УДК 004.056.5:159.9

# ІНФОРМАЦІЙНА БЕЗПЕКА У РОЗРІЗІ АНАЛІЗУ ПОВЕДІНКИ КОРИСТУВАЧІВ

**Олександр Супрун, Надія Карпенко**

INFORMATION SECURITY IN THE CONTEXT OF USER BEHAVIOR ANALYSIS

Oleksandr Suprun, Nadiia Karpenko

*Дніпровський національний університет імені Олеся Гончара, просп. Науки, 72, Дніпро, 49045, Україна*

***Abstract.*** *This article examines the issue of studying the psychological characteristics of employees in an organization. Individual safety behavior patterns can be formed for workers, which will later be adjusted based on the collected statistics of their behavior.*

**Вступ.** Користувач сучасної інформаційної системи у будь-якій організації породжує величезну кількість подій, які фіксуються у багатьох журналах, наприклад, журналах операційної системи, журналах прикладних систем, мережевих журналах тощо. При аналізі цих журналів звичайними методами, такими як, статичні шаблони або ручний аналіз діяльності співробітників, неможливо з високою ймовірністю розрізнити корисну діяльність і шкідливу, як від самого співробітника-інсайдера, так і від хакера, що маскується під «нормального» користувача системи.

У сучасних підприємств ключовим є процес роботи співробітника у робочому середовищі, що включає операційну систему та бізнес-додатки (CRM, ERP, браузери тощо). На сьогоднішній день аналізувати поведінку користувачів в інформаційній системі для виявлення шкідливої діяльності досить складно, оскільки для виконання і корисних і шкідливих дій вони використовують одні й ті самі програми. Наприклад, якщо користувач, який зв’язується з потенційними клієнтами по WhatsApp, вирішить вкрасти базу потенційних клієнтів і переслати конкуренту з використанням того ж самого месенджера WhatsApp, то на рівні журналів безпеки неможливо буде розрізнити ці дві події. Те саме може відбуватися з системою CRM або ERP, робота з якими зараз у переважній більшості випадків здійснюється у браузері. Співробітник може вивантажити на файлообмінний сервіс список клієнтів для передачі конкуренту і з погляду журналів інформаційної безпеки це також буде легальна операція. При побудові систем захисту інформації головна увага приділяється технічним аспектам впровадження тих, чи інших систем і набагато менше аналізується вплив особистості на інформаційну безпеку. Отже, слід визначити вплив психологічних особливостей особистості працівників на стан інформаційної безпеки підприємства, а також обґрунтувати доцільність використання індивідуальних та групових поведінкових шаблонів для підвищення ефективності політик безпеки та зниження ризиків витоку конфіденційної інформації.

**Літературний огляд.** Для того, щоб зрозуміти поточний стан питання, було зроблено огляд різноманітних джерел. Досить багато статей присвячено аналізу безпекових аспектів цифрової ідентичності, особливо в контексті аутентифікації користувачів у цифрових сервісах. Так автори статті [1] пропонують універсальну модель оцінки ризиків для аутентифікації, але не розглядають детально, як змінюються ризики для різних груп користувачів (наприклад, привілейовані користувачі, зовнішні партнери, IoT-пристрої) чи в різних секторах (державний, фінансовий, освітній тощо). Також відсутній аналіз впливу людського чинника, соціальної інженерії та поведінкових аспектів на ефективність обраних механізмів захисту.

Окремим напрямком є дослідження, присвячені комплексному аналізу алгоритмів для задач User and Entity Behavior Analytics (UEBA), тобто для систем, що аналізують поведінку користувачів і пристроїв у корпоративних мережах для виявлення аномалій та кіберзагроз. Так автори [2] досліджують логи дій користувача на робочому місці, але, нажаль, не розглядають можливість об'єднання різних видів даних, у тому числі психологічних особливостей конкретної людини, для підвищення точності виявлення аномалій.

У тезах [3] наголошується, що у компаніях із високим рівнем регламентації поведінки співробітників можна ефективно виявляти порушення інформаційної безпеки завдяки шаблонізованим діям користувачів та мотиваційним програмам, які стимулюють дотримання інструкцій. Автори також описують сучасний тренд - застосування технології process mining для контролю та оптимізації бізнес-процесів із використанням штучного інтелекту, що підвищує ефективність управління.

Науковці в галузі організаційної поведінки у своїх дослідженнях також приділяють увагу контексту безпеки і, зокрема, інформаційної безпеки. Автори статті [4] вивчають вплив окремих рис особистості (зокрема, "темної тріади") на інформаційну безпеку. Важливі висновки їх праці полягають в тому, що особистісні риси працівників можуть призводити до ненавмисних або навмисних порушень інформаційної безпеки. Особливо це стосується випадків, коли питаннями безпеки займаються кілька автономних працівників. Але вони приділяють більше уваги організаційно-методичним заходам протидії і зовсім не приділяють увагу технічним методам.

**Основна частина.** Для того щоб створювати системи поведінкового аналізу користувачів інформаційних систем треба добре розуміти закони, що впливають на поведінку людини, яка працює в організації [5-6]. Поведінка, на відміну від неорганізованого руху, характеризується тим, що вона, переслідуючи заздалегідь визначену мету, складається з послідовності дій, які закінчуються деяким результатом.

Приймаючи нового співробітника на роботу, організація не тільки визначає мету його діяльності і забезпечує інструментами задля досягнення поставлених цілей, але й видає йому конкретний "кредит довіри", який визначається допуском до робочого місця, а також допуском до інформаційних та інших ресурсів підприємства. Для забезпечення контролю за цим "кредитом довіри" в організаціях вводяться правила, що регламентують поведінку співробітників з різних ракурсів, наприклад:

- ✓ для забезпечення корпоративної етики – чіткі вимоги до поведінки сприяють формуванню відповідальної робочої атмосфери;
- ✓ для запобігання витоку конфіденційної інформації – регламенти інформаційної безпеки допомагають захистити комерційну таємницю, персональні дані працівників та клієнтів тощо;
- ✓ для спрощення дисциплінарного контролю – наявність письмових правил допомагає керівництву справедливо оцінювати поведінку працівників та вживати відповідних заходів у разі порушень.

Контроль за виконанням цих правил є нетривіальним завданням, оскільки правила часто описуються або дуже конкретно, наприклад, "Забороняється використовувати месенджер Telegram у роботі" або абстрактно: "Співробітник повинен перешкоджати витоку конфіденційної інформації". У першому випадку співробітник може скористатися іншим каналом для крадіжки конфіденційної інформації, у другому випадку може апелювати до неможливості визначити, що є конфіденційна інформація, а що ні.

**Експеримент.** Разом із співробітниками відділів інформаційної безпеки ми зібрали статистику різноманітних порушень, які були зроблені свідомо або несвідомо працівниками реальних організацій. Дана інформація збиралася з прив'язкою до часу роботи співробітника в організації на момент виявлення порушення. При цьому порушення, що зробили співробітники першого року роботи фіксувалися за допомогою технічних систем контролю, таких як антивіруси, системи моніторингу дій користувача, наприклад, аналіз скріншотів з

робочого місця користувача. Аналіз діяльності обраних користувачів виконувався вручну співробітниками відділу безпеки. Також аналізувались данні з систем DLP (Data loss prevention) усіх користувачів, незалежно від часу їх роботи в організації.

Проведені експериментальні дослідження виявили три етапи роботи співробітника в організації з погляду шаблонів поведінки:

1) Перші 2-3 місяці, поки триває випробувальний термін, співробітник вивчає цілі, інструменти та правила своєї роботи. Цей етап характеризується великою кількістю неефективних дій та помилок. Однак під час цього етапу вкрай малоймовірні усвідомлені інсайдерські загрози, оскільки співробітник перебуває під контролем наставника. Є певний відсоток порушень з необережності, пов'язаний із незнанням правил роботи з інформацією. Саме за цих причин, поведінкові шаблони, сформовані на даному етапі, будуть неінформативними.
2) На етапі становлення, що триває наступні 6-12 місяців, співробітник впевнено використовує основні інструменти, потрібні для виконання його обов'язків. На цьому етапі він вчиться використовувати інструменти максимально ефективно та безпечно. Поведінкові шаблони, сформовані в цей період, є найбільш цікавими, оскільки вони описують ефективну роботу та ще позбавлені ознак інсайдерської поведінки.
3) Після проходження другого етапу, який у більшості випадків закінчується через рік після початку роботи, співробітник може стати загрозою для внутрішньої безпеки підприємства. Потенційно такими співробітниками можуть стати:
    - ті, кого не влаштовує робота і вони бажають її змінити на нове місце;
    - ті, хто негативно налаштований по відношенню до компанії;
    - токсичні люди;
    - незадоволені власним статусом у колективі;
    - незадоволені рівнем оплати праці тощо.

Окрім цього слід виділити також інсайдерів, тобто тих, хто свідомо або несвідомо розповсюджує конференційну інформацію. У такому випадку поведінкові шаблони, сформовані на другому етапі, будуть використовуватися для оцінки загроз безпеки надалі. Такі шаблони формуються індивідуально для кожного співробітника, оскільки потрібно врахувати його особливості. У табл.1 наведено дані про відсоток працівників, які свідомо або несвідомо порушують інформаційну безпеку організації, в залежності від вищезазначених етапів адаптації людини на робочому місці.

Таблиця 1. – Виявлення свідомо і несвідомо зроблених порушень на різних етапах адаптації людини на новому робочому місці

| | Основні типи порушень | 1 етап | 2 етап | 3 етап |
|---|---|---|---|---|
| Неусвідомлені | Перехід за шкідливими посиланнями у месенджерах або поштових повідомленнях | 90% | 8% | 2% |
| | Порушення правил зберігання паролів | 95% | 4% | < 1% |
| | Порушення правил роботи з сайтами в інтернет | 90% | 5% | 5% |
| Усвідомлені | Крадіжка комерційної інформації на користь конкурентів чи особистих цілях | 0 | 4% | 96% |
| | Участь у змові з метою крадіжки інформації чи грошей | 0 | 7% | 93% |
| | Умисне зараження свого комп'ютера вірусами на користь зовнішніх хакерів | 0 | 0 | 100% |

**Висновки.** Психологія особистості відіграє значну роль у побудові інформаційної безпеки підприємства. Особистісні риси працівників, такі як рівень відповідальності, схильність до ризику, уважність та добросовісність, напряму впливають на їхню поведінку при роботі з конфіденційною інформацією. Наприклад, недбалі або імпульсивні працівники можуть випадково допустити витік даних або стати жертвами соціальної інженерії. Водночас дисципліновані й обізнані співробітники, які усвідомлюють важливість дотримання політик безпеки, сприяють зміцненню загальної захищеності організації.

Вивчення психологічних особливостей допоможе створити індивідуальні поведінкові шаблони співробітників. Проходження новими співробітниками тестів, які проводять HR, можуть допомогти виявляти 3-4 риси особистості, які потенційно можуть вплинути на ризики безпеки. Ці риси обов'язково слід враховувати під час формування базових поведінкових шаблонів користувача. Окрім цього, поведінкові шаблони повинні гнучко модифікуватися в залежності від зібраної статистики. Доцільним буде також дослідити, наскільки первинна оцінка співпадає з реальною діяльністю працівника, тобто, з його поведінковим шаблоном.

Окрім цього, кластери всередині організації також мають суттєвий вплив на стан інформаційної безпеки підприємства. Такі групи формують специфічну культуру поведінки, яка може як підтримувати політику безпеки, так і їй протирічити. Наприклад, якщо в кластері прийнято ділитися паролями або ігнорувати політики безпеки, то ця поведінка швидко поширюється на нових учасників. Виявлення таких груп і розуміння їхніх цінностей допомагає розробляти цільові стратегії для їх навчання та подальшої комунікації.

**Бібліографія**


1. Balogh, Z., Francisti, J., Hrabčák, M. (2024). Security Aspects of Digital Identity. In: Nguyen, N.T., et al. Recent Challenges in Intelligent Information and Database Systems. ACIIDS 2024. Communications in Computer and Information Science, vol 2144. Springer, Singapore. https://doi.org/10.1007/978-981-97-5937-8_1
2. Artioli, Pierpaolo, Antonio Maci and Alessio Magrì. A comprehensive investigation of clustering algorithms for User and Entity Behavior Analytics. // Frontiers in Big Data 7 (2024). https://doi.org/10.3389/fdata.2024.1375818
3. Супрун О. Проблема формування поведінкових шаблонів дій користувачів. / Олександр Супрун, Надія Карпенко // IX Всеукраїнська науково-практична конференція "Перспективні напрямки сучасної електроніки, інформаційних і комп'ютерних систем" (MEICS-2024), м. Дніпро, ДНУ ім. О. Гончара, 27-29 листопада 2024 р., с. 52-53. http://meics.dnure.dp.ua/files/MEICS-2024.pdf
4. Burch G.F., Batchelor J.H., Reid R., Fezzey T., Kelley C. The Influence of Employee Personality on Information Security [Електронний ресурс] // ISACA Journal. – 7 жовтня 2021. – Режим доступу: https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/the-influence-of-employee-personality-on-information-security – Назва з екрана.
5. Johnston, A.C. A closer look at organizational cybersecurity research trending topics and limitations. // Organizational Cybersecurity Journal: Practice, Process and People, 2022, Vol. 2 No. 2, pp. 124-133. https://doi.org/10.1108/OCJ-07-2022-0013
6. Kumrashan Indranil Iyer, "Behavioral Intelligence at Scale: Implementing UEBA for Enhanced Security Posture", International Journal of Science and Research (IJSR), Volume 11 Issue 7, July 2022, pp. 1971-1977, https://www.ijsr.net/getabstract.php?paperid=SR22074090532, DOI: https://www.doi.org/10.21275/SR22074090532