УДК 004.432 Інформаційні системи та технології

**Крихівський Михайло Васильович**

доцент кафедри інженерії програмного забезпечення,

Івано-Франківський національний технічний

Університет нафти і газу, м. Івано-Франківськ, Україна

ORCID 0009-0000-3285-4308

**Ваврик Тетяна Олександрівна**

Асистент кафедри інженерії програмного забезпечення,

Івано-Франківський національний технічний

Університет нафти і газу, м. Івано-Франківськ, Україна

ORCID 0000-0002-0612-0084

**Гобир Лідія Мирославівна**

асистент кафедри інженерії програмного забезпечення,

Івано-Франківський національний технічний

Університет нафти і газу, м. Івано-Франківськ, Україна

|  |
| --- |
| ORCID 0009-0007-3176-2314 |

**ТЕХНІЧНІ, ОРГАНІЗАЦІЙНІ ТА ПРАВОВІ АСПЕКТИ КІБЕРБЕЗПЕКИ**

Одним з головних викликів у галузі безпеки даних є постійно зростаюча складність кіберзагроз, таких як хакерські атаки, віруси та фішинг. Щоб протистояти цим загрозам, користувачі повинні постійно оновлювати свої заходи безпеки та бути готовими до реагування на нові виклики. На перспективи розвитку безпеки даних впливають такі технологічні тенденції, як штучний інтелект, машинне навчання та квантові обчислення. Нові технології можуть допомогти покращити ефективність і надійність заходів безпеки даних та зробити їх більш адаптивними до сучасних одночасно вони створюють нові виклики. У сучасному світі, де технології швидко розвиваються та використовуються в різних сферах життя, питання забезпечення технічної, організаційної та правової безпеки стає надзвичайно актуальним. Інновації в сфері техніки та інформаційних технологій забезпечують нам нові можливості, проте одночасно вони створюють нові виклики.

Виділяють [1] три складові безпеки даних: технічну, організаційну та правову. Технічна безпека даних є ключовою складовою в забезпеченні конфіденційності, цілісності та доступності цифрової інформації. Цей аспект безпеки включає в себе розробку та застосування технічних і технологічних засобів для захисту даних від несанкціонованого доступу, модифікації та втрати. Це передбачає використання шифрування, механізми автентифікації й авторизації, засоби моніторингу, аудиту, бекапу та відновлення. Технічна безпека даних відіграє важливу роль у захисті цифрової інформації від різноманітних загроз.

Організаційна безпека даних включає в себе розробку політик безпеки, процедур управління доступом до даних, навчання персоналу з питань безпеки, аудит безпеки. Роль організаційної безпеки даних полягає в розробці політик безпеки, управління доступом, навчанні й освіті, аудиті та внутрішньому контролі [2].

Організаційна безпека даних є важливою складовою управління безпекою та захистом цифрової інформації. Вона вимагає комплексного підходу, включаючи розробку політик, навчання персоналу та систематичні аудити для забезпечення ефективної захищеності даних в рамках організації.

Правова безпека даних визначає набір правил, законів і стандартів, які регулюють зберігання, обробку та передачу інформації з метою забезпечення конфіденційності та захисту особистих даних. Вона охоплює визначення правових вимог щодо зберігання, обробки та передачі даних, а також відповідність організацій з цими вимогами. Правова безпека даних - це система законодавчих норм, які регулюють збереження, обробку та передавання особистих даних з метою захисту приватності та конфіденційності користувачів Інтернету. Вона забезпечує виконання зобов'язань збереження та охорони інформації, а також встановлює права та обов'язки сторін у процесі обробки даних. Українське законодавство передбачає відповідальність за порушення правил обробки особистих даних, що має на меті забезпечити безпеку та захист інформації в цифровому середовищі. Із поширенням цифрових технологій і зростанням обсягів обміну і зберігання інформації, зростає і відповідальність за забезпечення захисту цих даних[3].

 Кожний із цих видів безпеки спрямований на захист даних і систем від різних видів загроз, але вони використовують різні підходи та інструменти для досягнення своїх цілей. Розглянемо основні відмінності між технічною, організаційною та правовою безпекою даних представлені у таблиці 1.

Таблиця 1 – основні відмінності між технічною, організаційною та правовою безпекою даних

|  |  |  |  |
| --- | --- | --- | --- |
| **Параметр** | **Технічна Безпека Даних** | **Організаційна Безпека Даних** | **Правова Безпека Даних** |
| Визначення | Застосування технічних засобів для захисту даних | Розробка політик, процедур та культури безпеки | Законодавство, стандарти та вимоги до захисту даних |
| Ракурс | Захист даних за допомогою технічних засобів | Управління та впровадження політик та процедур | Встановлення правових вимог та відповідність їм |
| Засоби | Шифрування, механізми автентифікації, бекапи | Розробка політик, навчання персоналу, аудит | Створення політик відповідно до законодавства |
| Переваги | Ефективна захист від технічних загроз | Внутрішній контроль, свідома культура безпеки | Законна відповідність та зменшення правового ризику |
| Обмеження | Може бути обмежений технічними можливостями | Залежить від участі персоналу та виконання політик | Вимагає постійного моніторингу та оновлення |
| Виклики | Потребує постійного оновлення і вдосконалення | Вимагає внутрішньої координації та комунікації | Відповідність різним міжнародним та регіональним законам |
| Приклади застосування | Шифрування даних, встановлення брандмауерів | Розробка політики доступу, навчання персоналу | Впровадження заходів для дотримання GDPR, CCPA та ін. |

Забезпечення захисту даних вимагає поєднання технічних, правових та організаційних заходів для запобігання інцидентам та забезпечення довіри користувачів. У підсумку, забезпечення технічної, організаційної та правової безпеки в сучасному світі є невід'ємною складовою успішного функціонування різних сфер діяльності. Це охоплює впровадження ефективних технічних заходів, розробку та виконання належних організаційних стратегій, а також вдосконалення правових механізмів для захисту інтересів суспільства та окремих осіб.

**Література**

1. Kravchenko, O., Veklych, V., Krykhivskyi, M., & Madryha, T. (2024). Cybersecurity in the face of information warfare and cyberattacks. *Multidisciplinary Science Journal*, *6*, 2024ss0219. https://doi.org/10.31893/multiscience.2024ss02192.
2. Кібербезпека бізнесу це не лише технічні заходи. <https://legalitgroup.com/kiberbezpeka-biznesu-tse-ne-lishe-tehnichni-zahodi/>
3. Закон України «Про основні засади кібербезпеки України» від 5 жовтня 2017 року. <https://zakon.rada.gov.ua/laws/show/2163-19>