

ЕКОНОМІКО-СОЦІАЛЬНІ ВІДНОСИНИ В ГАЛУЗІ ФІЗИЧНОЇ КУЛЬТУРИ ТА СФЕРІ ОБСЛУГОВУВАННЯ

Тези доповідей
VII Міжнародної науково-практичної конференції
(24–25 квітня 2025 року, м. Львів)

За загальною редакцією Наталії ПАВЛЕНЧИК

Львів
ЛДУФК ім. Івана Боберського
2025

УДК 336:71

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ LESSONS LEARNED У БЕЗПЕКОВИХ МОДЕЛЯХ ОРГАНІЗАЦІЙ

Руслана Содома

кандидат економічних наук, доцент

Львівський державний університет безпеки життєдіяльності (Україна)

Володимир Романів

аспірант

Львівський державний університет безпеки життєдіяльності (Україна)

Сучасні корпоративні організації стикаються з безпековими викликами, які потребують постійного вдосконалення стратегій управління ризиками. «Lessons Learned» — це ефективний підхід, що дає змогу аналізувати минулий досвід для запобігання повторенню інцидентів. Спробуємо розглянути, як «Lessons Learned» може інтегруватися в безпекові моделі організацій. «Lessons Learned» — це систематичний процес збору, аналізу та впровадження висновків з попередніх подій. У разі застосування «Lessons Learned» вжливо фокусуватись на основних принципах документування інцидентів, аналізі першопричин, впровадження коригувальних заходів та взаємозв'язках «Lessons Learned» із системами управління ризиками та стандартами безпеки (ISO 27001, NIST), зокрема такими, як:

ISO 27001: Використовують для управління інформаційною безпекою та передбачає постійний аналіз і вдосконалення системи захисту;

NIST (Національний інститут стандартів і технологій США): Пропонує підхід до кібербезпеки, який містить уроки, отримані з попередніх атак;

OHSAS 18001 / ISO 45001: Регулюють питання охорони праці та безпеки на робочому місці, де «Lessons Learned» допомагає запобігати виробничим інцидентам. Основні етапи імплементації «Lessons Learned»зображено на рисунку 1.

Інтеграція «Lessons Learned» у корпоративну культуру дає змогу зробити процес управління безпекою постійним та ефективним. Технологія є критично важливим інструментом для підвищення ефективності безпекових моделей у корпоративних організаціях. Організації, які прагнуть досягти високого рівня безпеки, мають забезпечити безперервний обмін знаннями

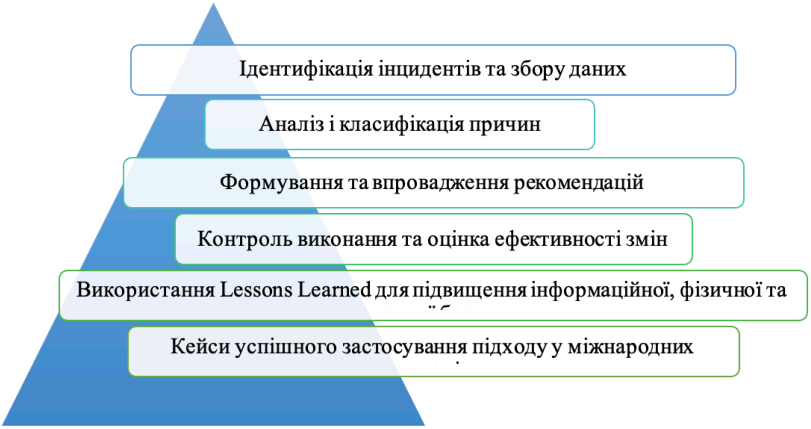


Рис 1. Основні етапи імплементації «Lessons Learned» у безпекових моделях [1].

та досвідом між співробітниками й підрозділами. Створити централізовану інформаційну платформу, де зберігаються всі кейси, інциденти та ефективні рішення для їхнього усунення. Це допоможе персоналові швидко отримувати доступ до накопиченого досвіду й використовувати його в реальних ситуаціях. Часто проводити тренінги та симуляційні вправи, де працівники навчатимуться на реальних та змодельованих інцидентах, аналізувати помилки та засвоюватимуть методи їхнього уникнення. Активно залучати всіх рівнів працівників до процесу «Lessons Learned». Це передбачає анонімне повідомлення про інциденти, дискусії в робочих групах та обговорення результатів у форматі відкритих зустрічей. Використовувати спеціалізовані програмні рішення для збору, аналізу й упровадження висновків, що спрощує управління безпековими інцидентами й сприяє ефективному розподілу ресурсів. Запроваджувати систему винагород та визнання для працівників, які активно беруть участь у впровадженні «Lessons Learned». Це може бути як фінансове стимулювання, так і нематеріальні бонуси, наприклад, можливість кар'єрного зростання. «Lessons Learned» має бути не разовою ініціативою, а частиною стратегічного підходу організації. Для цього треба регулярно переглядати й оновлювати політики безпеки на основі нових загроз та змін у середовищі. Для успішної реалізації необхідна підтримка керівництва, автоматизація процесів аналізу й упровадження навчання для персоналу. Подальші дослідження можуть стосуватися розроблення інструментів для спрощення збору й аналізу уроків безпеки.

Список використаних джерел:

1. Alyoshina T. V., Fisunenko N. O., Kyselov A. O., Kiselov S O., Karnauhov O. V. Innovative approaches to personnel security under the conditions of martial law. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*. 2024. № 4. P. 164–171.