Згалат-Лозинська Любов Олександрівна
кандидат економічних наук, доцент,
Приватне акціонерне товариство «Вищий навчальний заклад "Міжрегіональна Академія управління персоналом"»
Марченко Аліна Віталіївна
студентка,
Приватне акціонерне товариство «Вищий навчальний заклад "Міжрегіональна Академія управління персоналом"»

DOI: https://doi.org/10.36059/978-966-397-392-0-4

УПРАВЛІННЯ СИСТЕМОЮ КАДРОВОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Управління системою кадрової безпеки підприємства є однією з найважливіших складових управління в сучасних умовах бізнес-середовища, особливо в умовах зростаючих кіберзагроз та поширення кібератак [1]. Підприємства повинні постійно вдосконалювати свої системи кадрової безпеки, щоб ефективно захищати конфіденційні дані, забезпечувати відповідність законодавству та запобігати можливим інцидентам з порушенням безпеки [2]. У цьому тексті розглянемо ключові аспекти управління системою кадрової безпеки та шляхи їх впровадження на підприємстві.

Першим кроком у вдосконаленні системи кадрової безпеки є розробка стратегії. Підприємство повинно чітко визначити свої цілі та завдання у цій сфері, а також визначити методи та інструменти, необхідні для досягнення цих цілей [3]. Стратегія повинна враховувати специфіку бізнесу підприємства, його ризики та потенційні загрози, а також відповідати сучасним стандартам кібербезпеки. Отже, постійне вдосконалення та адаптація системи кадрової безпеки до нових технологічних викликів є критично важливим для забезпечення ефективного захисту інформаційних ресурсів підприємства.

Другим важливим аспектом є розробка та впровадження політик та процедур безпеки. Ці документи визначають правила та стандарти, які повинні дотримуватися всіма співробітниками підприємства щодо захисту інформації та персональних даних. Політики та процедури повинні охоплювати такі аспекти, як контроль доступу до інформації, захист від внутрішніх та зовнішніх загроз, а також процедури реагування на інциденти безпеки [4]. І також, партнерство з іншими суб'єктами бізнесу, а також з правоохоронними органами та спеціалістами з кібербезпеки може виявитися важливим ресурсом у розробці та впровадженні ефективних заходів з захисту інформаційних ресурсів підприємства.

Третім кроком є навчання персоналу з питань безпеки. Персонал повинен бути свідомим ризиків та загроз, що існують у цифровому середовищі, і знати, як правильно діяти в разі виявлення аномалій або підозрілих дій. Навчання має бути регулярним і охоплювати всіх співробітників, включаючи високопосадових керівників та кадрових працівників.

Четвертим кроком є систематичний аналіз та аудит системи кадрової безпеки. Підприємство повинно регулярно перевіряти ефективність своїх заходів безпеки, виявляти слабкі місця та прогалини, а також вносити відповідні корективи [2]. Аудит також допомагає підприємству виявляти нові загрози та реагувати на них вчасно [5].

П'ятим кроком у управлінні системою кадрової безпеки є залучення зовнішніх експертів та консультантів з кібербезпеки. Іноді підприємствам може бути важко впоратися з усіма викликами та потребами у сфері безпеки самостійно, тому експертна допомога ззовні може бути надзвичайно корисною. Залучення фахівців з кібербезпеки допоможе ідентифікувати потенційні загрози, розробити ефективні заходи безпеки та забезпечити відповідність стандартам та законодавству [4]. Ефективне управління системою кадрової безпеки також передбачає регулярну оцінку ризиків

і вжиття заходів щодо їх мінімізації, а також виявлення та вирішення проблем, що виникають у процесі її функціонування.

Шостим важливим аспектом є створення культури безпеки в організації. Це означає, що кожен співробітник повинен бути залучений до процесу захисту інформації та персональних даних, розуміти важливість цих питань і бути відповідальним за свої дії в цьому напрямку. Створення культури безпеки може бути досягнуте шляхом проведення інформаційних кампаній, тренінгів та регулярних перевірок, щоб підтримувати свідоме ставлення до питань безпеки серед персоналу [6]. Забезпечення культури безпеки серед персоналу, включаючи підвищення обізнаності щодо кіберзагроз, виконання правил та процедур безпеки, є важливою складовою успішної системи кадрової безпеки на підприємстві.

Нарешті, сьомим кроком є постійне вдосконалення та адаптація системи кадрової безпеки до змін у технологіях та загрозах. Кіберзагрози постійно еволюціонують, тому система управління кадровою безпекою повинна бути гнучкою та готовою до швидкого реагування на нові виклики. Це може означати оновлення технологічних засобів захисту, вдосконалення політик та процедур безпеки, а також посилення контролю за дотриманням внутрішніх правил та політик безпеки [1; 2; 4; 5].

Загалом, управління системою кадрової безпеки є складним та багатогранним процесом, який вимагає систематичного підходу та постійного вдосконалення. Шлях до успіху полягає в розробці чіткої стратегії, впровадженні ефективних політик та процедур, навчанні персоналу та систематичному аналізі та аудиті системи. Відповідальне та компетентне управління кадровою безпекою дозволяє підприємствам ефективно захищати свою інформацію та забезпечувати стабільну роботу у цифровому середовищі.

Література:

1. Ponemon Institute (2021). 2021 Cost of a Data Breach Report. Available at: https://www.ibm.com/security/data-breach

2. Cybersecurity and Infrastructure Security Agency (CISA) (2021). Best Practices for Cybersecurity Management in Organizations. Available at: https://www.cisa.gov/best-practices-cybersecurity-management-organizations

3. SANS Institute (2020). Information Security Policy Templates. Available at: https://www.sans.org/security-resources/policies

4. Brown A., & Jones B. (2019). Cybersecurity Policies and Procedures: Best Practices for Implementation. *International Journal of Cybersecurity Management.* No. 5(1). Pp. 35–48.

5. National Institute of Standards and Technology (NIST) (2020). NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

6. Anderson E., & Smith J. (2018). Building a Culture of Security: A Guide for Leaders. Available at: https://www.nist.gov/sites/default/files/documents/2017/05/09/building_culture_of_security.pdf