КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (21), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.21.297308
УДК 004.8

Ананченко Олексій Євгенович
Старший викладач кафедри технологій цифрового розвитку
Державний університет інформаційно-комунікаційних технологій
ORCID 0009-0005-3446-5994
ananchenko.oe@gmail.com

МЕТОДИКА ОЦІНКИ ЕФЕКТИВНОСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОСВІТНЬОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Анотація. У сучасних умовах розвитку інформаційних технологій питання забезпечення інформаційної безпеки набуває все більшої актуальності. Інформація стала ключовим ресурсом, що впливає на успіх та стабільність функціонування організацій, підприємств та установ. Незважаючи на те, що значна частина зусиль спрямована на створення та підтримку ефективних систем захисту інформації, питання оцінки їхньої ефективності залишається актуальним та важливим. У статті розглядається комплексна методика оцінки ефективності забезпечення інформаційної безпеки, яка базується на використанні сучасних підходів та інструментів для аналізу захищеності інформаційних систем. Запропонована методика охоплює різні аспекти інформаційної безпеки, включаючи технічні, організаційні, процедурні та людські фактори. Оцінка ефективності базується на комплексному аналізі множинних показників, що дозволяє отримати об'єктивну картину стану інформаційної безпеки організації. Основною частиною методики є розробка та застосування математичних моделей, які дозволяють здійснювати кількісну оцінку рівня інформаційної безпеки. Такі моделі враховують різноманітні фактори, зокрема рівень технічного захисту інформаційних систем, політику інформаційної безпеки, рівень навчання персоналу, реагування на інциденти та інші важливі аспекти. Крім того, у статті розглядаються питання оптимізації витрат на забезпечення інформаційної безпеки шляхом застосування економічних моделей та підходів. Запропонована методика включає декілька етапів: визначення ключових показників безпеки, збір та аналіз даних, розробка математичних моделей для оцінки ефективності, інтерпретація результатів та розробка рекомендацій щодо підвищення рівня захисту. Важливою складовою методики є системний підхід, який дозволяє враховувати взаємодію різних елементів системи інформаційної безпеки та їхній вплив на загальний рівень захисту. Практичне застосування розробленої методики дає можливість своєчасно виявляти вразливості у системі інформаційної безпеки, оптимізувати витрати на її забезпечення, підвищувати загальний рівень захищеності організації та знижувати ризики, пов'язані з інформаційними загрозами. Результати дослідження підтверджують ефективність запропонованого підходу та демонструють його застосовність у різних галузях діяльності, включаючи бізнес, державний сектор, освіту та інші сфери. Таким чином, запропонована методика оцінки ефективності забезпечення інформаційної безпеки є важливим інструментом для організацій, що прагнуть забезпечити надійний захист своєї інформації. Її використання сприяє підвищенню рівня інформаційної безпеки, що, у свою чергу, позитивно впливає на загальний рівень функціонування та стійкість організацій в умовах сучасних викликів та загроз.

Ключові слова: інформаційна безпека, оцінка ефективності, захищеність інформаційних систем, критерії безпеки, математичні моделі, оптимізація витрат, системний підхід.

ВСТУП

Інформаційна безпека в сучасних умовах стає однією з ключових складових успішного функціонування будь-якої організації, зокрема закладів вищої освіти. Університети та інші навчальні заклади зберігають і обробляють величезні обсяги даних,

що стосуються студентів, викладачів, досліджень та адміністративних процесів. Захист цієї інформації від несанкціонованого доступу, втрати або пошкодження є критично важливим завданням.

Останнім часом зростає кількість кіберзагроз, що спрямовані на освітні заклади. Це обумовлено тим, що університети часто мають слабкі місця в своїх системах захисту, обмежені ресурси для інвестицій у новітні технології безпеки та велику кількість користувачів з різними рівнями доступу та знань в сфері інформаційної безпеки. Крім того, освітні заклади активно взаємодіють з різними зовнішніми партнерами, що також підвищує ризики для інформаційної безпеки.

У зв'язку з цим, постає необхідність розробки ефективної методики оцінки рівня інформаційної безпеки закладів вищої освіти. Така методика має враховувати не лише технічні аспекти захисту інформації, але й організаційні заходи, економічні показники та людський фактор. Комплексний підхід до оцінки дозволить ідентифікувати слабкі місця в системах безпеки, розробити заходи для їх усунення та підвищити загальний рівень захищеності інформаційних ресурсів.

МЕТА І ЗАДАЧІ ДОСЛІДЖЕННЯ.

Ця стаття присвячена розробці та опису такої методики, яка включає в себе різні математичні моделі та інструменти для оцінки ефективності заходів інформаційної безпеки. Запропонована методика базується на багатокритеріальному аналізі, економічній оцінці витрат та вигод, аналізі ризиків і системній динаміці. Використання цих моделей дозволяє здійснити всебічну кількісну оцінку рівня інформаційної безпеки, що сприятиме підвищенню її ефективності та надійності.

Мета цієї роботи полягає в тому, щоб надати інструментарій для адміністрацій закладів вищої освіти, який допоможе у прийнятті обґрунтованих рішень щодо впровадження і вдосконалення заходів інформаційної безпеки.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ.

Стрімкий розвиток інформаційних технологій призводить до загострення питання про створення надійної багатофункціональної системи захисту, яка б забезпечила високий рівень захищеності освітніх органів державної структури від внутрішніх та зовнішніх загроз.

Великі університети в своєму складі мають великий професорсько-викладацький контингент, аспірантів та студентів, що в тій чи іншій мірі користуються інформаційно-телекомунікаційними мережами.

З точки зору інформаційної безпеки, інсайдер - співробітник вузу, що має доступ до конфіденційних даних, розміщених в комп'ютерній мережі університету. Інсайдерська атака може класифікуватись як шахрайство, саботаж або крадіжка інтелектуальної власності. Загальні канали витоку бувають зовнішні (CD, DVD, флеш-накопичувач) та внутрішні (електронна пошта співробітника, блоги, соціальні мережі).

Внутрішні порушники поділяються на лояльних інсайдерів (недбалі та маніпульовані), скривджених, нелояльних інсайдерів, мотивованих ззовні (мотивовані фінансово та впроваджені), та інших порушників (захист від цієї категорії інсайдерів не може бути забезпечений технічно).

Протидія інсайду загалом здійснюється на трьох рівнях:

- прийом на роботу – проводиться комплексна перевірка працівника (психологічні тести, інформація з баз даних та попереднього місця працевлаштування тощо);
- у процесі роботи – організаційно-технічні засоби, системи фізичного та інформаційного захисту (СФЗ та СІЗ), психологічна, юридична та технологічна протидія, моніторинг дій користувача, аудит вразливих місць організації;
- при звільненні – комплексний аналіз доступної інформації, перерозподіл прав доступу тощо.

Основні напрямки захисту від інсайдерів – захист документів, захист каналів витоку та моніторинг дій користувачів. Основний принцип систем захищеного документообігу - захист документа з моменту його створення і до моменту його знищення.

В університетах із значними обсягами наукових дослідів та дослідно-конструкторських робіт, в яких є або можуть бути бази даних обмеженого або таємного характеру, конфіденційні відомості, тощо, доцільно було б організувати центр управління інформаційною безпекою.

Security Operation Center - методологія, що визначає загальний підхід для консолідації та централізації функцій управління всім комплексом гетерогенних систем інформаційної безпеки (ІБ), і спрямована на збільшення ефективності СМІБ. Як правило включає в себе наступні складові:

- Security Information and Event Management System
- Security and Vulnerability Management System
- Compliance Management System

Security Information and Event Management System - засіб автоматизації процесу збору, агрегації і кореляції великого числа подій безпеки, одержуваних з різних джерел, таких як ОС, СУБД, МЕ, IDS/IPS, активне мережеве обладнання, засоби захисту і т.д.

Security and Vulnerability Management System - система оцінки захищеності, що забезпечує ідентифікацію і виявлення вразливостей в операційних системах, СУБД, мережевих службах, протоколах і додатках, а також надає механізми з управління життєвим циклом знайдених вразливостей в інформаційній мережі університету.

Compliance Management System - засіб автоматизації процесів оцінки відповідності IT-інфраструктури університету вимогам корпоративних політик ІБ та існуючих міжнародних стандартів.

Центр оперативного управління інформаційною безпекою(ЦОУІБ) – це централізований підрозділ вузу, який займається питаннями безпеки на організаційному і технічному рівні. Його призначенням є виявлення інцидентів та мінімізація втрат від них при виконанні НДДКР.

Інцидент - подія (або потенційна можливість події), яка веде до порушення вимог інформаційної безпеки, конфіденційності, цілісності або доступності інформаційних ресурсів, або будь-яка нестандартна подія, яка викликає або може викликати зниження якості науково-дослідної роботи або переривання доступності інформаційної системи користувачам.

Управління інцидентами - є діяльність по відновленню нормального обслуговування з мінімальними затримками і впливом на бізнес-операції, що є реактивним, сфокусованим на короткострокову перспективу сервісом відновлення. Вона включає в себе:

1. Виявлення та реєстрація інцидентів
2. Класифікація і початкова підтримка

3. Дослідження та діагностика
4. Вирішення і відновлення
5. Закриття
6. Володіння, моніторинг, відстеження і зв'язок.

Також інциденти призводять до таких негативних наслідків, як:

- Шкода іміджу та репутації університету
- Втрата ключових клієнтів – замовників НДДКР
- Дезорганізація науково-дослідної роботи
- Зниження рейтингу наукового персоналу
-

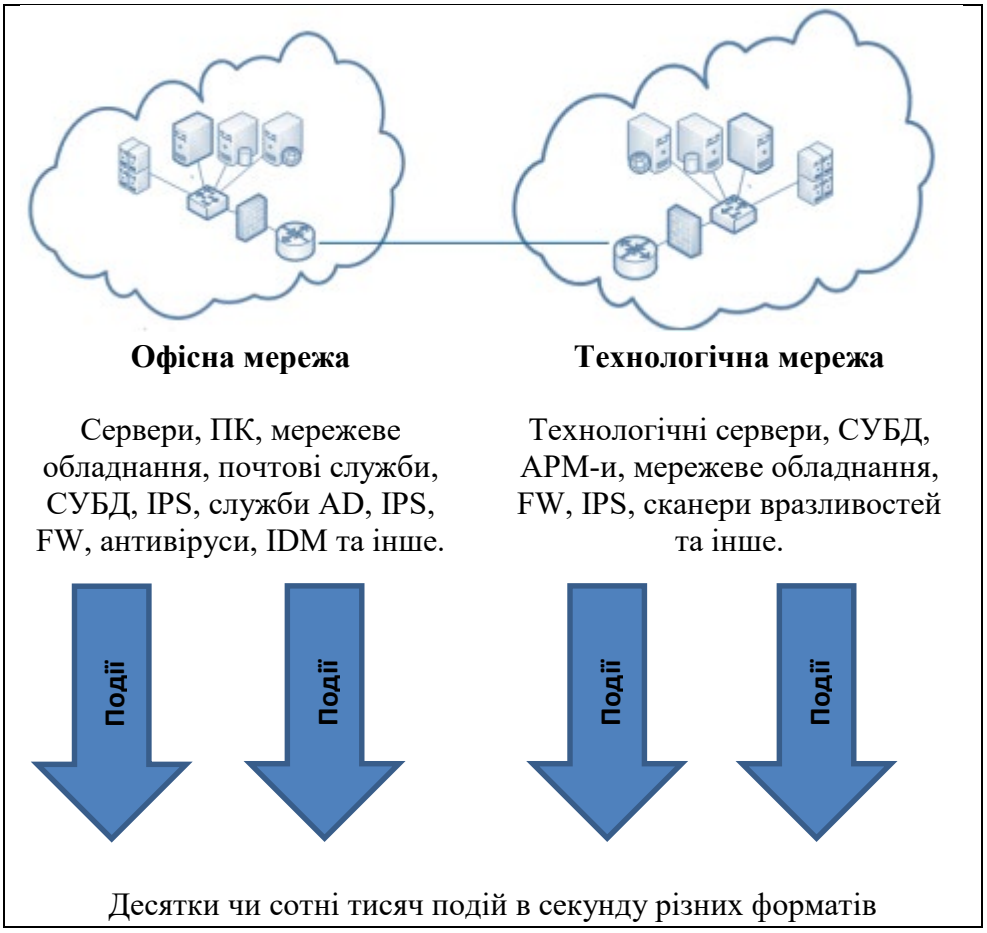

Рис. 1 Проблемні аспекти мережі в університетах

Актуальними проблемами ІБ для більшості університетів є: несвоєчасне виявлення інцидентів ІБ і відсутність актуальної інформації про поточний стан інформаційної безпеки.

Практично в університетах немає можливості своєчасно виявляти інциденти ІБ, тим більше, виявляти проблеми до того, як вони приведуть до інциденту.

В освітній галузі високі трудовитрати на виявлення, обробку та розслідування інцидентів при дефіциті кадрів. Процеси реагування на інциденти ІБ не регламентовані, фахівці не навчені і не мають ефективних інструментів. Для оцінки зрілості SOC в університетах використовують чотири напрямки, що фрагментарно наводяться в таблиці 1.

Таблиця 1

Напрями оцінки зрілості SOC

ВНЗ	Науковий потенціал	Процеси	Технології
Місія ЦОУІБ	Базові метрики	Базові метрики	Архітектура
Прозорість і вимірність	Навчання	Експлуатація ЦОУІБ	Збір даних
Фінансування	Сертифікація	Аналітика і розслідування загроз	Моніторинг і аналіз
Звітність	Досвід	ІТ-процеси ЦОУІБ	Кореляція подій
Взаємозв'язок з замовником НДДКР	Атестація	Взаємодія з замовниками НДДКР	Обслуговування системи

Процесний підхід – це підхід до організації та аналізу ВНЗ, заснований на виділенні і розгляді її наукових-процесів, кожен з яких протікає у взаємозв'язку з іншими процесами університету або зовнішнім середовищем. Важливе значення має захист персональних даних провідних науковців.

Розглянемо математичні моделі, які дозволяють здійснювати кількісну оцінку рівня інформаційної безпеки закладів вищої освіти:

1. Модель багатокритеріального аналізу (AHP) - дозволяє визначити вагу різних критеріїв, що впливають на інформаційну безпеку, та використовує їх для інтегрованої оцінки рівня безпеки.

Основні етапи:

1. Структурування проблеми – ієрархічна структура проблеми складається з головної мети, критеріїв та альтернатив.
2. Порівняння критеріїв – порівняння критеріїв здійснюється за допомогою парних порівнянь.
3. Розрахунок ваг за допомогою матриці парних порівнянь:

$$A = \begin{bmatrix} 1 & a_{12} & \cdots & a_{1n} \\ \frac{1}{a_{12}} & 1 & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{a_{1n}} & \frac{1}{a_{2n}} & \cdots & 1 \end{bmatrix}$$

де a_{ij} - відносна важливість критерію і порівняно з критерієм j.

Власні вектори і значення:

$$Aw = \lambda_{\max} w$$

де λ_{max} - найбільше власне значення матриці порівнянь, w - власний вектор, що представляє ваги критеріїв.

Визначення ваг:

$$w_i = \frac{a_i}{\sum_{i=1}^{n} a_i}$$

де w_i - вага критерію і, a_i - елемент власного вектора.

Обчислення узагальненої оцінки:

$$S_j = \sum_{i=1}^{n} w_i \cdot s_{ij}$$

де S_j - узагальнена оцінка альтернативи j, s_{ij} - оцінка альтернативи j за критерієм i.

2. Модель економічної оцінки (CBA) - оцінює економічну доцільність заходів інформаційної безпеки, використовуючи методику розрахунку чистої теперішньої вартості (NPV).

Основні етапи:

1. **Ідентифікація витрат і вигод –** витрати та вигоди визначаються для кожного року протягом періоду оцінки.
2. **Дисконтування –** дисконтування здійснюється для приведення майбутніх витрат і вигод до теперішньої вартості.

Формула дисконтування:

$$PV = \frac{FV}{(1+r)^t}$$

де PV - теперішня вартість, FV - майбутня вартість, r - ставка дисконтування, t - кількість років.

3. **Розрахунок чистої теперішньої вартості (NPV):**

$$NPV = \sum_{t=1}^{T} \frac{B_t - C_t}{(1+r)^t}$$

де B_t - вигоди в році t, C_t - витрати в році t, r - ставка дисконтування, T - період оцінки.

3. Модель аналізу ризиків - допомагає ідентифікувати і оцінити ймовірності і впливи потенційних загроз, що дозволяє ефективно управляти ризиками.

Основні етапи:

1. **Ідентифікація загроз –** визначення потенційних загроз, які можуть вплинути на систему.
2. **Оцінка ймовірностей і впливів –** оцінка ймовірностей виникнення загроз та їх впливу на систему.

Формула розрахунку ризику:

$$R = P \times I$$

де R - рівень ризику, P - ймовірність виникнення загрози, I - вплив загрози.

4. Модель системної динаміки – описує динамічні процеси в системі інформаційної безпеки, дозволяючи прогнозувати зміни та розробляти стратегії управління.

Основні етапи:

1. **Визначення компонентів системи.**
2. **Побудова діаграм причинно-наслідкових зв'язків:**
3. **Розробка диференціальних рівнянь:**

3.1. Кількість інцидентів:

$$\frac{dI}{dt} = -aI + bC$$

де I - кількість інцидентів, a - коефіцієнт зниження інцидентів, b - коефіцієнт впливу витрат на зниження інцидентів, C - витрати на безпеку.

3.2.Рівень навчання персоналу:

$$\frac{dL}{dt} = -cL + dT$$

де L - рівень навчання персоналу, c - коефіцієнт зниження рівня навчання, d - коефіцієнт впливу технічного захисту на навчання, T - рівень технічного захисту.

3.3. Технічний захист:

$$\frac{dT}{dt} = -eT + f$$

де T - рівень технічного захисту, e - коефіцієнт зниження технічного захисту, f - постійний рівень підвищення технічного захисту.

3.4.Витрати на безпеку:

$$\frac{dC}{dt} = g - hC$$

де C - витрати на безпеку, g - постійний рівень витрат на безпеку, h - коефіцієнт зниження витрат.

Ці математичні моделі забезпечують комплексний підхід до оцінки рівня інформаційної безпеки, враховуючи різні аспекти і дозволяючи приймати обґрунтовані рішення для підвищення захищеності інформаційних систем у закладах вищої освіти.

Для досягнення найбільш комплексної та точної оцінки рівня інформаційної безпеки закладів вищої освіти, доцільно використовувати комбінований підхід, який об'єднує декілька математичних моделей. Запропонована комбінація включає:

1. **Метод аналізу ієрархій (AHP)**
2. **Метод зважених сум (WSM)**
3. **Економічна модель оцінки ефективності інформаційної безпеки (CBA)**
4. **Модель аналізу ризиків**
5. **Модель системної динаміки**

Опис алгоритму

1. **Початок**
2. **Визначення критеріїв та побудова ієрархії (AHP)**
   - Визначення основних критеріїв безпеки.
   - Побудова ієрархії критеріїв та альтернатив.
   - Визначення ваг кожного критерію за допомогою парних порівнянь.
3. **Збір даних та оцінка альтернатив (WSM, AHP)**
   - Збір даних про різні альтернативи заходів безпеки.
   - Оцінка альтернатив за кожним критерієм.
   - Застосування методу зважених сум для обчислення інтегрального показника.
4. **Економічний аналіз (CBA)**
   - Визначення витрат та вигод для кожної альтернативи.
   - Обчислення чистої поточної вартості (NPV) та співвідношення вигод та витрат (BCR).
   - Інтеграція результатів CBA у метод зважених сум.
5. **Аналіз ризиків**
   - Оцінка ймовірності та впливу різних загроз.
   - Коригування оцінок альтернатив з урахуванням результатів аналізу ризиків.
6. **Системна динаміка**
   - Моделювання взаємодії компонентів системи безпеки з плином часу.
   - Прогнозування довгострокових наслідків впровадження заходів безпеки.
7. **Прийняття рішення на основі об'єднаних результатів**
   - Інтеграція результатів всіх моделей.
   - Прийняття рішення щодо вибору найбільш ефективних заходів інформаційної безпеки.
8. **Кінець**

Таблиця порівняння методів з числовими даними

Метрика	Метод порівняльного аналізу	Метод KPI	Метод експертних оцінок	Метод аналізу статистичних даних	Комбінована методика
Комплексність	4	5	6	5	9
Точність	±15%	±10%	±5%	±7%	±3%
Об'єктивність	70%	80%	50%	90%	95%
Гнучкість	5	6	7	5	9
Вартість	10,000 грн	50,000 грн	100,000 грн	50,000 грн	150,000 грн
Час виконання	1 місяць	3 місяці	6 місяців	6 місяців	4 місяці
Простота використання	8	7	5	6	6

Комбінована методика оцінки економічної безпеки закладів вищої освіти отримує найвищий бал за комплексність (9), оскільки вона охоплює всі аспекти безпеки, на відміну від методу порівняльного аналізу, який має найнижчий показник (4) через свою обмеженість. Щодо точності, комбінована методика забезпечує найвищий рівень (±3%), адже об'єднує результати різних моделей, тоді як метод порівняльного аналізу та KPI демонструють нижчу точність (±15% і ±10% відповідно) через неврахування всіх аспектів безпеки. Об'єктивність комбінованої методики також є найвищою (95%), що обумовлено поєднанням кількісних даних із різних джерел, тоді як метод експертних оцінок має найнижчу об'єктивність (50%) через значну суб'єктивність у процесі оцінювання. Гнучкість комбінованої методики оцінюється на рівні 9, оскільки її можна легко адаптувати до специфічних умов конкретного закладу, на відміну від методу аналізу статистичних даних, який отримує найнижчу оцінку за гнучкість (5) через свою залежність від наявних даних. Вартість методів значно варіюється: найбільш економічним є метод порівняльного аналізу (10,000 грн), тоді як комбінована методика є найдорожчою (150,000 грн) через свою складність та потребу в залученні експертів. Щодо часу виконання, метод порівняльного аналізу потребує лише один місяць, тоді як метод експертних оцінок займає до шести місяців. Комбінована методика займає середній час (4 місяці) через свою складність і необхідність обробки великої кількості даних. Простота використання також різниться: методи порівняльного аналізу та KPI є найпростіші у застосуванні (8 і 7 відповідно), тоді як методи експертних оцінок і аналізу статистичних даних потребують більше спеціалізованих знань (5 і 6 відповідно). Комбінована методика має середній рівень складності у використанні (6), що пов'язано з необхідністю інтеграції різних моделей та аналізу великого обсягу інформації.

Комбінована методика, хоча й потребує більше ресурсів і часу, забезпечує найвищі результати за комплексністю, точністю, об'єктивністю та гнучкістю. Це робить її найкращим вибором для закладів вищої освіти, які можуть дозволити собі її впровадження. Інші методи можуть бути використані як альтернатива у випадках обмежених ресурсів або часу.

ВИСНОВКИ

У статті представлено комплексну методику оцінки ефективності забезпечення інформаційної безпеки, яка охоплює технічні, організаційні, процедурні та людські

аспекти захисту інформаційних систем. Розроблені математичні моделі дозволяють здійснювати кількісну оцінку рівня безпеки, враховуючи різноманітні фактори, такі як рівень технічного захисту, політика безпеки та навчання персоналу. Запропонована методика має практичну значимість, оскільки її використання дозволяє своєчасно виявляти вразливості, оптимізувати витрати на забезпечення безпеки та підвищувати загальний рівень захищеності організації. Результати дослідження підтверджують ефективність методики та її універсальність у різних сферах діяльності, що робить її важливим інструментом для підтримки стабільного та безпечного функціонування організацій в умовах сучасних викликів.

Запропонована методика оцінки ефективності інформаційної безпеки має широке застосування в різних сферах, де критично важливим є захист конфіденційної інформації та забезпечення стійкості до кіберзагроз. В першу чергу, це бізнес-середовище, де компанії потребують надійного захисту комерційних даних, інтелектуальної власності, фінансової інформації та даних клієнтів. Також методика є актуальною для державного сектору, де вона може бути використана для захисту державних та персональних даних, а також для забезпечення безпеки інформаційних систем, що впливають на національну безпеку.

Окрім того, методика може бути застосована в освіті, охороні здоров'я, фінансовому секторі та промисловості. В навчальних закладах вона сприятиме захисту студентських записів, навчальних матеріалів та дослідницьких даних. У медичних установах методика допоможе забезпечити конфіденційність медичних записів та клінічних досліджень. У фінансовому секторі вона забезпечить захист від шахрайства та несанкціонованого доступу до фінансових даних, а в промисловості та енергетиці — запобігатиме кібератакам на критично важливі системи управління та мережі. Ця універсальна методика може бути адаптована до різних галузей, підвищуючи загальний рівень захищеності та стійкості до інформаційних загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Bekeshko, V. V., Voitsechovsky, M. I., & Khalilov, A. S. (2019). Methods and means of information security. Kyiv: NTUU "KPI".
2. ISO/IEC 27001:2013. (2013). Information technology – Security techniques – Information security management systems – Requirements. International Organization for Standardization.
3. Horodetskyi, B.V., & Gerasimenko, V.V. (2020). Information security: modern threats and protection. Kharkiv: Khnure.
4. Whitman, M.E., & Mattord, H.J. (2018). Principles of Information Security. Boston: Cengage Learning.
5. Germanchuk, V. V., & Petrov, V. O. (2017). Information security of organizations: concepts, methods and tools. Odesa: ONPU.
6. Schwab, K. (2017). The Fourth Industrial Revolution. New York: Crown Business.
7. Lipatov, S. V. (2018). Analysis and management of information security risks. Kyiv: KNEU.
8. National Institute of Standards and Technology (NIST). (2012). Guide for Conducting Risk Assessments. Special Publication 800-30, Revision 1.
9. Parker, D. B. (2016). Philosophy of information security. Moscow: DMK Press.
10. McCumber, J. (2004). Assessing and Managing Security Risk in IT Systems: A Structured Methodology. Boca Raton: Auerbach Publications.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (21), 2023
ISSN 2663 - 4023

Ananchenko Oleksiy
senior teacher of the Department of Digital Development Technologies
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID 0009-0005-3446-5994
ananchenko.oe@gmail.com

METHOD OF ASSESSING THE EFFICIENCY OF ENSURING INFORMATION SECURITY OF THE EDUCATIONAL INFORMATION SYSTEM

Abstract. In the modern conditions of the development of information technologies, the issue of ensuring information security is becoming more and more relevant. Information has become a key resource that affects the success and stability of the functioning of organizations, enterprises and institutions. Despite the fact that a significant part of efforts is aimed at creating and maintaining effective information protection systems, the issue of assessing their effectiveness remains relevant and important. The article examines a complex methodology for assessing the effectiveness of information security, which is based on the use of modern approaches and tools for analyzing the security of information systems. The proposed methodology covers various aspects of information security, including technical, organizational, procedural and human factors. The evaluation of efficiency is based on a complex analysis of multiple indicators, which allows to obtain an objective picture of the state of information security of the organization. The main part of the methodology is the development and application of mathematical models that allow quantitative assessment of the level of information security. Such models take into account various factors, including the level of technical protection of information systems, information security policy, the level of training of personnel, response to incidents and other important aspects. In addition, the article considers the issue of optimizing costs for ensuring information security by applying economic models and approaches. The proposed methodology includes several stages: determination of key security indicators, data collection and analysis, development of mathematical models for performance evaluation, interpretation of results and development of recommendations for increasing the level of protection. An important component of the methodology is a systematic approach that allows taking into account the interaction of various elements of the information security system and their impact on the overall level of protection. The practical application of the developed methodology makes it possible to timely identify vulnerabilities in the information security system, optimize the costs of its provision, increase the overall level of security of the organization and reduce the risks associated with information threats. The results of the study confirm the effectiveness of the proposed approach and demonstrate its applicability in various fields of activity, including business, public sector, education and other areas. Thus, the proposed methodology for assessing the effectiveness of information security is an important tool for organizations seeking to ensure reliable protection of their information. Its use contributes to increasing the level of information security, which, in turn, has a positive effect on the general level of functioning and stability of organizations in the face of modern challenges and threats.

Keywords: information security, performance evaluation, security of information systems, security criteria, mathematical models, cost optimization, system approach.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Bekeshko, V. V., Voitsechovsky, M. I., & Khalilov, A. S. (2019). Methods and means of information security. Kyiv: NTUU "KPI".
2. ISO/IEC 27001:2013. (2013). Information technology – Security techniques – Information security management systems – Requirements. International Organization for Standardization.
3. Horodetskyi, B.V., & Gerasimenko, V.V. (2020). Information security: modern threats and protection. Kharkiv: Khnure.
4. Whitman, M.E., & Mattord, H.J. (2018). Principles of Information Security. Boston: Cengage Learning.

5. Germanchuk, V. V., & Petrov, V. O. (2017). Information security of organizations: concepts, methods and tools. Odesa: ONPU.
6. Schwab, K. (2017). The Fourth Industrial Revolution. New York: Crown Business.
7. Lipatov, S. V. (2018). Analysis and management of information security risks. Kyiv: KNEU.
8. National Institute of Standards and Technology (NIST). (2012). Guide for Conducting Risk Assessments. Special Publication 800-30, Revision 1.
9. Parker, D. B. (2016). Philosophy of information security. Moscow: DMK Press.
10. McCumber, J. (2004). Assessing and Managing Security Risk in IT Systems: A Structured Methodology. Boca Raton: Auerbach Publications.