УДК 004.056

ЛЮДСЬКИЙ ФАКТОР ТА УПРАВЛІННЯ БЕЗПЕКОЮ. АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: МЕТОДОЛОГІЯ ТА ПРАКТИЧНІ КЕЙСИ

Анна Крась

HUMAN FACTOR AND SECURITY MANAGEMENT. INFORMATION SECURITY AUDIT: METHODOLOGY AND PRACTICAL CASES

Kras Anna

Волинський національний університет імені Лесі Українки, просп. Волі, 13, Луцьк, 43025, Україна

Abstract. *This paper examines the role of the human factor in information security systems, emphasizing that despite the presence of advanced technological solutions, policies, and procedures, employee behavior, knowledge, and motivation remain critical to effective cybersecurity. It details the main threats related to the human factor, including social engineering, accidental errors, insider threats, and sabotage. Special attention is given to the importance of continuous employee training, fostering a security-aware culture, implementing the principle of least privilege, using multi-factor authentication, monitoring, and conducting regular audits. The analysis covers international standards (ISO/IEC, NIST, COBIT) and practical audit cases, demonstrating the need for a comprehensive approach to managing human-related risks. The paper concludes that effective information security requires a balanced integration of technical measures, management strategies, and an understanding of the social and psychological dynamics within the organization.*

Наявна на сьогодні література [1-4] про людський фактор у сфері безпеки/кібербезпеки часто зосереджується на підвищенні обізнаності, навчанні та освіті – всіх пунктах, пов'язаних з «освітою» людей з метою захисту інформації. Існує надія та припущення, що люди дотримуватимуться очікувань організації щодо інформаційних активів, до яких вони мають доступ, аналогічно, дослідження підтверджують, що, попри надану освіту та запроваджені санкції за поведінку, яка порушує процедури та процеси безпеки, призначені для захисту інформації, уразливості, посилені людським фактором, все одно матеріалізуються — чи то через помилки, упущення, чи навмисні дії, що ставлять під загрозу конфіденційну інформацію організації.

Людський фактор в інформаційній безпеці охоплює психологічні й соціальні характеристики працівників, які створюють вразливості в IT-системах, в багатьох дослідженнях люди називають «слабким ланцюгом» системи безпеки. [4] Випадкові помилки, неуважність, а також свідомі дії призводять до витоків даних або зловмисного втручання, уникаючи технічних бар'єрів, навіть при наявності суворих політик та технологічних засобів захисту людські недоліки зумовлюють інциденти, «люди, всупереч усім технічним зусиллям, часто виявляють вразливості». [4] Згідно з опитуваннями [5] , 52% організацій вважають співробітників своїм найбільшим ризиком у кібербезпеці, а у 46% зафіксованих інцидентів саме помилки чи відсутність обізнаності персоналу сприяли компрометації систем, 30% подій пов'язані з навмисними діями недобросовісних працівників, тобто, людський фактор відіграє вирішальну роль, при організації захисту інформації необхідно враховувати соціально-психологічні особливості працівників.

Основні загрози, що виникають через людський фактор, можна згрупувати так: соціальна інженерія (social engineering), ненавмисні помилки і недбалість, інсайдерські загрози та саботаж, порушення політик та процедур. Щодо соціальної інженерії то це методи обману, що

експлуатують довіру та психологічні особливості людини (наприклад, фішингові листи, SMS-вишинг, атаки через соціальні мережі), зловмисники маніпулюють користувачами, щоб отримати конфіденційні дані або доступ до систем, часто обминаючи технічні контрзаходи. Випадкові дії чи невірні рішення працівників (натискання на шкідливе посилання, неправильне налаштування систем, забуття змінити пароль), є теж великою загрозою, оскільки навіть навчені користувачі можуть некоректно виконувати процедури, призводячи до витоку або пошкодження інформації. Саботаж це навмисні дії співробітників (зловмисників або невдоволених працівників), спрямовані на пошкодження ресурсів організації чи викрадення даних. До категорії саботажу належать безпосередньо саботажі, крадіжка інформації чи використання повноважень всупереч інтересам організації, за дослідженням, близько 30% кібератак пов'язані з навмисними діями внутрішніх співробітників. [4,5]

Регулярні тренінги з кібербезпеки, вправи з реагування на фішинг і симуляції інцидентів допомагають формувати в персоналу правильну модель поведінки, наприклад, Українські експерти наголошують на необхідності постійного навчання співробітників з питань кібербезпеки. ISO/IEC 27001 в Annex A закладає обов'язковість проведення кампаній підвищення обізнаності («awareness») і навчання персоналу.[6] Важливо інформувати та тренувати реальні навички (парування на фішингові повідомлення, сценарії реагування), а також позитивно стимулювати звітність про помилки без покарань, створюючи культуру безпеки. [6] Формалізовані правила використання IT-ресурсів (політика паролів, BYOD, доступу до даних) мають бути зрозумілими та суворо контролюватися, організація повинна визначити відповідальність працівників за безпечне поводження з інформацією (наприклад, шляхом укладання угод про нерозголошення) і регулярно перевіряти виконання цих правил. ISO 27001 рекомендує встановити чіткі політики та процедури обробки інформації та контроль їх дотримання у всіх підрозділах, важливо обирати та перевіряти кадри (background checks, моніторинг поведінки), адже працівники з вразливими рисами є більшим ризиком. [6]

Реалізація принципу найменшого привілею (access control) обмежує доступ користувачів лише до необхідних ресурсів, застосування багатофакторної аутентифікації, систем управління ідентифікацією та привілеями (IAM), моніторинг логів доступу зменшують можливості несанкціонованих дій, розмежування обов'язків (Separation of Duties) знижує ризик одноосібних дій порушників ну а технічні рішення (DLP-системи, антивіруси, фаєрволи) доповнюють управлінські заходи, створюючи багаторазовий захист. [5-7]

Розглянувши ряд формальних заходів перейдемо до більш практичних, фундаментальну роль в безпеці виконує виховання у колективі відповідальності за безпеку, заохочення повідомляти про підозрілі події, відсутність надмірних покарань за інциденти та підтримка ініціатив безпеки допомагають ефективніше долати людські помилки. Як зазначено в дослідженні, «щоб побудувати реальну стійкість, необхідно змінювати поведінку користувачів. Людей потрібно навчати так, щоб вони набували навичок приймати правильні рішення». [7] Автоматизація рутинних процесів (централізоване оновлення ПЗ, віддалений WAF, SIEM/UEBA-системи) мінімізує пряме ручне втручання людини в критичні завдання, таким чином, знижується ймовірність помилок через людський фактор, поєднання технічних контролів, політик та процедур, адаптованих до конкретних ризиків організації є ключем до безпеки, а регулярні перевірки та аудити допомагають виявляти слабкі місця і забезпечувати ефективність цих заходів. Комплексна стратегія безпеки баз передбачає «поєднання технічних контролів, політик та процедур» з урахуванням специфічних вимог організації, регулярні внутрішні аудити й оцінки відповідності (gap analysis) допомагають вчасно виявити «слабкі місця» у заходах безпеки. Таким чином забезпечується постійне вдосконалення системи безпеки: виявлені під час аудиту помилки ліквідуються, а співробітники отримують навчання з урахуванням нових загроз.

Для організації аудиту і систематизації підходів широко використовують міжнародні фреймворки та стандарти, наприклад ISO/IEC, NIST SP, COBIT. [7]

Тепер перейдемо до практичних кейсів, верховний аудит Словенії перевіряв кіберпідготовленість оператора національної електромережі (ELES) за рекомендаціями ENISA, ISO та NIST, в кейсі аудитори оцінили, наскільки організація готова до кібератак на енергетичну інфраструктуру, висновок показав, що необхідно поєднувати традиційні перевірки з дослідженнями в полі (наприклад, пентестами) та враховувати потенційний вплив людського фактору на безпеку, даний приклад підкреслює, що аудити ІБ критично важливі для захисту життєво важливих систем і вимагають високої кваліфікації аудиторів. [10]

У звіті одного з відділень ISACA описано аудит кібербезпеки середньої компанії з точки зору NIST CSF та COBIT5, команда аудитів встановила цілі оцінки мережі та процесів клієнта, виявила слабкі місця і розробила план коригування, особливістю кейсу було використання опублікованих керівництв для малих підприємств ISACA (що базуються на COBIT5 і NIST) – вони включають перелік «керівних принципів» та 55 контрольних пунктів, кожному з яких присвоюється рівень ризику (Critical, Severe, Important), відповідно на основі цих керівництв аудитори присвоїли рейтинг виявленим недолікам і надали конкретні рекомендації з пріоритетом усунення, результат – чіткий дорожній план зміцнення безпеки компанії з урахуванням її масштабу та ресурсів.

Отже, людський фактор є основоположним елементом у системі забезпечення інформаційної безпеки, що виступає основним ризиком та важливим ресурсом для підвищення стійкості організації. Аналіз літератури та сучасних досліджень підтверджує, що попри наявність технологічних рішень, політик та формалізованих процедур, саме поведінка, знання та мотивація працівників визначають ефективність кіберзахисту. Ефективна інформаційна безпека будується на технологіях та розумінні психології та соціальної динаміки всередині колективу, а ключем до стійкості є інтеграція навчання, контролю та культури відповідальності у повсякденну діяльність організації.

Бібліографія

1. Dreyer, P.; T. Jones; K. Klima; J. Oberholtzer; A. Strong; J. Welburn; Z. Winkelman; “Estimating the Global Cost of Cyber Risk: Methodology and Examples,” Rand Corporation, 2018, https://www.rand.org/pubs/research_reports/RR2299.html (date of access: 05.05.2025).
2. Fuenmayor R., Lpez-Garay H. The scene for Interpretive Systemology. *Systems Practice*. 1991. Vol. 4, no. 5. P. 401–418. URL: https://doi.org/10.1007/bf01104459 (date of access: 05.05.2025).
3. Security Fatigue / B. Stanton et al. *IT Professional*. 2016. Vol. 18, no. 5. P. 26–32. URL: https://doi.org/10.1109/mitp.2016.84 (date of access: 05.05.2025).
4. The Human Factor of Information Security: Unintentional Damage Perspective / E. Metalidou et al. *Procedia - Social and Behavioral Sciences*. 2014. Vol. 147. P. 424–428. URL: https://doi.org/10.1016/j.sbspro.2014.07.133 (date of access: 05.05.2025).
5. The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within. URL: https://www.kaspersky.com/blog/the-human-factor-in-it-security/#:~:text=against%20cyberattack%20is%20their%20own,IT%20security%20strategy%20at%20risk (date of access: 05.05.2025).
6. People controls in ISO 27001. URL: https://www.dataguard.com/knowledge/iso-27001/annex-a/6-people-controls/#:~:text=,employees%20to%20information%20security%20risks (date of access: 05.05.2025).
7. How to Reduce Human Risk: Best Practices for Security Teams. URL: https://hoxhunt.com/blog/how-to-reduce-human-risk#:~:text=,of%20users%20is%20a%20must (date of access: 05.05.2025).