УДК 159.9:005.95/.96:004.056
DOI https://doi.org/10.32782/IT/2024-4-26

Олеся ЧЕРНЯКОВА
кандидат психологічних наук, доцент, доцент кафедри філософії та психології, Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія», Харківське шосе, 210, Київ, Україна, 02121
***ORCID:** 0000-0002-0384-4829*

Бібліографічний опис статті: Чернякова, О. (2024). Психотехнології вирішення конфліктів розробників систем захисту інформації в умовах кіберзагроз. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 4, 222–226, doi: https://doi.org/10.32782/IT/2024-4-26

ПСИХОТЕХНОЛОГІЇ ВИРІШЕННЯ КОНФЛІКТІВ РОЗРОБНИКІВ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ В УМОВАХ КІБЕРЗАГРОЗ

Мінливі умови сучасності, спричинені цифрою трансформацією та інтенсифікацією інформаційного середовища значно підвищують складність роботи фахівців з інформаційної безпеки, що, у свою чергу, провокує виникнення міжособистісних і професійних конфліктів. Високий рівень стресу, необхідність оперативного реагування на загрози та багатозадачність створюють сприятливе підґрунтя для конфліктних ситуацій у командах, які розробляють та впроваджують системи захисту інформації.

***Мета.** Важливим викликом для сучасної науки є визначення ефективних психотехнологій для діагностики, попередження та вирішення конфліктів серед розробників систем інформаційної безпеки, з урахуванням специфіки їхньої професійної діяльності. Основна увага, на нашу думку, має бути приділена аналізу впливу когнітивних, емоційних і соціальних чинників на процеси комунікації та співпраці в команді.*

Стаття присвячена теоретичному аналізу психотехнологій вирішення конфліктів серед фахівців з інформаційної безпеки в умовах зростаючих кіберзагроз. В роботі розглянуто сутність ключових понять: «кіберзагроза», «конфлікт», а також визначено специфіку виникнення та протікання конфліктів у професійних колективах розробників систем захисту інформації. Особливий акцент зроблено на впливі стресогенних чинників, спричинених кіберзагрозами, на психологічний клімат у командах, що займаються захистом інформації.

***Методологічною основою** дослідження є міждисциплінарний підхід, який поєднує положення психології конфлікту, кібербезпеки та організаційної психології. Теоретичний аналіз дозволив виявити основні джерела конфліктів серед фахівців у сфері інформаційної безпеки, зокрема конкуренцію за ресурси, напруження через високий рівень відповідальності та ризиків, а також проблеми міжособистісної взаємодії в умовах інтенсивної роботи.*

На основі проведеного аналізу розроблено низку практичних рекомендацій, спрямованих на профілактику конфліктів. Зокрема, запропоновано методики підвищення стресостійкості фахівців, розвиток навичок конструктивної комунікації, впровадження програм тімбілдінгу та створення сприятливих умов для ефективної роботи команд. Особлива увага приділена використанню психотехнологій, що сприяють своєчасному розпізнаванню та вирішенню конфліктів, запобіганню їхньому загостренню та зниженню негативного впливу на професійну діяльність.

***Результати** дослідження можуть бути використані як основа для подальших прикладних розробок у сфері організації діяльності команд фахівців з інформаційної безпеки, а також для розробки навчальних програм, спрямованих на формування стресостійкості та підвищення ефективності командної взаємодії в умовах сучасних кіберзагроз.*

***Ключові слова:** психотехнології, вирішення конфліктів, інформаційна безпека, кіберзагрози, розробники систем захисту, емоційний інтелект, стрес-менеджмент.*

Olesia CHERNIAKOVA
PhD in Psychology, Associate Professor, Associate Professor at the Department of Philosophy and Psychology, Kyiv University of Intellectual Property and Law of the National University «Odessa Law Academy», 210, Kharkivske highway, Kyiv, Ukraine, 02121, cherniakovaolesia@gmail.com
***ORCID:** 0000-0002-0384-4829*

To cite this article: Cherniakova, O. (2024). Psykhotekhnolohii vyrishennia konfliktiv rozrobnykiv system zakhystu informatsii v umovakh kiberzahroz [Psychotechnologies for resolving conflicts between developers of information protection systems in the face of cyber threats]. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 4, 222–226, doi: https://doi.org/10.32782/IT/2024-4-26

PSYCHOTECHNOLOGIES FOR CONFLICT RESOLUTION OF DEVELOPERS OF INFORMATION PROTECTION SYSTEMS IN THE CONDITIONS OF CYBER THREATS

The changing conditions of modernity, caused by digital transformation and intensification of the information environment, significantly increase the complexity of the work of information security specialists, which, in turn, provokes the emergence of interpersonal and professional conflicts. High levels of stress, the need for prompt response to threats, and multitasking create a favorable environment for conflict situations in teams that develop and implement information protection systems.

An important challenge for modern science is to identify effective psychotechnologies for diagnosing, preventing, and resolving conflicts among information security system developers, taking into account the specifics of their professional activities. In our opinion, the main attention should be paid to the analysis of the influence of cognitive, emotional, and social factors on the processes of communication and cooperation in the team.

The article is devoted to the theoretical analysis of psychotechnologies for resolving conflicts among information security specialists in the face of growing cyber threats. The paper examines the essence of the key concepts: «cyber threat», «conflict», and also identifies the specifics of the emergence and course of conflicts in professional teams of information protection system developers. Special emphasis is placed on the influence of stress-producing factors caused by cyber threats on the psychological climate in teams involved in information protection.

***The methodological** basis of the study is an interdisciplinary approach that combines the principles of conflict psychology, cybersecurity and organizational psychology. Theoretical analysis allowed us to identify the main sources of conflicts among specialists in the field of information security, in particular, competition for resources, tension due to a high level of responsibility and risks, as well as problems of interpersonal interaction in conditions of intensive work.*

Based on the analysis, a number of practical recommendations aimed at conflict prevention were developed. In particular, methods were proposed to increase the stress resistance of specialists, develop constructive communication skills, implement team building programs and create favorable conditions for effective team work. Particular attention is paid to the use of psychotechnologies that contribute to the timely recognition and resolution of conflicts, preventing their escalation and reducing the negative impact on professional activity.

***The results** of the study can be used as a basis for further applied developments in the field of organizing the activities of teams of information security specialists, as well as for the development of training programs aimed at developing stress resistance and increasing the effectiveness of team interaction in the face of modern cyber threats.*

***Key words:** psychotechnologies, conflict resolution, information security, cyber threats, developers of protection systems, emotional intelligence, stress management.*

Актуальність проблеми вирішення конфліктів серед розробників систем захисту інформації в умовах кіберзагроз обумовлена зростаючою роллю інформаційної безпеки в сучасному цифровому світі. В умовах швидкого розвитку технологій кіберзагроз зростають вимоги до кваліфікації та ефективності роботи фахівців, що призводить до підвищення рівня стресу, напруження та професійних конфліктів у команді розробників. Це негативно впливає на продуктивність і безпеку інформаційних систем. Розробка психотехнологій для ефективного вирішення таких конфліктів є необхідною умовою для підтримання стабільності в командах і забезпечення належного рівня захисту інформації в умовах постійних загроз.

Аналіз останніх досліджень в рамках окресленої проблематики вказує на значний інтерес до цього питання як в Україні, так і за її межами. Вітчизняні науковці, зокрема, зосереджуються на дослідженні психологічних аспектів взаємодії в команді, розвитку емоційного інтелекту та механізмів управління стресом у високотехнологічних професіях. Відзначено важливість впливу організаційних факторів на виникнення конфліктів, а також розглядаються методи попередження та вирішення конфліктних ситуацій за допомогою психотехнологій, медіації та тренінгів.

Зарубіжні дослідження, зокрема в Європі та США, акцентують увагу на інтеграції психотерапевтичних і управлінських підходів для оптимізації міжособистісних відносин в умовах інтенсивних кіберзагроз. Зокрема, розглядаються специфічні методи роботи з командами високої напруги, зокрема в IT-секторі, де конфлікти можуть мати критичні наслідки для безпеки систем.

Перспективи подальших досліджень, на нашу думку, мають бути зосереджені на глибшому вивченні психосоціальних аспектів професійних конфліктів у кібербезпеці, зокрема на визначенні ефективних методів профілактики та нейтралізації стресу в умовах високого навантаження. Недостатньо вивченими залишаються питання автоматизації процесів вирішення конфліктів за допомогою новітніх технологій, таких як штучний інтелект або алгоритми для моніторингу емоційного стану працівників. Складнощі досліджень зумовлені складністю інтерпретації психосоціальних факторів, які впливають на виникнення та розвиток конфліктів в умовах

швидких змін у кіберпросторі та новітніх загроз.

Метою нашого дослідження є систематизація та формулювання практичних рекомендацій щодо комплексного підходу до профілактики, запобіганню та вирішенню конфліктів розробників інформаційних систем в умовах кіберзагроз.

В рамках дослідження шляхів вирішення конфліктів розробників систем захисту інформації в умовах кіберзагроз, в першу чергу, на нашу думку, варто визначити сутність та зміст поняття кібезагрози.

Кіберзагроза – це сукупність реальних або потенційних факторів і явищ, що становлять загрозу для інтересів особистості, суспільства та держави шляхом порушення доступності, цілісності, достовірності, автентичності та повноти інформації, яка обробляється чи передається в межах критично важливих об'єктів національної інформаційної інфраструктури (Сахав А. І., 2020, с. 267).

Наступним важливим етапом нашого дослідження є визначення психологічного змісту поняття конфліктів. Конфлікт є складною системою, що характеризується адаптивними структурами та еволюційними механізмами. Його глибоке вивчення потребує, з одного боку, застосування системного підходу, а з іншого – інтеграції знань із різних соціальних і наукових дисциплін. У зв'язку з цим у сучасній науці накопичено значний обсяг теоретичних і практичних розробок, спрямованих на дослідження цього явища. Перехід від індустріальної до інформаційної епохи зумовив виникнення нових типів конфліктів, відомих як інформаційні конфлікти (Шевченко С. М., 2022, с. 151).

Термін «конфлікт» походить від латинського слова, що означає «зіткнення». Різні наукові школи та течії пропонують власні теорії та концепції, які пояснюють природу конфлікту з різних точок зору, що ускладнює як його тлумачення, так і практичне використання в науковій діяльності. У науковій літературі нараховується велика кількість визначень цього поняття. Український дослідник Ю. Мацієвський виділяє три основні аспекти розуміння конфлікту: структурна несумісність інтересів, яка проявляється у взаємному виключенні групових цілей через обмежену кількість дефіцитних ресурсів; дії або взаємовідносини, спрямовані на завдання шкоди або знищення суперника; стан ворожості між окремими особами або групами (Жекало Г., 2015, с. 62).

Будь-який колектив формується з працівників, які істотно відрізняються один від одного за віком, рівнем освіти, стажем роботи, професійним і життєвим досвідом. Також спостерігаються відмінності у цілях і завданнях, які люди ставлять перед собою, та у способах їх досягнення. Важливо враховувати розбіжності у функціональних обов'язках, рольових позиціях і статусах. Крім того, значущими є особистісні особливості, різниця у ціннісних орієнтаціях, життєвих установках та підходах до вирішення проблем, які виникають у процесі роботи. Ці фактори створюють передумови для появи конфліктних ситуацій та виникнення конфліктів у колективах. Основною причиною розвитку конфліктів часто стає суперечність інтересів або прагнення відстояти свої позиції, що проявляється через конфліктну поведінку. У межах організації це може проявлятися у формі вилучення ресурсів, приховування важливої інформації, запровадження обмежень чи дискредитації. Такі дії, як правило, провокують негативні емоції, включно з гнівом, бажанням помсти та взаємною ворожістю. Ці емоції, у свою чергу, підсилюють конфліктну поведінку, що загострює суперечності інтересів. У результаті конфлікт має тенденцію до ескалації, перетворюючись на динамічний і швидкозростаючий процес (Щербакова І. М, Терещеня І. О., 2014, с. 186).

І. М. Щербакова та І. О. Терещеня у ході емпіричного дослідження дійшли висновку, що в трудових організаціях професійне вирішення конфліктів за участі психологів практично не здійснюється. Проте саме психолог має можливість і повинен виконувати функцію медіатора. У цій ролі він залишається нейтральним, не підтримуючи жодну зі сторін, що дозволяє об'єктивно та беземоційно вибудовувати конструктивний діалог між учасниками професійного конфлікту (Щербакова І. М, Терещеня І. О., 2014, с. 187). Пропонуємо більш детально зупинитися на тих наукових працях, які присвячені вивченню конфліктів саме в рамках інформаційної безпеки та кібербезпеки.

При вивченні стадій конфлікту в системах безпеки можна виокремити декілька ключових етапів, що характеризують розвиток конфліктної ситуації. Першим етапом є виникнення конфліктної ситуації, коли відбувається початкове загострення суперечностей. Другий етап– латентна стадія–характеризується прихованим існуванням конфлікту, що не демонструється явно. Третя стадія–активна–означає безпосередню реалізацію конфліктних дій, де виявляються відкриті зіткнення інтересів. Завершення конфлікту відбувається на останньому етапі, коли конфлікт досягає свого завершення або переходить на нову стадію. Глибина конфліктів в контексті інформаційної безпеки визначається складністю суперечностей, що є основою

конфлікту в інформаційній системі. Для оцінки глибини конфлікту можна виділити кілька рівнів. Початковий рівень характеризується виявленням одного інциденту, при якому відхилення оцінки множини ознак від еталонних значень не перевищує встановленої межі. На середньому рівні виявляються кілька інцидентів, що відбуваються одночасно, і відхилення оцінки ознак все ще знаходяться в межах допустимих значень. Високий рівень вказує на одночасне наявність декількох інцидентів, де відхилення від еталонних ознак перевищує певну межу, що свідчить про значну інтенсивність конфлікту в системі (Шевченко С. М., 2022, с. 156).

На нашу думку, вирішення проблеми конфліктів розробників систем захисту інформації в умовах кіберзагроз вимагає комплексного підходу. Зокрема, окремої уваги вимагає проблематика профілактики виникненню конфліктів, що включає розвиток емоційної компетентності, емоційного інтелекту, емпатії тощо серед студентів, що здобувають освіту на спеціальністю кібербезпека та інформаційні технології (Капітон А. М., 2022). В результаті аналізу наукової літератури, присвяченої окресленій проблематиці, нами було зроблено спробу розробити практичні рекомендації, спрямовані на профілактику та запобігання професійним конфліктам в контексті інформаційних технологій, отже:

1. Профілактика конфліктів: основним елементом профілактики є створення сприятливого психологічного клімату в команді розробників. Для цього важливо:

– Формування комунікаційних навичок: навчання фахівців ефективним технікам комунікації, включаючи активне слухання, відкрите обговорення проблем і питань без критики, що дозволяє знизити рівень непорозумінь та напруження.

– Чітке визначення ролей і відповідальності: упорядкування організаційної структури команди, визначення чітких функціональних обов'язків кожного члена колективу сприяє зменшенню територіальних конфліктів та дублювання обов'язків.

– Створення середовища для конструктивної критики: заохочення відкритого обговорення проблемних питань, де кожен розробник може висловити свою думку без страху бути осудженим. Це дозволяє знизити рівень конфліктів, пов'язаних з незадоволенням відсутністю можливості висловити свою позицію.

2. Запобігання конфліктам на етапах розробки системи захисту інформації полягає в:

– Забезпеченні інформаційної прозорості: створення відкритих каналів комунікації між різними підрозділами, що працюють над проектом, дозволяє своєчасно виявляти потенційні джерела напруження і конфліктних ситуацій.

– Планування та координація робіт: ретельне планування проекту, узгодження термінів та обсягів робіт між усіма учасниками забезпечує уникнення непорозумінь, пов'язаних з перевантаженням або, навпаки, недостатнім завантаженням працівників.

– Інтеграція системи управління стресом: враховуючи високий рівень стресу в умовах кіберзагроз, важливо застосовувати стратегії зниження останнього на організаційному рівні, такі як регулярні перерви, тренінги з управління стресом і підтримка добробуту працівників.

3. Вирішення конфліктів: у разі виникнення конфліктів серед розробників, необхідно використовувати такі психотехнології для їх вирішення:

– Психологічне втручання: проведення індивідуальних або групових консультацій із залученням психологів або спеціалістів з управління конфліктами, які допоможуть розкрити причини конфлікту та знайти конструктивне рішення.

– Медіація: призначення нейтральної особи для проведення медіації, яка допоможе сторонам конфлікту обговорити свої претензії і досягти взаємопогодженого рішення.

– Техніка «win-win»: пошук рішень, що задовольняють усі сторони конфлікту, враховуючи інтереси кожного учасника, з метою досягнення гармонії в роботі команди без втрат для результативності проекту.

4. Розвиток навичок емоційного інтелекту є важливим інструментом у профілактиці і вирішенні конфліктів. Це включає:

– Самоусвідомлення: розвиток здатності фахівців усвідомлювати власні емоції та їх вплив на робочі процеси, що допомагає знижувати рівень емоційних реакцій у напружених ситуаціях.

– Саморегуляція: навчання ефективним стратегіям самоконтролю, що дозволяє уникнути емоційних спалахів і вирішувати конфлікти в конструктивному руслі.

– Емпатія: розвиток здатності до емпатії допомагає зрозуміти точки зору колег, що сприяє взаєморозумінню і покращенню міжособистісних взаємин у команді.

5. Використання технологій для запобігання конфліктам: інтеграція технологічних рішень, таких як автоматизовані системи моніторингу роботи команди, платформи для спільної роботи та аналізу продуктивності, може значно знизити ймовірність виникнення конфліктів. Використання цих інструментів дозволяє

здійснювати контроль над процесами розробки та забезпечує своєчасне виявлення потенційних проблем.

Загалом, ефективне вирішення конфліктів серед розробників систем захисту інформації в умовах кіберзагроз вимагає поєднання організаційних заходів, психологічних підходів та використання інноваційних технологій для запобігання і вирішення проблем. Застосування таких методів дозволяє не лише покращити командну атмосферу, але й забезпечити безпеку інформаційних систем на високому рівні.

Перспективою подальшого дослідження є впровадження розроблених нами рекомендацій з метою визначення їх ефективності в контексті профілактики та запобіганню професійних конфліктів розробників інформаційних систем в умовах кіберзагроз.

ЛІТЕРАТУРА:

1. Жекало Г. Основні підходи до визначення поняття «конфлікт». *Східноукраїнський конфлікт: типологія, особливості, шляхи деескалації. Сер. Філософія*. 2015. № 2 (134). С. 62–65.

2. Сахав А. І. Поняття кіберзагроз на сучасному етапі. *Математичні методи, моделі та інформаційні технології у науці, освіті, економіці, виробництві* : матеріал доп. учасн. II Всеукраїнської науково-практичної Інтернет-конференції з проблем вищої освіти і науки, 29 квітня 2020 р. Маріуполь, 2020. С. 266–270.

3. Шевченко С. М., Складанний П. М., Негоденко О. В. Дослідження прикладних аспектів теорії конфліктів у системах безпеки. *Кібербезпека: освіта, наука, техніка*. 2022. № 2 (18). С. 150–162.

4. Щербакова І. М., Терещеня І. О. Психотехнології вирішення професійних конфліктів. *Наукові пошуки*. 2014. Вип. 10. С. 185–187.

5. Капітон А. М. Педагогічні умови формування професійної компетентності майбутніх фахівців з кібербезпеки. *Стратегічні пріоритети інформаційної безпеки держави у сфері оборони в умовах воєнного стану* : зб. матеріалів II Міжвід. наук.-практ. конф., 29 листоп. 2022 р. Київ: НУОУ, 2022. С. 115–116.

REFERENCES:

1. Zhekalo, H. (2015). Osnovni pidkhody do vyznachennia poniattia «konfdikt». *Skhidnoukrainskyi konflikt: typolohiia, osoblyvosti, shchliakhy deeskalatsii. Ser. Filosofiia*, 2 (134), 62–65 [in Ukrainian].

2. Sakhav, A. I. (2020). Poniattia kiberzahroz na suchasnomu etapi. *Matematychni metody, modeli ta informatsiini tekhnolohii u nautsi, osviti, ekonomitsi, vyrobnytstvi* : material dop. uchasn. II Vseukrainskoi naukovo-praktychnoi Internet-konferentsii z problem vyshchoi osvity i nauky, 29 kvitnia 2020 r. Mariupol, 266–270 [in Ukrainian].

3. Shevchenko, S. M., Skladannyi, P. M. & Nehodenko O. V. (2022). Doslidzhennia prykladnykh aspektiv teorii konfliktiv u systemakh bezpeky. *Kiberbezpeka: osvita, nauka, tekhnika*, 2 (18), 150–162 [in Ukrainian].

4. Shcherbakova, I. M., Tereshchenia, I. O. (2014). Psykhotekhnolohii vyrishennia profesiinykh konfliktiv. *Naukovi poshuky*, 10, 185–187 [in Ukrainian].

5. Kapiton, A. M. (2022). Pedahohichni umovy formuvannia profesiinoi kompetentnosti maibutnikh fakhivtsiv z kiberbezpeky. Stratehichni priorytety informatsiinoi bezpeky derzhavy u sferi oborony v umovakh voiennoho stanu : zb. materialiv II Mizhvid. nauk.-prakt. konf., 29 lystop. 2022 r. Kyiv: NUOU, 115–116 [in Ukrainian].