УДК 004.056 DOI https://doi.org/10.35546/kntu2078-4481.2024.1.32

Д. В. ЛУБКО
кандидат технічних наук, доцент,
доцент кафедри комп'ютерних наук
Таврійський державний агротехнологічний університет
імені Дмитра Моторного
ORCID: 0000-0002-2506-4145

М. Ю. МІРОШНИЧЕНКО
кандидат технічних наук,
старший викладач кафедри комп'ютерних наук
Таврійський державний агротехнологічний університет
імені Дмитра Моторного
ORCID: 0000-0003-4596-3110

АНАЛІЗ СУЧАСНИХ ПІДХОДІВ ТА МЕТОДИК В ОБЛАСТІ ЗАХИСТУ ІНФОРМАЦІЇ ТА ДАНИХ

У даній роботі на тему «Аналіз сучасних підходів та методик в області захисту інформації та даних» авторами Лубко Д. В. та Мірошниченко М. Ю. розглядається класифікація даних за ступенем конфіденційності та доступності як важливий компонент управління інформаційною безпекою. Метою статті є аналіз сучасних підходів до класифікації в області захисту інформації та використання цих методик для запобігання зловмисному впливу. Існує ряд технологій безпеки, які можуть допомогти захистити дані від несанкціонованого доступу, розголошення, змін або знищення; потрібно регулярно проводити аудити безпеки (аудити безпеки допоможуть вам визначити, чи ефективні ваші заходи безпеки). Автори у статті вказують, що класи безпеки можуть бути використані для різних цілей, включаючи: розробку політики безпеки (політика безпеки – це документ, який визначає правила та процедури, які повинні дотримуватися організації для захисту своїх даних, а також класи безпеки можуть бути використані для розробки політики безпеки, яка забезпечує адекватний захист для всіх даних, які використовує організація); вимірювання ефективності заходів безпеки (тобто організації повинні регулярно проводити аудити своїх заходів безпеки, щоб переконатися що вони ефективні, а самі класи безпеки можуть бути використані для оцінки ефективності заходів безпеки, оскільки вони допомагають визначити, чи достатньо захищені дані з урахуванням їхнього рівня чутливості); аудит безпеки (аудит безпеки – це незалежне дослідження, яке проводиться для оцінки стану безпеки організації, а самі класи безпеки можуть бути використані для аудиту безпеки, оскільки вони допомагають визначити, чи відповідає організація вимогам до безпеки даних). У роботі зазначається, що загрози для приватної інформації можуть виникати з різних джерел, і важливо мати широкий набір заходів безпеки для захисту даних. Це може включати криптографічне шифрування, двофакторну автентифікацію, регулярні аудити безпеки, навчання персоналу щодо соціальної інженерії та регулярне оновлення систем захисту інформації та даних.

Ключові слова: *класи безпеки, конфіденційність, захист інформації та даних, інформаційна безпека, загрози, заходи безпеки.*

D. V. LUBKO
Candidate of Technical Sciences, Associate Professor,
Associate Professor at the Department of Computer Science
Dmytro Motornyi Tavria State Agrotechnological University
ORCID: 0000-0002-2506-4145

M. YU. MIROSHNICHENKO
Candidate of technical Sciences,
Senior Lecturer at the Department of Computer Science
Dmytro Motornyi Tavria State Agrotechnological University
ORCID: 0000-0003-4596-3110

ANALYSIS OF MODERN APPROACHES AND METHODOLOGIES IN THE FIELD OF INFORMATION AND DATA PROTECTION

In this work on the topic "Analysis of modern approaches and methods in the field of information and data protection" by D. V. Lubko. and Miroshnichenko M. Yu. the classification of data according to the degree of confidentiality and

availability is considered as an important component of information security management. The purpose of the article is the analysis of modern approaches to classification in the field of information protection and the use of these techniques to prevent malicious influence. There are a number of security technologies that can help protect data from unauthorized access, disclosure, alteration or destruction; security audits should be conducted regularly (security audits will help you determine whether your security measures are effective). The authors of the article indicate that security classes can be used for a variety of purposes, including: developing a security policy (a security policy is a document that defines the rules and procedures that an organization must follow to protect its data, and security classes can be used to developing a security policy that provides adequate protection for all data used by the organization); measuring the effectiveness of security measures (i.e. organizations should regularly audit their security measures to ensure they are effective, and security classes themselves can be used to assess the effectiveness of security measures, as they help determine whether data is adequately protected given its level of sensitivity); security audit (a security audit is an independent study conducted to assess the security posture of an organization, and the security classes themselves can be used for a security audit because they help determine whether an organization meets data security requirements). The paper notes that threats to private information can come from a variety of sources, and it is important to have a broad set of security measures in place to protect data. This may include cryptographic encryption, two-factor authentication, regular security audits, social engineering training for staff, and regular updates to information and data protection systems.

Key words: *security classes, confidentiality, information and data protection, information security, threats, security measures.*

Постановка проблеми

Області інформаційної безпеки існує кілька класів безпеки, які використовуються для класифікації даних та систем відповідно до їхньої важливості та чутливості. Ці класи безпеки допомагають організаціям розробляти та впроваджувати ефективні заходи безпеки для захисту своїх даних. Нажаль кількість кібер-злочинів росте з кожним днем, велика частка цих злочинів це крадіжка особистих даних. Частіше всього це стається через халатність та необізнаність користувачів. Саме тому все це і є проблемою, яку потрібно вирішувати як особисто там і колективно.

Аналіз останніх досліджень і публікацій

Як показує проведений аналіз останніх досліджень і публікацій з даної проблемої області (питань захисту інформації та даних, питань інформаційної безпеки підприємства, питань безпеки, тощо) багато вчених та науковців активно працювали в цьому. А саме, це такі фахівці та науковці як: Камлик М. І., Козаченко Г. В., Остроухов В. В., Пономарьов В. П., Стрельцов А. А., Расторгуев С. П., Цимбалюк В. Л., Чубарук Т. І., Щербина В. М., Близнюк І. М., Братель О. Р., Бондаренко В. О., Бучило І. Л., Горбатюк О. М., Гуцалюк М. О., Ляшенко О. М., Гуцу С. Ф., Кормич Б. А., Марущак А. І., Сороківська О. А. [1–4]. Незважаючи на велику кількість праць та досліджень у цій сфері, недостатньо висвітлено ще багато аспектів питань забезпечення інформаційної безпеки та захисту даних.

Формулювання мети дослідження

Метою статті є аналіз сучасних підходів та методк в області захисту інформації та даних та використання цих методик для запобігання зловмисному впливу та дотримання безпеки.

Викладення основного матеріалу дослідження

Сьогодні кібербезпеку можна розглядати як важливий аспект політики будь-якої держави в умовах існування глобального інформаційного простору, широкого спілкування та взаємодії через Інтернет. Для її адекватного забезпечення розробляються відповідні технології захисту інформації, законодавство на державному рівні, апаратне та програмне забезпечення тощо [5].

Одним із найпоширеніших класів безпеки є класифікація за ступенем конфіденційності. Ця класифікація ґрунтується на тому, наскільки важливою є інформація для організації та чиї інтереси вона захищає. Дані класифікуються як конфіденційні, приватні, загальнодоступні або публічні. Конфіденційна інформація є найчутливішою та вимагає найвищого рівня захисту. *До цієї інформації належать:* таємниці держави, комерційні секрети та особиста інформація, наприклад, фінансові дані або медичні записи; дані про системи життєзабезпечення, такі як енергетичні мережі або мережі водопостачання; дані про критичну інфраструктуру, такі як транспортні системи або системи зв'язку; дані про наукові дослідження або розробки, які можуть бути використані конкурентами; дані про стратегічні плани та маркетингові цілі, які можуть бути використані для отримання конкурентної переваги; дані про інтелектуальну власність, яка має високу вартість, наприклад, патенти на нові технології [6]. Наведемо складові державного контролю у галузі захисту інформації (див. рис. 1).

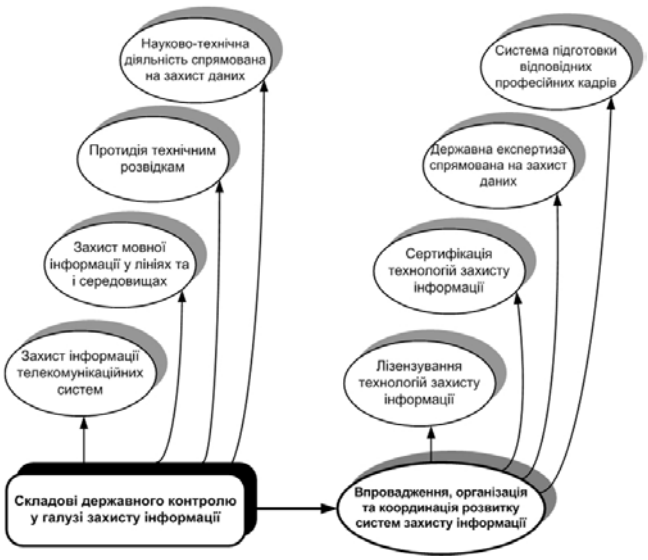

Рис. 1. Складові державного контролю у галузі захисту інформації

Також навелемо критичні загрози для конфіденційної інформації [6]:

1) Кібератаки на особисті дані: втрата конфіденційної інформації, такої як медичні записи чи фінансові дані через хакерські атаки [7].

2) Зловживання даними внутрішніми користувачами: несанкціонований доступ до конфіденційних даних зсередини організації.

Проаналізуємо заходи безпеки для захисту конфіденційної інформації: шифрування даних (використання сучасних алгоритмів шифрування для захисту конфіденційних даних); строгий контроль доступу (обмеження доступу до конфіденційної інформації тільки авторизованим користувачам); адміністрування безпеки (розробка та впровадження політики безпеки, яка відповідає характеру даних та загрозам); обізнаність з питань безпеки (регулярне навчання персоналу щодо безпеки даних).

Розглянемо також існуючі рівні безпеки (див. рис. 2). Якщо коротко, то вони мають три основних блока: міжнародний рівень безпеки, національний рівень безпеки та персональний.

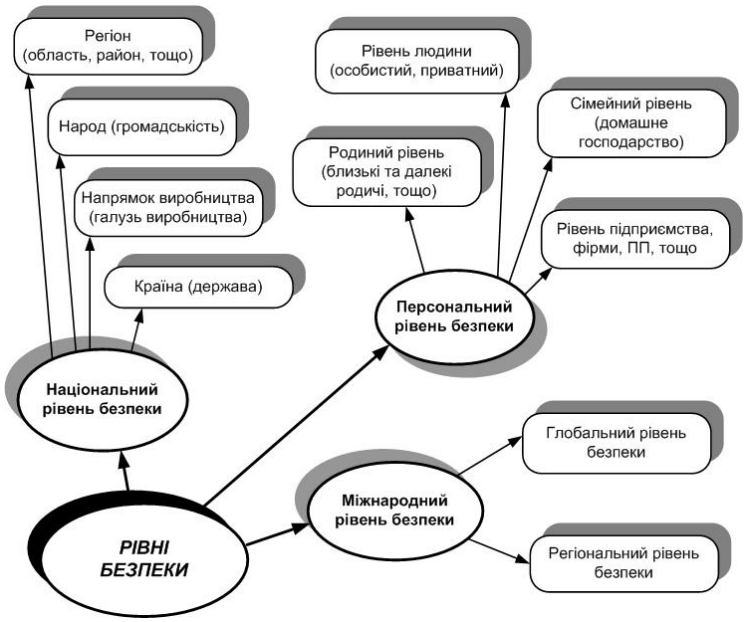

Рис. 2. Рівні безпеки

Для захисту конфіденційної інформації організації повинні застосовуватися такі наступні стандарти безпеки [8]:

− ISO/IEC 27005 – міжнародний стандарт, який визначає вимоги до системи управління інформаційною безпекою (СУІБ) [9].

− NIST SP 800-53 – стандарт Національного інституту стандартів і технологій США, який визначає вимоги до СУІБ для державних органів.

− PCI DSS – стандарт вимог до безпеки платіжних карток.

Приватна інформація є менш чутливою, але все одно вимагає захисту.

До цієї інформації належать: дані про співробітників, клієнтів або постачальників, які можуть бути використані для шахрайства або інших злочинів; дані про маркетингові кампанії або дослідження ринку, які можуть бути використані конкурентами; дані про інтелектуальну власність, яка має меншу вартість, наприклад, авторські права на музичні твори.

Далі проаналізуємо критичні загрози для приватної інформації [10]: фішингові атаки на співробітників (несанкціонований доступ до приватних даних через маніпуляцію персоналу); втрата даних через необережне поводження та недбале використання особистої інформації співробітниками; заходи безпеки для захисту приватної інформації; тренінги з безпеки (регулярна навчання персоналу щодо технік фішингу та особистої безпеки); регулярні аудити безпеки (періодична перевірка доступу та політик захисту даних); адміністрування безпеки (розробка та впровадження політики безпеки, яка відповідає характеру даних та загрозам).

Для захисту приватної інформації організації (а також приватні особи) повинні (або їм рекомендується) застосовувати такі стандарти безпеки як: ISO/IEC 27001; NIST SP 800-53; HIPAA – стандарт, який визначає вимоги до захисту медичних даних.

Загальнодоступна інформація не є чутливою та не вимагає особливого захисту. До цієї інформації належать: відомості про товари та послуги, новини та інші дані; дані, які були опубліковані в загальнодоступних джерелах.

Схема взаємодії основних компонентів інформаційної безпеки наведена на рисунку 3.

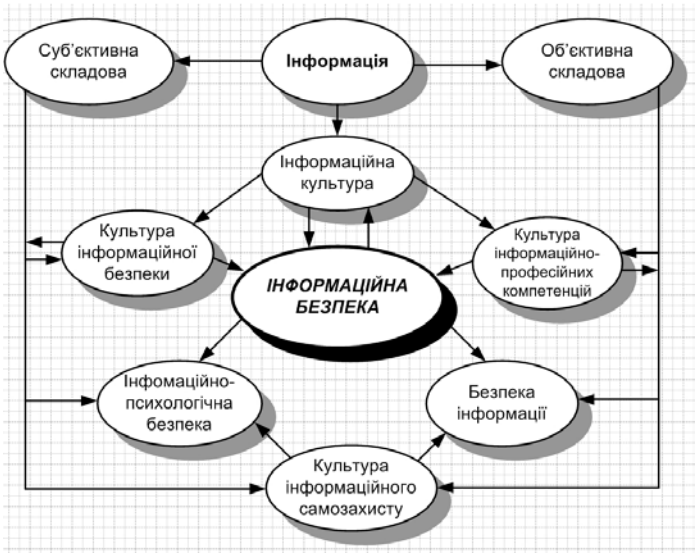

Рис. 3. Схема взаємодії компонентів інформаційної безпеки

Загрози для загальнодоступної інформації можуть бути менш драматичними, ніж для конфіденційної або приватної інформації, але все одно важливими для забезпечення безпеки цієї категорії [6].

А саме: використання даних без дозволу (несанкціоноване використання загальнодоступної інформації для реклами, шахрайства або інших цілей; втрата або пошкодження даних, втрата або пошкодження загальнодоступної інформації може призвести до збитків для організації або користувачів; тощо).

Заходи безпеки для захисту загальнодоступної інформації:

А. Використання загальнодоступних протоколів безпеки. Загальнодос-тупні дані повинні захищатися за допомогою загальнодоступних протоколів безпеки, таких як HTTPS або TLS.

Б. Регулярні резервні копії. Регулярні резервні копії загальнодоступних даних допоможуть захистити їх від втрати або пошкодження.

В. Адміністрування безпеки. Розробка та впровадження політики безпеки, яка відповідає характеру даних та загрозам.

Публічна інформація є доступною для всіх. До цієї інформації належать: відомості про державні органи, вибори та інші громадські події; дані, які були відкриті для громадськості.

Класифікація даних за ступенем конфіденційності та доступності є важливим компонентом управління інформаційною безпекою. Вона допомагає розробити ефективні заходи безпеки для захисту своїх даних.

Використання класів безпеки для захисту даних: потрібно організовувати регулярні тренінги для співробітників з питань безпеки; необхідно використовувати відповідні технології безпеки; потрібно регулярно проводити аудити безпеки. Аудити безпеки допоможуть вам визначити, чи ефективні ваші заходи безпеки.

Класи безпеки можуть бути використані для різних цілей, включаючи:

− Розробку політики безпеки. Політика безпеки – це документ, який визначає правила та процедури, які повинні дотримуватися організації для захисту своїх даних.

− Вимірювання ефективності заходів безпеки. Організації повинні регулярно проводити аудити своїх заходів безпеки, щоб переконатися, що вони ефективні.

− Аудит безпеки. Аудит безпеки – це незалежне дослідження, яке проводиться для оцінки стану безпеки організації.

Ось кілька ключових загроз інформації та даним, які варто врахувати: маніпуляція людьми; фізичний доступ до даних (фізичні загрози); втрати даних через нещасні випадки; недбалість або недосконаліть в захисті даних; внутрішні загрози; недостатня безпека в мережі; кібератаки; соціальні аспекти; законодавчі аспекти; фішинг.

Класифікація даних може бути використана для розробки та впровадження заходів безпеки [10]: конфіденційна інформація (організація може використовувати шифрування для захисту конфіденційної інформації, наприклад, фінансових даних або медичних записів; організація також може використовувати строгі правила контролю доступу, щоб обмежити доступ до конфіденційної інформації лише до авторизованих користувачів); приватна інформація (організація може використовувати тренінги з безпеки для підвищення обізнаності співробітників про фішингові атаки та інші загрози приватній інформації [7]; організація також може використовувати регулярні аудити безпеки для перевірки доступу до приватної інформації та відповідності політикам безпеки); агальнодоступна інформація (організація може використовувати загальнодоступні протоколи безпеки, такі як HTTPS, для захисту загальнодоступної інформації; організація також може використовувати регулярні резервні копії для захисту загальнодоступної інформації від втрати або пошкодження).

Класи безпеки є потужним інструментом, який може допомогти організаціям захистити свої дані. Розуміння класів безпеки та їх застосування є важливим для всіх, хто працює з інформацією. Критичні загрози для приватної інформації можуть бути різноманітними і походити з різних джерел. Критичні загрози постійно еволюціонують, оскільки з'являються нові технології та методи зламу.

Висновки

Загрози для приватної інформації можуть виникати з різних джерел, і важливо мати широкий набір заходів безпеки для захисту даних. Це може включати криптографічне шифрування, двофакторну аутентифікацію, регулярні аудити безпеки, навчання персоналу щодо соціальної інженерії та регулярне оновлення систем захисту інформації та даних. А загальні заходи безпеки, такі як використання сильних паролів, регулярні оновлення ПЗ, застосування шифрування та навчання персоналу щодо соціальної інженерії, можуть допомогти захистити приватну інформацію від цих загроз.

Список використаної літератури

1. Гуцу С.Ф. Правові основи інформаційної діяльності: навч. посіб. Харьків: *Нац. аерокосм. ун-т «Харк. авіац. ін-т».* 2009. 48 с.

2. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України : автореф. дис. на здобуття наук. ступеня докт. юрид. наук: спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». *Нац. ун-т внутр. справ*. Харьків. 2004. 42 с.

3. Марущак А.І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки. *Державна безпека України*. 2011. № 21. С. 92–95.

4. Сороківська О.А., Гевко В.Л. Інформаційна безпека підприємства : нові загрози та перспективи. *Вісник Хмельницького національного університету.* 2010. № 2. т. 2. С. 32–35.

5. Lubko D., Sharov S., Strokan O. Software development for the security of TCP-connections. Modern development paths of agricultural production: trends and innovations. *Cham: Springer international publishing*. 2019. С. 99–109.

6. Michaelsen J.R., Vacca J.W. Information security risk management: A guide to managing risks to information assets. *Springer*. 2018.

7. Grossman J. et al. XSS Attacks: Cross site scripting exploits and defense. *MA: Syngress, Elsevier*. 2007. 463 p.

8. NIST. National institute of standards and technology. Cybersecurity framework. URL: https://www.nist.gov/cyberframework (дата звернення: 15.02.2024).

9. ISO/IEC 27005:2011. Information security risk management.

10. Michael Whitman, Herbert Mattord. Information security: principles and practices. *Publisher: Cengage learning*. 2017. 656 p.

References

1. Hutsu S.F. (2009) Pravovi osnovy informatsiynoyi diyal′nosti: navch. posib. Khar′kiv: *Nats. aerokosm. un-t «Khark. aviats. in-t»* [in Ukrainian].

2. Kormych B.A. (2004) Orhanizatsiyno-pravovi osnovy polityky informatsiynoyi bezpeky Ukrayiny : avtoref. dys. na zdobuttya nauk. stupenya dokt. yuryd. nauk: spets. 12.00.07 «Administratyvne pravo i protses; finansove pravo; informatsiyne pravo». *Nats. un-t vnutr. sprav.* Khar′kiv [in Ukrainian].

3. Marushchak A.I. (2011) Informatsiyno-pravovi napryamy doslidzhennya problem informatsiynoyi bezpeky. *Derzhavna bezpeka Ukrayiny*. № 21, pp. 92–95 [in Ukrainian].

4. Sorokivs′ka O.A., Hevko V.L. (2010) Informatsiyna bezpeka pidpryyemstva : novi zahrozy ta perspektyvy. *Visnyk Khmel'nyts'koho natsional'noho universytetu.* № 2. t. 2, pp. 32–35 [in Ukrainian].

5. Lubko D., Sharov S., Strokan O. (2019) Software development for the security of TCP-connections. Modern development paths of agricultural production: trends and innovations. *Cham: Springer international publishing*. Pp. 99–109 [in Ukrainian].

6. Michaelsen J.R., Vacca J.W. (2018) Information security risk management: A guide to managing risks to information assets. *Springer*.

7. Grossman J. et al. (2007) XSS Attacks: Cross site scripting exploits and defense. *MA: Syngress, Elsevier*.

8. NIST. National institute of standards and technology. Cybersecurity framework. Взято 15 лютого 2024 з https://www.nist.gov/cyberframework

9. ISO/IEC 27005:2011. Information security risk management.

10. Michael Whitman, Herbert Mattord. (2017) Information security: principles and practices. *Publisher: Cengage learning*.