Мощук П. О.,
здобувач вищої освіти спеціальності
281 Публічне управління та адміністрування
Науковий керівник: Богатєнкова О. Є., асистент кафедри
економічної кібернетики, комп'ютерних наук та
інформаційних технологій
Миколаївський національний аграрний університет,
м. Миколаїв

МІНІМІЗАЦІЯ РИЗИКІВ ЛЮДСЬКОГО ФАКТОРУ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Розглядається вплив людського фактора на кібербезпеку критичної інфраструктури. Пояснюється, чому саме помилки працівників часто стають причиною інцидентів, а також описуються основні способи зменшення таких ризиків. Наголошується на важливості навчання персоналу, формування культури безпеки та застосування сучасних технічних засобів захисту.

Людський фактор сьогодні вважається однією з головних причин проблем у сфері кібербезпеки. Навіть якщо в організації впроваджені сучасні технічні рішення, одна необережна дія співробітника може дозволити зловмиснику обійти захист. За міжнародними даними, більшість успішних атак так чи інакше пов'язані з діями працівників або з недостатньою обізнаністю у сфері безпеки [4]. Найчастіші інциденти трапляються через відкриття підозрілих листів, використання простих паролів, порушення внутрішніх правил безпеки чи встановлення невідомих програм [2].

Критична інфраструктура охоплює енергетичні системи, транспорт, державні служби, банківську сферу та інші важливі галузі. Тому навіть одна помилка може вплинути на роботу цілих регіонів або держави. Саме через це важливо забезпечити вчасну підготовку персоналу, сформувати у співробітників відповідальне ставлення до кібербезпеки та постійно оновлювати їхні знання [1].

Одним із найкращих способів зменшення ризиків є регулярне навчання працівників. Це можуть бути тренінги, короткі онлайн-курси, лекції або симуляції фішингових атак. Такі заходи дозволяють зрозуміти, як персонал реагує на потенційні загрози, та виявити, кому потрібна додаткова підготовка [3]. Крім того, потрібно правильно налаштовувати системи доступу. Наприклад, кожен співробітник має отримувати лише ті повноваження, які справді потрібні для його роботи. Багатофакторна автентифікація та поділ мережі на сегменти значно ускладнюють роботу зловмисників навіть у разі компрометації одного облікового запису.

Сучасні технічні рішення також допомагають зменшувати вплив людського фактора. Системи моніторингу, аналіз поведінки користувачів та інші інструменти дозволяють виявляти підозрілі дії людей – як випадкові, так і навмисні. Окрему небезпеку становлять інсайдерські загрози, оскільки інсайдер має законний доступ до системи й може завдати шкоди непомітно для інших. Тому організаціям необхідно регулярно перевіряти журнали подій, проводити

аудит безпеки й підтримувати план реагування на інциденти [5].

Психологічні особливості людини також відіграють важливу роль. Часто працівники недооцінюють масштаби загроз і думають, що кібератака «не може статися саме в їхній організації». Через таку самовпевненість співробітники порушують базові правила, наприклад: зберігають паролі в записнику, підключають особисті флешки або відкладають оновлення програм. Усе це створює додаткові можливості для кіберзловмисників.

Ще однією проблемою є перевтома персоналу. Коли працівники отримують надто багато листів або працюють у напружених умовах, їх уважність знижується, і вони можуть легко пропустити фішинговий лист або неправильне повідомлення. Саме тому важливо зменшувати зайві навантаження на персонал і автоматизувати рутинні процеси, щоб працівники не втрачали концентрацію під час виконання важливих завдань.

Також слід зазначити, що культура кібербезпеки починається з керівництва. Якщо керівники організації не дотримуються внутрішніх правил і самі ігнорують протоколи безпеки, працівники наслідують їхню поведінку. Тому система захисту повинна впроваджуватися «згори вниз», а керівництво має бути першим, хто виконує всі встановлені вимоги.

Крім цього, важливо, щоб співробітники розуміли, яку роль вони відіграють у спільній системі безпеки. Коли працівники знають, що їхні дії можуть позитивно або негативно вплинути на всю організацію, вони стають більш уважними та відповідальними. Це поступово формує культуру безпеки, яка значно підвищує загальну кіберстійкість установи.

Таким чином, мінімізувати вплив людського фактора можна лише за умови поєднання кількох підходів: навчання співробітників, технічного контролю, правильного управління доступами, підтримки з боку керівництва та створення позитивної культури безпеки. Лише комплексна робота дозволяє зменшити кількість інцидентів і забезпечити надійний захист критичної інфраструктури від сучасних кіберзагроз.

Список використаних джерел

1. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19

2. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection. Controls. URL: https://www.iso.org/standard/75652.html

3. ENISA. Cybersecurity Culture in Organisations. URL: https://www.enisa.europa.eu/publications

4. Verizon. Data Breach Investigations Report (DBIR) 2024. URL: https://www.verizon.com/business/resources/reports/dbir

NIST Special Publication 800-53. Security and Privacy Controls for Information Systems. URL: https://csrc.nist.gov/publications