Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

ПИЛИПЕНКО ДМИТРО ЮРІЙОВИЧ

УДК 681.3.06

МОДЕЛЬ ІНСТИТУЦІОНАЛЬНОГО УПРАВЛІННЯ І МЕТОД ОЦІНЮВАННЯ КУЛЬТУРИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

05.13.21 – системи захисту інформації

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Харків – 2013

Дисертацією є рукопис.

Робота виконана у Харківському національному університеті радіоелектроніки Міністерства освіти і науки України.

Науковий керівник — доктор технічних наук, професор **Потій Олександр Володимирович,** Харківський національний університет радіоелектроніки, професор кафедри безпеки інформаційних технологій.

Офіційні опоненти:

доктор технічних наук, професор **Мохор Володимир Володимирович,** Інститут спеціального зв'язку та захисту інформації НТУУ "Київський політехнічний інститут", завідувач кафедри кібербезпеки та застосування інформаційних систем і технологій;

доктор технічних наук, професор **Рубан Ігор Вікторович,** Харківський університет повітряних сил ім. Івана Кожедуба, начальник кафедри математичного та програмного забезпечення автоматизованих систем управління.

Захист відбудеться "__" 2013 р. о ___ годині на засіданні спеціалізованої вченої ради К 64.052.05 у Харківському національному університеті радіоелектроніки за адресою: 61166, м. Харків, просп. Леніна, 14.

З дисертацією можна ознайомитися в бібліотеці Харківського національного університету радіоелектроніки за адресою: 61166, м. Харків, просп. Леніна, 14.

Автореферат розісланий "___" _____ 2013 р.

Вчений секретар
спеціалізованої вченої ради І. В. Лисицька

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Сьогодні із впевненістю можна стверджувати, що розуміння проблем управління діяльністю із захисту інформації (ЗІ) зазнає якісних змін. Велика кількість вчених, робочих груп і фахівців у галузі ЗІ стверджують про те, що організаційні аспекти діяльності із ЗІ мають підлягати управлінню, контролю та оцінюванню на тому ж рівні, що й технічні аспекти. Нещодавні аналітичні звіти (InfoWatch, Infosecurity Europe) свідчать про те, що організації з різним напрямком діяльності (комерційні, урядові, академічні) потерпають від інцидентів безпеки, причиною яких є діяльність власних співробітників. Інциденти безпеки, причиною яких є людський чинник, не завжди пов’язані із нестачею або недосконалістю заходів захисту. Причини їх виникнення пов’язані здебільшого із недотриманням вимог політики безпеки (ПБ). Хибне розуміння співробітниками цілей та задач безпеки призводить до того, що ПБ сприймається як обмеження і незручність, що ускладнює виконання професійних обов’язків. Це в свою чергу призводить до формування низького рівня культури інформаційної безпеки (КІБ).

Наявність зазначених вище проблем свідчить про те, що існуючі на сьогоднішній день моделі та підходи до управління діяльністю із ЗІ не спроможні ефективно розв’язати задачу управління організаційними аспектами діяльності із ЗІ, серед яких переважно відзначається проблема формування високого рівня КІБ та оцінювання поточного рівня КІБ, а також пов’язаної із цим проблеми уточнення розрізненої предметної галузі КІБ. Вирішення наведених проблем ми бачимо у використанні нових моделей та підходів, які дозволять здійснювати управління діяльністю із ЗІ більш ефективно, ніж у класичних підходах.

З цієї позиції найбільш перспективним підходом є інституціональне управління, що досліджується в рамках системодіяльнісної методології. Інституціональне управління дозволяє використовувати ПБ як механізм змушення, а КІБ як механізм спонукання. Сумісне використання наведених механізмів управління дозволяє сформувати інститут інформаційної безпеки (ІІБ) в організації. Розробка моделі інституціонального управління та методу оцінювання КІБ є актуальною науковою задачею, розв’язання якої дозволить зменшити ймовірність реалізації ризиків інформаційної безпеки, пов’язаних із діяльністю співробітників організації, за рахунок підвищення ефективності керуючих впливів керуючого суб’єкта діяльності із ЗІ.

Таким чином, розробка моделі інституціонального управління та методу оцінювання КІБ є актуальною науковою задачею, розв’язання якої дозволить зменшити ймовірність реалізації ризиків інформаційної безпеки, пов’язаних із діяльністю власних співробітників організації, за рахунок підвищення ефективності керуючих впливів керуючого суб’єкта діяльності із ЗІ.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконана в рамках: держбюджетної НДР №262-1 від 01.01.2011 р. «Розвиток, стандартизація, уніфікація, удосконалення та

впровадження інфраструктури відкритих ключів, включаючи національну систему електронного цифрового підпису (ЕЦП)» за наказом МОНУ №1177 від 30.11.2010 р. (ДР №0111U002628); госпдоговірної НДР №11-06 від 01.03.2011 р. «Розробка методів, комплексів та засобів ІВК для національних та міжнародних інформаційно-телекомунікаційних систем та інформаційних технологій» (ДР №0111U002634), у розробці яких автор брав участь як виконавець.

Мета та задачі дослідження. Мета дисертаційної роботи полягає у розробці онтологічних моделей предметної галузі інституту і культури інформаційної безпеки, моделі інституціонального управління діяльністю із захисту інформації і методу оцінювання рівня культури інформаційної безпеки, що дозволить зменшити ймовірність виникнення ризиків безпеки, які пов'язані із діяльністю суб'єктів захисту інформації, за рахунок підвищення ефективності керуючих впливів керуючого суб'єкта діяльності із захисту інформації.

Для досягнення поставленої мети розв'язуються такі задачі:

1. Аналіз сучасного стану розв'язання задач управління та оцінювання організаційних аспектів діяльності із захисту інформації.
2. Онтологічний аналіз та моделювання предметної галузі інституту та культури інформаційної безпеки.
3. Розробка моделі інституціонального управління діяльністю із захисту інформації.
4. Розробка методу оцінювання рівня культури інформаційної безпеки, що містить спосіб формування множини показників культури інформаційної безпеки та механізм комплексного оцінювання рівня культури інформаційної безпеки.
5. Розробка інструментальних засобів оцінювання рівня культури інформаційної безпеки.

Об'єкт дослідження – інституціональне управління як явище.

Предмет дослідження – модель інституціонального управління та метод оцінювання культури інформаційної безпеки.

Методи дослідження: онтологічне моделювання – для побудови онтологічних моделей предметної галузі інституту і культури інформаційної безпеки в нотації UML; методи теорії множин та елементи теорії управління організаційними системами – для побудови моделі інституціонального управління діяльністю із захисту інформації; математичний апарат лінгвістичних змінних – для формалізації якісних характеристик об'єкта оцінювання; методи теорії графів – для побудови дерева комплексного оцінювання.

Наукова новизна отриманих результатів:

1. Вперше розроблено онтологічні моделі предметної галузі інституту та культури інформаційної безпеки, які базуються на результатах контент-аналізу, що надає можливість сформувати термінологічне ядро предметної галузі та встановити зв'язки між компонентами культури інформаційної безпеки і суб'єктами діяльності із захисту інформації.

2. Набула подальшого розвитку узагальнена модель діяльності із захисту інформації, що на відміну від існуючих розкриває особливості формування керуючих впливів центру безпеки з урахуванням гіпотези раціональної поведінки агента безпеки, що за рахунок моделювання інституціонального управління діяльності із захисту інформації надає можливість формалізації процесу прийняття рішень центром та агентом безпеки.

3. Вперше запропоновано метод оцінювання рівня культури інформаційної безпеки, який ґрунтується на використанні матриць згортання, що дозволяє отримати комплексну оцінку рівня культури інформаційної безпеки за рахунок удосконалень механізму оцінювання на основі матриць згортання та використання способу формування множини показників культури інформаційної безпеки.

Практичне значення отриманих результатів:

1. Розроблена модель інституціонального управління діяльністю із ЗІ і метод оцінювання КІБ дозволяють зменшити ймовірність ризиків безпеки, які пов'язані із діяльністю персоналу організації, за рахунок підвищення якості керуючих впливів керівництва.

2. За рахунок удосконалення механізму комплексного оцінювання на основі матриць згортання підвищується прозорість процесу оцінювання та зменшується суб'єктивний вплив експерта, на відміну від класичного способу.

3. Розроблені інструментальні засоби у вигляді системи підтримки прийняття рішень (СППР) дозволяють підвищити швидкість прийняття рішень ЛПР, зменшити ймовірність помилок за рахунок часткової автоматизації процедури генерації матриць згортання, процедури згортання безпосередньо та ефективної візуалізації отриманих результатів.

Результати дисертації використовуються на підприємствах: ЗАТ «ІІТ» (акт від 11.10.2012 р., Харків, Україна), ЗАТ «VEMARA» (акт від 25.09.2012 р., Вільнюс, Литва), а також у навчальному процесі Харківського національного університету радіоелектроніки під час проведення лекційних робіт (акт від 11.10.2012 р., Харків, Україна).

Особистий внесок здобувача. Всі основні результати отримано автором особисто. В роботах, виконаних у співавторстві, автору належить: [1] – сформульовано основні критерії аналізу систем показників безпеки (таксономій); [2] – проведено аналіз таксономій показників безпеки Vaughn-Henning-Siraj та CISWG; [3] – запропоновано показник гнучкості ЗІ, що характеризує комплексну систему захисту інформації з точки зору можливості її удосконалення, розширення та надання нових якостей; [4] – розроблено онтологічну модель предметної галузі культури інформаційної безпеки та проведено аналіз взаємозв'язків між її компонентами; [5] – проведено уточнення першого контуру управління захистом інформації в рамках процесного підходу; [6] – запропоновано використовувати систему збалансованих показників BSC як механізм оцінювання ефективності стратегічного набору організації, до якого входять фінансовий аспект ЗІ, процеси ЗІ, технології ЗІ, безпека бізнесу та діяльність персоналу (КІБ).

Апробація результатів дисертації. Основні результати дисертаційної роботи представлені й обговорені на 14 наукових та науково-технічних конференціях, зокрема: 1) V-й Міжнародній науково-практичній конференції «Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій» (м. Запоріжжя, 22-24 вересня 2010 р.); 2) VI-й науковій конференції Харківського університету Повітряних Сил імені Івана Кожедуба «Новітні технології – для захисту повітряного простору» (м. Харків, 15-16 квітня 2010 р.); 3) Науково-технічній конференції з міжнародною участю «Компьютерное моделирование в наукоемких технологиях (КМНТ-2010)» (м. Харків, 18-21 травня 2010 р.); 4) XI-й Міжнародній науково-практичній конференції «Информационная безопасность» (м. Таганрог, РФ, 22-25 червня 2010 р.); 5) XIII-й Міжнародній науково-практичній конференції «Безопасность информации в информационно-телекоммуникационных системах» (м. Київ, 18-21 травня 2010 р.); 6) XIV-му Міжнародному молодіжному форумі «Радиоэлектроника и молодежь в XXI веке» (м. Харків, 18-20 березня 2010 р.); 7) VII-й науковій конференції Харківського університету Повітряних сил імені Івана Кожедуба «Новітні технології – для захисту повітряного простору» (м. Харків, 13-14 квітня 2011 р.); 8) Міжнародній науково-практичній конференції «Перспективи розвитку інформаційних та транспортно-митних технологій у митній справі, зовнішньоекономічній діяльності та управлінні організаціями» (м. Дніпропетровськ, 2 грудня 2011 р.); 9) IV-й Всеукраїнській науково-практичній конференції молодих вчених та студентів «Інформаційні процеси і технології «Інформатика – 2011» (м. Севастополь, 25-29 квітня 2011 р.); 10) XV-й Міжнародній науково-практичній конференції «Безопасность информации в информационно-телекоммуникационных системах» (м. Київ, 22-25 травня 2012 р.); 11) IX-й Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (м. Київ, 22 квітня 2011 р.); 12) VIII-й науковій конференції Харківського університету Повітряних сил імені Івана Кожедуба «Новітні технології – для захисту повітряного простору» (м. Харків, 18-19 квітня 2012 р.); 13) II-й Міжнародній науково-практичній конференції молодих вчених «Інфокомунікації – сучасність та майбутнє» (м. Одеса, 11-12 жовтня 2012 р.); 14) II-й науково-технічній конференції «Безпека інформаційних технологій (ITSEC-2012)» (м. Київ, 24-25 квітня 2012 р.).

Публікації. Результати наукових досліджень відображено у 20 друкованих працях. До них входять 6 статей, опублікованих у наукових фахових виданнях України, а також 14 матеріалів наукових конференцій.

Структура та обсяг дисертації. Дисертація складається із вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. Повний обсяг дисертації складає 196 сторінок (134 сторінки основного тексту), що включає 40 рисунків, у тому числі 3 рисунки на окремій сторінці, 15 таблиць, у тому числі одна таблиця на окремій сторінці, список використаних джерел із 125 найменувань на 14 сторінках, 8 додатків на 39 сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність теми дисертаційної роботи, сформульовано мету та окремі задачі дослідження, наукову новизну та практичну значущість отриманих результатів, показано зв'язок з науковими програмами, планами та темами, наведено дані про впровадження результатів роботи, публікації та апробації основних наукових результатів, особистий внесок здобувача.

У першому розділі дисертації проведено аналіз сучасного стану розв'язання задач управління діяльністю із ЗІ. Було визначено, що в існуючих стандартах безпеки та підходах до управління діяльністю із ЗІ питання формування та оцінювання КІБ потребують глибшого дослідження. Встановлено, що дослідження цих питань ускладнюється якісною природою організаційних аспектів діяльності із ЗІ і, насамперед, складністю розрахунку комплексної оцінки КІБ. Показано, що існуючі на сьогодні моделі КІБ мають певні недоліки, серед яких слід зазначити відсутність системного підходу в ході побудови моделей КІБ та відсутність механізму розрахунку комплексної оцінки рівня КІБ, що ускладнює його інтерпретацію для керівництва. Сформовано сутність протиріччя, що склалося у напрямку управління діяльністю із ЗІ: моделі зрілості, що існують на сьогодні, дозволяють здійснювати оцінювання рівня зрілості процесів ЗІ, технічні системи ЗІ можуть бути оцінені за допомогою систем показників безпеки, у той час як системні підходи до оцінювання персоналу організації у контексті діяльності із ЗІ відсутні.

Таким чином, сформульовано мету і задачі дослідження, обґрунтовано наукове завдання дисертаційної роботи, що полягає у зниженні ризиків безпеки, пов'язаних із діяльністю персоналу організації.

Другий розділ дисертації присвячено онтологічному моделюванню предметної галузі інституту та культури інформаційної безпеки й розробці моделі інституціонального управління діяльністю із ЗІ. Було встановлено, що використання великої кількості різних моделей, підходів та концепцій вченими-дослідниками під час аналізу КІБ як явища, призвело до формування розрізненої та занадто широкої предметної галузі. Вирішення наведеної проблеми полягає в онтологічному моделюванні предметної галузі, що дозволить провести її уточнення та сформувати термінологічне ядро. Для вибору компонент КІБ та обґрунтування їх адекватності було використано метод контент-аналізу.

Метод контент-аналізу дозволяє розв'язувати задачу аналізу літератури (наукових публікацій) у вигляді збору кількісних даних змістовного характеру. Контент-аналіз проведено в чотири етапи: побудовано логічну модель контент-аналізу, підготовлено дані для аналізу, проведено пілотний контент-аналіз, проведено фінальний контент-аналіз та сформовано таблицю контент-аналізу.

Побудована на першому етапі логічна модель контент-аналізу може бути подана у вигляді кортежу, вираз (1).

$$\mathrm{SubjModel} = \langle \mathrm{Category}, \mathrm{ContentUnit}, \mathrm{MeasurementUnit} \rangle, \qquad (1)$$

де Category – категоріальна модель предмета аналізу, ContentUnit – система одиниць контент-аналізу, MeasurementUnit – одиниці вимірювання.

Категоріальна модель контент-аналізу містить гіпотези, припущення та обмеження, які мають бути враховані під час аналізу. Як система одиниць контент-аналізу було обрано систему концептів, де під концептом розуміють окрему ідею (смислову одиницю). Як одиниця вимірювання використовується свідчення про наявність концепту у джерелі, що аналізується. На другому етапі було сформовано ряд джерел (загальною кількістю 41 публікація), які відповідають вимогам категоріальної моделі, зокрема знаходилися у вільному доступі. В результаті проведення пілотного контент-аналізу сформовано множину концептів $\text{Suggest} = \{\text{Suggest}_n \mid n = \overline{1,8}\}$. Множину Suggest було використано під час фінального етапу контент-аналізу, що дозволило отримати підсумкову таблицю контент-аналізу.

Таким чином, результати контент-аналізу дозволили зробити обґрунтований вибір ключових компонент, які впливають на формування та підтримку певного рівня КІБ. На основі обраних компонент було побудовано онтологічну модель предметної галузі КІБ, яку наведено на рис. 1.

В ході розробки онтологічної моделі предметної галузі КІБ було встановлено, що на формування КІБ впливають носії культури, яких було поділено на керуючих суб'єктів (керівництво) та керованих суб'єктів (персонал). Між носіями КІБ та компонентами (настанова співробітника, дисципліна, норми та цінності, підтримка керівництва) встановлено та розкрито взаємозв'язок.

Було з'ясовано, що в рамках управління діяльністю із ЗІ з точки зору керівництва КІБ слід розглядати в першу чергу як механізм спонукання, що сприяє дотриманню вимог та правил безпеки, сформульованих у ПБ. У свою чергу ПБ слід розглядати як механізм змушення. Сумісне використання наведених механізмів утворює більш складну структуру, а саме інститут інформаційної безпеки. Онтологічна модель предметної галузі ІІБ розкриває місце КІБ у контексті формування ІІБ (рис. 2).

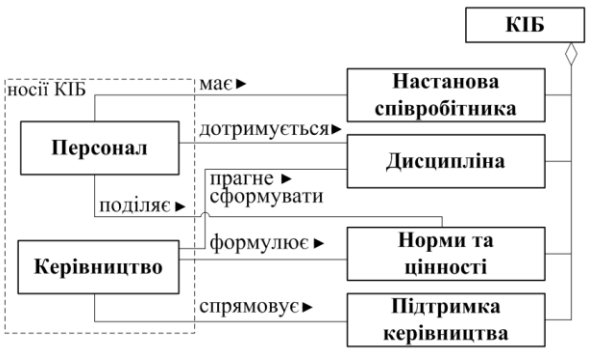

Рис. 1 – Онтологічна модель предметної галузі КІБ

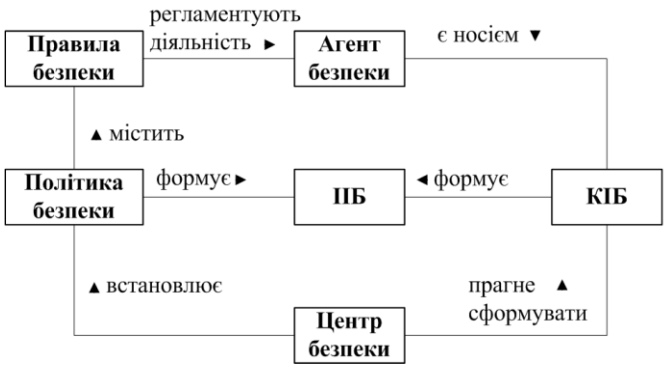

Рис.2 – Онтологічна модель предметної галузі ІІБ

Було встановлено, що ІІБ слід розглядати як різновид соціального інституту, функцією якого є регламентація дій персоналу та узгодження їх професійної деяльності із цілями та задачами захисту, що встановлює керівництво. Запропоновано онтологічну модель предметної галузі ІІБ, що створює передумови для розробки моделі інституціонального управління діяльністю із ЗІ, оскільки головною задачею інституціонального управління є формування ІІБ в організації. Для позначення керуючого та керованого суб'єктів діяльності із ЗІ було адаптовано традиційні терміни із теорії управління організаційними системами, а саме центр безпеки (керівництво) та агент безпеки (персонал).

Запропоновано модель інституціонального управління діяльністю із ЗІ, що враховує такі аспекти діяльності: мотиваційний, концептуальний, функціональний, оцінювальний (рис. 3). В рамках моделі встановлено взаємозв'язок між суб'єктами діяльності, побудовано моделі прийняття рішень центром безпеки та агентом безпеки відповідно.

Мотиваційний компонент розробленої моделі враховує множину потреб N суб'єкта захисту та пов'язаних з нею множиною мотивів M (блок A_{motiv}). Наявність множини потреб та множини мотивів призводить до формування множини цілей безпеки G_0.Модель прийняття рішень цетром безпеки (блок $A_{concept}$) має вигляд логічного кортежу, вираз (2):

$$\Psi_0 = \left\langle G_0, F_0, Obj, \Re_G, \Re_F, \Theta, I_0, U, R_{required} \right\rangle, \tag{2}$$

де G_0 – множина цілей захисту; F_0 – множина чинників, що враховуються центром безпеки; $Obj = \{obj_1, obj_2, ..., obj_n\}$ – множина задач захисту; $\Re_G$ – переваги центру безпеки на множині цілей захисту; $\Re_F$ – переваги центру безпеки на множині чинників; Θ – середовище безпеки; I_0 – інформація про середовище безпеки, яка відома центру безпеки; U – множина керуючих впливів (альтернатив), які доступні центру безпеки; $R_{required}$ – бажаний (необхідний) результат діяльності агентів безпеки, що формулює центр безпеки.

Результатом роботи моделі прийняття рішень цетром безпеки Ψ_0 є підмножина найкращих з точки зору центру безпеки керуючих впливів з множини альтернатив $u \subset U$ та бажаний результат діяльності агентів безпеки $R_{required}$, що змістовно слід інтерпретувати як рівень КІБ, який має бути досягнутий в організації.Нехай агент безпеки має переваги на множині допустимих дій A, тоді правило раціонального вибору має вигляд, поданий виразом (3):

$$P^{W_I}(Type_{agent}, Risk_{subj}, I, A) \subset \tilde{A}, \tag{3}$$

де $Type_{agent}$ – тип агента безпеки в контексті його відношення до центру безпеки (лояльний, нейтральний, протидіючий); $Risk_{subj}$ – міра суб'єктивного сприйняття

ризику агентом; I – інформація про середовище безпеки, яка відома агенту безпеки; A – множина дій, доступних агенту безпеки; Ã – підмножина дій, найкращих з точки зору агента безпеки.

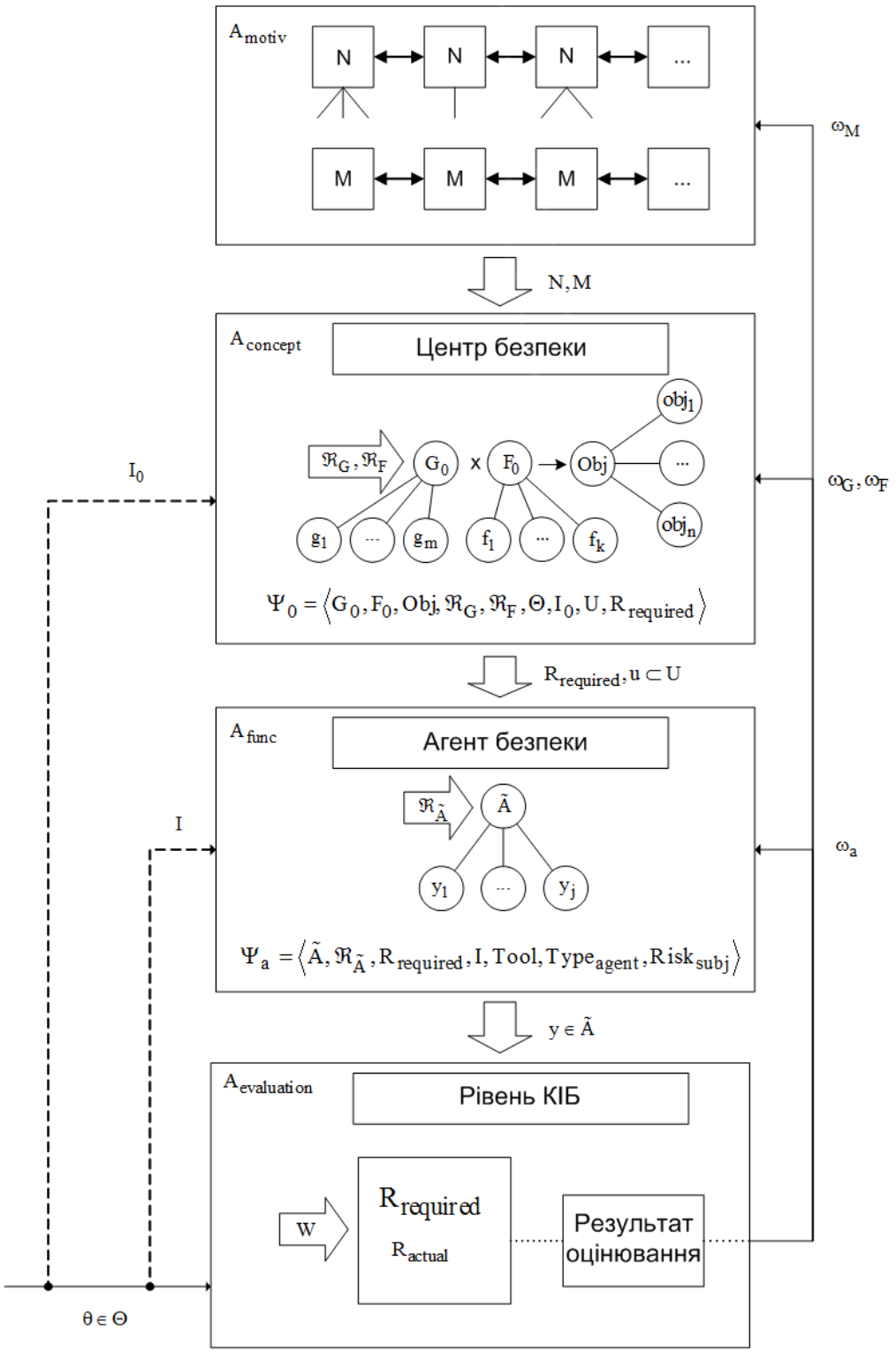

Рис. 3 – Модель інституціонального управління діяльністю із ЗІ

Таким чином, на основі правила раціонального вибору агент безпеки формує підмножину дій, що відповідно до його переваг є найкращими альтернативами. Згідно з гіпотезою раціональної поведінки, агент безпеки прагне вибрати ті дії, на яких досягається максимум його цільової функції $f(y), y \in \tilde{A}$, вираз (4):

$$P^{W_I}(Type_{agent}, Risk_{subj}, I, A) \subset \tilde{A} = Arg \max_{y \in \tilde{A}} f(y). \quad (4)$$

Таким чином, модель прийняття рішень агентом безпеки має такий вигляд (блок A_{func}):

$$\Psi_a = \left\langle \tilde{A}, \Re_{\tilde{A}}, R_{required}, I, Tool, Type_{agent}, Risk_{subj} \right\rangle, \quad (5)$$

де $\tilde{A}$ – підмножина дій, найкращих з точки зору агента безпеки; $\Re_{\tilde{A}}$ – переваги агента безпеки на множині дій $\tilde{A}$; $R_{required}$ – бажаний центром безпеки результат; I – інформація про середовище безпеки, що доступна агенту безпеки; Tool – множина рішень безпеки, що використовуються агентом під час здійснення діяльності із ЗІ; $Type_{agent}$ – тип агента безпеки; $Risk_{subj}$ – міра суб'єктивного сприйняття ризику агентом безпеки.

Діяльність агентів безпеки призводить до формування певного рівня КІБ, що подано змінною R_{actual} (блок $A_{evaluation}$). Оцінювання досягнутого рівня КІБ пропонується здійснювати на основі набору показників КІБ W. Порівнюючи фактичний рівень культури R_{actual} із бажаним $R_{required}$, центр безпеки за необхідності вносить корективи, які позначені в моделі зворотним зв'язком $\omega_M, \omega_G, \omega_F, \omega_a$ (рис. 3) і реалізуються на необхідному рівні моделі.

Таким чином, було сформовано термінологічне ядро й уточнено предметну галузь ІІБ та КІБ за рахунок онтологічного моделювання предметної галузі. Розроблені онтологічні моделі створили передумови до розробки моделі інституціонального управління та дозволили встановити взаємозв'язок між суб'єктами діяльності із ЗІ та компонентами КІБ. В рамках моделі інституціонального управління було запропоновано моделі прийняття рішень центром та агентом безпеки. Розроблена модель інституціонального управління дозволяє враховувати діяльність агента безпеки та формувати керуючі впливи з урахуванням гіпотези раціональної поведінки агента безпеки.

Третій розділ дисертаційної роботи присвячено розробці методу оцінювання КІБ, що дозволяє отримати комплексну оцінку рівня КІБ. Розроблений метод містить: спосіб формування множини показників КІБ, розробку шаблона показника КІБ нижнього рівня, методику побудови дерева комплексного оцінювання, опис показників нижнього рівня за шаблоном відповідно до ієрархії дерева комплексного оцінювання, шкалу оцінки КІБ, спосіб генерації матриць згортання.

Спосіб формування множини показників КІБ було проведено в два етапи: побудова базової множини показників КІБ, та її подальшого уточнення та доробки. Базова множина $P^{base} = \{P_n \mid \overline{1,N}\}$ була сформована шляхом вибору з систем-кандидатів показників безпеки (Vaughn-Hennig-Siraj, OCTAVE, CISWG, Erkan Kahraman, NIST), що відповідають введеним критеріям придатності та призначення. Було встановлено, що серед 24 відібраних показників містяться ті, що за відмінностей у назві мають однакове призначення. Отже, було проведено уточнення та доробку множини P^{base}, що дозволило отримати уточнену множину $\tilde{P}_{base}$. Оскільки не всі аспекти КІБ було охоплено сформованою множиною, було проведено її розширення шляхом розробки додаткових показників, спираючись на онтологічну модель КІБ. Спираючись на критерій придатності k, з множини концептів $Suggest_i$ відібрано елементи, які можуть бути використані для розробки додаткових показників, $Suggest_i \xrightarrow{k} P^{concept}$. Множину концептів $P^{concept}$ було далі перетворено на показники КІБ, $P^{concept} \to P^{ca}$. У результаті було отримано мінімально необхідну для оцінювання КІБ множину показників $P^{final} = \tilde{P}^{base} \cup P^{ca}$.

Побудова дерева комплексного оцінювання $G^{P^{final}}$ є необхідною складовою методу оцінювання рівня КІБ у зв'язку з обраним механізмом комплексного оцінювання на основі матриць згортання. Встановлено, що наведений механізм комплексного оцінювання потребує певних вимог до структури дерева комплексного оцінювання.

Перша вимога полягає у тому, що кожна вершина R_i дерева, що не є термінальною, має задовольняти умови, наведені у виразі (6). Іншими словами, кожна вершина, яка не є термінальною, повинна мати два ребра, що надає дереву дихотомічну структуру.

$$\begin{cases} R = P^{final} \setminus ПНР \\ R_i \subset R, i = \overline{1,|R|} \\ d(R_i) = 2 \end{cases}, \tag{6}$$

де R – множина вершин дерева, що не є термінальними; ПНР – множина показників нижнього рівня; $d(R_i)$ – ступінь i-ї вершини.

Друга вимога полягає у тому, що кількісні показники з множини P^{final} мають знаходитись в термінальних вершинах дерева, оскільки значення кількісних показників можна врахувати лише на нижньому рівні:

$$\begin{cases} R_i \neq ПНР_j \\ R_i \in R, ПНР_j \in ПНР \end{cases}. \tag{7}$$

Побудова дерева комплексного оцінювання $G^{P^{final}}$ передбачає побудову множини показників нижнього рівня $ПНР \subset P^{final}, ПНР = \{ПНР_m \mid m = \overline{1,M}\}$ та множини локальних оцінок $ЛО \subset P^{final}, ЛО = \{ЛО_k \mid k = \overline{1,K}\}$.

Таким чином, на основі множини показників КІБ P^{final} з урахуванням наведених обмежень було побудовано дерево комплексного оцінювання $G^{P^{final}}$ (рис 4). Коренева вершина побудованого дерева на 0 рівні ієрархії є комплексною оцінкою рівня КІБ, $КО \in P^{final}$. Локальні оцінки займають рівні з 1 по 4, $ЛО \subset P^{final}, ЛО = \{ЛО_k \mid k = \overline{1,12}\}$. Показники нижнього рівня знаходяться на п'ятому рівні, $ПНР \subset P^{final}, ПНР = \{ПНР_m \mid m = \overline{1,14}\}$. Впорядкована згідно з деревом комплексного оцінювання множина P^{final} представлена на рис. 5.

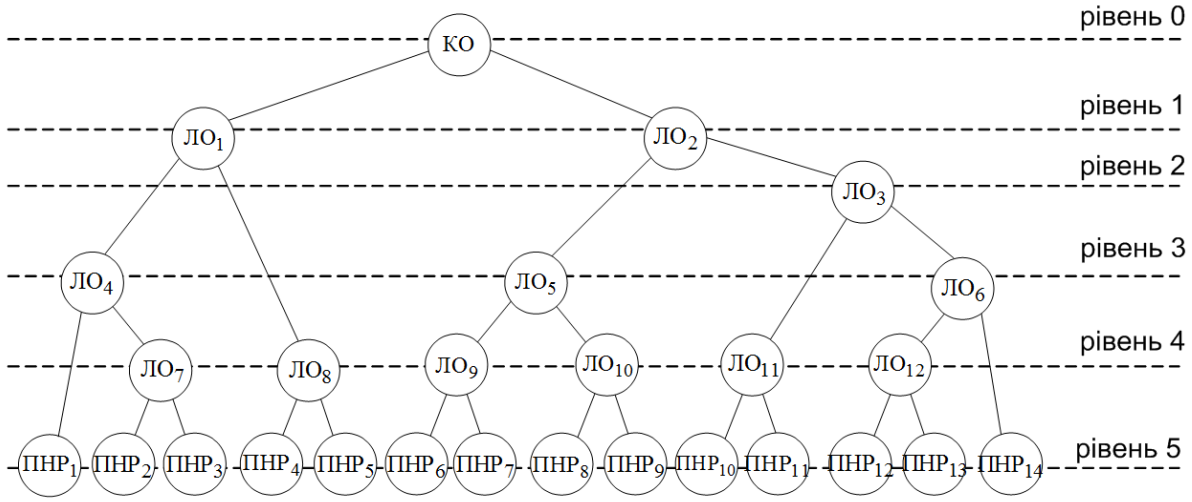

Рис. 4 – Дерево комплексного оцінювання $G^{P^{final}}$

Для опису елементів підмножини ПНУ було розроблено шаблон показника нижнього рівня. Шаблон показника можна подати у вигляді кортежу $T_p = \langle ID, Descr, OE, EG, Method \rangle$, де ID – ідентифікатор показника нижнього рівня, Descr – стисла характеристика показника, OE – об'єкт вимірювання, EG – мета вимірювання, Method – спосіб розрахунку значення показника.

Оцінювання рівня КІБ пропонується проводити згідно з якісною п'ятибальною шкалою, яка має таку вербальну інтерпретацію: низький (1), нижче середнього (2), середній (3), вище середнього (4), високий (5).

Традиційно, під матрицею згортання в теорії управління організаційними системами розуміють таблицю, номер рядка якої відповідає бальній оцінці за першим критерієм (показником), а номер стовпця відповідає другому критерію (показнику) з пари, що згортається. Комірка матриці A, яка знаходиться на перехрещенні рядка та стовпця, і є результатом згортання.

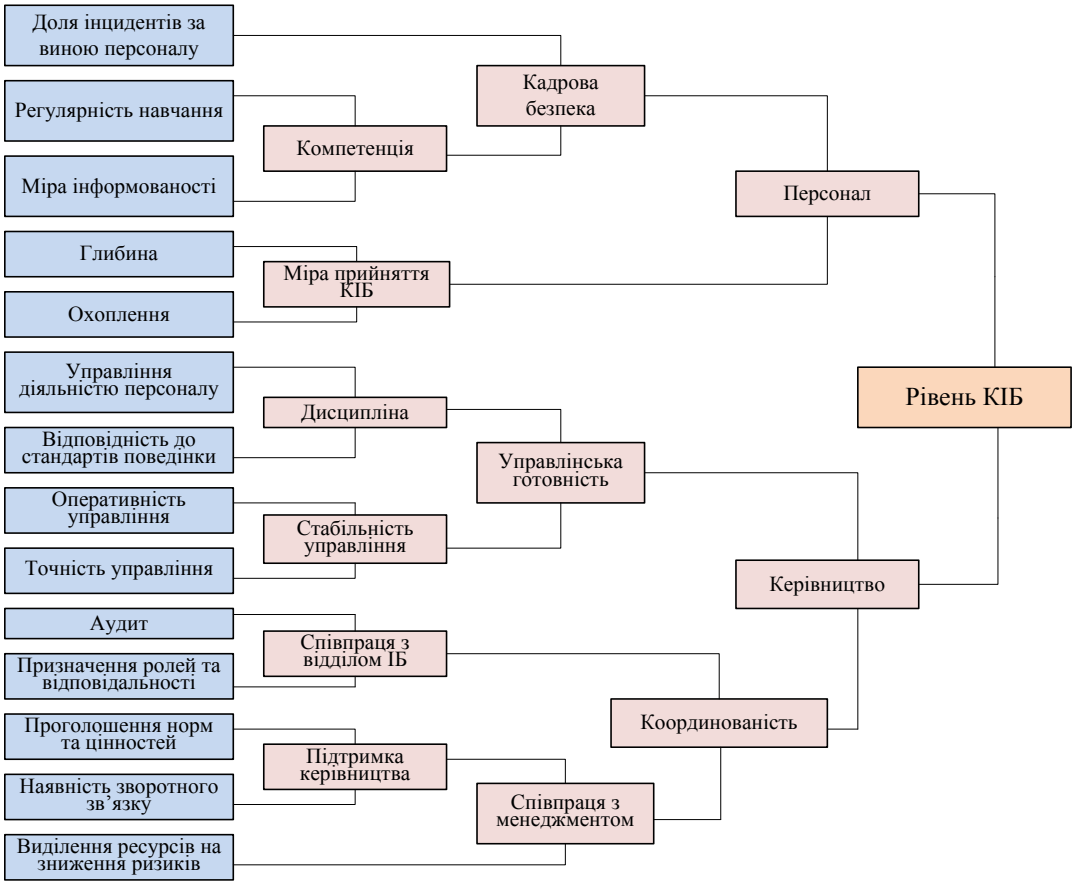

Рис. 5 – Впорядкована множина показників КІБ

З метою підвищення прозорості (за рахунок властивості відтворюваності) процедури генерації матриць згортання введено використання вагових коефіцієнтів. Врахування ситуації, коли високе значення одного з пари показників нівелюється низьким значенням іншого показника було здійснено введенням мінімальних порогових значень. Білінійна інтерполяція значень показників дозволяє уникнути необхідності в округленні значень показників, як того вимагає класичний спосіб, і зменшує похибку. Таким чином, генерація матриці згортання має вигляд:

$$\begin{cases} P_i \le P_{i\min} \cup P_j \le P_{j\min} \Rightarrow a(i,j) = \min(P_i, P_j) \\ P_i > P_{i\min} \cup P_j > P_{j\min} \Rightarrow a(i,j) = f_L(P_i, P_j) = W_l P_i + W_r P_j, \\ i = \overline{1,5}, j = \overline{1,5} \end{cases} \quad (9)$$

де P_i, P_j – значення показників КІБ; f_L – функція лінійного згортання; W_l, W_r – вагові коефіцієнти; $P_{i\min}, P_{j\min}$ – мінімальні порогові значення.

Процедура генерації матриць згортання має здійснюватися з урахуванням таких вимог: елементи матриці A мають бути додатними, $a(i,j) > 0$; матриця

має характеризуватися властивістю монотонності, тобто $a_{i,j} \geq a_{(i-1),j}, i = \overline{2,n}, j = \overline{1,m}$ та $a_{i,j} \geq a_{i(j-1)}, i = \overline{1,n}, j = \overline{2,m}$.

Таким чином, розроблено метод оцінювання КІБ, який дозволяє отримати комплексну оцінку рівня КІБ за рахунок сформованої множини показників P^{final}, що було впорядковано відповідно до структури дерева комплексного оцінювання $G^{P^{final}}$. Запропоновано ряд вдосконалень класичного механізму розрахунку комплексної оцінки на основі матриць згортання, що дозволяє отримувати більш точну оцінку рівня КІБ та уникнути необхідності в округленні значень показників КІБ.

У **четвертому розділі** дисертації проводиться розробка програмного засобу як система підтримки прийняття рішень та розрахунковий експеримент, метою якого є перевірка таких гіпотез:

1. Удосконалений спосіб на основі матриць згортання дозволяє отримати більш точну комплексну оцінку рівня КІБ, ніж класичний, що досягається зменшенням похибки за рахунок застосування білінійної інтерполяції.

2. Удосконалений спосіб на основі матриць згортання дозволяє краще, ніж класичний, відстежувати динаміку змін комплексної оцінки рівня КІБ.

У рамках розрахункового експерименту було згенеровано значення показників нижнього рівня для першого етапу оцінювання та трьох варіацій другого етапу: незначного зростання показників (Н), значного зростання показників (З), часткового зростання показників (Ч). Для розрахунку різниці між мінімальним та максимальним рівнем КІБ для заданого набору значень було введено такі типи експертів: песимістичний, нейтральний, оптимістичний. Отримані результати містяться у таблиці 1.

Таблиця 1 – Підсумкові результати розрахункового експерименту

Тип експерта	Рівень КІБ							
	Класичний спосіб				Удосконалений спосіб			
	1-й етап	2-й етап			1-й етап	2 етап		
		Н	З	Ч		Н	З	Ч
Песимістичний	1	1	1	1	1,02	1,09	1,52	1,02
Нейтральний	1	1	2	1	1,03	1,2	2,29	1,03
Оптимістичний	3	4	4	3	1,98	2,13	2,59	1,96

Аналіз таблиці 1 дозволяє оцінити різницю між мінімальною та максимальною оцінкою рівня КІБ. Для класичного способу різниця між максимальним та мінімальним рівнем КІБ становить 3 бали при незначному та значному зростанні значень на другому етапі (Н, З). Для удосконаленого способу ця різниця складає 1,07 бала при значному зростанні значень (максимальна різниця серед усіх розглянутих варіантів). Це свідчить про те, що класичний спосіб значною мірою схильний до суб'єктивних переваг експерта, ніж удосконалений, що підтверджує першу гіпотезу.

Таблиця 2 – Динаміка змін рівня КІБ при переході з першого на другий етап оцінювання

Тип експерта	Удосконалений спосіб/ Класичний спосіб		
	Н	З	Ч
Песимістичний	+ 0,07 / 0	+ 0,5 / 0	0 / 0
Нейтральний	+ 0,17 / 0	+ 1,26 / +1	0 / 0
Оптимістичний	+ 0,15 / +1	+ 0,61 / +1	- 0,02 / 0

Отримані результати (таблиця 2) дозволяють стверджувати те, що вдосконалений спосіб є більш чутливим до змін КІБ і в порівнянні з класичним способом дозволяє краще відстежувати динаміку змін рівня КІБ. Класичний спосіб спроможний відображати зміни рівня КІБ тільки у разі досягнення певної позначки, що відповідає поділкам на п’ятибальній шкалі. В усіх інших випадках динаміку змін рівня КІБ (особливо незначні зміни) відстежити неможливо, що підтверджує другу гіпотезу.

До недоліків процедури розрахунку комплексної оцінки КІБ слід віднести велику кількість розрахункових операцій, що перекладаються на експерта. Це призводить в першу чергу до зростання часових затрат і до можливості помилки під час розрахунків вручну. Розробка програмного засобу у вигляді СППР дозволяє вирішити ці проблеми за рахунок підвищення швидкості прийняття рішень експертом (ЛПР) та знизити ймовірність помилки за рахунок часткової автоматизації процесу генерації матриць згортання. Ефективна візуалізація результатів оцінювання рівня КІБ дозволяє проаналізувати стан діяльності із ЗІ та визначити аспекти, що найбільш потребують уваги.

СППР «КІБ» реалізовано на основі шаблону проектування програмного забезпечення Model-View-Controller (MVC). Шаблон MVC розділяє дані, інтерфейс користувача та керуючу логіку на три компоненти: модель даних, зображення та контролер. Модель даних у СППР «КІБ» подана зв’язним неорієнтованим графом. Кожний вузол, що відповідає локальній оцінці, містить вагові коефіцієнти та мінімальні порогові значення. Вузли, що відповідають показникам нижнього рівня, містять кількісні значення.

Як платформа для розробки СППР «КІБ» було обрано програмну платформу .NET Framework. СППР «КІБ» було розроблено в рамках парадигми товстого клієнта, що має такі переваги: автономність, чутливість інтерфейсу, використання стандартних компонент.

Організація взаємодії з СППР «КІБ» здійснюється за допомогою компонента «контролер» у два етапи: на першому етапі експерт здійснює розрахунок показників нижнього рівня та вводить їх у відповідні поля. На другому етапі експерт визначає вагові коефіцієнти та мінімальні порогові значення згідно зі структурою дерева комплексного оцінювання. Після визначення параметрів генерації матриць згортання, натискання кнопки «здійснити розрахунок» дозволяє отримати значення комплексної оцінки рівня КІБ. Для візуалізації значень множини показників КІБ генерується гістограма.

ВИСНОВКИ

Під час дисертаційних досліджень вирішено актуальне науково-практичне завдання, яке пов’язано із зменшенням ймовірності виникнення інцидентів безпеки, причиною яких є діяльність персоналу організації за рахунок розробки моделі інституціонального управління діяльністю із ЗІ та методу оцінювання рівня КІБ. Основні результати дисертаційної роботи полягають у наступному.

1. Вперше розроблено онтологічні моделі інституту та культури інформаційної безпеки, які ґрунтуються на результатах контент-аналізу. Це надало можливість уточнити розрізнену предметну галузь та сформувати ядро терміносистеми, встановити зв’язки між суб’єктами діяльності із ЗІ та компонентами моделі культури інформаційної безпеки.

2. Набула подальшого розвитку узагальнена модель діяльності із ЗІ, яка розкриває особливості формування керуючих впливів центру безпеки з урахуванням гіпотези раціональної поведінки агента. Моделювання інституціонального управління діяльності із ЗІ надає можливість формалізувати процеси прийняття рішень головними суб’єктами діяльності із ЗІ, а саме центром та агентом безпеки.

3. Вперше запропоновано метод оцінювання рівня КІБ, який ґрунтується на використанні матриць згортання, що дозволяє отримати комплексну оцінку рівня КІБ за рахунок удосконалень механізму комплексного оцінювання та використання способу формування множини показників КІБ. У рамках механізму комплексного оцінювання на основі матриць згортання запропоновано такі вдосконалення: використання вагових коефіцієнтів, використання мінімальних порогових значень та білінійної інтерполяції.

4. Для перевірки запропонованих удосконалень механізму комплексного оцінювання на основі матриць згортання було сформульовано гіпотези сутність яких полягає у тому, що удосконалений спосіб на основі матриць згортання дозволяє отримати більш точну оцінку рівня КІБ та дозволяє краще відстежувати динаміку змін рівня КІБ. Гіпотези було підтверджено результатами розрахункового експерименту. Розрахунки здійснено за допомогою розробленого програмного засобу у вигляді системи підтримки прийняття рішень.

5. Практичне значення отриманих результатів полягає у тому, що розроблена модель інституціонального управління і метод оцінювання КІБ дозволяють зменшити ймовірність виникнення ризиків безпеки, пов’язаних із діяльністю персоналу організації за рахунок підвищення якості керуючих впливів керівництва.

6. Вдосконалення механізму комплексного оцінювання на основі матриць згортання підвищує прозорість процесу оцінювання та зменшує суб’єктивний вплив експерта. Розроблені інструментальні засоби дозволяють підвищити швидкість прийняття рішень ЛПР та зменшити ймовірність помилок.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Потий А.В. Классификация показателей безопасности информации / А.В. Потий, Д.Ю. Пилипенко // Інформаційна та економічна безпека. – 2010. – Випуск 3(84). – С. 53.

2. Потій О. В. Аналіз систем показників безпеки інформації / О.В. Потій, Д.Ю. Пилипенко // Научно-технический журнал «Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения информационной безопасности». Харьков, ХНУРЭ, 2010. – Том 9. – №3. – С. 435 – 443.

3. Потій О. В. Властивості діяльності із забезпечення захисту інформації як системної категорії / О.В. Потій, Д.Ю. Пилипенко // Научно-технический журнал «Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения информационной безопасности». Харьков ХНУРЭ, 2012. – Том 11. – №2. – С. 299 – 303.

4. Potiy A.V. The prerequisites of information security culture development and an approach to complex evaluation of its level / A.V. Potiy, D.Y. Pilipenko, I.N. Rebriy // Науково-технічний журнал "Радіоелектронні і комп'ютерні системи" № 5(57). Харків "ХАІ". – 2012. – С. 72 – 77.

5. Потій О.В. Структура та модель системи захисту інформації в рамках процесного підходу / О. В. Потій, А. В. Лєншин, Д.Ю. Пилипенко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2010. – Вип. 1(20).

6. Потий А.В. Концепция стратегического управления информационной безопасностью / А.В. Потий, Д.Ю. Пилипенко // Радіоелектронні та комп'ютерні системи. – Харків «ХАІ», 2010, № 6 (47). – С. 53 – 58.

7. Потий А.В. Стратегическое управление информационной безопасностью на предприятии на основе системы сбалансированных показателей / А.В. Потий, Д.Ю. Пилипенко // Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій. V Міжнародна науково-практична конференція, 22-24 вересня 2010 р. – Тези доповідей. – З.: ЗНТУ, 2010 – С. 123 – 124.

8. Потий А.В. Система сбалансированных показателей как метод управления информационной безопасностью / А.В. Потий, Д.Ю. Пилипенко // Новітні технології – для захисту повітряного простору. VI Наукова конференція ХУПС, 15-16 квітня 2010 р. – Тези доповідей. – Х. : ХУПС, 2010. – С. 129.

9. Потий А.В. Проблемные вопросы разработки показателей безопасности информации / А.В. Потий, Д.Ю. Пилипенко // Компьютерное моделирование в наукоемких технологиях (КМНТ-2010). Научно-техническая конференция с международным участием, 18-21 мая 2010 г. – Труды конференции. – Х.: ХНУ, 2010 – С.202 – 205.

10. Потий А.В. Классификация метрических показателей безопасности информации / А.В. Потий, Д.Ю. Пилипенко // Материалы XI Международной научно-практической конференции «Информационная безопасность», Ч. 3. – Таганрог: ТТИ ЮФУ, 2010. – С. 227 – 231.

11. Потий А.В. Разработка метрических показателей безопасности на основе системы сбалансированных показателей / А.В. Потий, Д.Ю. Пилипенко // Безопасность информации в информационно-телекоммуникационных системах. XIII Международная научно-практическая конференция, 18-21 мая 2010г. – Тезисы докладов. – К.: ГСССЗЩ, 2010 – С. 58.

12. Потий А.В. Системы метрических показателей безопасности информации / А.В. Потий, Д.Ю. Пилипенко // 14-й Международный молодежный форум «Радиоэлектроника и молодежь в XXI веке». Сб. материалов форума, Ч.2. – Харьков: ХНУРЭ, 2010. – С. 53.

13. Потий А.В. Преимущества использования ССП в управлении информационной безопасностью интернет-магазина / А.В. Потий, Д.Ю. Пилипенко // Новітні технології – для захисту повітряного простору. VII Наукова конференція ХУПС, 13-14 квітня 2011 р. – Тези доповідей. – Х.: ХУПС, 2011. – С. 153.

14. Потий А.В. Предпосылки формирования культуры информационной безопасности / А.В. Потий, Д.Ю. Пилипенко // Перспективи розвитку інформаційних та транспортно-митних технологій у митній справі, зовнішньоекономічній діяльності та управлінні організаціями: матеріали міжнародної науково-практичної конференції, 2 грудня 2011. – Дніпропетровськ: Академія митної служби України, 2011. – С. 225 – 227.

15. Пилипенко Д.Ю. Разработка типового набора показателей безопасности информации на основе похода BSC / Д.Ю. Пилипенко // Інформаційні процеси і технології «Інформатика – 2011»: матеріали IV Всеукраїн. наук.-практ. конф. молодих вчених та студентів, 25-29 квітня 2011 р. – М-во освіти, молоді та спорту України, Севастоп. нац. тех. ун-т; наук. ред. С.В. Доценко – Севастополь : СевНТУ, 2011. – С. 192.

16. Потий А.В. Институциональное управление информационной безопасностью / А.В. Потий, Д.Ю. Пилипенко // Безопасность информации в информационно-телекоммуникационных системах. XV Международная научно-практическая конференция, 22-25 мая 2012 г. – Тезисы докладов. – К.: ГСССЗЩ, 2012 – С. 94 – 95.

17. Пилипенко Д.Ю. Формування набору показників безпеки інформації на основі підходу BSC та каталогу показників безпеки CISWG / Д.Ю. Пилипенко // Теоретичні і прикладні проблеми фізики, математики та інформатики. IX Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених, 22 квітня 2011 р. – Збірка тез доповідей учасників. Частина 2. – К.: 2011. – С. 45 – 46.

18. Потий А.В. Особенности институциональной модели управления информационной безопасностью / А.В. Потий, Д.Ю. Пилипенко // Новітні технології – для захисту повітряного простору. VIII Наукова конференція, 18-19 квітня 2012 р. – Тези доповідей. – Х.: ХУПС, 2012. – С. 155 – 156.

19. Потий А.В., Пилипенко Д.Ю. Культура информационной безопасности как системная категория / А.В. Потий, Д.Ю. Пилипенко // Інфокомунікації –

сучасність та майбутнє: матеріали другої міжнар. наук.-пр. конф. молодих вчених, 11-12 жовтня 2012 р. – Ч.1. – Одеса, ОНАЗ, 2012. – С. 6 – 8.

20. Потий А.В. Институциональная модель управления информационной безопасностью / А.В. Потий, Д.Ю. Пилипенко // II науково-технічна конференція «Безпека інформаційних технологій» (ITSEC-2012), 24-25 квітня 2012р. – Збірник тез доповідей. – Київ: НАУ, 2012 – С. 10.

АНОТАЦІЯ

Пилипенко Д.Ю. Модель інституціонального управління і метод оцінювання культури інформаційної безпеки. – На правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – Системи захисту інформації. – Харківський національний університет радіоелектроніки, Харків 2013.

Мета дисертаційного дослідження полягає у зменшенні ймовірності виникнення ризиків, які пов'язані з діяльністю персоналу організації, за рахунок розробки моделі інституціонального управління діяльністю із ЗІ та методу оцінювання рівня КІБ.

Вперше побудовано онтологічні моделі предметної галузі інституту та культури інформаційної безпеки, які ґрунтуються на результатах контент-аналізу. Новизна моделей полягає в уточненні розрізненої предметної галузі та формуванні її термінологічного ядра. Моделі описують взаємозв'язки між суб'єктами діяльності із ЗІ (центром та агентом безпеки) та компонентами моделі КІБ.

Подальшого розвитку набула узагальнена модель діяльності із ЗІ, яка розкриває особливості формування керуючих впливів центра безпеки з урахування гіпотези раціональної поведінки агента безпеки. Моделювання інституціонального управління діяльності із ЗІ надає можливість формалізувати процеси прийняття рішень головними суб'єктами діяльності із ЗІ, а саме центром та агентом безпеки.

Вперше запропоновано метод оцінювання рівня КІБ, який ґрунтується на використанні матриць згортання, що дозволяє отримати комплексну оцінку рівня КІБ за рахунок удосконалень механізму комплексного оцінювання на основі матриць згортання та способу формування множини показників КІБ. У рамках механізму комплексного оцінювання на основі матриць згортання запропоновано такі вдосконалення: використання вагових коефіцієнтів, використання мінімальних порогових значень та білінійної інтерполяції

Розроблено програмний засіб у вигляді системи підтримки прийняття рішень, що дозволяє підвищити швидкість прийняття рішень ЛПР, зменшити ймовірність помилки за рахунок часткової автоматизації процедури генерації матриць згортання та ефективної візуалізації отриманих результатів.

Ключові слова: інституціональне управління, захист інформації, культура інформаційної безпеки, комплексне оцінювання.

АННОТАЦИЯ

Пилипенко Д.Ю. Модель институционального управления и метод оценки уровня культуры информационной безопасности. – На правах рукописи.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.21 – Системы защиты информации. – Харьковский национальный университет радиоэлектроники, Харьков 2013.

Цель диссертационного исследования заключается в снижении вероятности реализации рисков безопасности, связанных с деятельностью персонала организации, за счет разработки модели институционального управления и метода оценки уровня КИБ.

Впервые разработаны модели предметной области института и культуры информационной безопасности, которые основываются на результатах контент-анализа. Новизна разработанных моделей заключается в уточнении разрозненной предметной области и формировании ее терминологического ядра. Модели раскрывают взаимосвязи между субъектами деятельности по ЗИ и основными компонентами модели КИБ.

Дальнейшее развитие получила обобщенная модель деятельности по ЗИ, которая раскрывает особенности формирования управляющих воздействий центром безопасности с учетом гипотезы рационального поведения агента безопасности. Моделирование институционального управления деятельности по ЗИ позволило формализовать процессы принятия решений ключевыми субъектами деятельности по ЗИ, а именно центром и агентом безопасности.

Впервые предложен метод оценивания уровня КИБ, который основывается на использовании матриц свертки. Метод позволяет получить комплексную оценку уровня КИБ за счет усовершенствований механизма комплексной оценки и использования способа формирования множества показателей КИБ. В рамках механизма комплексного оценивания на основе матриц свертки предложены следующие усовершенствования: использование весовых коэффициентов для повышения прозрачности процедуры оценивания, минимальных пороговых значений для учета ситуации, когда низкое значение одного из показателей нивелирует высокое значение другого, билинейной интерполяции для избегания необходимости округления значений показателей нижнего уровня и повышения точности итогового результата.

Разработано программное средство в виде системы поддержки принятия решений, использование которого позволяет повысить скорость принятия решений ЛПР, уменьшить вероятность ошибки за счет частичной автоматизации процедуры генерации матриц свертки и автоматизации процедуры свертки непосредственно, эффективной визуализации конечных результатов.

Ключевые слова: институциональное управление, защита информации, культура информационной безопасности, комплексное оценивание.

ABSTRACT

Pilipenko D. Y. **Institutional model of information security management and method of information security culture evaluation**. – Manuscript.

PhD thesis (candidate of engineering science) by specialty 05.13.21 – Information systems security. – Kharkiv National University of Radio Electronics, Kharkiv, 2013.

The purpose of this study considers reduction of information security risks probability caused by personnel activities and behavior by means of development of institutional model of information security management and method of information security culture evaluation. The model and method mentioned improve the quality and precision of control actions performed by agent of management.

The new ontology models of subject domain of information security institution and information security culture are proposed. The novelty of these models consists in development of subject domain terminology core and adjustment of wide and uncoordinated subject domain. The interconnections between the subjects of security activities and main components of ISC are established.

The generalized mathematical model of security activities management received further development as the institutional model of information security activities management. The developed institutional model includes motivational aspect of security activities and contains decision-making model of security center, decision-making model of security agent and evaluation model of ISC.

The new method of complex information security culture evaluation is proposed in context of institutional management. The method mentioned allows complex evaluation of ISC level via the use of evaluation mechanism based on convolution matrices and the set of ISC metrics.

A software tool for ISC level evaluation is proposed as an expert support system. The software tool allows to increase the speed of decision-making process via facilitation of evaluation process, decrease the probability of mistake via partial automation of convolution matrices generation and convolution procedure itself.

Keywords: institutional management, information security, information security culture, complex evaluation.

Відповідальний випусковий В.М. Свищ

Підп. до друку 10.08.13 Формат 60х84 1/16. Спосіб друку – ризографія.

Умов. друк. арк. 1,2. Облік. вид.арк. 1,0. Тираж 100 прим.
Зам № 2-141. Ціна договірна

ХНУРЕ. Україна. 61166, Харків, просп. Леніна, 14

Віддруковано в навчально-науковому
видавничо-поліграфічному центрі ХНУРЕ
61166, Харків, просп. Леніна, 14