IMPLEMENTATION OF NEW TOOLS AND METHODS FOR INCREASING THE LEVEL OF CYBER SECURITY OF CRITICAL INFRASTRUCTURE OBJECTS

Existing methods and means of ensuring cyber security of critical information infrastructure objects, developed on the basis of international standards and best practices, are quite effective in peacetime conditions, but do not take into account the hybrid nature of war, in which new threats appear, in particular, such as physical destruction , capture by the enemy, the lack of possibility of constant monitoring and control, limitations in defense resources and available personnel, problems in the supply of recovery equipment, interruptions in information exchange processes, the need for frequent changes in operating conditions, dynamic growth in the number and quality of cyber-attacks, etc., due to which their efficiency drops significantly. In view of this, there is a need to develop new and improve existing methods and means of cyber protection in order to increase the level of cyber security of critical infrastructure. The safety of the population and the performance of combat tasks by the troops depend on ensuring the cyber security of critical information infrastructure facilities as an integral part of critical infrastructure facilities.

Keywords: vulnerability management, SCAP, description of a pattern-based cyber-attack with a managed system behavior trajectory, risk assessment, visual analytics, anti-phishing infrastructure, knowledge and experience sharing system.

Давидюк Андрій Вікторович, аспірант кафедри Безпеки інформаційних технологій НАУ, молодший науковий співробітник ІПМЕ ім. Г.Є. Пухова НАН України, Technical researcher NATO CCDCOE.

Andrii Davydiuk, Phd student of the Department of information technology security of NAU, junior scientific researcher G.E. Pukhov IMEE NAS of Ukraine, Technical researcher NATO CCDCOE.
E-mail: andrey19941904@gmail.com.
Orcid ID: 0000-0003-1238-2598.

DOI: 10.18372/2410-7840.25.17938
УДК 004.056:061.68

РОЗРОБКА МЕТОДОЛОГІЇ ОЦІНКИ ВІДПОВІДНОСТІ СТАНДАРТУ ISO 27001

Євгеній Курій, Віталій Сусукайло, Іван Опірський

Даний науковий документ пропонує розробку методології оцінки відповідності організацій новій версії стандарту ISO 27001, яка була представлена в кінці 2022 року. Висока значущість інформаційної безпеки в сучасному світі вимагає від компаній адаптувати свої практики та політики до нових вимог стандарту. Автори аналізують останні дослідження у галузі впровадження стандарту ISO 27001 та недоліки релевантних матеріалів для оцінки відповідності. Методологія включає аналіз нових вимог стандарту, порівняння їх із зіставленням існуючих практик організацій, визначення «гепів» (розривів/невідповідностей) між ними, розробку плану впровадження змін та моніторингу відповідності. Запропоновані рекомендації допоможуть організаціям забезпечити ефективний перехід на новий стандарт, мінімізувати ризики і зберегти високий рівень інформаційної безпеки. Ця методологія є актуальним інструментом для організацій, що прагнуть адаптувати свої практики і політики до нової версії стандарту ISO 27001 та підтримувати безпеку своєї інформації на високому рівні. Дана розробка враховує унікальні потреби організацій та сприяє їхньому успішному впровадженню нових практик і вимог інформаційної безпеки. Ця стаття має на меті допомогти читачам зрозуміти складність та важливість проведення початкової оцінки на невідповідність перед впровадженням стандарту та висвітлити ефективність застосування детального чекліста під час проведення аналізу на невідповідності. Для підтримки дослідження був проведений детальний аналіз літератури та статей, що стосуються впровадження стандарту ISO 27001 в організаціях.

Ключові слова: *інформаційна безпека, кібербезпека, ISO 27001, фреймворк інформаційної безпеки, система управління інформаційною безпекою, оцінка на невідповідність, аналіз на невідповідність.*

ВСТУП

В сучасному цифровому світі збільшується значення інформації та даних, що обробляються, зберігаються та передаються організаціями. Відповідно, зростає і загроза порушення цілісності, конфіденційності та доступності цих даних. Саме тому організації мають звертати особливу увагу на забезпечення високого рівня інформаційної безпеки. Один із способів досягнення цієї мети - впровадження стандарту ISO 27001.

Стандарт ISO 27001, повна назва якого "ISO/IEC 27001:2022", є міжнародним стандартом, розробленим Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC). Цей стандарт визначає вимоги до систем управління інформаційною безпекою (СУІБ) для організацій будь-якого типу та розміру.

Стандарт ISO 27001 надає рамки для розроблення, впровадження, функціонування, моніторингу, оцінки та вдосконалення системи управління інформаційною безпекою в організації. Головна мета стандарту – забезпечити ефективний підхід до захисту конфіденційності, цілісності та доступності інформації, а також управління ризиками, пов'язаними з інформаційною безпекою.

Стандарт ISO 27001 включає в себе ряд важливих елементів, зокрема:

- встановлення політики інформаційної безпеки;
- визначення вимог щодо забезпечення інформаційної безпеки відповідно до бізнес-стратегії та потреб організації;
- визначення заходів з управління ризиками та впровадження контрольних заходів;
- встановлення механізмів для виявлення та обробки інцидентів і відхилень;
- забезпечення постійного вдосконалення системи управління інформаційною безпекою.

Цей стандарт є важливим інструментом для організацій, які бажають забезпечити високий рівень захисту своєї інформації, дотримуватися законодавчих вимог щодо захисту даних, а також покращити свою репутацію в очах клієнтів та партнерів.

Найвідоміший у світі стандарт управління інформаційною безпекою допомагає організаціям захистити свої інформаційні активи, що є життєво важливим у сучасному цифровому світі.

Оскільки компанії тривалий час користувалися попередньою версією стандарту ISO 27001, що датується 2013 роком, і нова версія була представлена лише наприкінці 2022 року, виникає недостача актуальних та релевантних матеріалів, які б могли б допомогти організаціям в ефективній оцінці відповідності їхніх існуючих практик новим вимогам стандарту, особливо українською мовою.

У світлі цієї проблеми, автори статті взяли на себе завдання розробити власну методологію оцінки організацій на відповідність новій версії стандарту ISO 27001. Дана методологія має на меті надати компаніям і фахівцям з інформаційної безпеки інструмент для систематичного аналізу їхніх існуючих практик та політик на предмет відповідності новим вимогам та принципам стандарту.

Стандарт ISO 27001 є визнаним міжнародним стандартом, що визначає вимоги до систем управління інформаційною безпекою (СУІБ) для організацій будь-якого типу та розміру. Цей стандарт надає рамки для розроблення, впровадження, функціонування, моніторингу, оцінки та вдосконалення СУІБ

Міжнародні стандарти ISO / IEC 27001/02 [1, 2] допомагають організаціям різних секторів забезпечувати конфіденційність, цілісність та доступність інформації за рахунок застосування процесу управління ризиками та надає впевненості зацікавленим сторонам у тому, що ризики адекватно оцінюються та управляються.

На сьогодні даний стандарт є одним із найпопулярніших фреймворків інформаційної безпеки у світі. За відносно недавніми даними статистики [3], у 2020 році більше 44 000 організацій по всьому світу бути сертифіковані відповідно до вимог ISO/IEC 27001, і відомо, що протягом пандемії ця цифра тільки зросла. Із виходом нової редакції стандарту, всі ці компанії опинилися перед проблемою адаптації існуючої системи управління інформаційної безпеки до вимог нового стандарту.

Одним із важливих етапів впровадження ISO 27001 є аналіз на невідповідність, який дозволяє ідентифікувати відмінності між існуючими практиками організації та вимогами стандарту [4].

Аналіз останніх досліджень та публікацій в галузі впровадження стандарту ISO 27001 та методології аналізу на невідповідність (gap assessment) дозволяє краще розуміти актуальний стан і тенденції у цій сфері. Нижче наведено певні підсумки досліджень, які можуть бути корисними для розробки методології оцінки відповідності організацій новій версії стандарту ISO 27001:

- перехід до нової версії стандарту: дослідження демонструють, що багато компаній зіткнулися з викликом переходу з попередньої версії ста-

ндарту ISO 27001 на нову. Зміни у вимогах та підходах вимагають від організацій адаптувати свої існуючі системи управління інформаційною безпекою [5];

- розробка методологій переходу: відсутність релевантних матеріалів для оцінки відповідності може вести до розробки власних методологій переходу організацій на нову версію стандарту. Дослідження показують, що успішні підходи до оцінки відповідності включають ретельний аналіз нових вимог та їх порівняння з існуючими практиками [6, 7];
- впровадження ризик-орієнтованого підходу: останні дослідження наголошують на значущості впровадження ризик-орієнтованого підходу при оцінці відповідності до стандарту ISO 27001. Це дозволяє зосередитися на тих аспектах, які мають найбільший вплив на безпеку інформації [8];
- застосування технологій: деякі дослідження вказують на важливість застосування технологій для полегшення процесу аналізу на невідповідність та моніторингу відповідності. Автоматизовані інструменти допомагають збирати, аналізувати та звітувати про дані, пов'язані з інформаційною безпекою [9];
- оптимізація процесу аудиту: дослідження вказують на можливість оптимізації процесу аудит для оцінки відповідності. Впровадження структурованих аудиторських програм може зробити процес більш ефективним і зменшити зусилля, потрібні для оцінки відповідності. [10];
- управління змінами: дослідження підкреслюють важливість ефективного управління змінами при переході до нової версії стандарту. Організації повинні ретельно планувати та впроваджувати зміни відповідно до нових вимог [11].

Ці підсумки досліджень можуть бути використані для розробки більш конкретної та адаптованої методології оцінки відповідності новій версії стандарту ISO 27001, яка враховує унікальні потреби організацій та їхніх існуючих інформаційних практик.

Постановка завдання полягає в аналізі сучасних методів оцінки організацій на відповідність стандарту ISO 27001 та розробку власної методології оцінки відповідності організацій до нової версії стандарту ISO 27001, зокрема на проведення аналізу на невідповідність (gap assessment).

Основною метою є визначення переваг та недоліків наявних методів оцінки організацій на відповідність стандарту ISO 27001 та створенні систематичного та структурованого підходу для допомоги організаціям ефективно адаптувати свої практики і політики інформаційної безпеки до нових вимог стандарту та забезпечити високий рівень інформаційної безпеки, а також провести аналіз останніх досліджень та публікацій на цю тему. Отримані результати мають бути використані для розробки пропозицій щодо вдосконалення наявних методів оцінки організацій на відповідність стандарту ISO 27001, зокрема його оновленій версії 2022 року.

ОСНОВНА ЧАСТИНА

Оцінка на невідповідності

Оцінка на невідповідності є невід'ємною та ключовою передумовою перед початком впровадження стандарту ISO 27001, який стосується інформаційної безпеки. Цей етап визначає ступінь відповідності поточних практик, політик та процесів організації вимогам, які встановлює стандарт. Незважаючи на те, що це може здаватися витратним та складним процесом, він є незамінним у забезпеченні успішноті та ефективності впровадження.

Отже, оцінка на невідповідності є критичним етапом перед впровадженням нового стандарту ISO 27001, оскільки вона сприяє раціональному підходу до впровадження, мінімізації ризиків та забезпеченню ефективності та надійності інформаційної безпеки в організації.

Існує кілька ключових причин, чому оцінка на невідповідності є важливою передумовою:

1. Виявлення «гепів»: Оцінка на невідповідності допомагає виявити розриви або «гепи» між існуючими практиками організації та вимогами стандарту. Це дає змогу чітко побачити, де саме потрібні зміни та вдосконалення;
2. Визначення пріоритетів: Оцінка на невідповідності допомагає організації визначити, які аспекти її поточних практик вимагають найбільшої уваги та зусиль для відповідності стандарту;
3. Мінімізація ризиків: Сучасна ділова атмосфера пов'язана з великими загрозами інформа-

ційної безпеки. Оцінка на невідповідності допомагає ідентифікувати слабкі місця та ризики в існуючих системах, що може бути вирішальним для запобігання можливим інцидентам;

4. Ефективне планування: Результати оцінки невідповідності допомагають розробити докладний план впровадження змін, який сприяє раціональному та ефективному розгортанню нових практик та політик;

5. Збереження ресурсів: Оцінка на невідповідності дозволяє організації визначити, які аспекти вже відповідають вимогам, тим самим зменшуючи навантаження на ресурси при впровадженні;

6. Забезпечення поступовості: Процес оцінки невідповідності допомагає організації планувати інтеграцію вимог поетапно, забезпечуючи плавний перехід та мінімізуючи вплив на операційну діяльність;

7. Підвищення свідомості: В процесі оцінки на невідповідності робиться акцент на усвідомлення необхідності змін та виконання вимог стандарту серед працівників, що сприяє внутрішній підтримці;

Отже, оцінка на невідповідності є критичним етапом перед впровадженням стандарту ISO 27001, оскільки вона сприяє раціональному підходу до впровадження, мінімізації ризиків та забезпеченню ефективності та надійності інформаційної безпеки в організації.

Використання чекліста для оцінки на невідповідність

Використання чекліста для здійснення оцінки на невідповідність перед впровадженням стандарту ISO 27001 має велике значення через ряд переваг, які цей інструмент може принести.

Чекліст виступає як структурована та організована система, яка спрощує процес оцінки та допомагає ефективно ідентифікувати розриви між поточними практиками організації та новими вимогами стандарту.

Важливість використання чекліста для оцінки на невідповідності включає такі аспекти:

- структурований підхід: чекліст надає структурований підхід для оцінки. Він включає усі ключові вимоги стандарту, розбиті на конкретні елементи, що допомагають систематично пройти крізь процес оцінки;
- повнота та вичерпність: чекліст допомагає впевнитися, що жодна важлива деталь не була пропущена під час оцінки. Він охоплює всі аспекти, які повинні бути перевірені для відповідності;
- підвищення ефективності: Використання чекліста допомагає уникнути непотрібного дублювання та недорозумінь. Всі учасники процесу оцінки працюють з однаковою базою даних, що сприяє збільшенню ефективності та точності;
- порівняння та аналіз: чекліст дає можливість здійснювати порівняння між існуючими практиками та новими вимогами. Це допомагає точно визначити, де саме відбувається невідповідність;
- ясність та документованість: Використання чекліста забезпечує ясність у процесі оцінки та документує результати. Це допомагає забезпечити прозорість та зручність для майбутнього моніторингу;
- послідовність: чекліст встановлює послідовність дій, що сприяє організації процесу оцінки та уникненню пропусків;
- внутрішній та зовнішній аудит: чекліст може бути використаний як база для внутрішнього аудиту для попередньої оцінки відповідності перед офіційним аудитом стандарту;
- відстеження прогресу: чекліст дозволяє відстежувати ступінь виконання та впровадження змін в організації протягом часу;
- референсний матеріал: чекліст може служити як посібник для персоналу та аудиторів, які відповідають за оцінку відповідності.

Отже, використання чекліста для оцінки на невідповідності є необхідним елементом перед початком впровадження стандарту ISO 27001.

Він сприяє систематизації та ефективності процесу оцінки, забезпечуючи комплексний та вичерпний підхід до вимог стандарту.

Окрім цього він надає і ряд інших переваг (рис. 1).

Процес проведення оцінки на відповідності за допомогою чекліста є структурованим та організованим підходом для перевірки рівня відповідності організації до конкретних вимог стандарту, такого як ISO 27001.

Цей процес включає кілька кроків, що допомагають ідентифікувати розриви (гапи) між поточними практиками організації та вимогами стандарту.

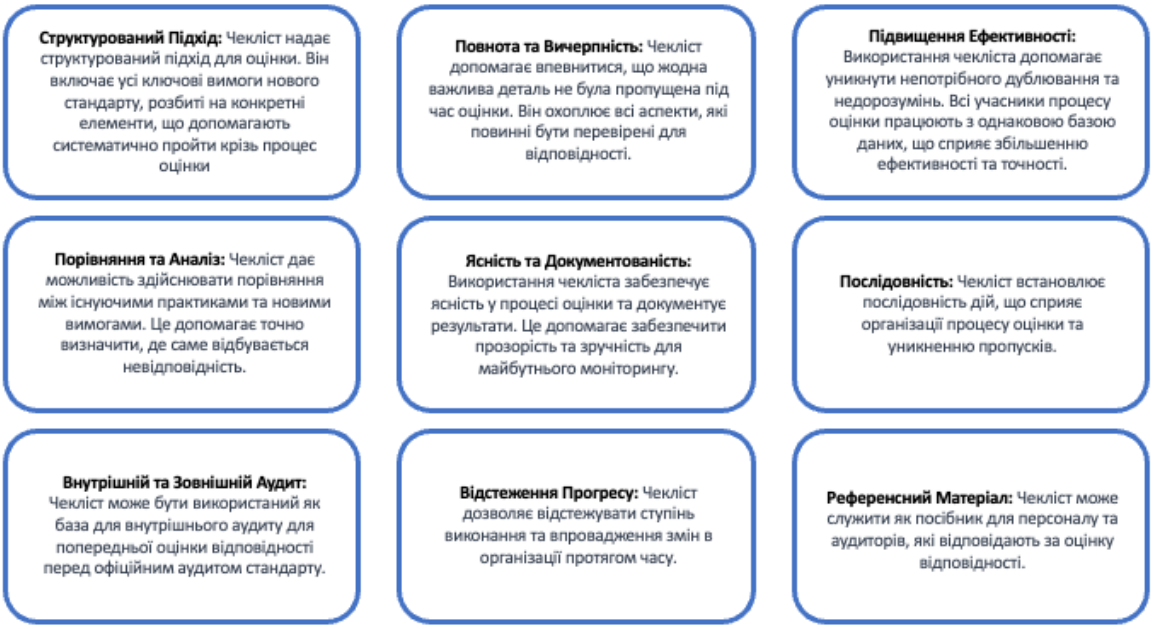

Рис. 1. Переваги використання чекліста для проведення оцінки на відповідність стандарту ISO 27001

Оцінка на відповідності за допомогою чекліста може бути виконана як внутрішньою, так і зовнішньою командою та є провідною частиною процесу впровадження стандарту.

Під час проведення процесу оцінки на невідповідності за допомогою чекліста потрібно дотримуватися певної послідовності дій, що виражена алгоритмом (рис. 2)

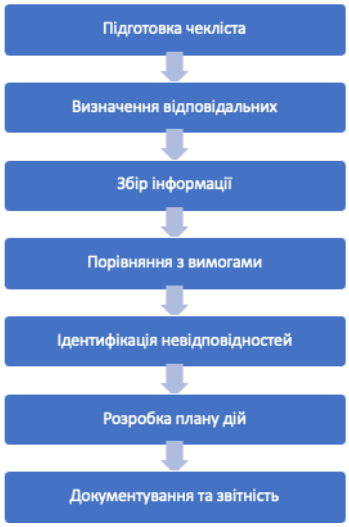

Рис. 2. Основні кроки процесу проведення оцінки на відповідності за допомогою чекліста

Відповідно до наведеного рисунку, процес проведення оцінки на відповідності за допомогою чекліста поділяється на наступні етапи:

- підготовка чекліста: Розробка чекліста, в якому перераховані всі ключові вимоги нового стандарту, які потрібно перевірити. Включення в чекліст деталізованих пунктів та підпунктів, які відповідають кожній вимозі;
- визначення відповідальних осіб: Призначення відповідальних осіб, які будуть виконувати перевірку відповідності за кожним пунктом чекліста. Це можуть бути співробітники з відповідних відділів, які мають розуміння вимог стандарту;
- збір інформації: Збір необхідної інформації про поточні практики, політики та процеси організації. Це може включати документацію, звіти, процедури та інші ресурси, що стосуються інформаційної безпеки;
- порівняння з вимогами: Для кожного пункту чекліста проводиться порівняння поточних практик з вимогами стандарту. Відзначається, чи відповідають організаційні практики кожній вимозі, або ж виникли «гепи» або «невідповідності»;
- ідентифікація невідповідностей: Для виявлених невідповідностей визначається, які конк-

ретно аспекти потрібно вдосконалити або змінити, щоб вони відповідали вимогам стандарту;

• розробка плану дій: Для кожної виявленої невідповідності розробляється план дій, який включає необхідні кроки, відповідальних осіб та терміни впровадження змін;

• документування та звітність: Створення звіту, який можна використовувати для моніторингу та подальшого аудиту.

Процес проведення оцінки на відповідності за допомогою чекліста допомагає організаціям систематично та ефективно оцінити свою відповідність до вимог стандарту, виділити області для вдосконалення та забезпечити високий рівень інформаційної безпеки. Нижче наведено приклад чекліста, який може використовуватися для оцінки організацій на відповідність міжнародному стандарту ISO 27001 (рис. 3).

	A	B	C	D	E	F	G	H	I
1		Область оцінки відповідності							
2	Пункт	Секція	Пункти для оцінювання	Завдяння до виконання	Артефакти/Документована інформація	Результати оцінювання	Статус відповідності	Статус	Коректуючі дії
3	5	Організаційні контролі							
4	5.1	Політики інформаційної безпеки	1. Чи розроблена Політика Інформаційної Безпеки та інші доменні політики? 2. Чи затверджені всі політики керівництвом? 3. Чи належним чином політики доносяться до зацікавлених сторін і чи отримується підтвердження ознайомлення з цими політиками? 4. Чи підлягають політики з безпеки регулярному перегляду? 5. Чи проводяться перегляди політик, коли змінюються обставини?	1. Розробити і впровадити полі+D4:D5тику інформаційної безпеки. 2. Переконатися, що політика включає такі вимоги: а) бізнес-стратегію та вимоги; б) нормативні акти, законодавство та контракти; в) поточні та передбачувані ризики та загрози інформаційної безпеки. 3. Переконатися, що політика містить твердження щодо: а) визначення інформаційної безпеки; б) цілей інформаційної безпеки або фреймворку для встановлення цілей інформаційної безпеки; в) принципів для керівництва всіма діяльностями, пов'язаними з інформаційною безпекою; г) зобов'язання виконувати вимоги, пов'язані з інформаційною безпекою; д) зобов'язання до постійного вдосконалення системи управління інформаційною безпекою; е) призначення відповідальності за управління інформаційною безпекою для визначених ролей; и) процедури для обробки винятків. 4. Затвердити політику інформаційної безпеки керівництвом. 5. Сповістити про політику персонал та зацікавлені сторони. 6. Запланувати періодичні перегляди політики.	1. Політ ика Інформаційної Безпеки. 2. Реєстр політик		Невідповідність	0%	
5	5.2	Ролі і відповідальності з інформаційної безпеки	Чи чітко визначені та розподілені ролі та відповідальності з інформаційної безпеки відповідно до потреб організації?	1. Визначити ролі та відповідальності з інформаційної безпеки для: а) захисту інформації та інших пов'язаних активів; б) проведення конкретних процесів із забезпечення інформаційної безпеки; в) діяльності з управління ризиками інформаційної безпеки та, зокрема, прийняття залишкових ризиків (наприклад, власникам ризиків); г) всього персоналу, який використовує інформацію організації та інші пов'язані активи. 2. Переконатися, що розподіл ролей та відповідальностей із інформаційної безпеки відбувається відповідно до політики інформаційної безпеки та доменних політик. 3. Визначити та задокументувати кожну область безпеки, за яку індивіди несуть відповідальність. 4. Сповістити кожну область безпеки відповідному персоналу. 5. Визначити та задокументувати рівні авторизації. 6. Призначити менеджера (або команду) із інформаційної безпеки та визначити їхні відповідальності.	1. Ролі та відповідальності із інформаційної безпеки задокументовані в політиках. 2. Опціонально: Матриця RBAC (ролей і прав доступу)		Невідповідність	0%	

Рис. 3. Чекліст для проведення оцінки на невідповідність згідно вимог стандарту ISO 27001

Даний чекліст містить наступні секції:

• пункт – числове позначення, яке відповідає конкретному розділу або розділу стандарту. Використовується для швидкої навігації під час оцінювання відповідності;

• секція – назва розділу або підрозділу стандарту, який визначає конкретну тему або область вимог;

• пункти для оцінювання – перелік конкретних вимог стандарту, які підлягають перевірці під час оцінювання відповідності. Вони слугують основою для проведення оцінювання;

• завдання для виконання – перелік конкретних дій або завдань, які потрібно виконати для того, щоб забезпечити відповідність вимогам стандарту. Вони можуть включати розробку, реалізацію та впровадження практик або процедур;

• артефакти/документована інформація: – додаткові документи, файли, записи або матеріали, які можуть служити доказами виконання вимог стандарту. Вони підтримують доказову базу в процесі оцінювання;

• результати оцінювання – ця секція заповнюється аудитором або оцінювачем під час проведення оцінювання відповідності. Вона містить оцінку того, наскільки наявні контролі і практики відповідають вимогам стандарту;

• статус відповідності – цей статус визначає, наскільки наявні контролі і практики відповідають вимогам стандарту. Він може бути "Відповідає", "Не відповідає" або "Частково відповідає", вказуючи на рівень відповідності;

• статус – цей показник визначає відсоток виконаних вимог стандарту відносно загальної кількості вимог;

• коректуючі дії – перелік дій і активностей, які необхідно реалізувати для досягнення повної відповідності до вимог стандарту. Ці дії спрямовані на усунення виявлених відмінностей та вдосконалення системи.

Цей процес оцінювання відповідності вимогам стандарту допомагає забезпечити високу якість та відповідність системи до прийнятих стандартів, забезпечуючи ефективну роботу та довіру до результатів.

Таким чином, перед початком впровадження стандарту ISO 27001, важливо провести оцінку на невідповідності, що допоможе визначити сфери, які потребують покращення і доопрацювання, а також допоможе ефективно пріоритезувати завдання і виділити необхідні ресурси. Разом з тим, використання контрольного списку або чекліста допоможе зробити цей процес оцінки цілісним і систематичним і забезпечить повноцінне покриття усіх важливих вимог і контролів стандарту, що у свою чергу допоможе переконатися, що організація відповідає стандарту та що ви вживаєте усіх необхідних заходів для захисту своїх інформаційних активів.

ВИСНОВКИ

У даній статті була розглянута важливість та методологія проведення оцінки на відповідність в рамках впровадження стандарту ISO 27001. Перехід до нової версії стандарту вимагає від організацій ретельної підготовки та адаптації своїх інформаційно-безпекових практик до нових вимог. Процес оцінки на відповідність стає ключовим етапом в цій підготовці.

З врахуванням сучасної динамічної обстановки в галузі інформаційної безпеки, важливою стає не лише сама відповідність стандарту, а й здатність організації адаптуватися до змін та навколишнього середовища. Оцінка на відповідність допомагає ідентифікувати ризики, невідповідності та «гепи» між поточними інформаційно-безпековими практиками та новими вимогами стандарту. Цей процес дозволяє розробити стратегічний план впровадження змін та вдосконалення, спрямований на забезпечення найвищого рівня інформаційної безпеки.

Використання чекліста як інструменту для проведення оцінки на відповідність надає систематичності та структурованості процесу. Він сприяє ефективній ідентифікації невідповідностей, забезпечує повноту та точність перевірки, а також дозволяє легко відслідковувати прогрес у впровадженні змін.

Оцінка на відповідність є важливою передумовою для успішного впровадження нових інформаційно-безпекових практик, вирішення недоліків та забезпечення найвищого рівня захищеності інформації. Цей процес допомагає організаціям досягти відповідності до стандарту ISO 27001, підвищити рівень свідомості персоналу щодо інформаційної безпеки та забезпечити стійкий та надійний захист від сучасних загроз. Разом з тим, використання контрольного списку або чекліста допомагає зробити цей процес оцінки цілісним і систематичним і забезпечити повноцінне покриття усіх важливих вимог і контролів стандарту.

ЛІТЕРАТУРА

[1] ISO/IEC 27001: Information Technology Security Techniques, Information Security Management Systems Requirements. 2013. URL: https: //www.iso.org/standard/54534.html.

[2] ISO/IEC 27002: Information Technology Security Techniques, Code of Practice for Information Security Controls. 2013. URL: https://www.iso.org/standard/54533.html.

[3] ISO Survey of Management System Standards reveals 17% increase in certifications. 2020. URL: https:// www.quality . org /article / 2020-iso-survey-management-system-standards-reveals-17-increase-certifications.

[4] ISO 27001 Gap Analysis. URL: https://www.itgovernance.co.uk/iso27001-gap-analysis.

[5] Y. Kurii, I. Opirskyy, L. Bortnik ISO/IEC 27001: 2022, analysis of changes and compliance features of the new version of the standard // Materials of IXth International Scientific and Technical Conference information protection and information systems security, May 25-26, 2023. Lviv, Ukraine, pp 15-17, ISBN 978-966-941-829-6.

[6] MSECB Transition Policy on Management System Certification to ISO/IEC 27001:2022. URL: https: //msecb.com/wp-content/uploads/2023 / 01 / MS-ECB-Transition-Policy-on-MS-Certification-to-ISO-IEC-27001.pdf?utm_source=sendinblue&utm_ campaign=Clients%20ISOIEC%20270012022%20 Transition%20Policy&utm_medium=email.
[7] ISO 27001 2013 vs. 2022 revision. What has changed? URL: https: // advisera. com/ 27001academy/blog/ 2022/02/09/iso-27001-iso-27002/.
[8] Pacaiova, H., Nagyova, A. Risk based thinking. New approach for modern enterprises' management, Advances in Intelligent Systems and ComputingVolume 783. 2019. pp. 524-5362019 AHFE International Conference on Human Factors, Business Management and Society, 2018 Orlando21, July 2018, through 25 July 2018, Code 215359.
[9] Susukailo V., Opirsky I., Yaremko O. Methodology of ISMS Establishment Against Modern Cybersecurity Threats. In: Klymash M., Beshley M., Luntovskyy A. (eds) Future Intent-Based Networking. Lecture Notes in Electrical Engineering, vol 831. 2022. Springer, Cham. https: // doi.org / 10.1007/ 978-3-030-92435-5_15.
[10] What is an ISO 27001 internal audit? URL: https: / /www.vanta.com/glossary/iso-27001-internal-audit.
[11] How to manage changes in an ISMS. URL: https: //advisera.com/27001academy/blog/2015/09 /14/ how-to-manage-changes-in-an-isms-according-to-iso-27001-a-12-1-2/.

DEVELOPMENT OF A METHODOLOGY FOR ASSESSING COMPLIANCE WITH ISO 27001 STANDARD

This document proposes the methodology for assessing organizations' compliance with the new version of the ISO 27001 standard, which was introduced at the end of 2022. The high significance of information security in the modern world requires companies to adapt their practices and policies to the new requirements of the standard. The authors analyze recent research in the field of ISO 27001 implementation and the shortcomings of relevant materials for compliance assessment. The methodology includes the analysis of the new standard requirements, comparing them with the current practices of organizations, identifying gaps between them, developing a plan for implementing changes, and monitoring compliance. The provided recommendations will help organizations ensure an effective transition to the new standard, minimize risks, and maintain a high level of information security. This methodology is a relevant tool for organizations seeking to adapt their practices and policies to the new version of the ISO 27001 standard and maintain the security of their information at a high level. This development takes into account the unique needs of organizations and contributes to their successful implementation of new information security practices and requirements. The purpose of this article is to help readers understand the complexity and importance of conducting an initial gap assessment prior to implementing a standard and to highlight the effectiveness of using a detailed checklist when performing a gap analysis. To support the study, a detailed analysis of literature and articles related to the implementation of the ISO 27001 standard in organizations was conducted.

Keywords: information security, cybersecurity, ISO 27-001, information security framework, information security management system, gap assessment, gap analysis.

Курій Євгеній Олегович, асистент кафедри захисту інформації Національного університету «Львівська політехніка».

Yevhenii Kurii, assistant at the Department of Information Security, "Lviv Polytechnic" National University.
E-mail: yevhenii.o.kurii@lpnu.ua.
Orcid ID: 0000-0002-3423-5655.

Сусукайло Віталій Андрійович, асистент кафедри захисту інформації Національного університету «Львівська політехніка».

Vitalii Susukailo, assistant at the Department of Information Security, "Lviv Polytechnic" National University.
E-mail: vitalii.susukailo@gmail.com.
Orcid ID: 0000-0003-4431-9964.

Опірський Іван Романович, д.т.н., професор, завідувач кафедри захисту інформації Національного університету «Львівська політехніка».

Ivan Opirskyy, Doctor of Technical Sciences, Professor, Head of the Department of Information Security, "Lviv Polytechnic" National University.
E-mail: ivan.r.opirskyi@lpnu.ua.
Orcid ID: 0000-0002-8461-8996.

DOI: 10.18372/2410-7840.25.17939
УДК 316.772.4:004

СИНТЕЗ МОДЕЛІ СОЦІАЛЬНИХ САНКЦІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ВІРТУАЛЬНИХ СПІЛЬНОТ У СОЦІАЛЬНИХ МЕРЕЖАХ В УМОВАХ АНТАГОНІСТИЧНОГО СЕРЕДОВИЩА

Сергій Євсеєв, Юрій Тимонін, Сергій Веретюк, Тетяна Войтко, Дмитро Оленюк