УДК 004.9
DOI https://doi.org/10.15589/znp2023.4(493).21

INFORMATION SECURITY DECISION SUPPORT SYSTEM FOR AN ACCOUNTING COMPANY USING A STRUCTURAL AND CONCEPTUAL DESIGN ALGORITHM

СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БУХГАЛТЕРСЬКОЇ КОМПАНІЇ З ВИКОРИСТАННЯМ АЛГОРИТМУ СТРУКТУРНО-КОНЦЕПТУАЛЬНОГО ПРОЄКТУВАННЯ

Iryna V. Fedosova
irivasilevna1964@gmail.com
ORCID: 0000-0003-3923-8270
Mykyta A. Shcherbatykh
scherbatyhna@gmail.com
ORCID: 0009-0001-1540-9795

І. В. Федосова,
докт. пед. наук, професор
М. А. Щербатих,
здобувач вищої освіти

State higher educational institution "Priazov State Technical University", Dnipro
Державний вищий навчальний заклад «Приазовський державний технічний університет», м. Дніпро

Abstract. *The purpose* of the research is a thorough study of aspects of designing a user decision support system in the field of information security for accounting enterprises. The use of conceptual and structural approaches are key in achieving high efficiency of this system. *The methodology* used in the study is aimed at minimizing the possibility of errors related to the human factor when interacting with electronic correspondence of the enterprise. Special attention is paid to incoming and outgoing electronic correspondence, as their improper processing can lead to the leakage of important corporate information. *The results* of the implementation of the developed system are a high level of protection against risks associated with employee errors. This applies to both internal factors and possible threats from the outside. The system allows for reliable control over the processing of electronic correspondence, reducing the likelihood of leaking confidential information. *Scientific novelty:* the work is distinguished by its scientific contribution, emphasizing the relevance of the application of conceptual and structural approaches in modern cyberspace. Analysis of innovative approaches to information security determines promising directions for the development of such systems. *Practical significance:* the obtained results have significant practical significance for accounting enterprises. Reliability of information security in modern conditions is becoming key, and approaches developed in the work help companies avoid potential threats and preserve confidential data. In recent years, Ukraine has seen a significant increase in the number of cyberattacks in both the corporate and public sectors. Modern hacker groups no longer act in isolation, but join forces in large and well-coordinated groups. Their technical training and huge financial resources, obtained illegally, create great challenges for information security.
Key words: concept; structure; decision support system; cyberattack; hacker; cyberspace.

Анотація. *Метою* дослідження є ретельне вивчення аспектів проєктування системи підтримки прийняття рішень користувача в сфері інформаційної безпеки для бухгалтерських підприємств. Використання концептуального та структурного підходів є ключовими у досягненні високої ефективності цієї системи. *Методика,* використовувана у дослідженні, спрямована на мінімізацію можливостей виникнення помилок, пов'язаних з людським фактором, при взаємодії з електронною кореспонденцією підприємства. Особлива увага приділяється вхідній та вихідній електронній кореспонденції, оскільки їх неправильна обробка може призвести до витоку важливої корпоративної інформації. *Результати* впровадження розробленої системи полягають у високому рівні захищеності від ризиків, пов'язаних з помилками працівників. Це стосується як внутрішніх факторів, так і можливих загроз ззовні. Система дозволяє забезпечити надійний контроль над обробкою електронної кореспонденції, зменшуючи ймовірність витоку конфіденційної інформації. *Наукова новизна:* робота відзначається своїм науковим внеском, акцентуючи увагу на актуальності застосування концептуальних та структурних підходів у сучасному кіберпросторі. Аналіз інноваційних підходів до інформаційної безпеки визначає перспективні напрямки розвитку подібних систем. *Практична значимість:* отримані результати мають вагоме практичне значення для бухгалтерських підприємств. Надійність інформаційної безпеки в сучасних

умовах стає ключовою, і вироблені в роботі підходи допомагають компаніям уникнути потенційних загроз і зберегти конфіденційні дані. За останні роки в Україні відзначається значний приріст кількості кібератак як у корпоративному, так і в державному секторах. Сучасні хакерські групи вже не діють ізольовано, а об'єднують зусилля великими та добре координованими групами. Їх технічна підготовка та величезні фінансові ресурси, отримані незаконним чином, створюють великі виклики для інформаційної безпеки.
Ключові слова: концепція; структура; система підтримки прийняття рішень; кібератака; хакер; кіберпростір.

ПОСТАНОВКА ПРОБЛЕМИ

В епоху цифрової інформації все частіше й гостріше виникає питання про захист даних від зловмисників. Існує безліч способів отримання доступу до цінної інформації підприємства. Найактуальнішими прикладами подібних способів є:

1. Атаки з використанням програм-викрадачів. Атаки з використанням програм-викрадачів включають шкідливе програмне забезпечення, яке шифрує файли жертви, вимагаючи викуп за їх звільнення. Це залишається серйозною загрозою як для окремих осіб, так і для організацій.

2. Атаки ланцюговим методом постачання. Зловмисники все частіше націлюються на ланцюг постачання, щоб скомпрометувати програмне або апаратне забезпечення до того, як воно потрапить до кінцевих користувачів. Прикладом цього стала атака SolarWinds наприкінці 2020 року.

3. Внутрішні загрози. Ці загрози виходять від окремих осіб всередині організації, які зловживають своїм доступом для порушення безпеки даних. Це може бути спричинено необережністю або, у деяких випадках, злим наміром.

Але згідно зі статистикою Purplesec, 98% спроб цифрових атак здійснюється з використанням прийомів соціальної інженерії [1].

Соціальна інженерія – це метод, який використовують кіберзлочинці для маніпулювання окремими особами з метою розголошення конфіденційної інформації або вчинення дій, що ставлять під загрозу безпеку. Вона використовує людську психологію і довіру, щоб отримати доступ до конфіденційних даних, систем або фізичних місцезнаходжень.

Ось кілька поширених видів соціальної інженерії:

1. Фішинг. Зловмисники надсилають вводячи в оману електронні листи або повідомлення, які, здається, отримані з надійних джерел, заохочуючи отримувачів переходити за шкідливими посиланнями або надавати конфіденційну інформацію [2].

2. Претекст. Це включає в себе створення вигаданого сценарію або претексту для отримання інформації чи отримання доступу. Зловмисник може видати себе за когось, на кого можна покластися, щоб обдурити ціль [3, с. 4].

3. Квізи та опитування. Кіберзлочинці використовують, здається, безшкідні квізи чи опитування в соціальних мережах для збору особистої інформації, яка може бути використана у злих намірах.

4. Уособлення в соціальних мережах. Зловмисники можуть створювати фальшиві профілі на платформах соціальних мереж, щоб видати себе за довірених осіб чи організацій з метою маніпулювання цілями.

5. Зворотна соціальна інженерія. У цьому сценарії зловмисник видає себе за особу, яка потребує допомоги, сподіваючись на корисність об'єкта для отримання інформації чи доступу [4].

6. Шахрайство з технічною підтримкою. Шахраї видають себе за співробітників технічної підтримки поважних компаній, щоб переконати осіб надати віддалений доступ чи фінансову інформацію.

З вищезазначеного можна зробити висновок, що для того, щоб попередити користувача від становлення жертвою соціальної інженерії, йому потрібна підтримка у прийнятті рішень, що стосуються будь-яких аспектів отримання та відправлення даних, які можуть бути скомпроментовані зловмисниками.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Згідно з останніми дослідженнями компанії Purplesec, у Сполучених Штатах Америки кіберзлочинність зросла на 600% через пандемію COVID-19. Підраховано, що до 2025 року кіберзлочини в усьому світі будуть обходитися в 10,5 трлн доларів щорічно. Глобальні щорічні витрати на кіберзлочинність оцінюються в 6 трлн доларів на рік. Вартість кіберзлочинності становить 1% від світового ВВП [5].

У середньому атака шкідливого програмного забезпечення коштує компанії понад 2,5 мільйона доларів (включаючи час, необхідний для усунення атаки). У 2021 році шкідливі програми-викрадачі були в 57 разів більш руйнівними, ніж у 2015 році. У США нараховується 30 мільйонів малих та середніх підприємств, і більше 66% усіх малих та середніх підприємств стикнулися хоча б з одним інцидентом з 2018року по 2020 рік. Середня вартість витоку даних для малого бізнесу може складати від 120 000 до 1,24 мільйонів доларів. Витрати на витік даних зросли з 3,86 млн доларів до 4,24 млн доларів у 2021 році, що є найвищим середнім показником загальних витрат за 17-річну історію підготовки цього звіту. Середня вартість була на 1,07 мільйона доларів вище в тих випадках, коли причиною взлому був фактор віддаленої роботи.

Більше 50% усіх кібератак спрямовані на підприємства малого та середнього бізнесу. Підприємства в середньому зіштовхуються з 130 порушеннями

безпеки щороку для кожної організації [6]. Щорічна кількість порушень безпеки в корпоративних організаціях зросла на 27,4%. У середньому підприємствам потрібно 50 днів для усунення інсайдерської атаки та 23 дні для відновлення після атаки програм-викрадачів.

Щороку жертвами кіберзлочинності стають 71,1 мільйонів людей. Фізичні особи втрачають в середньому 4 476 доларів. Приватні особи втрачають 318 мільярдів доларів через кіберзлочинність. Жертви фішингових шахрайств втрачають в середньому 225 доларів [7].

Спеціалісти з соціальної інженерії виділяють наступні основні захисні методи для організацій:

- розробка продуманої політики класифікації даних, яка враховує ті, здавалося б, безшкідні типи даних, які можуть призвести до отримання важливої інформації;
- забезпечення захисту інформації про клієнтів за допомогою шифрування даних або використання управління доступом;
- навчання співробітників навичкам визначення соціального інженера, проявів підозри при спілкуванні з людьми, яких вони не знають особисто;
- заборона персоналу на обмін паролями або використання загальних;
- заборона на надання інформації з відділу з секретами кому-небудь, хто не є особисто відомим або не підтверджений якимось способом;
- використання особливих процедур підтвердження для всіх, хто запитує доступ до конфіденційної інформації.

Для захисту великих компаній і їх працівників від шахраїв, що використовують техніки соціальної інженерії, часто застосовуються комплексні багаторівневі системи безпеки. Нижче наведені деякі особливості та обов'язки таких систем:

- Фізична безпека. Бар'єри, що обмежують доступ до приміщень компанії та корпоративних ресурсів. Важливо пам'ятати, що ресурси компанії, такі як сміттєві контейнери, розташовані поза межами території компанії, фізично не захищені.
- Дані. Ділова інформація: облікові записи, кореспонденція тощо. При аналізі загроз і плануванні заходів з захисту даних потрібно визначити принципи обробки паперових і електронних носіїв даних.
- Додатки. Програми, які використовуються користувачами. Для захисту середовища важливо врахувати, як зловмисники можуть використовувати в своїх цілях поштові програми, служби миттєвого обміну повідомленнями та інші додатки.
- Комп'ютери. Сервери та клієнтські системи, які використовуються в організації. Захист користувачів від прямих атак на їх комп'ютери шляхом визначення строгих принципів, які вказують, які програми можна використовувати на корпоративних комп'ютерах.
- Внутрішня мережа. Мережа, через яку взаємодіють корпоративні системи. Вона може бути локальною, глобальною або бездротовою. У останні роки через зростання популярності методів віддаленої роботи, межі внутрішніх мереж стали в багатьох відношеннях умовними. Працівникам компанії потрібно роз'яснити, що вони мають робити для організації безпечної роботи в будь-якому мережевому середовищі.
- Периметр мережі. Межа між внутрішніми мережами компанії та зовнішніми, такими як Інтернет або мережі партнерських організацій.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою цієї статті є розгляд концептуального та структурного проєктування, можливостей їх комплексного застосування, а також аналіз варіантів їх використання для проєктування системи прийняття рішень, заснованої на аспектах соціальної інженерії.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Концептуальне проєктування є початковим етапом проєктування, на якому приймаються рішення, що визначають подальший образ системи, а також проводиться дослідження та узгодження параметрів створених технічних рішень з можливою їх організацією.

Термін «концепція» застосовується для опису принципу дії не лише в технічних системах, а й у наукових, художніх та інших видів діяльності.

Таким чином, проєктування на концептуальному рівні відбувається на рівні змісту або змісту поняття системи. Образ об'єкта чи його складових може створюватися в уяві людини внаслідок творчого процесу або генеруватися відповідно до деяких алгоритмів у процесі взаємодії людини та ЕОМ за допомогою автоматизованих систем підтримки етапу концептуального проєктування.

Структурне проєктування розуміється як методологія побудови алгоритмів, програм та систем, включаючи інформаційні, на основі якої лежить виявлення структури задачі, визначення складових компонентів та виділення зв'язків між ними.

Процес роз'єднання складних задач (об'єктів, систем) на відносно незалежні одна від одної підзадачі (частини, підсистеми) називається декомпозицією.

Процедура декомпозиції може використовуватися повторно до окремих компонентів, виділених на попередніх етапах структуризації. Процес завершується в тому випадку, коли отримані компоненти, на думку проєктувальника, не потребують подальшої декомпозиції, наприклад, коли виділені елементарні операції або коли отримано підзадачі, розробка яких не викликає складнощів. Процедура багаторазового застосування декомпозиції отримала назву поетапної деталізації.

Виділяють такі типові методи структурного проєктування:

- Спадне проєктування;
- Модульне програмування.

Спадне проєктування (або проєктування «зверху вниз») полягає в застосуванні процедури поетапної деталізації: складна задача розбивається на більш прості, які, в свою чергу, поділяються далі до того моменту, доки вся задача не буде реалізована.

Модульне програмування: пов'язане зі створенням і використанням спеціальних програмних одиниць – модулів. Кожен модуль містить певну кількість підпрограм, які використовують одні й ті самі глобальні дані. Крім того, у модулі об'єднують підпрограми, що належать до однієї функціональної групи, наприклад, математичні, підпрограми обробки графіки. Підпрограми модулів можуть бути використані як у основній програмі, так і в інших модулях.

Враховуючи специфіку цілей та особливостей комбінування підходів, для проєктування системи підтримки прийняття рішень для корпоративних цілей, таких як бухгалтерія, найкращим чином підійде спадний підхід.

У кінцевому підсумку рішення задачі представляє собою ієрархічну структуру відносно незалежних підзадач. На кожному рівні цієї ієрархії підзадачі описуються з певним рівнем деталізації. Чим вище рівень, тим більш конкретними стають підзадачі, і тим менше в них абстрактного (рис. 1). Під абстракцією розуміють певну сутність, в якій виділені основні, важливі ознаки і в той же час вилучені вторинні, часткові ознаки. Абстракція є результатом мислиневого процесу людини, який називається абстрагуванням.

Кожній підзадачі може відповідати підпрограма, а сама початкова задача представлена у вигляді ієрархічно пов'язаних між собою підпрограм. При практичній реалізації спадного проєктування, а саме, програмування, можлива ситуація, коли підпрограми нижчих рівнів ще не реалізовані. У цьому випадку замість них використовують спеціальні відладочні модулі – так звані «заглушки», що дозволяють імітувати конкретний випадок роботи підпрограми. Наприклад, якщо потрібно обчислити значення деякої складної функції, але самий її програмний код ще не написаний, то функція замінюється одним оператором, що повертає певне припустиме заздалегідь обране значення. Після того, як інші частини програми, пов'язані з обчисленням функції, будуть написані і влагоджені, реалізують цю функцію.

Для створення системи підтримки прийняття рішень, що стосуються вирішення конфліктних ситуацій застосуванням методів соціальної інженерії, необхідно використовувати комплексне поєднання двох проєктувальних підходів. Великий спектр можливостей соціальної інженерії робить цю загрозу дуже небезпечною і витратною для компаній, які дбають про свою інформацію. У таких країнах, як США, Канада, через небезпеки в інформаційному полі, важлива кореспонденція передається на фізичних носіях або надсилається факсом. З точки зору кібератак це можна назвати «спрощенням в цілях безпеки», але велика кількість паперової роботи може призвести до втрат важливих документів і виробничих затримок. Вирішенням цієї проблеми може стати закрита мережа для обміну інформацією, в концепції якої буде стояти об'єднання концепції захисту інформації від зовнішніх загроз у вигляді простого спаму або небажаної пошти, яка може безшкодно ігноруватися користувачем з підтримкою системи, а також досвіду і консультацій фахівців з соціальної інженерії, які, підтримуючи команду IT фахівців компанії, можуть надавати актуальну інформацію про прийоми, які постійно оновлюються, і прийоми впливу на психологічну складову людини. Спільними зусиллями концептуальної ідеї соціального шахрайства, а також технологічної підтримки сучасних досягнень у галузі програмування, буде створено проєкт системи, яка на основі вступної інформації і змінних параметрів буде визначати, якій кореспонденції можна довіряти, а якій не варто.

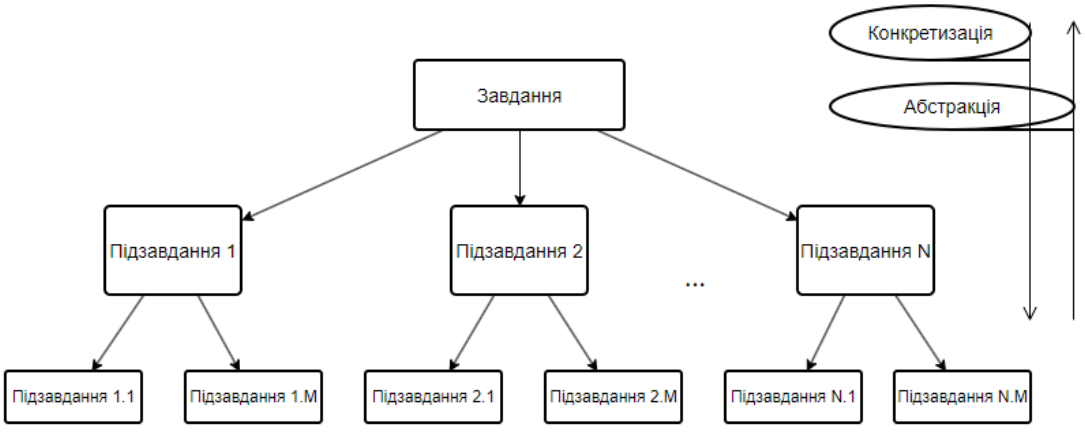

Рис. 1. Співвідношення абстрактного та конкретного в описі підзадач при спадному проєктуванні

ВИСНОВКИ

Отже, на основі об'єднаного підходу, а також додаткової інформації від довірених джерел, які спеціалізуються на методах соціальної інженерії, можливо створити проєкт системи, яка зможе захистити користувача від атак ззовні. Система буде формувати попереджувальні повідомлення для користувача, що листи або файли безпечні, а з якими потрібно зберігати увагу та, в найкращому варіанті, не відкривати або видаляти. Така система буде дуже корисною для використання бухгалтерськими підприємствами, як приватними, так і державними. Таким чином, за допомогою IT-технологій процес перевірки безпеки стає швидше та ефективніше, що запобігає витокам даних.

REFERENCES

[1] Internet Security Threat Report. (2019). Retrieved from https://www.symantec.com/securitycenter/threat-report

[2] Mitnick, K. D., Simon, W. L. (2004). The Art of Deception. — Publisher: Company IT. URL: https://royallib.com/book/mitnik_kevin/iskusstvo_obmana.html

[3] Mitnick, K. (2004) Introduction, CSEPS Course Workbook. — Mitnick Security Publishing

[4] How to Protect Internal Network and Company Employees from Attacks, Microsoft TechNet. Retrieved from https://learn.microsoft.com/en-us/previous-versions/tn-archive/cc875841(v=technet.10)?redirectedfrom=MSDN

[5] 90 percent of financial institutions were targeted by ransomware in the last year. (2018). Retrieved from https://betanews.com/2018/05/22/financial-institutions-ransomware/

[6] The Latest in Phishing: First of 2019. (2020). Retrieved from https://www.proofpoint.com/us/security-awareness/post/latest-phishing-first-2019

[7] Verizon Data Breach Investigations Report (2018). Retrieved from https://www.phishingbox.com/news/phishing-news/verizon-data-breach-investigations-report-2018

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Звіт про загрози Інтернет-безпеці. (2019). URL: https://www.symantec.com/securitycenter/threat-report

[2] Мітнік, К. Д., Саймон, В. Л. (2004). Мистецтво обману. — Видавництво: Компанія АйТі. URL: https://royallib.com/book/mitnik_kevin/iskusstvo_obmana.html

[3] Мітнік, К. (2004). Введення, CSEPS Course Workbook. — Mitnick Security Publishing

[4] Як захистити внутрішню мережу та співробітників компанії від атак, Microsoft TechNet. URL: https://learn.microsoft.com/en-us/previous-versions/tn-archive/cc875841(v=technet.10)?redirectedfrom=MSDN

[5] 90 відсотків фінансових установ були зачеплені розкраданням даних у минулому році. (2018). URL: https://betanews.com/2018/05/22/financial-institutions-ransomware/

[6] Останні дані про фішинг: початок 2019 року. (2020). URL: https://www.proofpoint.com/us/security-awareness/post/latest-phishing-first-2019

[7] Звіт Verizon про розслідування витоків даних (2018). URL: https://www.phishingbox.com/news/phishing-news/verizon-data-breach-investigations-report-2018

Дата надходження статті до редакції: 24.10.2023
Дата затвердження статті до друку: 01.11.2023