(r)} F_{ij}^{(r)}(t) \qquad (1)$$

описує прийняте ПРД рішення $r = R_i$ на $i \in S$ етапі ПА, де $P_{ij}^{(r)}$ — імовірність переходу ПА від етапу i до етапу j, а $F_{ij}^{(r)}(t)$ — функція розподілу тривалості перебування ПА на етапі i з прийняттям ПРД рішення r за умови, що етап j наслідуватиме i. Функції $F_{0j}^{(r)}(t)$ і $F_{j0}^{(r)}(t)$, $j \in \tilde{S} = S / \{0\}$, $r \in R_j$ та їх перші похідні неперервні за $t > 0$ та експоненційно зростають. Вважатимемо, що коректному завершенню відповідного етапу ПА відповідатиме значення $i = 0$, а $i \neq 0$ відповідатиме факту реєстрації на цьому етапі ПА ситуації, описаної у СПБ. Нехай за одиницю часу перебігу i-го етапу ПА внаслідок прийняття ПРД рішення r витрачається $k_i^{(r)}$ умовних одиниць доступності. Значення $\left|k_i^{(r)}\right|$ обмежені для всіх $i \in S$, $r \in R_i$, а імовірності $P_i^{(r)}$ задовольняють відношенням $\sum\limits_{j \in S} P_i^{(r)} = 1$, $P_{ij}^{(r)} \geq 0$, $i, j \in S$, $r \in R_i$. Отже, під час перебігу $i \in S$ етапу ПА ПРД аналізує r_i варіантів зі скінченної множини R_i, вибираючи варіант r, що еквівалентно ідентифікації всіх значень кортежу $\left\langle Y_{ij}^r(t), P_{ij}^{(r)}, F_{ij}^{(r)}(t), k_i^{(r)} \right\rangle$, $i, j \in S$. Якщо $i = 0$, $j \in S$, $R_0 = \{0\}$, то величина $P_{0j}^{(r)} \neq 0$ описує імовірність переходу ПА у стан j і визначається як емпірично встановлене відношення кількості порушень СПБ на етапі j до загальної кількості зареєстрованих порушень СПБ для всього ПА, а функція $F_{0j}^{(r)}(t)$ описує розподіл тривалості реакції ІСКЗ на виявлений ПРД факт порушення СПБ на етапі j. Якщо $i = \overline{1, N}$, $\forall r \in R_i$, $P_{i0}^{(r)} = 1$, $P_{ij}^{(r)} = 0$, $j \neq 0$ функція $F_{i0}^{(r)}(t)$ описує розподіл тривалості реакції ІСКЗ на виявлений факт порушення СПБ, пов'язаний з прийнятим ПРД рішенням r на етапі i. За умови неперервності експлуатації ІСКЗ використовуватимемо експоненційну міру втрат доступності $e^{-\alpha t}$, де α — норма втрат, а загальні втрати доступності для всього ПА опишемо як

$$\int_0^t k_i e^{-\alpha\tau} d\tau = k_i \alpha^{-1}\left(1 - e^{-\alpha\tau}\right). \tag{2}$$

Якщо перебіг ПА від початкового етапу i_0 після n-го переходу досягає етапу i_n, який характеризується прийнятим ПРД рішенням u_n за тривалості етапу τ_n, то оптимальні стратегії прийняття рішень для ПРД опишемо послідовністю імовірнісних мір $\beta_n(z_n)$, де $z_n = \left(i_0, u_0, \tau_0, \ldots, i_{n-1}, u_{n-1}, \tau_{n-1}, i_n\right)$ описує історію перебігу ПА з моменту його початку. Позначимо: $d_i^{(r)}$ — щільність міри стратегії β_n; $i_n = i$; $u_n = r$, $r \in R_i$; $g_i(t, \alpha, \beta)$ — загальні втрати доступності ІСКЗ, ПА якої кероване стратегією β з нормою переоцінювання α протягом циклу експлуатації тривалістю t; $\upsilon_i(t, \alpha, \beta) = g_i(t, \alpha, \beta) / t$ — нормовані за тривалістю t втрати доступності ІСКЗ. Підсумкові ж обмеження щодо конфіденційності ІСКЗ з урахуванням стратегії управління перебігом ПА узагальнимо так:

$$\sum_{j \in S} c_{rj} x_{rj} \geq b_r, \; r \in R = \bigcup_{j \in S} R_j, \tag{3}$$

де c_{rj} — втрати конфіденційності, пов'язані з прийняттям ПРД рішення r внаслідок реєстрації факту порушення СПБ на етапі j, b_r — задані адміністратором порогові значення допустимих втрат конфіденційності при реалізації рішення r, x_{rj} — бульова змінна, яка набуває значення 1, якщо внаслідок прийнятого ПРД рішення r зафіксовано факт порушення СПБ на етапі j або 0, якщо факту порушення СПБ не зафіксовано. Теорія математичного програмування [11] дозволяє стверджувати, що якщо система обмежень (3) сумісна, то існує невипадкова стаціонарна стратегія β^*, яка мінімізує нормовані загальні втрати доступності ПА $\upsilon(\alpha, \beta) = \left(\upsilon_0(\alpha, \beta), \upsilon_1(\alpha, \beta), \ldots, \upsilon_N(\alpha, \beta)\right)$ за довільної стратегії β і норми переоцінювання $\alpha > 0$. Вектор $\upsilon(\alpha, \beta)$ містить $\upsilon(\alpha, \beta) - (N+1) \times 1$ елементів, при чому

$$\upsilon_i(\alpha,\beta)=\lim_{t\to\infty}\upsilon_i(t,\alpha,\beta),\ i\in S. \tag{4}$$

Отже, необхідно синтезувати α-оптимальну стаціонарну марковську стратегію β^*, яка мінімізуватиме нормовані загальні втрати доступності напівмарковського ПА $\upsilon(\alpha,\beta)$ за довільного початкового розподілу станів процесу

$$y=(y_0,y_1,\ldots,y_N),\ \sum_{i\in S}y_i=1,\ i\in S. \tag{5}$$

Імовірність переходів напівмарковського ПА з етапу *i* на етап *j* з прийняттям ПРМ рішення $r\in R_i$ описуватимемо стохастичною матрицею $P^{(r)}=\left\{p_{ij}^{(r)}\right\}$, елементи якої дозволяють, враховуючи (1), визначити сумісну імовірність $Q_{ij}^{(r)}(t)$ того, що за час *t* ПА перейде з етапу *i* на етап *j* $(i\neq j)$ у наслідок прийняття ПРД рішення $r\in R_i$:

$$Q_{ij}^{(r)}(0)=0,\ \text{якщо}\ t=0;\ \sum_{i,j\in S}Q_{ij}^{(r)}(t)=\sum_{i,j\in S}p_{ij}^{(r)}=1,\ \text{якщо}\ t>0. \tag{6}$$

На основі матриці $Q^{(r)}(t)=\left\{Q_{ij}^{(r)}(t)\right\}$ перейдемо до функції розподілу тривалості перебування ПА на етапі *i* у разі прийняття ПРД рішення $r\in R_i$:

$$H_i^{(r)}=\sum_{i,j\in S}Q_{ij}^{(r)}(t). \tag{7}$$

Отже, напівмарковський процес управління ПА Z_t, перебуваючи у момент часу *t* на етапі *i* описуватиметься кортежем $\left\langle N,y,Q_{ij}^{(r)}(t)\right\rangle$, коли $i,j\in S$, $r\in R_i$. Спираючись на положення теорії відновлення [12], для одноелементних множин рішень R_i отримаємо такий вираз для визначення $\upsilon_i(t,\alpha,\beta)$

$$\upsilon_i(t,\alpha,\beta)=\left(1-H_i(t)\right)\left(1-e^{-\alpha t}\right)\alpha^{-1}k_i+\sum_{j\in S}\int_0^y\left(\left(1-e^{-\alpha t}\right)\alpha^{-1}k_i+\upsilon_j(t-\tau)e^{-\alpha t}\right)dQ_{ij}(\tau),$$

який при переході до скінченних множин R_i з урахуванням ймовірностей $d_i^{(r)}$ прийняття ПРД рішення *r* на етапі *i* перетворимо на

$$\upsilon_i(t,\alpha,\beta)=\sum_{r\in R_i}d_i^r\left(\left(1-H_i^{(r)}(t)\right)\left(1-e^{-\alpha t}\right)\alpha^{-1}k_i^{(r)}\right)+\sum_{j\in S}\sum_{r\in R_i}\int_0^y d_i^r\left(\left(1-e^{-\alpha t}\right)\alpha^{-1}k_i^{(r)}+\upsilon_j(t-\tau)e^{-\alpha t}\right)dQ_{ij}(\tau), \tag{8}$$

де $k_i^{(r)}$ — втрати доступності за одиницю часу перебування ПА на етапі *i* при прийнятті ПРМ рішення $r\in R_i$, $\upsilon_j(t-\tau)$ — нормовані загальні втрати доступності з урахування переоцінювання (2) за умови, що історія перебігу ПА відома з моменту часу $t=0$ і розпочалася етапом *j*. Здійснимо подальше спрощення (8), застосувавши перетворення Лапласа–Стілтьєса до (4) з метою переходу від $\upsilon_i(\alpha,\beta)$ до $\upsilon_i(\alpha)$. Аналіз рівняння (7) дозволяє стверджувати, що $H_i^{(r)}(\infty)=1$, тоді перший доданок у рівнянні (8) при $t\to\infty$ дорівнює нулю, а застосовуючи частинне інтегрування до решти, позначивши $L^*_{s=\alpha}\left\langle H_i^{(r)}(\tau)\right\rangle$ — перетворення Лапласа–Стілтьєса функції $H_i^{(r)}(\tau)$, отримаємо:

$$\begin{aligned}F_j^{(r)}(t)&=\sum_j\int_0^t\left(1-e^{-\alpha t}\right)dQ_{ij}^{(r)}(\tau)=\left(1-e^{-\alpha t}\right)\sum_j dQ_{ij}^{(r)}(\tau)\Big|_0^t-\sum_j\alpha\int_0^t e^{-\alpha t}H_i(\tau)d\tau=\\&=(1-\alpha)L_{s=\alpha}\left\langle H_i^{(r)}(\tau)\right\rangle=1-L^*_{s=\alpha}\left\langle H_i^{(r)}(\tau)\right\rangle=1-h_i^{(r)}(\alpha).\end{aligned} \tag{9}$$

Введемо функцію $\Phi_i^{(r)}(t)=\int_0^r e^{-\alpha t}v_j(t-\tau)dQ_{ij}^{(r)}(t)$, яку за $t\to\infty$ представимо як $\Phi_i^{(r)}(t)=\int_0^\infty e^{-\alpha t}v_j(\alpha)dQ_{ij}^{(r)}(\tau)=v_j(\alpha)q_{ij}^{(r)}(\alpha)$, де $q_{ij}^{(r)}(\alpha)=L^*_{s=\alpha}\left\langle Q_i^{(r)}(\alpha)\right\rangle$. Застосуємо вищеописані вирази для визначення $F_j^{(r)}(t)$ і $\Phi_i^{(r)}(t)$ для перетворення виразу для визначення $\upsilon_i(t)$, коли $t\to\infty$

$$\upsilon_i(t)=\varepsilon_i(\alpha)+\sum_{j\in S}q_{ij}^{(r)}(\alpha)v_j(\alpha), \tag{10}$$

де $\varepsilon_i(\alpha)=\sum_{r\in R_i}d_i^{(r)}\left(\varepsilon_i^{(r)}(\alpha)\right)$;

$$\varepsilon_i^{(r)}(\alpha)=k_i^{(r)}\left(1-h_i^{(r)}(\alpha)\right)\alpha^{-1}, \tag{11}$$

а між векторами $\mathrm{E}(\alpha)=\left(\varepsilon_0(\alpha),\varepsilon_1(\alpha),\ldots,\varepsilon_N(\alpha)\right)^T$ і $V(\alpha)=\left(v_0(\alpha),v_1(\alpha),\ldots,v_N(\alpha)\right)^T$ існує зв'язок

$$V(\alpha)=\left\{I-q(\alpha)\right\}^{-1}\mathrm{E}(\alpha), \tag{12}$$

де $q(\alpha)=\left\{q_{ij}(\alpha)\right\}=\left\{\sum_{r\in R_i}d_i^{(r)}\left(q_{ij}^{(r)}(\alpha)\right)\right\}$, а I — одинична матриця розмірністю $N\times N$.

Позначивши $\left\{I-q(\alpha)\right\}^{-1}=\mu(\alpha)$, перейдемо до матричного запису (12), увівши в нього вектор y, описаний у (5): $y\upsilon(\alpha)=\sum_{i\in S}\sum_{j\in\tilde S}\sum_{r\in R_i}y_i\mu_{ij}(\alpha)\varepsilon_j^{(r)}(\alpha)d_i^{(r)}$.

Перепозначивши $x_{rj}=d_i^{(r)}$; $d_i^{(r)}\in\{0,1\}$; $\sum_{j\in S}d_i^{(r)}=1$, сформулюємо у термінах математичного програмування цільову функцію і систему обмежень задачі оптимізації доступності, описаної напівмарковським процесом ПА, з обмеженнями на втрати конфіденційності:

$$f(\alpha,X)=\sum_{i\in S}\sum_{j\in\tilde S}\sum_{r\in R_i}y_i\mu_{ij}(\alpha,X)\varepsilon_j^{(r)}x_{rj}\to\min$$
$$\begin{cases}\sum_{j\in\tilde S}c_{rj}x_{rj}\ge b_r,\\ \sum_{r\in R_i}x_{rj}=1,\end{cases} \tag{13}$$

де $i\in S$, $j\in\tilde S$, $r\in R_i$. Задача оптимізації (13) є задачею математичного програмування з нелінійною цільовою функцією і лінійною системою обмежень, яку можна було б розв'язати стандартними методами нелінійного програмування, але присутність у (13) бульових змінних обумовлює доцільність коментування процесу розв'язку. Позначимо область допустимих розв'язків системи обмежень задачі (13) як $Z=\left\{s_j\right\}$, $j=1,\ldots,N$, де s_j — множина номерів *r*, які задовольняють рівності $x_{rj}=1$. Знайшовши розв'язки m нерівностей $\sum_{j\in\tilde S}c_{rj}x_{rj}\ge b_r$, завершимо процес знаходження Z за m кроків, розпочавши з початкового вектора $Z^{(0)}$, який містить всі значення $r=R_i$. Якщо на *r*-му кроці значення $r=r_1$ з вектора $Z^{(r-1)}$ збіжиться з одним із розв'язків *r*-ї нерівності $\alpha_j\in\{0,1,\varphi\}$ із (13), де φ — невизначений бульовий параметр, то $s_j^{(r)}$ елемент Z визначатимемо аналізуючи такі варіанти: якщо $\alpha_j=1$, то за $r_1\in s_j^{(r-1)}$ вважаємо $s_j^{(r)}=\{r_1\}$, а якщо $r_1\overline{\in}s_j^{(r-1)}$, то вважаємо $s_j^{(r)}=\varnothing$; якщо $\alpha_j=0$, то $s_j^{(r)}=s_j^{(r-1)}\big/\{r_1\}$; для всіх інших α_j вважаємо $s_j^{(r)}=s_j^{(r-1)}$.

Отриманий на *m*-му кроці алгоритму вектор-розв'язок системи обмежень (13) $Z^{(m)}=\left\{\alpha_1^{(m)},\ldots,\alpha_N^{(m)}\right\}$ складається з $\alpha_j^{(m)}$, $j=1,\ldots,N$, елементів, кожний з яких містить множину значень $\{r\}$, $r\in R=\{1,\ldots,m\}$. Підставивши отримані з вектора $Z^{(m)}$ значення $\alpha_j^{(m)}$, які належать області допустимих розв'язків системи обмежень (13), у цільову функцію $f(\alpha,X)$, знаходимо елементи вектора X, що її мінімізують, і описують оптимальну стратегією роботи ПРД за заданих обмежень на конфіденційність ІСКЗ.

Методика для практичного застосування вищеописаної моделі

Сформулюємо методику застосування вищеописаної моделі, вважаючи, що у СПБ описано два типи помилок ПА: критична помилка (КП) — коли ПРД, спираючись на результати роботи більшості класифікаторів ансамблів з урахуванням ваг їх рішень, визнає суб'єкта, який автентифікується, таким, що не має права доступу; підозра на помилку (ПП) — коли ПРД, спираючись на результати роботи більшості класифікаторів ансамблів з урахуванням ваг їх рішень, визнає суб'єкта, який автентифікується таким, що має права доступу, проте помітна кількість класифікаторів не автентифікувала суб'єкта. Враховуючи критичне застосування інформаційної системи, у ситуації ПП доцільним є інформування адміністратора для винесення остаточного вердикту щодо надання суб'єкту доступу, але така дія значно подовжує тривалість ПА, знижаючи, відповідно, доступність ІСКЗ.

Нехай у СПБ у випадку реєстрації КП передбачено $R=\{r_1,r_2,r_3\}$ послідовність дій, а у випадку реєстрації ПП — $R=\{r_1,r_4\}$, тоді у термінах вищеописаної моделі $N=2$, а $m=4$. Зважатимемо, що ПРД має ступінчасту, комплексну, послідовно з'єднану блочну структуру. Кожен блок-ступінь ПРД включає відповідні підблоки виділення інформативних ознак і класифікації, об'єднані у ансамбль. Рішення, яке приймає класифікатор кожного з підблоків є незалежним. Нехай $F_j(t)$ — функція розподілу тривалості ПА між двома зареєстрованими ситуаціями КП або ПП, які опишемо змінною *j*. Тоді $G_j^{(k)}(t)$ — функція розподілу втрат доступності від реакції СПБ *r* на факт реєстрації ситуації *j*. Вважатимемо, що функції $F_j(t)$ та $G_j^{(k)}(t)$ описуватимуться експоненційним законом з коефіцієнтами λ_j та $\mu_j^{(k)}$, відповідно

$$F_j(t)=1-e^{-\lambda_j t};\quad G_j^{(k)}(t)=1-e^{-\mu_j^{(r)}t}, \tag{14}$$

де $\lambda_j=T_{j1}^{-1}$, $\mu_j^{(r)}=T_{j2}^{-1}$, T_{j1}^{-1} — величина, обернена до середньої тривалості ПА між двома зареєстрованими ситуаціями *j*, а T_{j2}^{-1} — величина, обернена середньої кількості втрат доступності від реакції СПБ *r* на зареєстровану ситуацію *j*. Нехай $d_i^{(k)}$ — стаціонарна стратегія ПРД, яка контролює ПА, що перебуває на етапі *i*, приймаючи рішення *k*, яке стохастично описується імовірністю *r*: $d_i^{(k)}\in\{0,1\}$, $\sum\limits_{k\in K} d_i^{(r)}\in 1$, $i\in S$, тоді (14) можна записати як

$$F_j(t)=1-e^{-\lambda t};\quad G_j^{(r)}(t)=1-e^{-\mu t}, \tag{15}$$

де $\lambda=\sum\limits_{j=1}^{N}\lambda_j$, $\mu=\sum\limits_{j}^{N}d_j^{(r)}\mu_j^{(r)}$. Нехай $i=0$ означає штатний перебіг ПА, $i=1$ означає реєстрацію КП, а $i=2$ — реєстрацію ПП, тоді сформуємо множини $S=\{0,1,2\}$ і $\tilde{S}=\{1,2\}$ і за вибраних значень T_{11}, T_{21}, $T_{12}^{(1)}$, $T_{22}^{(1)}$, $T_{12}^{(2)}$, $T_{12}^{(3)}$, $T_{22}^{(4)}$ на основі (14) і (15) розрахуємо $F_0(t)$, $F(t)$, $F_1(t)$, $F_2(t)$, $G_1^{(1)}(t)$, $G_1^{(2)}(t)$, $G_1^{(3)}(t)$, $G_2^{(1)}(t)$ і $G_2^{(4)}(t)$. Нехай c_{kj} — норми втрат конфіденційності від реалізації описаної у СПБ реакції *k* у відповідь на реєстрацію ситуації *j*, тоді для продовження розв'язку задамо вартісні коефіцієнти c_{11}, c_{12}, c_{21}, c_{31}, c_{42}. Вважатимемо, що на етапі $i=0$ прийнято рі-

шення $r=0$ і задано імовірності $p_{00}^{(0)}$, $p_{01}^{(0)}$, $p_{02}^{(0)}$, $\sum_{i=0}^{2} p_{0i}^{(0)}=1$. Тоді, підставивши вищезнайдені значення T_{j1}, T_{j2}, $F_j(t)$, $G_j^{(k)}(t)$, $k=1,2,3$, у (6) і (7), отримаємо аналітичний вигляд функцій $Q_{00}^{(0)}(t)$, $Q_{01}^{(0)}(t)$, $Q_{02}^{(0)}(t)$, $Q_{10}^{(1)}(t)$, $Q_{10}^{(2)}(t)$, $Q_{10}^{(3)}(t)$, $Q_{20}^{(1)}(t)$, $Q_{20}^{(4)}(t)$ (для описуваної постановки задачі $Q_{11}^{(k)}(t)=Q_{12}^{(k)}(t)=0$) і функцій $H_0^{(0)}(t)$, $H_1^{(0)}(t)$, $H_1^{(2)}(t)$, $H_1^{(3)}(t)$, $H_2^{(1)}(t)$, $H_2^{(4)}(t)$, відповідно. Далі, приймаючи $x_{00}=1$, $x_{kj}=d_j^{(k)}$, $r\in R_j$, $j\in\tilde{S}$, на основі вищерозрахованого отримаємо аналітичний вигляд матриці $q(\alpha,x)=\sum_{r\in R_j} x_{ki}q_{ij}^{(r)}$, $i,j\in S$. Розрахуємо визначник $D(\alpha,x)$ матриці $\left[I-q(\alpha,x)\right]$, використавши який за $\left[I-q(\alpha,x)\right]^{-1}=\left[\mu_{ij}(\alpha,x)\right]$ знайдемо $\mu_{00}(\alpha,x)$, $\mu_{01}(\alpha,x)$, $\mu_{02}(\alpha,x)$, $\mu_{10}(\alpha,x)$, $\mu_{11}(\alpha,x)$, $\mu_{12}(\alpha,x)$, $\mu_{20}(\alpha,x)$, $\mu_{21}(\alpha,x)$, $\mu_{22}(\alpha,x)$. На основі (11), задавши $k_0^{(0)}$, $k_1^{(1)}$, $k_1^{(2)}$, $k_1^{(3)}$, $k_2^{(1)}$, $k_2^{(4)}$, знайдемо величини $\varepsilon_0^{(0)}$, $\varepsilon_1^{(1)}$, $\varepsilon_1^{(2)}$, $\varepsilon_1^{(3)}$, $\varepsilon_2^{(1)}$, $\varepsilon_2^{(4)}$. Знайдемо розв'язки $r_1=\{\{1:1,1:2,1:3\},\{2:1,2:2\},\{3:1,3:2\},\{4:1,4:2\}\}$ системи обмежень–нерівностей (13) $\tilde{C}$, враховуючи, що їх вільні члени b_k задовольняють умовам $2c_1<b_1<c_{11}$, $b_2<c_{21}$, $b_3<c_{31}$, $b_4<c_{42}$. Знаючи r_1, на основі початкового вектора $Z^{(0)}=\{\{1,2,3\},\{1,4\}\}$, на останньому кроці алгоритму отримаємо п'ять пар функцій $Z_{1221}^{(4)}$ і $Z_{1222}^{(4)}$, $Z_{2121}^{(4)}$ і $Z_{2122}^{(4)}$, $Z_{2211}^{(4)}$ і $Z_{2212}^{(4)}$, $Z_{3121}^{(4)}$ і $Z_{3122}^{(4)}$, $Z_{3211}^{(4)}$ і $Z_{3212}^{(4)}$, де вектор-розв'язок $x_j\ \tilde{C}$ у кожній парі не містить пустої множини. В результаті за відомих α та $y=(1,0,\ldots,0)$ розрахуємо допустимі значення цільової функції (13) $f_j(\alpha,x_j)$, $j=1,\ldots,5$, і виберемо з них найменше, якому відповідатиме вектор-розв'язок $x_j^*\in x_j$, який задає оптимальну стратегію роботи ПРД з урахуванням обмежень на втрати конфіденційності ПА.

Апробація вищеописаної методики для оптимізації ПА ІСКЗ

Застосуємо авторську методику оптимізації стратегії роботи ПРД з урахуванням обмежень на втрати конфіденційності ПА за таких вихідних даних: $T_{11}=8$; $T_{21}=8$; $T_{12}^{(1)}=1$; $T_{22}^{(1)}=1$; $T_{12}^{(2)}=2$; $T_{12}^{(3)}=1$; $T_{22}^{(4)}=0{,}5$. Тоді отримаємо $F_0(t)=1-e^{-0{,}25t}$; $F(t)=1-e^{-0{,}25t}$; $F_1(t)=1-e^{-0{,}125t}$; $F_2(t)=1-e^{-0{,}125t}$; $G_1^{(1)}(t)=1-e^{-t}$; $G_1^{(2)}(t)=1-e^{-0{,}5t}$; $G_1^{(3)}(t)=1-e^{-t}$; $G_2^{(1)}(t)=1-e^{-t}$ і $G_2^{(4)}(t)=1-e^{-2t}$. Задавши $c_{11}=7\cdot10^4$; $c_{12}=7\cdot10^4$; $c_{21}=300$; $c_{31}=400$; $c_{42}=600$; $p_{00}^{(0)}=0{,}7$; $p_{01}^{(0)}=0{,}1$; $p_{02}^{(0)}=0{,}2$, отримаємо функції $Q_{00}^{(0)}(t)=0{,}7-0{,}7e^{-0{,}25t}$; $Q_{01}^{(0)}(t)=0{,}1-0{,}1e^{-0{,}125t}$; $Q_{02}^{(0)}(t)=0{,}2-0{,}2e^{-0{,}125t}$; $Q_{10}^{(1)}(t)=1-e^{-t}$; $Q_{10}^{(2)}(t)=1-e^{-0{,}5t}$; $Q_{10}^{(3)}(t)=1-e^{-t}$; $Q_{11}^{(1)}(t)=Q_{11}^{(2)}(t)=$ $=Q_{11}^{(3)}(t)=Q_{12}^{(1)}(t)=Q_{12}^{(2)}(t)=Q_{12}^{(3)}(t)=0$; $Q_{20}^{(1)}(t)=1-e^{-t}$; $Q_{20}^{(4)}(t)=1-e^{-2t}$ і функцій $H_0^{(0)}(t)=1-0{,}7e^{-0{,}25t}-e^{-0{,}125t}$; $H_1^{(0)}(t)=1-e^{-0{,}25t}$; $H_1^{(2)}(t)=1-e^{-0{,}5t}$; $H_1^{(3)}(t)=H_2^{(1)}(t)=1-e^{-t}$; $H_2^{(4)}(t)=1-e^{-2t}$.

Отримаємо матрицю $q[\alpha,x]$ і визначник $D(\alpha,x)$ в загальному вигляді:

$$q[\alpha,x]=\begin{bmatrix} 0{,}175(\alpha+0{,}25)^{-1} & 0{,}013(\alpha+0{,}125)^{-1} & 0{,}025(\alpha+0{,}125)^{-1} \\ (x_{11}+x_{31})(\alpha+1)^{-1}+x_{21}(\alpha+0{,}5)^{-1} & 0 & 0 \\ x_{12}(\alpha+1)^{-1}+x_{42}(\alpha+2)^{-1} & 0 & 0 \end{bmatrix};$$

$$D(\alpha,x)=1-0,025(\alpha+0,125)^{-1}\left(x_{12}(\alpha+1)^{-1}+2x_{42}(\alpha+2)^{-1}\right)-$$
$$-0,013(\alpha+0.125)^{-1}\left(x_{11}(\alpha+1)^{-1}+x_{21}(\alpha+0,5)^{-1}\right)-0,175(\alpha+0.25)^{-1};$$

Далі отримаємо $\mu_{00}(\alpha,x)=0$; $\mu_{01}(\alpha,x)=0,013\left(D(\alpha,x)(\alpha+0,125)\right)^{-1}$;

$\mu_{02}(\alpha,x)=(\alpha+0,125)\left(0,025D(\alpha,x)\right)^{-1}$; $\mu_{10}(\alpha,x)=D(\alpha,x)^{-1}\left((x_{11}+x_{31})(\alpha+1)^{-1}+x_{21}(\alpha+0,5)^{-1}\right)$;

$\mu_{11}(\alpha,x)=D(\alpha,x)^{-1}\left(1-0,175(\alpha+0,25)^{-1}-0,013(\alpha+0,125)^{-1}\left(x_{12}(\alpha+1)^{-1}+2x_{42}(\alpha+2)^{-1}\right)\right)$;

$\mu_{12}(\alpha,x)=0,025\left(D(\alpha,x)(\alpha+0,125)\right)^{-1}\left((x_{11}+x_{31})(\alpha+1)^{-1}+x_{21}(\alpha+0,5)^{-1}\right)$; $\mu_{20}(\alpha,x)=D(\alpha,x)^{-1}\times$

$\times\left(x_{12}(\alpha+1)^{-1}+2x_{42}(\alpha+2)^{-1}\right)$; $\mu_{21}(\alpha,x)=0,013\left(D(\alpha,x)(\alpha+0,125)\right)^{-1}\left(x_{12}(\alpha+1)^{-1}+2x_{42}(\alpha+2)^{-1}\right)$;

$\mu_{22}(\alpha,x)=D(\alpha,x)^{-1}\left(1-0,018(\alpha+0,25)^{-1}-0,013(\alpha+0,125)^{-1}\left((x_{11}+x_{31})(\alpha+1)^{-1}+x_{21}(\alpha+0,5)^{-1}\right)\right)$.

Взявши $k_0^{(0)}=-7\cdot10^4$; $k_1^{(1)}=-7\cdot10^4$; $k_1^{(2)}=-150$; $k_1^{(3)}=-400$; $k_2^{(1)}=-7\cdot10^4$; $k_2^{(4)}=1,2\cdot10^4$; розрахуємо $\varepsilon_0^{(0)}(\alpha)=7\cdot10^4\left(1-0,175(\alpha+0,25)^{-1}-0,038(\alpha+0,125)^{-1}\right)\alpha^{-1}$; $\varepsilon_1^{(1)}(\alpha)=\varepsilon_2^{(1)}(\alpha)=$

$=-7\cdot10^4\left(1-(\alpha+1)^{-1}\right)\alpha^{-1}$; $\varepsilon_1^{(2)}(\alpha)=-150\left(1-0,5(\alpha+0,5)^{-1}\right)\alpha^{-1}$; $\varepsilon_1^{(3)}(\alpha)=-400\left(1-(\alpha+1)^{-1}\right)\alpha^{-1}$;

$\varepsilon_2^{(4)}(\alpha)=-1,2\cdot10^4\left(1-2(\alpha+2)^{-1}\right)\alpha^{-1}$, що дозволяє знайти розв'язки r_1 окремих нерівностей $\tilde{C}$:

$r_1=\{1:(1,0),(0,1),(0,0);2:(1,0),(0,0);3:(1,0),(0,0);4:(0,1),(0,0)\}$. На основі r_1, якщо $Z^{(0)}=\{\{1,2,3\},\{1,4\}\}$, розрахуємо $Z_{1221}^{(4)}=\{\{1\},\{4\}\}$ і $Z_{1222}^{(4)}=\{\{1\},\text{ø}\}$; $Z_{2121}^{(4)}=\{\{2\},\text{ø}\}$ і $Z_{2122}^{(4)}==\{\{2\},\{1\}\}$; $Z_{2211}^{(4)}=\{\{3\},\text{ø}\}$ і $Z_{2212}^{(4)}=\{\{3\},\{1\}\}$; $Z_{3121}^{(4)}=\{\{2\},\{4\}\}$ і $Z_{3122}^{(4)}=\{\{2\},\text{ø}\}$; $Z_{3211}^{(4)}=\{\{3\},\{4\}\}$ і $Z_{3212}^{(4)}=\{\{3\},\text{ø}\}$ і отримаємо узагальнений розв'язок $\tilde{C}$: $\left(1:\{\{1\},\{4\}\},2:\{\{2\},\{1\}\},3:\{\{3\},\{1\}\},4:\{\{2\},\{4\}\},5:\{\{3\},\{4\}\}\right)$, якому відповідають такі *true*-значення бульових змінних $x=\{1:x_{11}=1,x_{42}=1;2:x_{21}=1,x_{12}=1;3:x_{21}=1,x_{42}=1;4:x_{31}=1,x_{12}=1;5:x_{31}=$ $=1,x_{42}=1;\}$, яким відповідають активні блоки-класифікатори ПРД відповідно до отриманої оптимальної стратегії управління ПА за мінімальної допустимої втрати конфіденційності $\alpha=0,1$.

Застосуємо класичний для теорії планування експерименту підхід до оцінювання адекватності запропонованої моделі залежності втрат конфіденційності ПА і показника доступності ІСКЗ. Сформуємо матрицю вхідних параметрів виду $X=\{ID_{ij},PW_{ij},VPW_{ij}\}$, де $i=\overline{1,N}$ — номер суб'єкта, який бажає отримати доступ до ІСКЗ, $j=\overline{1,M}$ — кількість спроб автентитифікації для кожного *i*-го суб'єкта, ID_{ij}, PW_{ij}, VPW_{ij} — введені *i*-м суб'єктом при *j*-й спробі автентифікації дані ідентифікаційної карти, секретний пароль і індивідуальні параметри, виділені з представленої на всіх ПРД фонограми із записом парольного вислову, відповідно. Для репрезентативності результатів експерименту $N=20$, $M=70$. Далі проведемо експерименти з розпізнавання суб'єктів за інформацією з X за допомогою ПРД, яку описано у [10]. Її структура задовольняє вищенаведеним у статті вимогам. Сформуємо матрицю $Y_e=(y_{ij})$, де $y_{ij}=\{r_{ij},t_{ij}\}$ — множина, у якій r_{ij} — результат розпізнавання *i*-го суб'єкта в *j*-й спробі автентифікації ПРД, яку описано у [10], а t_{ij} — тривалість процедури автентифікації. Проведемо оптимізацію налаштувань параметрів ансамблю класифікаторів цієї ПРД, значення яких розрахуємо відповідно до запропонованої у статті моделі залежності втрат конфіденційності ПА і показника доступності ІСКЗ, встановивши пороговий рівень втрат конфіденційності у 5 %. Сформуємо матрицю $Y_e'=(y_{ij}')$, де $y_{ij}'=\{r_{ij}',t_{ij}'\}$ — множина, у якій r_{ij}' —

результат розпізнавання *i*-го суб'єкта в *j*-й спробі автентифікації ПРД, параметри якої оптимізовано на основі вищезапропонованої моделі, а t'_{ij} — тривалість процедури автентифікації. Розрахуємо для *i*-го суб'єкта дисперсію відхилень відгуків оптимізованої ПРД від результатів еталонної ПРД, описаної у [10]: $s_i^2 = M^{-1}\sum_{j=1}^{M}\left(y_{ij} - y'_{ij}\right)^2$. Розрахуємо середнє значення дисперсії для всіх суб'єктів, які приймали учать у дослідженнях: $s^2 = N^{-1}\sum_{i=1}^{N} s_i^2$. В результаті оцінювання фактичних відхилень s_i^2 від s^2 за допомогою критерію Фішера виявилося, що всі відхилення не перевищують табличних значень, що підтверджує адекватність запропонованої у статті моделі.

Проведемо дослідження описаної у [10] ІСКЗ, змінюючи налаштування її ПРД відповідно до вищенаведеної моделі. Визначатимемо оптимальні стратегії управління ПРД, змінюючи порогове значення параметра втрат конфіденційності α в діапазоні $[1, 2, \ldots, 15]\cdot 10^{-2}$. Для кожного значення α виконаємо аналогічні вищеописаним обчислення для виявлення оптимальної стратегій управління ПА. Для кожної оптимальної стратегії управління ПА, отриманої для відповідного порогового значення α, визначимо середнє емпіричне значення параметра доступності $\bar{d}_e$, для чого узагальнимо дані про тривалість 100 ПА кожного 10 суб'єктів, які приймали участь у дослідженні. Отриману за результатами експериментів залежність втрат конфіденційності ПА і середнього емпіричного значення параметра доступності ІСКЗ показано на рис. 1.

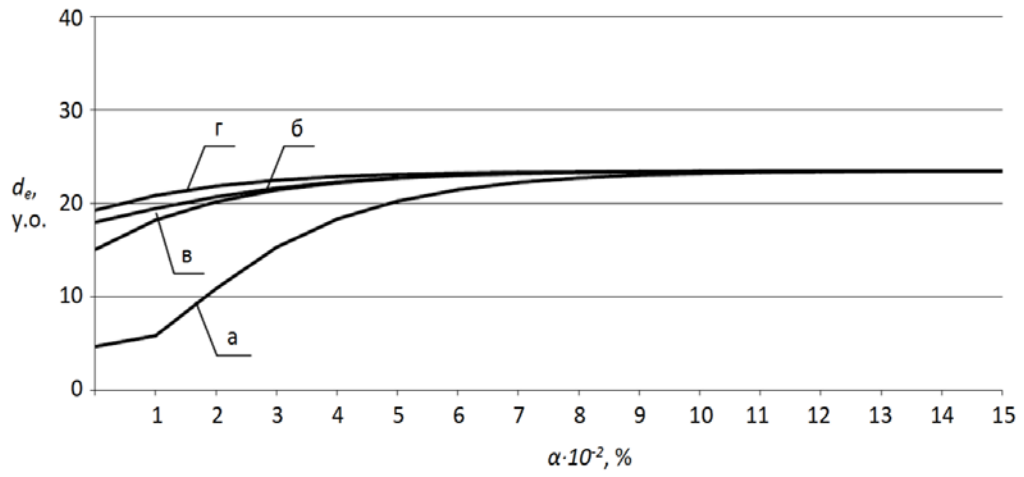

Рис. 1. Залежність втрат конфіденційності ПА і середнього емпіричного значення параметра доступності ІСКЗ в залежності від типу класифікаторів, використаних у блоках ПРД: а — персептрон; б — GMM-HMM-класифікатор; в — глибока нейромережа; г — згортальна нейромережа

Наведені на рис. 1 результати емпіричних досліджень залежності конфіденційності ПА і доступності ІСКЗ збігаються з розрахованими на основі запропонованої методики, що підтверджує адекватність авторської моделі. Із наведених на рис. 1 результатів можна зробити такі висновки: зі зменшенням вимог щодо строгості ПА доступність ІСКЗ зростає, але, починаючи зі значення $\alpha \approx 10\cdot 10^{-2}$, зростання доступності припиняється, що можна пояснити остаточною адаптацією ПРД до прийняття рішень для вищеописаного колективу суб'єктів; за малих значеннях α доступність ІСКЗ є порівняно низькою, що зумовлено реєстрацією великої кількості ПП та КП, на опрацювання яких витрачається час; ПРД, основані на найпростіших (персептронних) і найскладніших (GMM-HMM [10]) класифікаторах, забезпечують найнижчі показники доступності ІСКЗ за малих значень α, що зумовлено реєстрацією великої кількості КП у першому і великої кількості ПП у другому випадках; найкращі показники щодо доступності ІСКЗ за будь-яких значень α показали, що ПРД основана на глибоких і глибоких згортальних нейромережах, ефективність яких у задачах біометричної ідентифікації суб'єктів за індивідуальними особливостями їх голосів виявилася найвищою.

Висновки

Описана у [10] процедура автентифікації для доступу до ІСКЗ підтримується ПРД, яка здійснює розпізнавання суб'єкта за даними ідентифікаційної карти, за паролем, за біометричними характеристиками голосу. Для прийняття рішення за кожною з вищезгаданих індивідуальних ознак у ПРД реалізовано ансамбль класифікаторів з можливістю ранжування генерованих ними рішень відповідно до обраної адміністратором стратегії управління. Узагальнюючи ранжовані результати розпізнавання від кожного з класифікаторів ансамблю ПРД, керуючись СПБ, приймає остаточне рішення щодо автентифікації аналізованого суб'єкта. Такий підхід до організації ПА робить його вкрай надійним але входить у суперечність із домінуючою у сфері інформаційної безпеки тріадою CIA, зокрема, у суперечність входять, перший і третій компоненти тріади. Отже, виникає потреба у формалізації математичного апарату який би дозволив описати залежність між конфіденційністю комплексної ступінчастої процедури автентифікації, керованої ПРД, та доступністю інформаційних ресурсів ІСКЗ, що б дозволило гнучкіше налаштовувати роботу ПРД відповідно до умов експлуатації ІСКЗ.

У статті вперше запропоновано модель залежності втрат конфіденційності ПА і показника доступності ІСКЗ яка, на відміну від існуючих, формалізує як задачу математичного програмування процес синтезу оптимальної напівмарковської стратегії управління прийняттям рішень у марковському процесі автентифікації суб'єктів, що бажають отримати доступ до ресурсів ІСКЗ. Це дозволяє мінімізувати втрати доступності ПА за рахунок встановлення адміністратором порогового значення для параметра конфіденційності системи.

У статті сформульовано методику застосування вищеописаної моделі вважаючи, що у СПБ описано ситуації «критична помилка» і «підозра на помилку», які можуть ідентифікуватися ПРД під час перебігу ПА. Згадані ситуації визначено з урахуванням того, що ПРД має ступінчасту, комплексну, послідовно з'єднану блочну структуру, а кожен блок-ступінь підсистеми включає відповідні підблоки виділення інформативних ознак і класифікації, об'єднані у ансамбль.

Результати проведених емпіричних досліджень залежності конфіденційності ПА і доступності ІСКЗ збігаюаються з розрахованими на основі запропонованої методики, що підтверджує адекватність авторської моделі. Також результати експериментів показали, що зі зменшенням вимог щодо строгості ПА доступність ІСКЗ зростає, але при перевищенні пороговим значенням втрат конфіденційності рівня $\alpha \approx 10 \cdot 10^{-2}$ зростання доступності припиняється, що можна пояснити остаточним завершенням процесу адаптації ПРД до індивідуальних особливостей суб'єктів, на розпізнавання яких було навчено систему. Виявилося, що за малих значень α доступність ІСКЗ є порівняно низькою, що зумовлено реєстрацією великої кількості ситуацій «критична помилка» і «підозра на помилку», на опрацювання яких витрачається час. ПРД, основані на найпростіших (персептронних) і найскладніших (GMM-HMM) класифікаторах, забезпечують найнижчі показники доступності за малих значень α, що зумовлено реєстрацією великої кількості ситуацій «критична помилка» у першому і великої кількості ситуацій «підозра на помилку» у другому випадках. Нарешті, найкращі показники щодо доступності за будь-яких значень α показали, що ПРД основані на глибоких і глибоких згортальних нейромережах, ефективність яких у задачах біометричної ідентифікації суб'єктів за індивідуальними особливостями їх голосів виявилася найвищою.

Подальші дослідження будуть спрямовані на застосування положень теорії планування експерименту для уточнення числових коефіцієнтів моделі з метою кращої її адаптації до специфіки інформаційної системи критичного застосування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] M. M. Bykov, V. V. Kovtun, A. Smolarz, M. Junisbekov, A. Targeusizova, and M. Satymbekov, "Research of neural network classifier in speaker recognition module for automated system of critical use," *Proc. SPIE*, 10445, 1044521 (August 7, 2017), 2017. https://doi.org/10.1117/12.2280930.

[2] Rossouw von Solms, and Johan van Niekerk, "From information security to cyber security." [Electronic resource], Access mode: http://profsandhu.com/cs5323_s18/Solms-Niekerk-2013.pdf .

[3] "ISO/IEC 27005:2011. Information technology – Security techniques – Information security risk management (second edition) ," Введ. 2011-05-19, Женева, 68 с., 2011.

[4] "NIST Special Publication 800-30. Guide for Conducting Risk Assessments," Gaithersburg, 95 с., 2012.

[5] Richard A. Caralli, James F. Stevens, Lisa R. Young, and William R. Wilson, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process," *Hanscom AFB*, 154 с., 2007.

[6]"EBIOS Méthode de gestion des risques," Париж, 95 с., 2010.

[7] "IEC/ISO 31010:2009. Risk management – Risk assessment techniques," Женева, 90 с., 2009.

[8] “Conceptual Modeling of Information Systems”. [Electronic resource]. Access mode: http://infocat.ucpel.tche.br/disc/mc/cmis.pdf .

[9] Mykola M. Bykov, Viacheslav V. Kovtun, Igor D. Ivasyuk, Andrzej Kotyra, and Aisha Mussabekova, “The automated speaker recognition system of critical use,” *Proc. SPIE*, 10808, 2018, 108082V (1 October 2018). https://doi.org/10.1117/12.2501688.

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

[11] Я. В. Гончаренко, «Математичне програмування.» [Електронний ресурс], Режим доступу: http://fmi.npu.edu.ua/files/StorinkaVikladacha/RNikiforov/met-matprog.pdf .

[12] Б. А. Севастьянов, «Теория восстановления.» [Электронный ресурс], Режим доступа: http://zyurvas.narod.ru/knyhy2/Sevastyanov.pdf .

Рекомендована кафедрою комп’ютерних систем управління ВНТУ

Стаття надійшла до редакції 31.10.2018

Ковтун В’ячеслав Васильович — канд. техн. наук, доцент, доцент кафедри комп’ютерних систем управління, e-mail: kovtun_v_v@vntu.edu.ua .

Вінницький національний технічний університет, Вінниця

V. V. Kovtun[1]

Modeling the Dependence of the Confidentiality of Authentication and Availability in the Information System for Critical Use

[1]Vinnytsia National Technical University

Current trends in the organization of the authentication process in information systems for critical use are primarily aimed at improving its reliability, however, this approach contradicts the CIA triad that dominates information security, in particular, the first and third components of the triad come into conflict. Consequently, there is a need to formalize the mathematical apparatus that would allow describing the relationship between confidentiality of a complex stepwise authentication procedure and the availability of the information system's for critical use resources, which would allow flexible adjustment of the access control subsystem in accordance with the operating conditions of the information system. The article first proposed the dependence of the loss of the confidentiality of the authentication process and the availability indicator of an information system for critical use. In this model, unlike the existing ones, the process of an optimal semi-Markov decision management strategy in a Markov authentication process of subjects wishing to gain access to the information system's for critical use resources synthesis is formalized as a mathematical programming task, which allows minimizing the loss of availability of the authentication process, the confidentiality of which should not fall below the threshold set by the administrator. The article outlines the methodology for applying the model described above, taking into account that the “critical error” and “suspicion of error” situations are described in the system security policy, which can be identified by the access control subsystem during the authentication process. These situations are defined taking into account the fact that the access control subsystem has a stepped, complex, sequentially connected block structure, and each block-level subsystem includes the corresponding sub-blocks for the informative features selection and classifications combined into an ensemble. The experiments carried out using the created model showed that as the requirements for the authentication process are less stringent, the availability of the information system for critical use increases, but when the loss threshold reaches $\alpha \approx 10 \cdot 10^{-2}$, the availability increase stops, which can be explained by the final completion of the subsystem adaptation delimiting access to the individual features of the subjects for which the system has been trained. It turned out that for small α values, the availability of the information system for critical use is relatively low, which is due to the registration of a large number of “critical error” and “suspicion of error” situations, which take time to process. Access restriction subsystems based on the simplest (perceptron) and complex (GMM-HMM) classifiers provide low availability indicators for small values of α, which is caused by the registration of a large number of “critical error” situations in the first and a large number of “suspicion of error” in the second situations. Finally, the best indicators of accessibility for any α values were shown by access control subsystems, based on deep and deep convolution neural networks, the effectiveness of which for the tasks of biometric identification of subjects based on the individual features of their voices was high.

Keywords: information system for critical use, authentication process, access control subsystem, system security policy, confidentiality, availability.

Kovtun Viacheslav V. — Cand. Sc. (Eng.), Assistant Professor, Assistant Professor of the Chair of Computer Control Systems, e-mail: kovtun_v_v@vntu.edu.ua

В. В. Ковтун[1]

Моделирование зависимости конфиденциальности аутентификации и доступности в информационной системе критического применения

[1]Винницкий национальный технический университет

Современные тенденции организации процесса аутентификации в информационных системах критического применения ориентированы прежде всего на повышение его надежности, впрочем, такой подход входит в противоречие с доминирующей в сфере информационной безопасности триадой CIA, в частности, в противоречие входят первый и третий компоненты триады. Следовательно, возникает потребность в формализации математического аппарата, который бы позволил описать зависимость между конфиденциальностью комплексной ступенчатой процедуры аутентификации и доступностью ресурсов информационной системы критического применения, что позволило бы гибко настраивать работу подсистемы разграничения доступа в соответствии с условиями эксплуатации информационной системы. В статье впервые предложена модель зависимости потерь конфиденциальности процесса аутентификации и показателя доступности информационной системы критического применения в которой, в отличие от существующих, процесс синтеза оптимальной полумарковских стратегии управления принятием решений в марковской процессе аутентификации субъектов, желающих получить доступ к ресурсам информационной системы критического применения, формализован как задача математического программирования, что позволяет минимизировать потери доступности процесса аутентификации, конфиденциальность которого не должна снизиться ниже заданного администратором порогового значения. В статье сформулирована методика применения вышеописанной модели с учетом того, что в системной политике безопасности описаны ситуации «критическая ошибка» и «подозрение на ошибку», которые могут идентифицироваться подсистемой разграничения доступа во время процесса аутентификации. Упомянутые ситуации определены с учетом того, что подсистема разграничения доступа имеет ступенчатую, комплексную, последовательно соединенную блочную структуру, а каждая блок-ступень подсистемы включает соответствующие подблоки выделения информативных признаков и классификации, объединенные в ансамбль. Проведенные с использованием созданной модели эксперименты показали, что с уменьшением требований к строгости процесса аутентификации доступность информационной системы критического применения растет, но по достижению пороговым значением потерь конфиденциальности уровня $\alpha \approx 10 \cdot 10^{-2}$ рост доступности прекращается, что можно объяснить окончательным завершением процесса адаптации подсистемы разграничение доступа к индивидуальным особенностям субъектов, на распознавание которых была обучена система. Оказалось, что при малых значениях α доступность информационной системы критического применения является сравнительно низкой, что обусловлено регистрацией большого количества ситуаций «критическая ошибка» и «подозрение на ошибку», на обработку которых тратится время. Подсистемы разграничения доступа основанные на простейших (персептронных) и сложных (GMM-HMM) классификаторах обеспечивают низкие показатели доступности при малых значениях α, что обусловлено регистрацией большого количества ситуаций «критическая ошибка» в первом и большого количества ситуаций «подозрение на ошибку» во втором случаях. Наконец, лучшие показатели по доступности при любых значениях α показали подсистемы разграничения доступа, основанные на глубоких и глубоких сверхточных нейросетях, эффективность которых в задачах биометрической идентификации субъектов по индивидуальным особенностями их голосов оказалась высокой.

Ключевые слова: информационная система критического применения, процесс аутентификации, подсистема разграничения доступа, системная политика безопасности, конфиденциальность, доступность.

Ковтун Вячеслав Васильевич — канд. техн. наук, доцент, доцент кафедры компьютерных систем управления, e-mail: kovtun_v_v@vntu.edu.ua