SECTION 8. MODERN PSYCHOLOGICAL AND PEDAGOGICAL TEACHING METHODS

DOI https://doi.org/10.30525/978-9934-26-659-1-24

DEBATE AS A METHOD OF AWARENESS OF PSYCHOLOGICAL RISKS IN THE STRUCTURE OF SOCIAL ENGINEERING

ДЕБАТИ ЯК МЕТОД УСВІДОМЛЕННЯ ПСИХОЛОГІЧНИХ РИЗИКІВ У СТРУКТУРІ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Voronova S. V.
Candidate of Pedagogical Sciences, Associate Professor of the Department of Cyberpsychology and Rehabilitation State University of Intelligent Technologies and Telecommunications Odesa, Ukraine

Воронова С. В.
кандидат педагогічних наук, доцент кафедри кіберпсихології та реабілітації Державний університет інтелектуальних технологій і зв'язку м. Одеса, Україна

Еволюція цифрових загроз чітко вказує на те, що найбільш критична вразливість сучасних систем безпеки лежить не в площині програмного коду, а в особливостях людської психіки. Соціальна інженерія, яку визначають як сукупність технік психологічного маніпулювання з метою спонукання осіб до розголошення конфіденційної інформації або виконання дій, що компрометують безпеку, стала основним вектором атак для суб'єктів різного рівня. Вона базується на глибокому розумінні людської психології та використанні специфічних тригерів, які змушують мозок переходити від раціонального до автоматичного, емоційного режиму прийняття рішень. Головна небезпека цих атак полягає в тому, що вони покладаються на людські помилки, які набагато менш передбачувані, ніж вразливості в операційних системах. Зловмисники розуміють, що неконтрольовані емоції, такі як страх, цікавість, паніка або розчарування, мають силу викликати людські помилки, змушуючи жертву реагувати, не замислюючись про наслідки. Аналітичні дані підтверджують, що понад 90% успішних витоків даних ініціюються за допомогою методів соціальної інженерії, що робить «людський фактор» центральним елементом стратегії кіберзахисту. Дослідники наголошують, що кібербезпека має стати не набором правил, а «способом мислення» [3]. Це потребує переходу від інформаційної моделі (надання фактів) до трансформаційної моделі

(зміна поведінки через досвід). Саме тут дебати як метод усвідомлення психологічних ризиків демонструють свій найвищий потенціал, оскільки дозволяють учасникам не просто вивчати загрози, а безпосередньо протидіяти ним в контрольованому середовищі ворожого інформаційного впливу.

Дебати визначають як форму активного навчання, що поєднує теоретичне опанування матеріалу з практичним відпрацюванням навичок критичного мислення, аргументації та публічного виступу [2]. У світовій та вітчизняній практиці використовуються різні формати дебатів. Кожен із них має унікальну структуру, яка визначає динаміку взаємодії та пріоритетні навички, що розвиваються. Формат дебатів К. Поппера вважається класичним для вищої школи. Він орієнтований на розвиток критичного мислення, командної роботи та толерантності до різних поглядів. Основна мета – не просто перемогти, а всебічно дослідити проблему, оскільки команди заздалегідь готують аргументацію для обох сторін (стверджувальної та заперечної). Структура формату К. Поппера передбачає участь двох команд по три спікери. Важливою особливістю є наявність стадій перехресного опитування, під час яких учасники ставлять запитання опонентам для виявлення слабких місць у їхній позиції [1]. Парламентські дебати (Британський парламентський формат) моделюють роботу законодавчого органу і є стандартом для міжнародних університетських турнірів. Вони характеризуються високим темпом, необхідністю швидкого аналізу та використанням інформаційних запитів, що дозволяють учасникам втручатися в промову опонента. У Британському парламентському форматі беруть участь чотири команди по дві особи: дві команди на боці Уряду та дві на боці Опозиції. Такий поділ вимагає не лише боротьби з прямою опозицією, а й здатності вигідно відрізнити свою позицію від позиції іншої команди на своєму боці (так зване «розширення»). Дебати Лінкольна-Дугласа – це індивідуальний формат (сам на сам), що фокусується на етичних та ціннісних питаннях. На відміну від політичних дебатів, тут менше уваги приділяється статистиці та фактам, а більше – філософському обґрунтуванню та моральним принципам. Цей формат найчастіше застосовують кандидати на посаду президента під час виборчих кампаній [4]. Водночас варто підкреслити, що всі формати об’єднує низка спільних характеристик: наявність сторін «ствердження» та «заперечення»; актуальна або суспільно значуща проблема; регламентована послідовність виступів учасників із чітко визначеними часовими межами; обов’язковий зворотний зв’язок між дебатантами й суддями.

У контексті соціальної інженерії дебати стають платформою для «проживання» ролі як захисника, так і зловмисника, що дозволяє

деконструювати маніпулятивні стратегії зсередини. В межах дисципліни «Соціальна інженерія» здобувачі вищої освіти знайомляться з технологією проведення дебатів під час вивчення теми «Концептуальні основи соціальної інженерії». Вони беруть участь у дебатах «Соціальна інженерія у системі інформаційної безпеки є ризиком», мета яких сформувати системне уявлення про феномен соціальної інженерії та його значення в системі інформаційної безпеки; розвинути здатність до критичного осмислення інформації та аргументованого відстоювання позиції.

Одна команда стверджує, що «Соціальна інженерія = Ризик». Її позиція – соціальна інженерія є надзвичайно небезпечним інструментом, що підриває довіру, базується на маніпуляціях і не може гарантувати захист у довгостроковій перспективі. Аргументами виступають: людський фактор = слабка ланка (жодне навчання не може повністю виключити можливість помилки або емоційного впливу), маніпулятивна природа (соціальна інженерія за своєю суттю базується на обмані й психологічному тиску, що ставить під сумнів її етичність навіть у «захисному» форматі), ризик легалізації маніпуляцій (використання соціальної інженерії для «захисту» може створити середовище, де маніпуляції сприйматимуться як норма), швидке зростання атак (хакери розвивають методи соціальної інженерії швидше, ніж компанії встигають навчати персонал), недостатня ефективність (навіть після численних тренінгів співробітники залишаються вразливими до емоційних, кризових чи стресових факторів). Друга команда стверджує, що «Соціальна інженерія = Захист». Її позиція – соціальна інженерія може бути корисним та етичним інструментом підвищення рівня інформаційної безпеки та виявлення психологічних ризиків, якщо застосовується для навчання, тренінгів та симуляцій атак. Аргументами виступають: інструмент виявлення вразливостей (тестування соціоінженерних атак дозволяє виявити слабкі місця в поведінці персоналу до того, як ними скористаються хакери), підвищення кібергігієни (навчальні симуляції фішингу, телефонних атак чи підроблених повідомлень допомагають співробітникам бути пильними), зміцнення людського фактору (соціальна інженерія допомагає тренувати стійкість персоналу), комплексний підхід (тільки комбінація технологій і психологічної підготовки створює справжню кіберстійкість).

Ефективність дебатів як методу усвідомлення психологічних ризиків підтверджується результатами опитування здобувачів вищої освіти. Порівняльний аналіз результатів опитування, проведеного до та після дебатів, засвідчив позитивну динаміку у сформованості когнітивних, аналітичних і рефлексивних компонентів навчальних

результатів. До початку дебатів більшість респондентів характеризували власне розуміння феномену соціальної інженерії як фрагментарне або поверхневе, переважно асоціюючи його з загрозами інформаційній безпеці. Оцінки ролі соціальної інженерії мали поляризований характер, а готовність до аргументованого відстоювання власної позиції та критичного аналізу альтернативних поглядів перебувала на середньому або нижче середнього рівні. Після проведення дебатів зафіксовано зростання показників усвідомленого розуміння соціальної інженерії як багатовимірного явища, що може виступати не лише інструментом атаки, а й засобом захисту в системі інформаційної безпеки. Респонденти демонстрували вищий рівень упевненості у власній аргументації, більшу відкритість до перегляду початкових установок та зростання здатності критично оцінювати аргументи опонентів. Особливо показовими є зміни у відповідях на відкриті запитання, де після дебатів простежується ускладнення міркувань, використання фахової термінології, посилання на приклади практичного застосування соціальної інженерії. Це свідчить про перехід від інтуїтивних уявлень до більш системного та рефлексивного мислення.

Дослідження дебатів як методу усвідомлення психологічних ризиків у структурі соціальної інженерії дозволяє зробити висновок, що цей підхід є критично необхідним доповненням до технічних засобів захисту. Дебати трансформують концепцію безпеки з «переліку заборон» у «навичку критичного аналізу».

Література:

1. Конон Н. Є., Авдєєва І. Д. Місце дебатних практик в діяльності міжнародних неурядових організацій. *Науково-теоретичний альманах «Грані».* 2017. Т. 20. № 12. С. 62–67.

2. Котурбаш Н., Михайлишин Г. Технологія дебатів у системі професійної підготовки майбутніх фахівців з вищою освітою. *Професіоналізм педагога: теоретичні й методичні аспекти*. 2025. Вип. 23 (1). С. 182–195. DOI: 10.31865/2414-9292.23.2025.334077

3. Building Resilience Against Social Engineering Attacks. Learning management system: official site. 2023. URL: https://lmsolutionsllc.com/2023/06/13/building-resilience-against-social-engineering-attacks/

4. Nazwa A. Application of Debate Learning Method to Improve Students' Emotional Intelligence. *Asian Journal of Multidisciplinary Research and Analysis*. 2024. Vol. 2, No. 2. P. 390–395.