№ 9(50) 2025
НАУКА і ТЕХНІКА СЬОГОДНІ
серії: право, економіка, педагогіка, техніка, фізико-математичні науки

УДК 378.048.2 + 378.21 + 001.18

https://doi.org/10.52058/2786-6025-2025-9(50)-1281-1296

Ліщина Валерій Олександрович кандидат технічних наук, доцент, завідувач кафедри комп'ютерних наук, факультет комп'ютерних та інформаційних технологій, Луцький національний технічний університет, Луцьк, https://orcid.org/0000-0002-2371-3850

Козубцова Леся Михайлівна кандидат технічних наук, доцент, завідувач кафедри математики та фізики, Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, м. Київ, https://orcid.org/0000-0002-7866-8575.

Козубцов Ігор Миколайович доктор педагогічних наук, кандидат технічних наук, старший науковий співробітник, професор кафедри комп'ютерних наук, факультет комп'ютерних та інформаційних технологій, Луцький національний технічний університет, Луцьк, https://orcid.org/0000-0002-7309-4365

Глобін Андрій Вікторович науковий співробітник науково-дослідного відділу (технічного забезпечення засобів зв'язку та автоматизації) Наукового центру зв'язку та інформатизації, Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, https://orcid.org/0000-0001-5335-6869

МОДЕЛЬ ФОРМАЛІЗОВАНОГО АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ НА ПРЕДМЕТ ВИКОНАННЯМ ВИМОГ СТАНДАРТІВ

Анотація. В науковій статті авторами привернуто увагу на аудит інформаційної безпеки організації як системної дії, спрямований на контроль та перевірку стану та оцінку адекватності засобів і методів захисту інформації, що обрані адміністратором, відповідно до відомих загроз. Ефективність захисту підприємства є своєчасна налаштована робота системи захисту та періодична робота відповідальних осіб задіяних до аудиту інформаційної безпеки. Робота аудитора дуже скрупульозна і за часту дуже рутинна, яку логічно потрібно спростити. У зв'язку з цим виникає необхідність науково-обґрунтованого визначення та формалізації сукупності критеріїв, що відображають рівень захищеності об'єкта та виявлення показників, за якими можливо провести об'єктивні процедури перевірки. Аналіз останніх досліджень і публікацій

дозволив виявити, що неможливо дати універсальні формалізовані показники та критерії проведення аудиту, застосовні у всіх завданнях та видах аудиту. Отже, метою наукової статті є апробація процесу формування формалізованої аудиторської методики та практико-орієнтованої інструкції при проведенні аудиту інформаційної безпеки на предмет відповідності стандартам та нормативним вимогам інформаційної безпеки. В результаті дослідження встановлено, що переважна більшість базових стандартів у сфері забезпечення інформаційної безпеки об'єктів захисту на підприємствах має явно виражений описовий характер та не містять конкретних вказівок до практичних дій. Основна труднощі у проведенні аудиту інформаційної безпеки щодо відповідності вимогам стандартів полягає у відсутності чіткої і послідовної методики аудиту. Враховуючи вище зазначене в роботі запропоновано авторське бачення щодо методики аудиту інформаційної безпеки організації. Розроблена авторська модель аудиторського контролю охоплює 10 ключових напрямів інформаційної безпеки. Наведено, як зразок, змісту чек-листа для аудиторської перевірки за напрямом «Політика інформаційної безпеки». Застосований адаптивний і гнучкий підходи у розробці чек-листа, що дозволяє розширення можливостей аудитором під конкретні завдання.

Ключові слова: модель, аудит, інформаційна безпека, стандарт, контроль, показники, методика, формалізація.

Lishchyna Valerii Oleksandrovych Candidate of Technical Sciences, Associate Professor, Head of the Department of Computer Science, Faculty of Computer and Information Technologies, Lutsk National Technical University, Lutsk, https://orcid.org/0000-0002-2371-3850

Kozubtsova Lesia Mykhailivna Candidate of Technical Sciences, Associate Professor, Head of the Department of Mathematics and physics, Heroiv Krut Military Institute of Telecommunications and Informatization, Kyiv, https://orcid.org/0000-0002-7866-8575

Kozubtsov Igor Mykolaiovych Doctor of Pedagogical Sciences, Candidate of Technical Sciences, Senior Researcher, Professor, Department of Computer Science, Faculty of Computer and Information Technologies, Lutsk National Technical University, Lutsk, https://orcid.org/0000-0002-7309-4365

Hlobin Andrii Viktorovych researcher of the Research Department (Technical support of communication and automation equipment) Scientific Center for Communication and Informatization, Heroiv Krut Military Institute of Telecommunications and Informatization, Kyiv, https://orcid.org/0000-0001-5335-6869

№ 9(50)
2025
НАУКА і ТЕХНІКА СЬОГОДНІ
серії: право, економіка, педагогіка, техніка, фізико-математичні науки

MODEL FOR FORMALIZED AUDIT OF AN ORGANIZATION'S INFORMATION SECURITY FOR COMPLIANCE WITH STANDARD REQUIREMENTS

Abstract. In this scientific article, the authors draw attention to the audit of an organization's information security as a systematic action aimed at controlling and verifying the status and assessing the adequacy of the means and methods of information protection chosen by the administrator in accordance with known threats. The effectiveness of an enterprise's protection depends on the timely configuration of the protection system and the periodic work of the persons responsible for the information security audit. The work of an auditor is very meticulous and often very routine, which logically needs to be simplified. In this regard, there is a need for a scientifically based definition and formalization of a set of criteria that reflect the level of protection of an object and the identification of indicators by which objective verification procedures can be carried out. An analysis of recent studies and publications has revealed that it is impossible to provide universal formalized indicators and criteria for conducting audits that are applicable to all tasks and types of audits. Therefore, the purpose of this scientific article is to test the process of developing a formalized audit methodology and practice-oriented instructions for conducting information security audits for compliance with information security standards and regulatory requirements.

The study found that the vast majority of basic standards in the field of information security for protected objects at enterprises are clearly descriptive in nature and do not contain specific instructions for practical actions. The main difficulty in conducting an information security audit for compliance with standards is the lack of a clear and consistent audit methodology. Considering the above, the paper proposes the author's vision of the methodology for auditing an organization's information security. The author's model of audit control covers 10 key areas of information security. An example of the contents of a checklist for an audit in the area of "Information Security Policy" is provided. An adaptive and flexible approach was used in developing the checklist, which allows the auditor to expand the possibilities for specific tasks.

Keywords: model, audit, information security, standard, control, indicators, methodology, formalization.

Постановка проблеми. Аудит інформаційної безпеки (ІБ), як системна дія, спрямований на контроль та перевірку стану ІБ об'єкта захисту (зокрема, організації), а також оцінку адекватності засобів і методів захисту інформації, що застосовуються, відповідно до існуючих загроз. Адже основа ефективного захисту підприємства є своєчасна налаштована робота системи захисту та

періодична робота відповідальних осіб задіяних до аудиту інформаційної безпеки [1]. Тому, загальне завдання аудиту ІБ полягає у перевірці відповідності системи захисту об'єкта сукупності критеріїв, що визначають вимоги до захищеності. Робота аудитора дуже скрупульозна і за часту рутинна, яку логічно потрібно спростити. У зв'язку з цим виникає необхідність науково-обґрунтованого визначення та формалізації сукупності критеріїв, що відображають рівень захищеності об'єкта та виявлення показників, за якими можливо провести об'єктивні процедури перевірки. Критерії мають бути чітко визначеними і, максимально можливо, вимірюваними [2]. Варто зазначити, що на початку становленні системи захисту інформації і кібербезпеки як такої, що раніше не була відомою виявилась задачею надскладною [3].

Аналіз останніх досліджень і публікацій. Аналіз останніх досліджень і публікацій за обраним напрямком досліджень представлено не лише в авторських публікаціях.

Як у вступі згадувалось на етапі зародження ІБ та кібербезпеки перед науковцями всього світу стояло не просте завдання – обґрунтування вибору критерії оцінювання, але які мають бути чітко визначеними і максимально можливо вимірюваними. В науковому суспільстві розпочалися дискусії щодо відпрацювання єдиного підходу до побудови методики оцінки кібернетичної захищеності організації [4]. Від складності рішення наукової задачі з науковою новизною в перше, варто додати чисельні бар’єри відсутності єдиного термінологічного апарату дослідження.

Автори публікації [5] проявили нестандартні підходи при розробці методика оцінки кібернетичної захищеності системи зв’язку організації. Нагальна потреба у якому спонукала до типової формалізації з розробки типової методики оцінки кібернетичної захищеності інформаційно-телекомунікаційної системи [6]. На практиці виявилось розчарування. Оскільки можлива існування загроз нульового дня призводить до того, що типові методики без обґрунтування вибору критерії оцінювання стають не зовсім працездатними без оцінювання ефективності виконання заходів, спрямованих на забезпечення кібернетичної безпеки [7].

Для цього потрібна методика оцінювання ефективності виконання заходів забезпечення кібербезпеки, наприклад для об’єктів критичної інформаційної інфраструктури організації [8].

Водночас під загально-методичним керівництвом О. Чернонога, велися роботи з розробки методики аудиту інформаційних систем за держзамовленням [9] та ініціативними випереджаючим напрямками [10]. В роботі [11] подано зміст аудиту і тестування вразливості інформаційно-телекомунікаційної системи (ІТС) будь-якого підприємства. Технологія аудиту зводиться до активних заходів тестування на проникнення ІТ-інфраструктури.

Варто зазначити, що об'єктами аудиту ІБ можуть бути будь-які об'єкти та процеси [12], наведемо наприклад деяких з них: автоматизована чи інформаційна система, або їх окремі компоненти; організаційно-управлінські процеси; технічні засоби; бізнес-процедури; діяльність підприємства у цілому.

За формою проведення аудит ІБ може бути організаційно-нормативним [13] (вразі того предметом аналізу є заходи та нормативні документи щодо забезпечення ІБ) та технічним (коли предметом аналізу є технічні засоби обробки інформації).

Сукупність методів аналізу ризиків ІБ базується на двох моделях:

– перша модель визначає ризик на основі зіставлення відповідності об'єкта захисту набору вимог щодо ІБ, що виходять із стандартів, нормативно-правових актів та умов експлуатації систем;

– друга модель визначає ризик на основі оцінки ймовірностей реалізації загроз та атак, а також величин потенційно можливої матеріальної шкоди.

Концептуально моделі аудиту ІБ можна об’єднати в три практичні та три теоретичні підходи до проведення аудиту.

Практичними підходами є: аудит на основі аналізу ризиків; аудит на основі аналізу стандартів ІБ; аудит з урахуванням експериментальних досліджень об'єкта.

Теоретичними підходами є: аудит на основі моделювання процесів; аудит на основі моделі оцінки; аудит з урахуванням моделі зрілості.

Одним із найбільш поширених методів аудиту є підхід на основі аналізу стандартів ІБ, хоча б тому, що стандарти формують сукупність вимог та рекомендацій щодо забезпечення ІБ на основі накопиченого професійного досвіду, а також є документами, що регламентують, що застосовуються у професійній спільноті.

Аудит ІБ може проводитися щодо відповідності налаштування вимогам міжнародних стандартах ISO/IEC TS 33030:2017 [14], ISO/IEC 21827:2008, ISO/IEC 27001:2022 [15], необхідних організації відповідно до завданням на аудит. Варто зазначити, що стандарт ISO/IEC 27002:2022 [16] є базовим документам, визначальним основні напрями забезпечення інформаційної безпеки організацій, й у багатьох випадків може бути основою проведеної аудиторської перевірки.

Аспект, що недостатньо вивчений. Аналіз останніх досліджень і публікацій дозволив виявити, що неможливо дати універсальні формалізовані показники та критерії проведення аудиту, застосовні у всіх завданнях та видах аудиту.

Мета статті. Отже, метою статті є апробація процесу формування формалізованої аудиторської методики та практико-орієнтованої інструкції, при проведенні аудиту ІБ на предмет відповідності стандартам та нормативним

вимогам. В рамках запропонованої методики можлива розробка аналогічних інструкцій стосовно будь-якого стандарту.

Результат дослідження з обґрунтування формалізації проведення аудиту інформаційної безпеки.

Слід зазначити, що переважна більшість базових стандартів у сфері забезпечення ІБ об'єктів захисту та управління ІБ на підприємствах має явно виражений описовий характер із вказівками щодо сукупності керівних дій і не містять: критеріїв повноти керівних дій; дискретних, однозначно трактованих показників здійсненності та результативності дій; методів досягнення результатів; інструкцій щодо реалізації перевірок на відповідність.

Основні труднощі у проведенні аудиту ІБ щодо відповідності вимогам стандартів полягають у відсутності чіткої і послідовної методики аудиту, як наприклад в роботі [5]. У свою чергу при аудиті ІБ слід виключити суб'єктивності, виходячи з розуміння, що результати аудиту будуть достовірнішими, чим більшою мірою вони будуть формалізовані. Виключити суб'єктивності повністю, на жаль, неможливо.

Формалізація аудиторських процесів є актуальною і поки що мало вивченим напрямом досліджень. Робилися різні спроби формалізації, в основному стосовно окремих аспектів аудиту із застосуванням так званого «аудиторського підходу на основі еталонної моделі» [9].

Завдання формалізації аудиторського процесу має на меті повторюваність та незалежність процедур і результатів аудиту.

Однією з найкращих практик можна назвати створення так званих «чек-листів» (контрольних карт), що відображають послідовність проведення аудиторської процедури, процеси, що перевіряються, та їх дискретизовані показники.

Розглянемо аудиторські завдання та дії в рамках оцінки відповідності ІБ організації вимогам стандарту ISO/IEC 27002:2022. Цей стандарт визначає вимоги до безпеки з урахуванням таких факторів: оцінка ризиків ІБ; нормативні вимоги; специфічні принципи, характерні для середовища організації.

Стандарт виділяє три ключові категорії інформації, захист яких має забезпечуватися першочергово: персональні дані; облікові дані організації; інтелектуальна власність.

Сукупність заходів визначена так: наявність політик ІБ; розподіл обов'язків із забезпечення ІБ; навчання з питань ІБ; інформування про інциденти ІБ; управління безперервністю бізнесу.

Захист персональних даних та приватного життя має високу актуальність для цивілізованого суспільства [17].

Виходячи з суспільних потреб, для кожної з категорій інформації необхідні захисні заходи. Також і навпаки: захисні заходи мають бути спрямовані на захист

всіх категорій інформації. Складемо узагальнену матрицю захисту (табл. 1), у якій визначимо 15 функцій захисту F_{11} … F_{53} , кожну з яких можна оцінити за сукупністю відповідності вимогам.

Таблиця 1

Узагальнена матриця захисту

Заходи	**Категорії інформації**		
	Персональні дані	**Облікові дані організації**	**Інтелектуальна власність**
Політики ІБ	F11	F12	F13
Розподіл обов'язків	F21	F22	F23
Навчання персоналу	F31	F32	F33
Інформування про інциденти	F41	F42	F43
Управління безперервністю бізнесу	F51	F52	F53

Процеси управління ІБ у стандарті ISO/IEC 17799:2005 розділені на 10 напрямків [18]:

1) політика безпеки;
2) організація інформаційної безпеки;
3) управління активами;
4) безпека людських ресурсів;
5) фізична та екологічна безпека;
6) управління комунікаціями та операціями;
7) придбання, розробка та обслуговування інформаційних систем;
8) управління безперервністю бізнесу;
9) управління інцидентами інформаційної безпеки;
10) дотримання відповідності вимогам.

Цілі та засоби контролю, зазначені в ISO/IEC 17799:2005, призначені для впровадження з метою задоволення вимог, визначених шляхом оцінки ризиків. ISO/IEC 17799:2005 призначений як загальна основа та практичне керівництво для розробки стандартів безпеки організації та ефективних практик управління безпекою.

Безпосередні дії аудитора спрямовані на виявлення відповідності захищеності об'єкта за вказаними 10 напрямками. При цьому перевірки необхідно виконувати максимально об'єктивними та повторюваними методами. Розроблена авторська модель аудиторського контролю, у межах виділених напрямів, наведено на рис. 1.

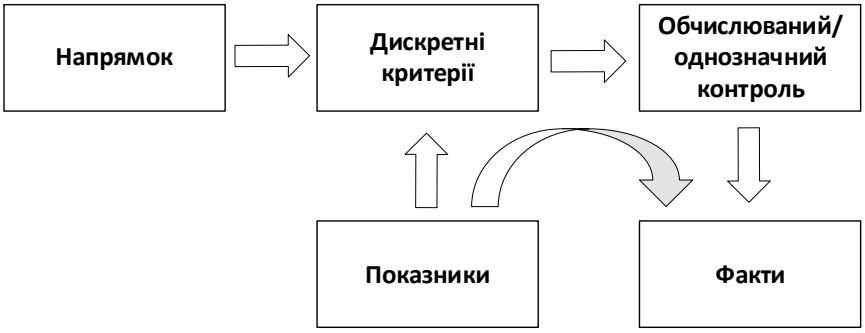

Рис. 1. Модель аудиторського контролю

Відповідно до запропонованої моделі, аудитор: визначає факти, що належать до процедур, що перевіряються, та методів захисту інформації; збирає докази (підтвердження) визначених фактів; використовує виключно об'єктивні дискретні критерії; фіксує результати перевірки як однозначно трактованих чи обчислюваних показників.

Принциповим є питання системи об'єктивних показників і критеріїв аудиторського контролю. З цією метою аудитори, зокрема, можуть керуватися стандартом ISO/IEC 27001:2022. Процедури аудиту щодо сукупності вимог системи стандартів ISO 2700x та в рамках циклу *PDCA* мають самостійну концепцію і в даному випадку не розглядаються.

У табл. 2 наведено, як приклад, перелік цілей та заходів управління, що обрані зі стандарту ISO/IEC 27001:2022 для спрямування «Політика інформаційної безпеки» [15].

Таблиця 2

Цілі та заходи управління політикою інформаційною безпекою

A.5.1.1	Документування політики інформаційної безпеки	Політика інформаційної безпеки має бути керівництвом затверджена, видана та доведена до відома всіх співробітників організації, а також сторонніх організацій
A.5.1.2	Перегляд політики інформаційної безпеки	Політика інформаційної безпеки організації має бути піддана аналізу та перегляду через задані проміжки часу або з появою суттєвих змін характеристик цілей безпеки

Наведена інформація, безумовно, є визначальною для аудиторської оцінки відповідності, оскільки вказує на необхідні факти, які аудитором повинні бути підтверджені або спростовані, але не містить критеріїв перевірки. Таким чином є потреба у створенні формалізованої схеми та/або алгоритму аудиторських дій, що базується на дискретних критеріях та однозначно визначених об'єктивних

обчислюваних показниках. Подібна модель може бути представлена у вигляді «чек-листів» однозначно поставлених питань, на які можуть бути лише гранично чіткі відповіді, що виключають суб'єктивність.

Для створення чек-листів відповідних відповідей скористаємося сформульованими у стандарті ISO/IEC 27001:2022 цілями та заходами і сукупністю вимог. Розглянемо запропоноване рішення на прикладі напряму «Політика інформаційної безпеки». Відповідно до зазначених стандартів, мета політики ІБ – забезпечити участь вищого керівництва організації у вирішенні питань, пов'язаних із забезпеченням ІБ відповідно до цілей діяльності організації (бізнесу), законів та нормативних актів.

У чинному законодавстві України немає прямих вимог щодо форми та змісту політик ІБ, у зв'язку з чим можна спостерігати досить різноманітні підходи організацій до формування політик ІБ. У той же час саме ISO/IEC 17799:2005 містить вказівки на мінімальні вимоги до змістовності політики ІБ, огляд яких опускаємо.

На основі сукупності перерахованих вимог ISO/IEC 17799:2005 та вказівок, аудитором складається перелік питань, які становитимуть чек-лист і на які він шукатиме відповіді у вигляді доказів та підтверджуючих фактів у процесі проведення аудиту.

Вимоги до критерію оцінювання. Критерії оцінювання мають бути: об'єктивні, дискретні, обчислювані, вимірювальні.

Вимоги до переліку питань, що входять до чек-листа: відповідь на питання має бути чіткою та однозначною, що перевіряється, але в жодному разі не міркування.

У табл. 3 наведено зразковий зміст чек-листа для аудиторської перевірки за напрямом «Політика інформаційної безпеки». Запропонований чек-лист може бути розширений аудитором під конкретні завдання. Пояснимо принципи складання чек-листа. Усі питання згруповані за трьома рівнями (кількість рівнів може бути й більшою).

Ідея рівнів у тому, що при негативній відповіді на питання більш високого (першого) рівня немає сенсу шукати відповіді на питання нижчого (в даному випадку – другого) рівня. Існують також альтернативні моделі рівневого представлення оцінок безпеки об'єктів у процесі проведення аудиту [19].

Як очевидно з табл. 3, всі підтвердження, що збираються, подаються або у вигляді дискретних значень (так/ні, присутній/відсутня, відповідає/не відповідає, і т.п.), або в обчислюваних (середній бал з тестування, відсоток ознайомлених або навчених співробітників, і т.п.). Не слід плутати перевірку (методом тестування) знань змісту конкретної політики ІБ організації як внутрішнього локального нормативного документа та знань співробітниками теорії та методології захисту інформації загалом.

Таблиця 3

Чек-лист роботи аудитора

№ п/п	Рівень	Питання визначення контрольного показника	Відповідь		Спосіб підтвердження факту
			Дискретний	Обчислю-ваний	
1	1	Чи є політика безпеки як документ?	Та ні	-	Наявність документа
2	2	Чи затверджено політику безпеки керівництвом (належним чином)	Та ні	-	Наявність реквізитів, підписів, печатки
	2	Чи розміщена політика безпеки у вільному доступі, у тому числі для сторонніх контрагентів	Та ні	-	а) місце розміщення; б) спосіб доступу
…	…	….	…	…	…
N	1	Чи навчалися співробітники з тематики ІБ?	-	% співробітників, що навчилися	Наявність документів про підвищення кваліфікації та професійної перепідготовки

Можна сформулювати такі принципи складання чек-листів:

– виконання кожної вимоги нормативного документа визначається контрольним показником;

– кожен контрольний показник виявляється у вигляді гранично чіткого, однозначно трактованого питання, що передбачає однозначну об'єктивну відповідь;

– відповідь питання може бути або дискретним, або у вимірних обчислюваних значеннях;

– всі питання, що формують контрольні показники, поділяються на рівні;

– питання першого (вищого) рівня визначають глобально факти виконання вимог;

– питання другого та наступних (нижчих) рівнів деталізують ступінь виконання вимог та характеризують рівень захищеності;

– аудитор збирає відповіді питання з підтвердження фактів;

– при негативних відповідях питання верхніх рівнів, перевіряти твердження з питань нижніх рівнів немає сенсу;

– якість формулювань контрольних питань визначається їх об'єктивністю, що виражається у незаперечності відповідей навіть із позицій сторонньої зацікавленості.

У загальному випадку, виходячи з викладеного принципу формування чек-листів, кожне питання (показник) S_i описується у вигляді наступної функції (1):

$$S_i(j) = \{X_i \mid Z_i\}, \quad (1)$$

де i – номер питання, j – рівень питання, X – дискретне значення відповіді (1 – «так», «виконується», «є»; 0 – «ні», «не виконується», «відсутня»);

Z – обчислюване значення відповіді (у частках, відсотках чи інших одиницях, наприклад: 1 – «повністю відповідає», 0,75 – «переважно, 0,5 – «наполовину», 0,25 – «меншою мірою», 0 – «не відповідає»).

Для контролю першого рівня доцільно застосовувати питання лише з дискретними відповідями.

Вимогами щодо проходження аудиту буде 100% результати за критеріями першого рівня: $S_i(1) = 1$ і набір мінімальної (заздалегідь встановленої до початку аудиту) результативності за другим та наступним рівнями.

Для другого та наступних рівнів задаються мінімальні пороги результативності, які можуть бути сформульовані таким чином:

– для другого рівня: не менш як на 80% питань мають бути отримані позитивні відповіді;

– для третього рівня: не менш як на 60% питань мають бути отримані позитивні відповіді.

При підготовці до аудиту повинні бути складені чек-листи за всіма наявними в стандарті 10 напрямках, причому, кожен з питань $S_i(n)$ ставиться у відповідність до розв'язуваної функції (функціями) F_{11} … F_{53} у вигляді матриці відповідності (табл. 4). Слід досягати максимальної зв'язності показників та функцій, для чого обчислюється загальна кількість виконаних заходів відповідно до вимог за горизонталями t та вертикалями k.

Таблиця 4

Матриця відповідності функцій захисту за чек-листами

	F11	**……**	**……**	**……**	**F53**	**Разом**
S1(1)	+					t1(1)
Si(1)		+	+			……
……	……	……	……	……	……	……

	F11	**……**	**……**	**……**	**F53**	**Разом**
S1(2)			+			……
……	……	……	……	……	……	……
Si(3)	+					ti(3)
Разом	k1	……	……	……	k15	–

Обчислюються суми всіх відповідей кожного рівня за формулою (2):

$$C_N = \sum_{i=1}^{n} t_i(j) \quad (2)$$

де j – поточний рівень.

Обчислюється кількість відповідностей відповідей та функцій (3):

$$D_N = \sum_{i=1}^{n} S_i(j), \quad (3)$$

Релевантність складеної моделі оцінюється за принципом однорідності, тобто отримані значення C_N і D_N не повинні істотно відрізнятися один від одного (для випадку з 15 функціями F_{11} … F_{53}, C_N орієнтовно лежить в діапазоні 3 … 5).

У процесі перевірки аудитор для виявлення адекватності та дієвості заходів щодо захисту інформації може також включати до чек-листів перевірочні заходи (або організувати їх у вигляді окремої програми дослідження безпеки).

До таких заходів можуть належати тести на стійкість організаційної структури до інформаційно-психологічних чи інформаційно-технічних впливів.

І якщо оцінка стійкості до інформаційно-технічних впливів проводиться у межах технічного та інструментального аудиту, то оцінка стійкості до інформаційно-психологічних впливів може бути корисним доповненням до документарного аудиту виявлення практичного рівня стійкості колективу організації щодо загроз інформаційної безпеки.

Такі тестові заходи може бути розроблено аудитором з урахуванням структурних моделей соціально-психологічних загроз безпеки інформації.

Запропонований метод проведення аудиту полягає у формалізації матриці захисту та розробки об'єктивних чек-листів.

При цьому сформовано принципи складання таких чек-листів та оцінки їхньої релевантності.

Таким чином, аудит інформаційної безпеки на основі сформованої та описаної моделі, при його практичному застосуванні дасть не лише об'єктивний повторний та однозначний результат оцінки рівня інформаційної безпеки організації, а й дозволить виявити слабкі сторони в системі захисту та сформувати рекомендації щодо підвищення рівня захищеності об'єкта. Тому застосування даної моделі є доцільним при проведенні аудиту інформаційної безпеки в державних структурах.

Висновки. Отже, у цій роботі сформовано формалізовану модель аудиту інформаційної безпеки організації щодо відповідності вимогам стандартів, що

базується на принципах незалежності та об'єктивності аудиторської діяльності. Запропоновано підхід, що спирається на систему об'єктивних показників, порівнянних із функціями захисту, і полягає у формуванні чек-листів з відповідними критеріями співвідношення показників та методами підтвердження фактів, що виявляються в результаті аудиторської перевірки.

Перспективи подальших досліджень у даному напрямку. На основі запропонованої моделі прогнозується подальші дослідження націлити на обгартування методики розробки чек-листів стосовно будь-якого стандарту та нормативного документа, на предмет відповідності, якому може бути потрібне проведення аудиторської перевірки.

В подальших дослідженнях на основі запропонованої методики можлива розробка інструкцій стосовно будь-якого стандарту.

Література:

1. Рой Я.В., Мазур Н.П., Складанний П.М. Аудит інформаційної безпеки – основа ефективного захисту підприємства. *Кібербезпека: освіта, наука, техніка.* 2018. Том 1. №1. С. 86–93.

2. Sirotskiy A. Metric approach to assessing information security in banking organizations. *Sistemy bezopasnosti*. 2016. No. 25. P. 126–129.

3. Козубцов І.М., Черноног О.О., Козубцова Л.М., Артемчук М.В., Нещерет І.Г. Вибір окремих показників оцінювання здатності функціонування системи захисту інформації і кібербезпеки інформації в інформаційно-комунікаційних системах спеціального зв'язку. *Кібербезпека: освіта, наука, техніка*. 2022. Том 4. №16. С. 19–27.

4. Козубцов І.М., Куцаєв В.В., Козубцова Л.М., Терещенко Т.П., Черноног О.О. Обговорення єдиного підходу до побудови методики оцінки кібернетичної захищеності ІТС організації. Міжнародна науково-практична конференція "*Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку*" (Харків, 14-15 березня 2018 р.). Харків. НАНГ України, 2018. С. 15 – 16.

5. Козубцов І.М., Козубцова Л.М., Куцаєв В.В., Терещенко Т.П. Методика оцінки кібернетичної захищеності системи зв'язку організації. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2018. №1 (31). С. 43 – 46.

6. Козубцов І.М., Козубцова Л.М. Постановка завдання на розробку методики оцінки кібернетичної захищеності інформаційно-телекомунікаційної системи. Міжнародна науково-практична конференція «*Спільні дії військових формувань і правоохоронних органів держави: проблеми та перспективи*» (Одеса, 12-13 вересня 2019 р.) Військова академія, 2019. С. 228 – 229.

7. Козубцова Л.М., Бескровний О.І., Козубцов І.М. Структура методики оцінювання ефективності виконання заходів, спрямованих на забезпечення кібернетичної безпеки об'єктів критичної інформаційної інфраструктури. І Міжнародна науково-технічна конференція "*Системи і технології зв'язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку*" (Київ, 25-26 листопада 2021 р.). К.: ВІТІ, 2021. С. 160.

8. Козубцова Л.М., Хлапонин Ю.І., Козубцов І.М. Методика оцінювання ефективності виконання заходів забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури організацій. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2021. №2 (41). С. 17 – 22.

9. Артемчук М.В., Штонда Р.М., Нещерет І.Г., Терещенко Т.П., Цимбал І.В., Придатченко В.О. Методика проведення незалежного аудиту інформаційної безпеки установи щодо ефективності забезпечення захисту інформації. *Вісник ВІТІ. Комунікаційні та інформаційні системи*. 2021. Випуск № 2. С. 4 – 17.

10. Kozubtsov I., Lishchyna N., Kozubtsova L., Trush I., Yashchuk A. Information technology of information security audit of objects of critical infrastructure. *Published on CEUR Workshop Proceedings*. 2022. Pp. 97–106.

11. Якименко Ю., Рабчун Д., Мужанова Т., Запорожченко М., Щавінський Ю. Технічний аудит захищеності інформаційно-телекомунікаційних систем підприємств. *Кібербезпека: освіта, наука, техніка.* 2023. Том 4. №20. С. 45–61.

12. Reijers H.A. Business Process Management: The evolution of a discipline, *Computers in Industry*. 2021. Vol. 126. 103404.

13. Makarenko S.I. Information security audit: milestones, conceptual framework, classification of activities. *Sistemy upravleniya, svyazi i bezopasnosti*, 2018. No. 1. Pp. 1–29.

14. ISO/IEC TS 33030:2017 «Information technology – Process assessment – An exemplar documented assessment process». Published (Ed. 1, 2017). https://www.iso.org/standard/55121.html.

15. ISO/IEC 27001:2022 «Information security, cybersecurity and privacy protection — Information security management systems – Requirements». Published (Ed. 3, 2022). https://www.iso.org/standard/27001.

16. ISO/IEC 27002:2022 «Information security, cybersecurity and privacy protection – Information security controls». https://www.iso.org/ru/standard/75652.html.

17. Посібник з європейського права у сфері захисту персональних даних. К.: К.І.С., 2020. 432 с.

18. ISO/IEC 17799:2005 «Information technology – Security techniques – Code of practice for information security management».

19. Burns A.J., Posey C., Roberts T.L., Lowry P.B. Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*. 2017. Vol. 68. P. 190–209.

References:

1. Roi, Ya.V., Mazur, N.P., & Skladannyi, P.M. (2018). Audyt informatsiinoi bezpeky – osnova efektyvnoho zakhystu pidpryiemstva [Information security audit – the basis for effective enterprise protection]. *Cybersecurity: education, science, technology*, 1, 1, 86–93 [in Ukrainian].

2. Sirotskiy, A. (2016). Metric approach to assessing information security in banking organizations. *Sistemy bezopasnosti*, 25, 126–129.

3. Kozubtsov, I.M., Chernonoh, O.O., Kozubtsova, L.M., Artemchuk, M.V., & Neshcheret, I.H. (2022). Vybir okremykh pokaznykiv otsiniuvannia zdatnosti funktsionuvannia systemy zakhystu informatsii i kiberbezpeky informatsii v informatsiino-komunikatsiinykh systemakh spetsialnoho zv'iazku. [Selection of individual indicators for assessing the functioning of information protection and cybersecurity systems in special communications information and communication systems]. *Cybersecurity: education, science, technology*, 4, 16, 19–27 [in Ukrainian].

4. Kozubtsov, I.M., Kutsaiev, V.V., Kozubtsova, L.M., Tereshchenko, T.P., & Chernonoh, O.O. (2018). Obhovorennia yedynoho pidkhodu do pobudovy metodyky otsinky kibernetychnoi zakhyshchenosti ITS orhanizatsi. [Discussion of a unified approach to developing a methodology for assessing the cyber security of an organization's IT systems] *International Scientific and*

Practical Conference "Application of Information Technologies in the Training and Activities of Law Enforcement Forces". (pp. 15–16). Kharkiv. NANG of Ukraine [in Ukrainian].

5. Kozubtsov, I.M., Kozubtsova, L.M., Kutsaiev, V.V., & Tereshchenko, T.P. (2018). Metodyka otsinky kibernetychnoi zakhyshchenosti systemy zv'iazku orhanizatsii. [Methodology for assessing the cyber security of an organization's communication system]. *Modern information technologies in the field of security and defense*, 1(31), 43–46 [in Ukrainian].

6. Kozubtsov, I.M., & Kozubtsova, L.M. (2019). Postanovka zavdannia na rozrobku metodyky otsinky kibernetychnoi zakhyshchenosti informatsiino-telekomunikatsiinoi systemy [Setting the task of developing a methodology for assessing the cyber security of information and telecommunications systems]. *International Scientific and Practical Conference "Joint Actions of Military Formations and Law Enforcement Agencies of the State: Problems and Prospects"* (pp. 228–229). Odessa: Military Academy [in Ukrainian].

7. Kozubtsova, L.M., Beskrovnyi, O.I., & Kozubtsov, I.M. (2021). Struktura metodyky otsiniuvannia efektyvnosti vykonannia zakhodiv, spriamovanykh na zabezpechennia kibernetychnoi bezpeky ob'iektiv krytychnoi informatsiinoi infrastruktury [Structure of the methodology for evaluating the effectiveness of measures aimed at ensuring the cyber security of critical information infrastructure facilities] *International Scientific and Technical Conference "Systems and Technologies of Communication, Informatization, and Cybersecurity: Current Issues and Development Trends"*. (pp. 160). Kyiv: VITI [in Ukrainian].

8. Kozubtsova, L.M., Khlaponyn, Yu.I., & Kozubtsov, I.M. (2021). Metodyka otsiniuvannia efektyvnosti vykonannia zakhodiv zabezpechennia kiberbezpeky ob'iektiv krytychnoi informatsiinoi infrastruktury orhanizatsii [Methodology for assessing the effectiveness of cybersecurity measures for critical information infrastructure facilities of organizations] *Modern Information Technologies in Security and Defense*, 2 (41), 17–22 [in Ukrainian].

9. Artemchuk, M.V., Shtonda, R.M., Neshcheret, I.H., Tereshchenko, T.P., Tsymbal, I.V., & Prydatchenko, V.O. (2021). Metodyka provedennia nezalezhnoho audytu informatsiinoi bezpeky ustanovy shchodo efektyvnosti zabezpechennia zakhystu informatsii [Methodology for conducting an independent audit of an institution's information security regarding the effectiveness of information protection] *Bulletin of VITI. Communication and Information Systems*, 2, 4–17.

10. Kozubtsov, I., Lishchyna, N., Kozubtsova, L., Trush, I., & Yashchuk, A. (2022). Information technology of information security audit of objects of critical infrastructure. *Published on CEUR Workshop Proceedings*, 97–106.

11. Yakymenko, Yu., Rabchun, D., Muzhanova, T., Zaporozhchenko, M., & Shchavinskyi, Yu. (2023). Tekhnichnyi audyt zakhyshchenosti informatsiino-telekomunikatsiinykh system pidpryiemstv [Technical audit of the security of information and telecommunications systems of enterprises]. *Cybersecurity: education, science, technology*, 4, 20, 45–61 [in Ukrainian].

12. Reijers, H.A. (2021). Business Process Management: The evolution of a discipline. *Computers in Industry*, 126, 103404.

13. Makarenko, S.I. (2018). Information security audit: milestones, conceptual framework, classification of activities. *Sistemy upravleniya, svyazi i bezopasnosti*, 1, 1–29.

14. ISO/IEC TS 33030:2017 «Information technology – Process assessment – An exemplar documented assessment process». (2017), https://www.iso.org/standard/55121.html.

15. ISO/IEC 27001:2022 «Information security, cybersecurity and privacy protection – Information security management systems – Requirements». (2022), https://www.iso.org/standard/27001.

16. ISO/IEC 27002:2022 «Information security, cybersecurity and privacy protection – Information security controls». (2022), https://www.iso.org/ru/standard/75652.html.

17. Posibnyk z yevropeiskoho prava u sferi zakhystu personalnykh danykh (2020). [Guide to European law in the field of personal data protection]. Kyiv: K.I.S. [in Ukrainian].

18. ISO/IEC 17799:2005 «Information technology – Security techniques – Code of practice for information security management».

19. Burns, A.J., Posey, C., Roberts, T.L., & Lowry P.B. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, 68, 190–209.