Висновки

Проведені дослідження показали, що для сучасних ІКСМ найоптимальнішим варіантом буде використання шаблону непрямої системи автентифікації. Роль автентифікаційного сервера, що приймає запити на автентифікацію від інших серверів повинен відігравати сервер бази даних. На сервері бази даних повинна підтримуватись єдина актуальна база особистих даних користувачів, що спрощує процес адміністрування. Комплекс засобів захисту ІКСМ для забезпечення надійного захисту повинен розміщуватися на сервері бази даних, але при цьому за рахунок відповідних клієнтських додатків охоплювати всі комп'ютери робочих груп, адміністраторів та керівництва, а також всі сервери, що містяться в автоматизованій системі.

Література

[1] Теоретические основы компьютерной безопасности. Учебное пособие для вузов / П.Н. Девянин, О.О. Михальский, Д.И. Правиков. – М.: Радио и связь, 2010. – 192 с.

[2] Богуш В.М., Довидьков О.А. Теоретичні основи захищених інформаційних технологій. – К.: ДУІКТ, 2009. – 414 с.

[3] Белов Е.Б. Основы информационной безопасности. Учебное пособие для вузов / Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. – М.: Горячая линия – Телеком, 2006. – 544 с.

УДК 004.056.53 (045)

Чунарева А.В., Чунарев А.В. Анализ существующих шаблонов систем аутентификации в информационно-коммуникационных системах и сетях

Аннотация. *В данной статье проведен анализ шаблонов аутентификации в современных информационно-коммуникационных системах и сетях. В результате проведения анализа выделены преимущества и недостатки применения существующих шаблонов для обеспечения надежной защиты. Выделены наиболее эффективные с точки зрения разграничения и контроля доступа к информационным ресурсам.*

Ключевые слова: *защита информации, аутентификация, верификатор, информационно-коммуникационная система и сеть, система защиты.*

Chunariova A.V., Chunariov A.V. Analysis of existing authentication systems of information and communication systems and networks

Abstract. *This article analyzes patterns of authentication in modern information and communication systems and networks. As a result, the analysis highlighted the advantages and disadvantages of the existing templates to provide protection. Select the most efficient in terms of differentiation and control of access to information resources.*

Keywords: *information security, authentication, the verifier, information and communication system and network security system.*

Отримано *13 вересня 2012 року,* затверджено редколегією *8 листопада 2012 року*
(рецензент д.т.н., професор О.К. Юдін)

СИСТЕМА АНАЛІЗУ ТА ОЦІНКИ РІВНЯ ЗАХИЩЕНОСТІ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ ВІД СОЦІОТЕХНІЧНИХ АТАК

Дарина Горніцька, Марія Захарова, Андрій Кладочний

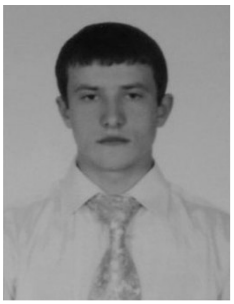
Національний авіаційний університет

ГОРНІЦЬКА Дарина Анатоліївна

Рік та місце народження: 1985 рік, м. Київ, Україна.
Освіта: Національний авіаційний університет, 2007 рік.
Посада: аспірант Національного авіаційного університету.
Наукові інтереси: інформаційна безпека, соціотехнічні атаки.
Публікації: більше 20 наукових публікацій, серед яких наукові статті та патенти на винаходи.
E-mail: darja85@ukr.net

ЗАХАРОВА Марія В'ячеславівна , к.т.н., доцент

Рік та місце народження: 1978 рік, м.Томарі, Росія.
Освіта: Черкаський інженерно-технологічний інститут (Черкаський державний технологічний університет), 2001 рік.
Посада: завідувач кафедри інформатики та інформаційної безпеки з 2012 року.
Наукові інтереси: інформаційна безпека
Публікації: більше 40 наукових публікацій.
E-mail: zmaria@yandex.ru



КЛАДОЧНИЙ Андрій Іванович

Рік та місце народження: 1990 рік, смт. Катеринопіль, Черкаська область, Україна.
Освіта: бакалавр, Національний авіаційний університет, 2012 рік.
Посада: студент Національного авіаційного університету група АМ-532.
Наукові інтереси: інформаційна безпека, системи оцінки захищеності.
Публікації: авторське свідоцтво "Програмна система оцінки захищеності від соціотехнічних атак».
E-mail: yozzuk@gmail.com

Анотація. *В роботі представлена структурна схема системи аналізу та оцінки рівня захищеності державних інформаційних ресурсів від соціотехнічних атак, яка базується на логіко-лінгвістичному підході та методології синтезу систем аналізу та оцінки рівня захищеності державних інформаційних ресурсів від атак даного класу. На основі запропонованих рішень розроблений алгоритм та програмний засіб, який, з одного боку, дозволяє здійснювати об'єктивну оцінку рівня підготовленості персоналу до соціотехнічних атак, а з іншого – оцінити загальний рівень захищеності державних інформаційних ресурсів, грунтуючись на групових відповідях. Ефективність розробленого продукту було доведено в ході експерименту, суть якого розкрита в даній роботі. Розроблений програмний продукт реалізує принципово новий підхід до атестації кадрів, задіяних в обслуговуванні державних інформаційних ресурсів, зокрема, пов'язаних з їх безпекою.*

Ключові слова: *методологія синтезу, система аналізу, соціотехнічні атаки, державні інформаційні ресурси, аналіз загроз, оцінка захищеності.*

Вступ

Одним з основних етапів побудови комплексної системи захисту інформації з метою забезпечення безпеки державних інформаційних ресурсів (ДІР) є розробка моделі загроз. При цьому для організацій державного сектору, для яких характерні багаточисленність персоналу, розвинута мережа філіалів, велика кількість загальнодоступної інформації, слабка організація пропускного режиму та недостатня підготовка персоналу відповідним правилам безпеки, згарози що реалізуються шляхом соціотехнічних атак (СА) є найбільш небезпечними. Про це свідчить велика увага до безпеки персоналу, приділена у міжнародному стандарті ISO / IEC 27002:2005 [1]. Отже, сьогодні існує нагальна потреба у ефективних засобах, які б дозволили у автоматизований спосіб здійснювати оцінку рівня підготовленості персоналу, пов'язаного з обслуговуванням ДІР, до СА, а також оцінювати загальний рівень безпеки ДІР стосовно атак даного класу.

Аналіз існуючих досліджень

На основі аналізу джерел в яких розглядається СА на інформаційні ресурси [2-5], оцінки якості експерта для реалізації експертиз у сфері інформаційної безпеки [6-7] та системи захисту, що засновані на експертному оцінюванні та логіко-лінгвістичному підході [5] розроблена система опитування персоналу (СОП), яка дозволяє проводити тестування співробітників за заздалегідь підготовленими та ранжируваними експертною групою запитами. Слід зазначити, що вона складається з експертів, якість яких заздалегідь перевірена [6].

Основна частина дослідження

Структурна схема СОП (рис. 1) містить: підсистеми експертного управління (ПЕУ) та профілів користувачів (ППК), модулі лінгвістичного розпізнавання (МЛР) та генерації звітів (МГЗ).

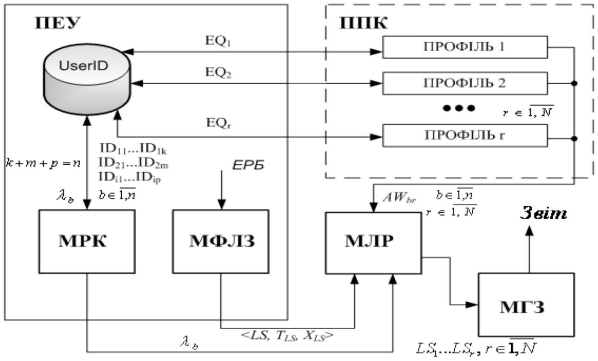


Рис. 1. Структурна схема СОП

Основою СОП є ПЕУ, яка дозволяє експертам керувати компонентами базових експертних запитів

$ID_{11}…ID_{1k}$, $ID_{21}…ID_{2m}$, $ID_{i1}…ID_{ip}$, де i – кількість загроз СА, визначених раніше, а k, m, p – кількість складових запиту першої, другої та i-ї СА відповідно. Підсистема ПЕУ враховує профіль користувача EQ_r в залежності від посади, де r – кількість профілів персоналу, дозволяє вилучати компоненти запиту, додавати нові та проводити ранжирування за методом Сааті (модуль ранжирування компонент (МРК)) [7] шляхом побудови матриці попарних порівнянь (рис. 2).

Експерт також має змогу формувати еталонні рівні безпеки *ЕРБ* – нечіткі числа, на основі яких проводиться розрахунок рівня захищеності ДІР, за що відповідає модуль формування лінгвістичних змінних (МФЛЗ) ПЕУ. Лінгвістична змінна (ЛЗ) „рівень безпеки” (*LS*), що задається кортежем <*LS*, T_{LS}, X_{LS}>, її базова терм-множина $T_{LSw} = \bigcup_{w=1}^{5} T_{LS_w}$ та інтервали передаються на МЛР для розпізнавання та інтерпретації рівня безпеки.

Система передбачає, що для кожного типу посад експерти повинні скласти свій базовий експертний запит, тобто для різних посад передбачені різні компоненти запитів, а отже функціонування ПЕУ (рис. 3) пов’язане з ППК, яка дозволяє створювати нові профілі персоналу та вилучати зайві.

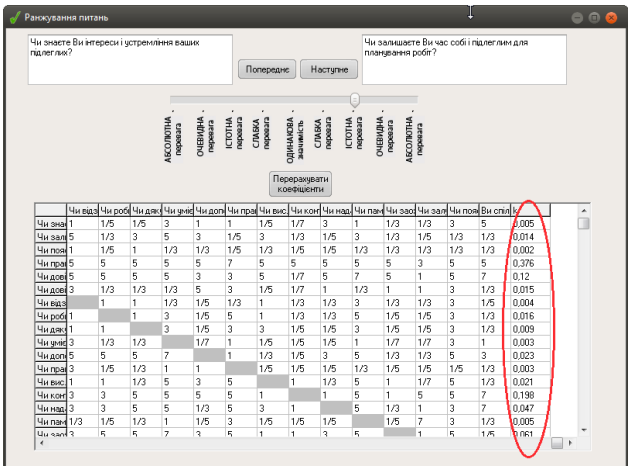


Рис. 2. Ранжирування запитів

При створенні нового профілю експерт має змогу сформувати базовий експертний запит для зазначеної посади та одразу провести його ранжирування.

Інформаційна місткість та стійкість різних варіантів даного протоколу є обернено пропорційними величинами. Окреме значення має МГЗ, який дозволяє реалізувати визначення загального рівня захищенності ДІР від СА в організації при сукупній оцінці відповідей всього опитаного персоналу або визначити рівень захищеності в залежності від профілю. Звіти формуються у графічному вигляді та відображають визначений рівень безпеки по відношенню до *ЕРБ* (рис. 4).

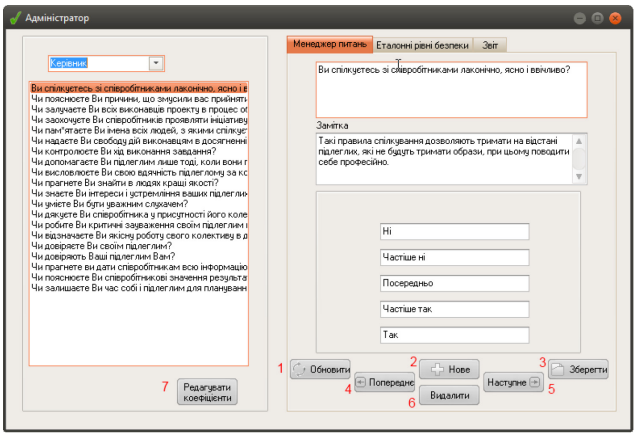


Рис. 3. Приклад роботи ПУЕ

Ґрунтуючись на запропонованій структурній схемі СОП можливо створити програмне забезпечення (ПЗ), яке дозволить здійснювати оцінку рівня підготовленості персоналу до СА, а також оцінювати загальний рівень безпеки ДІР в організації стосовно атак даного класу.

Алгоритм роботи зазначеного ПЗ представлений на рис. 5.

Принцип роботи розробленого ПЗ полягає в наступному: для того, щоб розпочати тестування, потрібно на головній формі у списку обрати необхідний профіль і натиснути кнопку „Тест”.

Після цього відкриється відповідна форма тестування - одне за одним будуть з’являтися запити. Наявність на формі тестування кнопки, за допомогою якої користувач може отримати пояснення щодо поточного компоненту запиту залежить від стану прапорця „Підказка” на головній формі.

Коли прапорець знаходиться у вімкненому стані – кнопка підказки присутня на формі, коли у вимкненому – відсутня. Побачити результати опитування можна лише відповівши на всі запити.

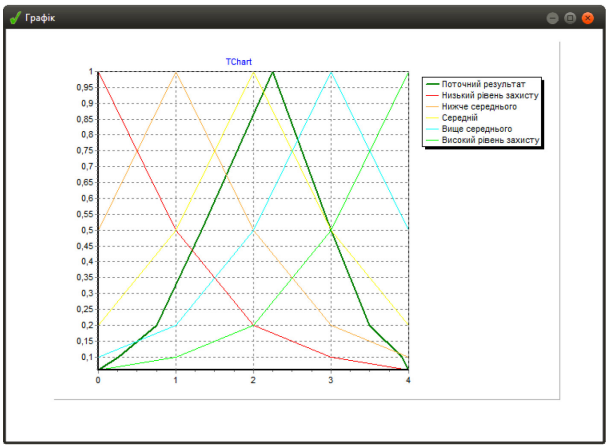


Рис. 4. Звіт захищеності ДІР від СА

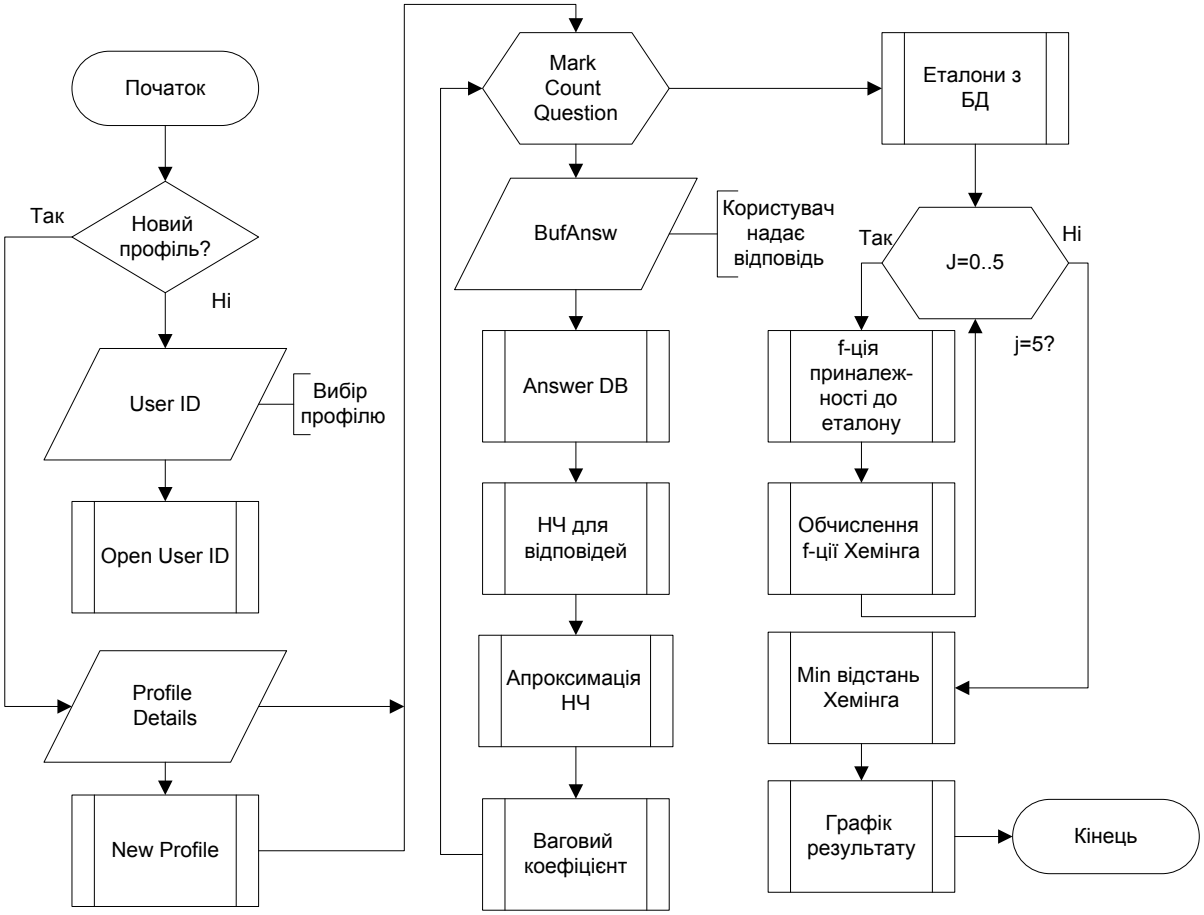


Рис. 5. Алгоритм роботи ПЗ

Після натискання кнопки ,,Закінчити" з'явиться вікно з повідомленням про рівень захисту за результатами наданих відповідей, а після закриття цього вікна – графік, що відображає поточний стан захищеності ДІР від СА відносно еталонних рівнів захищеності. Із розробленим ПЗ було проведено експеримент, який довів його працездатність та валідність.

Експеримент проводився на персональному комп'ютері (ПК) з наступною конфігурацією: операційна система Microsoft Windows 7 Ultimate Service Pack 1 7601 x64 на ПК Lenovo IdeaPad G570 (59-304824), процесор Intel Core i5 2410M (2,3 ГГц), оперативна пам'ять DDR3 4 Гб, жорсткий диск WDC WD7500BPVT-24HXZT1, відеоадаптер ATI Mobility Radeon HD6370 1024Мб.

Для проведення експерименту було змодельовано три ситуації із різними рівнями підготовленості опитуваного: коли надавались усі невірні відповіді, коли опитуваний надає всі вірні відповіді і коли результати відповідей мають посередній характер.

В останньому випадку було показано зміну результатів тесту при зміні відповіді на один запит до ,,Високого" рівня та один запит до ,,Низького" рівня захищеності. При цьому були отримані наступні результати: для невідготовленого співробітника, коли опитуваний на всі запити надавав невірні відповіді, рівень його підготовленості до СА повністю співпав з еталонним рівнем захисту ,,Низький"; у випадку, коли опитуваний надав усі вірні відповіді рівень захисту цілковито співпав з еталонним рівнем ,,Високий"; при збалансованій кількості вірних та невірних відповідей результат тестування співпав з еталонним рівнем ,,Середній".

В ході експерименту також було випробувано зміну результатів тестування на один запит, коли користувач змінює відповідь, яка відображає зміни до ,,Низького" рівня захищеності. При цьому результат тестування не суттєво змістився ліворуч від еталонного рівня ,,Середній", але залишився йому відповідним.

Характер зміщення залежить від вагового коефіцієнта кожного компоненту запиту, який було визначено експертом в налаштуваннях програми. Аналогічним чином було прослідковано зміну коли один із параметрів покращується. У результаті рівень захисту залишився ,,Середній", проте саме його значення на графіку змістилося праворуч відповідного еталону.

Висновки

На основі розробленої структури СОП було розроблено програмний засіб, який дозволить застосувати нові підходи до проблем підбору та атестації кадрів у державних організаціях і установах. Працездатність та ефективність розробленого ПЗ було доведено шляхом експерименту.

Практичне застосування ПЗ не потребує зусиль з боку співробітників та дозволить швидко та ефективно виявляти співробітників організації, які можуть піддатися СА, що в свою чергу дозволить своєчасно провести роз'яснювальну роботу та провести навчання персоналу і підвищити загальний рівень безпеки орагнізації та ДІР згідно із вимогами ISO/IEC 27002:2005 [1].

Література

[1] ISO/IEC 27002:2005 Информационные технологии. Свод правил по управлению защитой информации с учетом Технической поправки 1, опубликованной 2007-07-01.

[2] Горніцька Д. А. Система социотехнических атак в информационной среде / Д. А. Горніцька, О. Г. Корченко, В. П. Харченко // Проблемы экономики и управления на железнодорожном транспорте. Материалы второй международной научно-практической конференции. – К.: ЭКУЖТ, 2007. – С. 137-138.

[3] Горницкая Д. А. Атаки на ресурсы информационных систем в современном информационном обществею / Д. А. Горницкая, А. Г. Корченко, Е. В. Пацыра // Информационные технологии в гуманитарном образовании. Материалы I Международной научно-практической конференции. – Пятигорск: 2008. – Ч.II. – С.224-233.

[4] Горніцька Д. А. Визначення коефіцієнтів важливості для експертного оцінювання у галузі інформаційної безпеки / Д. А. Горніцька, О. Г. Корченко, В. В. Волянська // Захист інформації. – 2012. – №1. – С.108–121.

[5] Корченко А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / Корченко А. Г. – К. : "МК-Пресс", 2006. – 320с.

[6] Горніцька Д. А. Дослідження методів апріорної оцінки якості експерта для реалізації експертиз у сфері інформаційної безпеки / О. Г. Корченко, Д. А. Горніцька, Т. Р. Захарчук // Захист інформації. – Київ, 2010. – №4. – С.53–60.

[7] Горніцька Д. А. Визначення коефіцієнтів важливості для експертного оцінювання у галузі інформаційної безпеки / О. Г. Корченко, Д. А. Горніцька, В. В. Волянська // Захист інформації. – Київ, 2012. – №1. – С.108-121.

УДК 004.056.5 (045)

Горницкая Д.А., Захарова М.В., Кладочный А.И. Система анализа и оценки уровня защищенности государственных информационных ресурсов от социотехнических атак.

Аннотация. *В работе представлена структурная схема системы анализа и оценки уровня защищенности государственных информационных ресурсов от социотехнических атак, основанная на логико-лингвистическом подходе и методологии синтеза систем анализа и оценки уровня защищенности государственных информационных ресурсов от атак данного класса. На основе предложенных решений разработан алгоритм и программное средство, которое, с одной стороны, позволяет осуществлять объективную оценку уровня подготовленности конкретного лица из числа персонала к социотехнических атак, а с другой - оценить общий уровень защищенности государственных информационных ресурсов, основываясь на ответах группы пользователей . Эффективность разработанного продукта было доказано в ходе эксперимента, суть которого раскрыта в данной работе. Разработанный программный продукт реализует принципиально новый подход к аттестации кадров, задействованных в обслуживании государственных информационных ресурсов, в частности, связанных с их безопасностью.*

Ключевые слова: *методология синтеза, системы анализа, социотехнические атаки, государственные информационные ресурсы, анализ угроз, оценка защищенности.*

Gornitska D.A., Zaharova M.V., Kladochniy A.I. System analysis and evaluation of the level of protection of state information resources from social engineering attacks

Abstract. *In the article presented block diagram ofsystem analysis and evaluation of the protection level of state information resources from social engineering attacks based on logical-linguistic approach and methodology for the synthesis of systems analysis and assessment of the level of protection of state information resources from attack by the class. On the basis of the proposed solutions have developed an algorithm and a tool, which, on the one hand, allows for an objective assessment of the level of preparedness of a particular person from the staff to social engineering attacks, and the other - to assess the overall level of security of government information resources, based on the responses of users. The effectiveness of the developed product has been proved in the experiment, the essence of which is disclosed in the paper. The software product implements a new approach to certification of personnel involved in the maintenance of state information resources, particularly related to their safety.*

Keywords*: methodology for the synthesis, systems analysis, social engineering attacks, government information resources, threat analysis, evaluation of security.*

Отримано *12 вересня 2012 року,* затверджено редколегією 13 *листопада 2012 року*
(рецензент д.т.н., професор О.Г. Корченко)