УДК 004.056.52

А.М. Давиденко, Київ
О.А. Суліма, Київ

АНАЛІЗ ФУНКЦІОНАЛЬНИХ МОЖЛИВОСТЕЙ ОКРЕМИХ КОМПОНЕНТ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ

Abstract. In the paper, the features of the relationship between processes implemented in the information system and processes operating in the subject area of interpretation served by the information system are proposed and studied. In this connection, different levels of description of the subject area of interpretation and their use in the processes of protection against negative factors are considered. , which may lead to the unauthorized use of data from the information system application tasks.

Актуальність

Інформаційна система (IS), що орієнтована на надання послуг користувачам, має бути захищена від співпраці з несанкціонованими користувачами. Базовими компонентами захисту приймаються наступні:

- система захисту доступу до IS;
- система надання повноважень користувачам h_i;
- загальна система безпеки SB та інші.

У рамках даної роботи, в основному, будемо займатися системою надання повноважень (SNP) на використання та перетворення даних з різних компонент, що входять в IS і може певною мірою захищати систему від несанкціонованих користувачів. Основною компонентною, яку захищає SNP, є база даних, за якими звертається користувач, а її елементами є дані x_i.

Для обгрунтованого захисту, необхідно визначати величину рівня такого захисту, який може визначатися рівнем конфіденційності груп даних. Це означає, необхідність розв'язання наступних задач в рамках системи SNP:

- визначити рівень конфіденційності $r_i(x_i)$;
- визначити класифікацію даних для об'єднання їх в групи;
- визначити необхідну кількість значень рівнів конфіденційності даних m.

Рівень конфіденційності даних $r_i(x_i)$ в процесі функціонування системи може змінюватися. Тому встановлення рівня конфіденційності повинно реалізуватися оперативно.

При цьому можуть мати місце ситуації, коли визначена оцінка необхідного рівня конфіденційності не відповідає рівням, що вже використовуються в системі. Тоді, необхідно додатково визначити, до якого найближчого рівня конфіденційності віднести отриману оцінку окремих даних. Оскільки рівень конфіденційності $r_i(x_i)$ і рівень значимості даних мають відмінні інтерпретації, то методи оцінки $r_i(x_i)$ та $\aleph_i(x_j)$ між собою

повинні бути узгодженими. Рівень безпеки, який забезпечується для окремої IS, є інтегральним параметром, який об'єднує поряд з іншими характеристиками і рівень конфіденційності, як одну з оцінок, та рівень значимості окремих компонент системи.

Можливість класифікації даних обумовлюється наступними факторами:

- структурою системи, яка тісно пов'язана з її функціональними характеристиками та рядом інших вимог;
- задачами, що обумовлюються проблемами захисту і в першу чергу, використанням різних систем оцінок, що визначають необхідний рівень захисту;
- інтерпретацією інформаційного наповнення системи та інтерпретацією задач, що на її основі можуть розв'язуватися чи досліджуватися.

Визначення необхідних значень рівня конфіденційності даних чи компонент системи обумовлюється необхідністю забезпечувати безпеку не тільки функціонування самої системи типу IS, а і необхідністю забезпечувати безпеку предметної області, в якій розв'язуються задачі, що використовують ті чи інші дані системи IS. У цьому полягає суть використання поняття конфіденційності як оцінки певного рівня конфіденційності даних, що розміщаються в IS. Оскільки принципова різниця між оцінкою, що ґрунтується на величині рівня конфіденційності та іншими оцінками, що використовуються для визначення рівня безпеки, наприклад, величини ризику, полягає у тому, що оцінка рівня конфіденційності в основному пов'язана з величиною безпеки не самої IS, а безпеки предметної області, у якій розв'язується задача, що використовує конфіденційні дані, то необхідно більш детально розглянути задачу зв'язку системи IS з предметною областю W_i. Природно припустити, що будь-яка система типу IS чи просто інформаційна система, тісно пов'язана з предметною областю W_i, на яку IS орієнтована. Це означає, що в IS доцільно розміщати не тільки дані, які можуть бути потрібні користувачам для розв'язання тих чи інших задач, а й інформацію про користувачів та, в першу чергу, про предметну область W_i, яку IS повинно обслуговувати. Оскільки $r(x_i)$ пов'язана з небезпеками в середовищі W_i, то доцільно розширити інформацію про такі небезпеки. Для опису таких небезпек не достатньо даних з їх мінімальною інтерпретацією, яка забезпечується структурою даних, а необхідно IS розширити наступними даними та інформаційними елементами IS:

- значеннями даних, що відображають небезпечні ситуації в зовнішньому середовищі W_i;
- дані про користувачів, на яких у системі є інформація, що необхідна для розв'язання задач захисту доступу в систему IS;
- інформація та дані про можливі аномалії, що можуть виникати в W_i і суттєво впливати на зменшення величини рівня безпеки із зовнішнього середовища;

– інформація про окремі фрагменти реалізації різних способів перетворення та використання даних, що знаходяться у системі, які можуть або повинні використовуватися потенціальними користувачами системи IS.

Постановка задачі

Задача визначення необхідного значення рівня конфіденційності $r(x_i)$ для даних чи елементів x_i може розв'язуватися в рамках IS в автоматичному режимі без втручання власників відповідних даних у процес визначення величини $r_i(x_j)$, як це має місце в традиційних ситуаціях [1, 2]. Приймемо, що система SNP співпрацює тільки з санкціонованими користувачами, оскільки це повинна забезпечувати система доступу разом із засобами захисту доступу ($SD\&ZD$). Таким чином, визначення можливості надання чи не надання інформації певного рівня конфіденційності $r_j(x_i)$ санкціонованому користувачу, на рівні з іншими критеріями, визначається з урахуванням можливості псевдо передачі цих даних несанкціонованому користувачу (NK). Використання терміну псевдо передачі означає, що можуть існувати механізми, які дозолять користувачу типу NK отримати дані, що характеризуються рівнем конфіденційності $r_j(x_i)$, який є не допустимим для передачі відповідних даних NK. У цьому випадку необхідно розв'язати задачу, яка повинна встановити на основі яких можливостей SK може отримати доступ до даних заданого рівня конфіденційності. Щоб систематизувати можливі підходи до вирішення цієї задачі приймемо наступні визначення, якими будемо користуватися в даній роботі.

Визначення 1. Система доступу разом із засобами захисту доступу ($SD\&ZD$) розв'язує задачу визначення: чи користувач, що звернувся до IS, є санкціонований і ця задача розв'язується на основі аналізу даних, що характеризують самого користувача.

У відповідності з приведеним визначенням приймемо, що $SD\&ZD$ розв'язує задачу авторизації користувача, що можна описати наступним співвідношенням:

$$\{SD[k(p_1^k,\dots,p_r^k)]\&ZD(p_1^{SD},\dots,p_l^{SD}) \to Al^D\left(p_1^k,\dots,p_r^k,p_1^{/D},\dots,p_e^{lD}\right)\} \to$$
$$\to \{[(k \to sk)\&\neg(k \to NK)] \vee [(k \to NK)\&\neg(k \to sk)]\},$$

де p_i^k – параметр користувача, p_e^{lD} – параметр системи доступу, Al^D – алгоритм ідентифікації та авторизації користувача, що звернувся до IS із запитом по інформацію, k – користувач, статус якого є невизначеним в $SD\&ZD$.

Визначення 2. Система надання повноважень розв'язує проблему, що полягає у визначенні: чи задача, для розв'язання якої користувач SK звернувся до системи, має повноваження на використання відповідних даних, тобто чи використання задачею Za_i даних $r_j(x_i)$ не призведе до недопустимих ситуацій в середовищі W_i, на яке орієнтована відповідна задача.

Приведене визначення свідчить, що система SNP не стільки надає повноваження користувачу, скільки надає повноваження задачі на використання тих чи інших даних. Таким чином загальна система безпеки IS організує процес свого функціонування з наступними чинниками, що звертаються до системи:

- користувачем, якого ідентифікує і верифікує $(SD\&ZD)$ на основі даних і параметрів, які характеризують його, а система в результаті аналізу цих параметрів надає користувачу статус санкціонованого чи не санкціонованого або $SK \vee NK$;
- задачею, яку представляє SK системі і потребує тих чи інших даних для активізації свого процесу функціонування або процесу розв'язання.

Зі сторони IS система безпеки SB використовує систему надання повноважень SNP для надання повноважень на використання даних, що потрібні для розв'язання задачі, яку представив користувач.

Виходячи з цього можна стверджувати, що крім даних про користувачів, які використовуються системою $(SD\&ZD)$, засоби системи SB повинні володіти даними, які необхідні для встановлення повноважень деякої задачі Za чи встановлення відсутності повноважень у задачі Za_i використовувати дані, які відповідна задача потребує або визначення статусу задачі типу $N\ Za_i$. Формально цю ситуацію можна описати наступним співвідношенням:

$$\left\{\left[K(p_1^k,\dots,p_r^k)\&Za_i\left(p_1^z,\dots,p_g^z\right)\right]\rightarrow(SD\&ZD)\rightarrow Al^D(p_1^k,\dots,p_r^k,p_1^D,\dots,p_0^D)\right\}\rightarrow$$

$$\rightarrow\left\{Sk\left[Za\left(p_1^z,\dots,p_g^z\right)\right]\rightarrow(SNP)\rightarrow Al^{NP}\left(p_1^z,\dots,p_g^z,p_1^p,\dots,p_g^p\right)\right\}\rightarrow$$

$$\rightarrow\left\{Sk\left[Za\left[r_{j1}(x_1),\dots,r_{jm}(x_m)\right]\right]\rightarrow C[Za_i(y_{i1},\dots,y_{ie})]\right\},$$

де p_i^z – параметри задачі, Al^{NP} – алгоритм визначення необхідних повноважень у задачі Za_i, p_i^p – параметри системи SNP, $r_{ij}(x_i)$ – дані x_i, що мають рівень конфіденційності r_{ji}, y_i – результат розв'язання задачі, C – мета розв'язання задачі Za_i.

Вирішення задачі

Для розв'язання таким чином сформульованої задачі забезпечення певного рівня безпеки системою $SB(IS)$ необхідно визначитися з параметрами задачі Za_i та з описом мети C_i розв'язання задачі $Za_i(y_{i1},\dots,y_{ie})$. Дані, які знаходяться в IS, і особливо дані, що використовуються в прикладній задачі $Za_i(y_{i1},\dots,y_{ie})$, не представляють собою деякі абстрактні величини. Вони завжди мають в рамках IS і, відповідно, в рамках W_i певну інтерпретацію, що записується у вигляді $j^S(x_i)$, якщо мова йде про інтерпретацію, що розміщається IS, та $j^W(x_i)$, якщо мова йде про інтерпретацію x_i в предметній області W_i. Прикладом інтерпретації x_i в IS є служити інформація про допустимий діапазон значень даних x_i.

Практика побудови системи IS переважно не передбачає розміщення більш менш повної інтерпретації даних $j(x_i)$ в IS. Це призводить до того, що обґрунтування тієї чи іншої структури даних в IS залишається за межами IS у рамках процесів проектування системи. Це суттєво зменшує загальні можливості системи, особливо ті, що стосуються забезпечення заданого рівня безпеки даних, яку будемо позначати $\mu = f(SB)$. У рамках даного підходу дані, що розміщаються в IS, забезпечуються інтерпретаційними описами, повнота яких визначається рівнем конфіденційності r_i, рівнем значимості $\aleph_i$ та рівнем безпеки μ системи IS в цілому. Завдяки цьому проблема визначення необхідного рівня конфіденційності даних $r(x_i)$ може бути розв'язаною в рамках SNP, яка є функціональною компонентою всієї системи безпеки. По своїй суті опис інтерпретації $j(x_i)$ даних x_i відображає взаємозв'язки x_i з оточенням в W_i, рівень значимості x_i для W_i та рівень небезпеки, до якої може привести не коректний або не допустимий спосіб використання даних x_i в рамках W_i. Приймемо наступні положення, що відображають взаємозв'язок IS з предметною областю інтерпретації, до якої відносяться дані.

Положення 1. Будь-яка IS має власну W_i або власний фрагмент w_{ij} в загальній W_i.

Положення 2. Інтерпретація всіх даних x_i з IS $j(x_{is}),\ldots,j(x_{im})$ виводиться з опису інтерпретації W_i або $J(W_i) \to \forall j(x_i)[x_i \in IS]$.

Положення 3. Предметна область W_i представляє собою структурований опис всіх елементів $x_i \in W_i$ та всіх подій $y_i \in W_i$, які можуть виникати в W_i у результаті активізації процесів $f_i(x_{i1},\ldots,x_{im})$, що записується у вигляді співвідношення $y_i = f_i(x_{i1},\ldots,x_{im})$.

Для опису $y_i = f_i(x_{i1},\ldots,x_{im})$ використовуються системи правил, які залежать від способів опису W_i. Предметна область W_i може описуватися на різних рівнях загальності серед яких прийнято виділяти наступні [3, 4]:

- структурний рівень $S(W_i)$;
- логічний рівень $L(W_i)$;
- семантичний рівень $\sigma(W_i)$;
- розширений рівень опису $R(W_i)$;
- комбінований рівень опису $K(W_i)$.

Той чи інший рівень опису предметної області W_i і, відповідно, даних x_i використовується в залежності від задач, які передбачається розв'язувати, наприклад, структурний рівень опису $S(W_i)$ переважно використовується у випадках, коли задачі, що розв'язуються в рамках IS, представляють собою впровадження в IS та видачі з IS окремих даних. Якщо задачі, що розв'язуються в IS, орієнтовані на реалізацію перетворень даних з IS з метою отримання нових даних, необхідно використовувати логічний рівень опису предметної області [5].

Очевидно, що інтерпретаційні описи даних, які відносяться до W_i,

повинні так чи інакше переноситися і в системи IS, які орієнтовані на обслуговування відповідної W_i. У кожній предметній області W_i можуть виникати негативні події, які визначаються на основі критеріїв, прийнятих в окремих W_i.

Такі негативні події можуть призводити до виникнення аномальних фрагментів або негативних ситуацій. Відображення таких негативних ситуацій у поточних описах фрагментів W_i залежить від рівня опису, який використовується.

Наприклад в описі, що реалізується на логічному рівні, негативні ситуації відображаються виникненням логічних аномалій [6].

При описі на семантичному рівні окремних фрагментів негативні ситуації відображаються у вигляді семантичних аномалій. Розширений рівень опису використовує не тільки текстові описи, а й інші форми відображення предметної області, наприклад, графічні фрагменти відображення різних аспектів, що мають місце в предметній області. Прикладом таких розширень можуть бути графічне відображення залежностей між змінними чи аналітичні описи залежностей і таке інше. Комбіновані методи відображення передбачають сумісне використання структурних і текстових форм відображення. Прикладом таких способів відображення можуть бути блок-схеми процесів, що відображаються у відповідних описах та інші. Введемо наступне визначення.

Визначення 3. Негативними факторами, що можуть виникати у W_i в результаті використання даних x_i з рівнем конфіденційності r_{ji} санкціонованим користувачем для розв'язання необґрунтованої задачі Za_i, є відповідні аномалії, що мають власну інтерпретацію.

У приведеному визначенні мова йде про санкціонованого користувача, яким є користувач, що пройшов ідентифікацію в системі ($SD\&ZD$). Це означає, що захищена IS системою доступу буде співпрацювати з користувачем SK. У рамках даного підходу довільний k_i звертається до IS не просто за отриманням тих чи інших даних, а у випадку, коли ці дані мають певний рівень r_i, тому k_i повинен надати системі обґрунтування необхідності їх використання для розв'язання конкретної задачі Za_i і ці обґрунтування представляють собою наступне:

- опис мети задач $C_i(K_i)$;
- параметри задачі $Za_i(P_{i1}^z, \ldots, P_{im}^z)$;
- обґрунтування необхідності розв'язання відповідної задачі.

Опис мети задачі по суті представляє собою опис фрагменту процесу функціонування, реалізація якого є однією із можливих складових всієї мети або $c_i(W_i) \in C[Za_i, W_i]$ та є обґрунтуванням необхідності використання даних типу $r_{ji}(x_i)$. Необхідність використання даних типу $r_{ji}(x_i)$ в Za_i підтверджуються фрагментами алгоритму $Al_i(Za_i)$, що розв'язує задачу, яка приводить до досягнення мети і використовує дані $r_{ji}(x_i)$. Опис фрагмента $Al_i(Za_i)$ та $c_i(Za_i) \in C(Za)$ реалізується на рівні, який відповідає рівню, що

використовується для розв'язання задач. Наприклад, якщо для опису використовується $L(W_i)$, то фрагмент алгоритму представляє собою відповідний фрагмент опису логічних перетворень з представленими даними серед яких є дані типу $r_{ji}(x_i)$. Оскільки система SNP на кінцевому етапі надає або не надає повноваження на використання $r_{ji}(x_i)$, то для цього достатньо визначити чи представлена користувачем SK ціль розв'язання задачі описує недопустиму в W_i ситуацію або подію. Якщо це має місце, то SNP не надає повноважень на використання $r_{ji}(x_i)$ користувачу SK при розв'язанні представленої користувачем задачі Za_i. Якщо ціль $C_i(Za_i)$ розпізнана, але не відома її інтерпретація, то SNP перевіряє представлені фрагменти $\varphi_i[Al_i(Za_i)]$ з метою визначення чи вони не приводять до виникнення логічної аномалії, прикладом якої може служити виникнення логічної суперечності в результаті здійснення відповідного перетворення.

Приведений опис може інтерпретуватися таким чином, що класифікація даних відповідно рівня їх конфіденційності у системі типу IS може в окремих випадках бути надмірною, оскільки щоразу, коли SK звертається за даними x_i, система SNP перевіряє чи їх використання в задачі Za_i не призводить до виникнення негативних ситуацій в W_i. У цьому випадку ситуація є досить складною і потребує початкового встановлення структури класифікації даних відповідно до параметру конфіденційності даних в силу наступних причин:

- процес визначення повноважень SK до використання в задачі Za_i даних $r_i(x_i)$ потребує певного часу та обчислювальних ресурсів і щоразу реалізувати цей процес по відношенню до даних, які, не можуть привести до аномалій в W_i, немає сенсу;
- при проектуванні IS на основі аналізу W_i встановлюється початкова необхідна кількість рівнів конфіденційності даних та формується структура організації цих даних і умови активізації SNP, які активізуються лише у випадку, коли SK звертається за певними даними типу $r_{ji}(x_i)$;
- проектування системи SNP потребує початкових даних для її реалізації основними з яких є: кількість рівнів конфіденційності $m(r_i)$, інтерпретація відповідних рівнів конфіденційності $j(x_i)$.

Важливим при такому підході є питання про формування шкали вимірювання рівня конфіденційності. Переважно така шкала будується на основі втрат, до яких приводить необґрунтоване, а тим більше, несанкціоноване використання $r_i(x_i)$. Такий підхід вносить певну суб'єктивність у відповідний рівень оцінки. Така суб'єктивність підсилюється у зв'язку з тим, що рівень конфіденційності з часом може зменшуватися через розвиток W_i та змінами, які в ній можуть відбуватися. Тому приймемо наступний підхід до динамічної корекції рівня конфіденційності окремих даних та до способу модифікації шкали конфіденційності. Така модифікація може полягати у зміні:

– величин масштабів рівня конфіденційності на окремих фрагментах шкал такого вимірювання;
– величин рівня конфіденційності на окремих рівнях, які були встановлені на етапі проектування;
– розмірів шкали вимірювання рівня конфіденційності.

Насамперед величини рівня конфіденційності тих чи інших даних будемо вимірювати не в коштах, що визначають величини втрат у випадку необґрунтованого використання $r_i(x_i)$, а у величині впливу відповідної аномалії на середовище, у якому вона виникла. Крім того, для визначення рівня впливу аномалій на W_i, будемо враховувати розміри аномалії, що може виникнути по відношенню до фрагментів, на які така аномалія впливає. Для кожного рівня загальності опису W_i шкали вимірювання величини впливу аномалії An_i будуть різні і рівень загальності опису An_i буде визначати рівень точності такого вимірювання. Оскільки шкала вимірювання величин конфіденційності формується на основі аналізу впливу аномалій на середовище W_i або $An_i \to W_i$, то відповідні величини визначаються на етапі проектування системи SNP. У процесі роботи SNP зміни масштабу вимірювання $r_i(x_i)$ здійснюються на основі даних про розміри аномалії, яка представлена в описі процесу розв'язання задачі та на основі визначення частоти використання тих чи інших даних, що описуються параметром конфіденційності $r_i(x_i)$ і призвели до виникнення цих аномалій. Крім самого опису процесу реалізації відповідного фрагменту алгоритму, що використовує мету задачі (Za_i), система SNP використовує додаткові параметри, які характеризують $r_i(x_j)$. До таких параметрів відносяться наступні:

– інтервал часу використання $r_i(x_j)$ в процесі розв'язання (Za_i), який входить в інтервал часу реалізації всього процесу розв'язання Za_i;
– всі дані, що зберігаються в IS, мають окремі описи інтерпретації такого параметру, тому при використанні деякого параметру $r_i(x_j)$ в задачі Za_i такий параметр повинен мати величину рівня семантичної узгодженості, який в межах заданого діапазону відповідає величині, яка характеризує x_i в IS як окремий параметр даних типу $r_i(x_j)$;
– зв'язність даних типу $r_i(x_j)$ визначає кількість елементів з якими елемент $r_i(x_j)$ може взаємодіяти в процесі реалізації $Al_i(Za_i)$. При цьому враховується рівень конфіденційності таких елементів.

Ці параметри приписуються елементам $r_i(x_j)$ на стані проектування і використовуються: при визначенні рівня обґрунтованості, наданні цих даних, визначенні повноважень до їх використання відповідною задачею. Користувач SK, який активізує виконання задачі Za_i і потребує дані типу $r_i(x_j)$, повинен мати інформацію про ці параметри, які визначаються середовищем задачі, що розв'язується, і такі дані повинен надавати для обґрунтування необхідності отримання повноважень на активізацію задачі

Za_i. Кожний фрагмент інформації, який будемо позначати символом $\Psi_i(x_j)$, представляє собою деяку числову величину, яка розширюється описом текстової інтерпретації, що формально описується наступним співвідношенням:

$$\Psi_i(x_j) = x_j\iota < \alpha_{i1} * \ldots * \mathrm{A}_{ik} *> I < \xi_{j1}, \ldots, \xi_{jm} >,$$

де $\Psi_i(x_j)$ – елемент інформації з IS, x_j – числова величина $\Psi_i(x_j)$, α_{ij} – фраза текстового опису інтерпретації $\Psi_i(x_j)$, яка пов'язує x_j з текстовими та іншими описами предметної області W_i, ξ_{ij} – параметри x_j, про які йшла мова вище. Якщо має місце $r_i(x_j)$, то це означає, що рівень конфіденційності поширюється на весь інформаційний елемент $\Psi_i(x_j)$. Залежно від рівня конфіденційності r_i, відповідний фрагмент може використовуватися обмежене число раз. Така величина використовується для опису $r_i(x_j)$ і є невідома SK. Величина, яка є параметром $\xi_{ij}[r_i(x_j)]$ відіграє ключову роль при визначенні повноважень на використання $r_i(x_j)$.

Висновок

У роботі запропоновано та досліджено особливості взаємозв'язку між процесами, що реалізуються в IS, та процесами, що функціонують в предметній області інтерпретації, яку обслуговує IS У звязку з цим розглядаються різні рівні опису предметної області інтерпретації та їх використання у процесах захисту від негативних факторів, які можуть обумовлювати несанкціоноване використання даних з IS прикладними задачами.

1. *Лазарев И.А*. Информация и безопасность. композиционная технология информационного моделирования сложных объектов принятия решений / И.А. Лазарев. – М.: Московский городской центр научно-технической информации, 1997. – 336 с.
2. *Зегжда Д.П.* Как построить защищённую информационную систему / Д.П. Зегжда, А. М. Ивашко. – СПб.: Мир и семья, 1997. – 312 с.
3. *Коростіль О.Ю.* Аналіз методів інтерпретації текстових моделей / О.Ю. Коростіль // Моделювання та інформаційні технології. Зб. наук. праць ІПМЕ ім. Г.Є. Пухова НАН України, 2012. – Вип. 62. – С.47-58.
4. *Коростіль О.Ю.* Розширення параметрів текстових описів інформаційних потоків / О.Ю. Коростіль // Моделювання та інформаційні технології. Зб. наук. праць ІПМЕ ім. Г.Є. Пухова НАН України, 2012. – Вип. 65. – С.24-31.
5. *Коротков М.А.* Основы формальных логических языков / М.А. Коротков, Е.О. Степанов. – СПб.: ГИТМО, 2003. – 85 с.
6. *Шенфилд Д.* Математическая логика / Д. Шенфилд. – М.: Наука, 1975. – 528 с.

Поступила 20.09.2018р.