4. Modic, D., Anderson, R. Reading this may harm your computer: The psychology of scams. – *Journal of Cybersecurity*, 2015. – Vol. 1(1). – P. 87–97.

5. Cole R. Scammed by Love: The Role of Loneliness, Trust, and Age in Financial Losses from U.S. Online Romance Scams // *Innovation in Aging*. – 2024.

6. Understanding the Role of Demographic and Psychological Factors in Users' Susceptibility to Phishing Emails: A Review // *MDPI*. – 2022. – Vol. 15(4), p. 2236.

Гуменюк Вікторія Олегівна
Студентка групи 202_СПС ННІ права та психології НАВС

Науковий керівник:
Пакриш Олександр Євгенійович
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій ННІ права та психології НАВС

ЗНАЧЕННЯ ЛЮДСЬКОГО ФАКТОРУ У КІБЕРБЕЗПЕЦІ

У сучасному світі, де більшість інформаційних процесів відбувається у цифровому просторі, питання кібербезпеки набуває вирішального значення. Ми живемо в епоху, коли інформація стала не лише ресурсом, а й об'єктом постійних атак. Щодня відбуваються мільйони кібератак на приватні особи, підприємства й навіть державні установи. Попри стрімкий розвиток технологій захисту – антивірусів, систем виявлення вторгнень, шифрування даних, – головним і найвразливішим елементом системи безпеки залишається людина. Саме людський фактор, тобто дії, помилки чи поведінкові особливості користувачів, визначає, наскільки ефективною буде будь-яка система кіберзахисту.

Людський фактор у кібербезпеці – це сукупність психологічних, поведінкових і організаційних аспектів, які впливають на безпеку інформаційних систем. Іншими словами, це все, що пов'язано з тим, як люди взаємодіють із технологіями.

Людина може бути як найсильнішою, так і найслабшою ланкою в системі. З одного боку, жодна система не може ефективно працювати без відповідальних і навчених працівників. З іншого – саме через необережність, неуважність або навмисні дії люди часто виникають серйозні порушення безпеки.

Помилки користувачів є однією з найпоширеніших причин кіберінцидентів. Наприклад, відкриття шкідливих файлів, натискання на підозрілі посилання, введення паролів на фішингових сайтах або ненавмисне розголошення конфіденційних даних.

Такі помилки часто спричинені не злим умислом, а браком знань чи звичайною неуважністю. Дослідження різних компаній показують, що близько 88% усіх витоків даних пов'язані саме з людським фактором – помилками, порушенням політик безпеки або соціальною інженерією.

Аналогічно, за даними Crowe, у 74% кібератак людська дія відіграла ключову роль. Особливу загрозу становить явище соціальної інженерії – це коли зловмисники використовують психологічні прийоми, щоб змусити людину самостійно відкрити їм доступ до системи.

Найчастіше це відбувається через електронні листи або повідомлення, які виглядають правдоподібно. Людина натискає на шкідливе посилання або вводить пароль, вважаючи, що спілкується з колегою чи офіційною службою. Подібні атаки доводять, що технологічні системи можуть бути надійними, але людська довірливість залишається найслабшим місцем у будь-якому захисті.

Не менш небезпечними є так звані «інсайдерські загрози», коли співробітники навмисно порушують правила безпеки. Це може бути зрада, корупційний вплив або звичайне невдоволення умовами праці. В одному з наукових звітів за 2023 рік зазначається, що приблизно чверть кіберінцидентів відбувається через навмисні дії співробітників. Тобто небезпека походить не лише ззовні, а й із середини організації.

Велику роль відіграє також психологічний стан людини. Стрес, перевтома, перевантаження інформацією або багатозадачність суттєво збільшують ризик помилок. Працівники, які працюють у режимі постійного тиску або поспіху, частіше ігнорують процедури безпеки чи шукають «короткі шляхи» виконання завдань. Таким чином, створення комфортного робочого середовища є не лише питанням турботи про персонал, а й одним із аспектів кіберзахисту.

Попри те, що людський фактор є причиною більшості інцидентів, саме людина може стати ключем до їх запобігання. Для цього потрібно інвестувати у навчання, підвищення обізнаності та формування культури безпеки. Як свідчить досвід компаній, що впроваджують програми підготовки персоналу, регулярні тренінги, симуляції фішингових атак і навчальні кампанії значно знижують кількість успішних кібератак.

Сьогодні важливо не лише навчити працівників технічним правилам – створювати складні паролі, не відкривати невідомі файли, – а й пояснити, як працюють психологічні пастки, на які розраховують хакери. Сучасний підхід до кіберзахисту базується на поєднанні технологічних і людських ресурсів. Технології здатні відслідковувати аномальну поведінку користувачів, автоматично оновлювати системи, обмежувати доступи.

Але жодна технологія не може повністю замінити людське мислення, інтуїцію й відповідальність. Саме тому ефективна кібербезпека передбачає створення систем, які враховують людські обмеження.

Наприклад, інтерфейси мають бути зрозумілими, попередження – чіткими, а процеси – такими, щоб користувачеві було простіше діяти безпечно, ніж ризиковано.

Важливим напрямом є формування культури кібербезпеки в організаціях. Це означає, що питання безпеки повинно бути не лише технічним завданням IT-відділу, а спільною відповідальністю кожного працівника. Коли керівництво демонструє, що безпека – це цінність, а не формальність, персонал починає ставитися до цього серйозніше. Успішні компанії впроваджують системи мотивації, винагороджують уважність, проводять конкурси на кращі безпечні практики.

Історія кіберінцидентів показує, що навіть одна людська помилка може спричинити мільйонні збитки. Наприклад, у 2017 році під час атаки WannaCry багато організацій зазнали втрат не через недосконаліть технологій, а через те, що працівники не встановили оновлення безпеки. Інший приклад – недавня атака на авіакомпанію Qantas, де зловмисники змогли отримати доступ до системи через один телефонний дзвінок і довірливу відповідь працівника. Це яскраво ілюструє, що навіть найдосконаліші системи можуть бути зруйновані одним людським рішенням.

Отже, людський фактор – це не лише слабкість, а й ресурс, який можна перетворити на перевагу. Якщо організація правильно працює зі своїми людьми, навчає їх, мотивує, створює сприятливе середовище та розумно поєднує технології з людською відповідальністю, рівень кібербезпеки зростає в рази. Кіберзахист – це не тільки питання програм і систем, це насамперед питання культури, поведінки й свідомості кожного користувача.

Підсумовуючи, можна сказати, що жодна технологія не здатна повністю усунути людський фактор, але його можна контролювати, передбачати й використовувати на користь безпеки. Люди залишаються головною силою й водночас головним викликом кібербезпеки. Саме від рівня їхньої підготовки, уваги та відповідальності залежить, наскільки захищеним буде наш цифровий світ.

Список використаних джерел:

1. Crowe. The Human Factor in Cybersecurity. – Режим доступу: https://www.crowe.com/

2. BCS365. The Importance of Employee Training in Cybersecurity. – Режим доступу: https://www.bcs365.com/

3. Kaspersky. Human Factor Report 2023. – Режим доступу: https://www.kaspersky.com/

4. LevelBlue. Behavioral Insights and Mitigation Strategies. – Режим доступу: https://www.levelblue.com/

5. Наука Онлайн. Вплив людського фактора на якість систем безпеки. – Режим доступу: https://nauka-online.com/

6. SpringerLink. Human factors in cybersecurity: An interdisciplinary review. – Режим доступу: https://link.springer.com/ Threatscape. The Human Factor in Cyber Security. – Режим доступу: https://www.threatscape.com/

7. The Guardian. Qantas cyberattack: staff error leads to data exposure. – Режим доступу: https://www.theguardian.com/

Yarotska Anastasiia Stanislavivna
Student of academic group 301_SPS,
Institute of Law and Psychology, NAIA

Scientific supervisor:
Pakrysh Oleksandr Yevheniiovych
Candidate of Technical Sciences,
Associate Professor, Associate Professor of the Department of Information Technologies, Institute of Law and Psychology, NAIA

PSYCHOLOGICAL TYPES OF CYBERCRIMINALS

In the modern world, where almost every person has easy access to the Internet, and it is not limited to a home desktop computer, new ways of illegal, criminal behavior are opening up, and therefore, with the advent of the Internet, cybercriminals have appeared in our lives. According to the definition of the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine", a cybercrime is a socially dangerous guilty act in cyberspace and/or with its use. A cybercriminal, accordingly, is a person who committed such a crime.

As each type of illegal behavior in cybercrime has a certain collective profile of the offender, I propose to examine it from several points of view: the general characteristics of the cybercriminal (who are these people and what controls them), psychological types of cybercriminals by motivation for committing crimes and by approaches to illegal activities in cyberspace. I chose to characterize psychological types by their type of activity.

The general profile of a cybercriminal begins with the same general criminal craving/desire to obtain a benefit that is impossible (or difficult) to obtain in a law-abiding way. However, by the nature of the diversity of cyberspace, these benefits are radically different. A cybercriminal is primarily attracted by anonymity, invisibility in an infinite number of Internet connoisseurs. As in the real world, a person who wants to commit a crime is attracted to remaining unexposed, and ultimately unpunished.