на певний прогрес у законодавчій та інституційній сферах, масштаби поширення злочинності та корупції сьогодні загрожують національній безпеці та конституційному ладу України. Діяльність органів виконавчої влади, координація їх зусиль щодо протидії кримінальним проявам є малоефективною, не повною мірою відповідає державним інтересам і вимогам національної безпеки України, не забезпечує ефективного захисту конституційних прав і свобод людини і громадянина, правопорядку в державі», а п. 2 резолютивної частини вказаного Рішення передбачає необхідність належного наукового супроводження процесів подолання відповідних істотних недоліків; подальше дослідження проблем кримінальних загроз національній безпеці та інформаційного аспекту протидії вказаним загрозам є перспективним та актуальним напрямком наукової роботи у сфері забезпечення національної безпеки.

Література: ***1.*** *Рішення РНБО України «Про стан злочинності у державі та координацію діяльності органів державної влади у протидії злочинним проявам та корупції», введене в дію Указом Президента №870/2009 від 27. 10. 2009 р.;* ***2.*** *Закон України «Про Службу безпеки України» від 25. 03. 1992 р.;* ***3.*** *Закон України «Про основи національної безпеки України» від 19. 06. 2003 р.;* ***4.*** *Кримінальний кодекс України від 05. 04. 2001 р.;* ***5.*** *Горшенков Г. Г. Антикриминальная безопасность личности: Дис. ... д-ра юрид. наук : 12. 00. 08 : Ставрополь, 2009. 447 с.;* ***6.*** *Плешаков В. А., Нечевина Н. Д. Криминологическая безопасность в системе общественной безопасности// Предупреждение преступности и обеспечение безопасности в городах: Материалы международной науч.-практ. конф. (7–8 апреля 1999 г.) / Моск. юрид. ин-т МВД России. -М., 1999. -С. 135–144;* ***7.*** *Бабаев М. М., Плешаков В. А. Криминологическая безопасность в системе национальной безопасности (опыт структурного анализа) // Криминологический журнал, 2005, № 7;* ***8.*** *Доктрина інформаційної безпеки України;* ***9.*** *Емелянов Г. В., Стрельцов А. А. Проблемы обеспечения безопасности информационного общества // Информационное общество. 1999. №2. - С. 15–18.;* ***10.*** *Красноступ М. Д. Інформаційна безпека України: сутність та проблеми // Інформаційні технології та захист інформації. – 1999. - №1. - С. 108–110;* ***11.*** *Баранов А. А. Концептуальные вопросы информационной безопасности Украины // Нормативно-правовая база защиты информации: Сб-к материалов. - К., 1997. - С. 53–58;* ***12.*** *Рубан В. Я. Інформаційна безпека України: сутність та проблеми // Стратегічна панорама. - 1998. - № 3. - С. 174;* ***13.*** *Лопатин В. Н. Информационная безопасность России: Автореф. дис…докт. юрид. наук.– СПб., 2000. – 28 с.;* ***14.*** *Шамрай В. О. (n.d./2002). Інформаційна безпека як складова національної безпеки України [WWW документ]. URL http:// www.crime-research.org/ articles.html (08 листопада 2004 року);* ***15.*** *Васенин В. А., Галатенко А. В. Компьютерный терроризм и проблемы информационной безопасности в Интернет // Высокотехнологичный терроризм. Материалы российско-американского семинара РАН в сотрудничестве с Национальными академиями США. Москва, 4–6 июня 2001 г. - М., 2002. - С. 211–225;* ***16.*** *Литвиненко О. В. Інформаційний простір як чинник забезпечення національних інтересів України. - К., 1998. - 50 с.;* ***17.*** *Ліпкан В. Націобезпекознавча парадигма //Право України 2003 рік, №2;* ***18.*** *Данильян О. Г., Дзьобань О. П., Панов М. І. Національна безпека України: структура та напрямки реалізації: Навчальний посібник. - Х.: Фоліо, 2002–285 с;* ***19.*** *Расторгуев С. П. Информационная война. - М.: Радио и связь, 1998. - 415 с.;* ***20.*** *Почепцов Г. Г. Информационные войны. - М.: «Рефл-бук», К.: «Ваклер», 2000. - 567 с.;* ***21.*** *Емельянов Г. В., Ленский В. Е., Стрельцов А. А. Проблемы обеспечения информационно-психологической безопасности России // Информационное общество. - 1999. - № 3. - С. 47–51;* ***22.*** *Крылов В. В. Информация как элемент криминальной деятельности // Вестник Московского университета, Серия № 11 (Право). - 1998. - № 4. - С. 59–63;* ***23.*** *Хананашвили М. М. Информационные неврозы. - М.: Медицина, 1986. – 310 с.;* ***24.*** *Дремин В. Н. Глобализация информационных систем как фактор глобализации преступности // Інформаційні технології та безпека. - Вип. 1. – К., 2002. - С. 56–59;* ***25.*** *Мальцев В. В. Категория «общественно-опасное поведение» и ее уголовно-правовое значение // Государство и право. - 1995. - № 9. - С. 58–60.*

УДК 621.391

СТРУКТУРА ТА МОДЕЛЬ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В РАМКАХ ПРОЦЕСНОГО ПІДХОДУ

Олександр Потій, Анатолій Лєншин, Дмитро Пилипенко
Інститут інформаційних технологій

Анотація: **Запропонована модель управління процесами захисту інформації, що дозволяє впроваджувати у практику захисту інформації вимоги стандарту ISO/IEC 27001. Визначено два контури управління – контур управління за результативністю та контур управління за зрілістю.**

Summary: **Information security processes management model allows to implement security requirements of the ISO/IEC 27001 in practice is proposed. Two control loops based on effectiveness and on maturity are defined.**
*Ключові слова: З***рілість процесів, система управління безпекою інформації.**

I Вступ

Сьогодні методологічну основу управління інформаційною безпекою визначають міжнародні та національні стандарти ISO/IEC 17799:2005, ISO/IEC 27001, ДСТУ ISO/IEC 13335, які в свою чергу враховують вимоги стандартів управління якістю серії ISO 9001:2001 [1]. Як базова концепція побудови системи управління інформаційною безпекою (СУІБ) у міжнародному стандарті ISO/IEC 27001 [2] пропонується концепція Демінга-Шухарата «Plan-Do-Check-Act» (PDCA), яка описується так:

– планування (Plan) – встановлення політики, цілей, процесів та процедур захисту інформації, що є релевантними для управління ризиками інформаційної безпеки та удосконалення діяльності із захисту інформації для досягнення результатів відповідно до загальних стратегій, політики та цілей організації;

– здійснення (Do) – реалізація та впровадження політики безпеки, заходів та процесів (процедур) захисту інформації;

– перевірка (контроль) (Check) – оцінювання та, за можливістю, вимірювання процесів захисту інформації на відповідність політиці безпеки, цілям та практиці захисту, документування результатів контролю;

– дія (Act) – реалізація корегуючих та превентивних заходів, що базуються на результатах внутрішнього аудиту безпеки, аналізу стану інформаційної безпеки та на іншій базі, пов'язаній з безпекою інформації з метою досягнення постійного удосконалення процесів захисту інформації.

У такому контексті цикл PDCA може бути застосований як до кожного окремого процесу захисту інформації, так і до системи процесів у цілому. Використання концепції Демінга-Шухарта [3, 4] дозволяє організації реалізувати процес постійного удосконалення захисту інформації, спрямований на постійне зростання результативності та ефективності захисту інформації. Під управлінням безпекою інформації розумітимемо сукупність дій та заходів, що спрямовані на забезпечення ефективного планування, організації та контролю процесів захисту інформації. Метою управління є досягнення максимального результату від захисту інформації за умовою мінімізації витрат на створення, впровадження та експлуатацію системи захисту інформації.

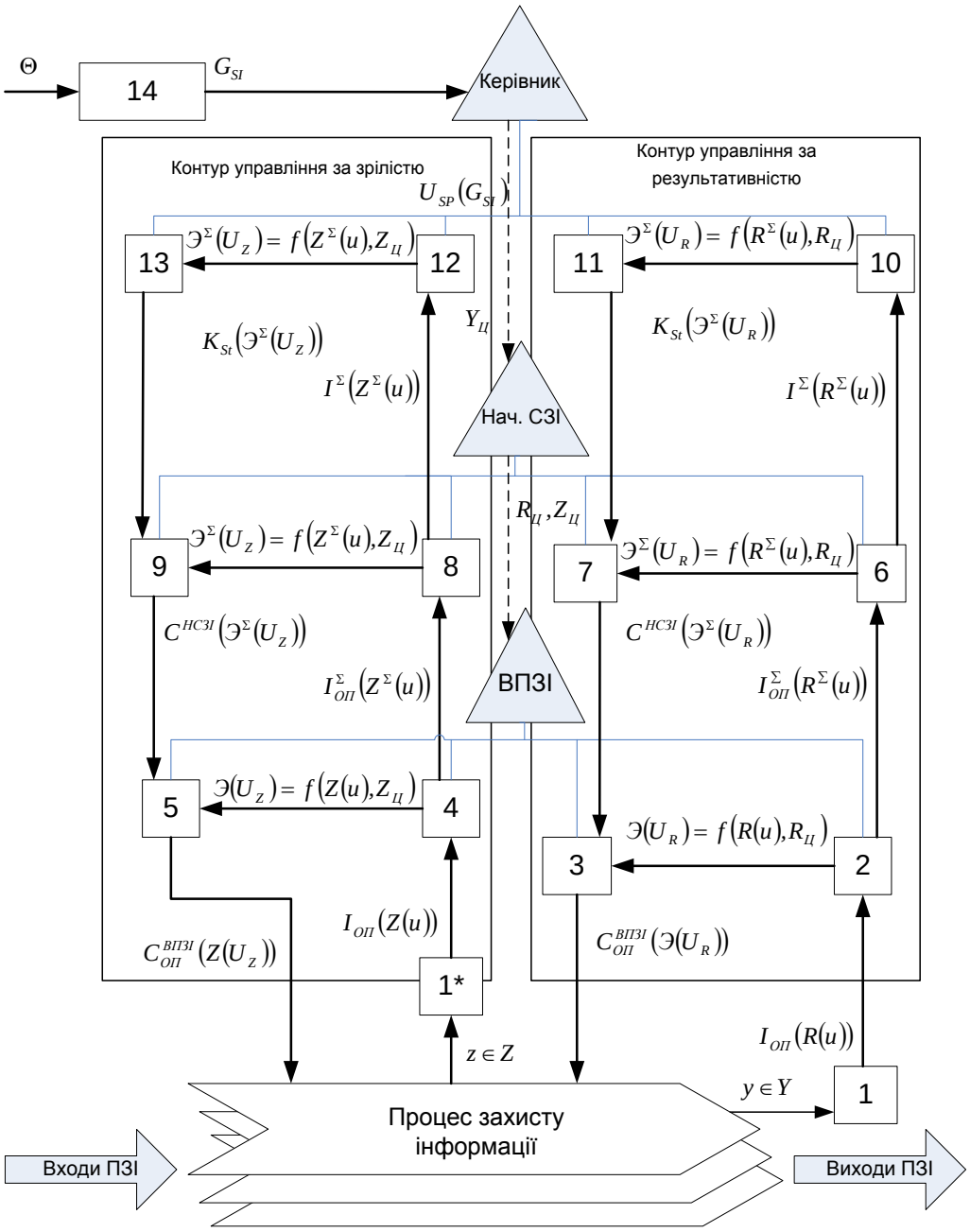
Функції системи управління формулювалися неодноразово. До основних функцій управління відносять функції планування, організації, контролю, координації, мотивації [5 – 7]. Спираючись на класичні підходи до управління можна запропонувати загальну модель управління інформаційною безпекою, яка спирається на функції та задачі управління. З позиції процесного підходу ці функції також необхідні для управління процесом захисту інформації, але вони мають розглядатися у рамках моделі PDCA. Для моделювання СУІБ у роботі використовується модель PDCA та процесна модель діяльності із захисту інформації.

II Структура системи управління захистом інформації в рамках процесного підходу

У рамках процесного підходу *систему управління захистом інформації* (СУЗІ) визначатимемо як сукупність засобів управління захистом інформації, що заснована на виділенні процесів захисту інформації та управління цими процесами за певними правилами, критеріями та методиками.

Структура та модель СУЗІ, що пропонується у роботі, базується на розумінні процесного підходу до управління інформаційною безпекою, який сформульовано у міжнародному стандарті ISO/IEC 27001 [2] та процесного підходу до захисту інформації, що розкрито у цій роботі. Запропонована модель є удосконаленням моделі, що запропонована у роботі [8]. Суть удосконалення полягає у врахуванні вимог стандарту ISO/IEC 27001 (в оригінальній моделі ці вимоги не розглядаються), чіткому виділенні двох контурів управління та формалізації інформаційних потоків. Впровадження запропонованої моделі сприяє підготовці організацій до сертифікації системи управління інформаційної безпеки на відповідність вимогам ISO/IEC 27001 [2]. Загальну структуру СУЗІ наведено на рис. 1. СУЗІ функціонує таким чином.

Керівник організації здійснює аналіз зовнішнього середовища безпеки та стану безпеки в організації (на підприємстві, установі) на основі встановленої множини показників безпеки інформації (блок 14). Це здійснюється в рамках загального аналізу стану організації. З урахуванням відомих факторів керівник розробляє стратегічні цілі в сфері забезпечення безпеки інформації G_{SI} та формує стратегію їх досягнення $U_{SP}(G_{SI})$.



КО – керівник організації; Нач.СЗІ – начальник служби захисту інформації; ВПЗІ – власник ПЗІ;
1 – засоби отримання оперативної управлінської інформації про виконання ПЗІ; 2 – засоби аналізу оперативної інформації щодо ПЗІ власником процесу; 3 – засоби розробки оперативних управлінських рішень власником ПЗІ; 4 – засоби аналізу зрілості ПЗІ власником процесу; 5 – засоби розробки заходів з удосконалення ПЗІ власника процесу; 6 – засоби аналізу оперативної інформації про відхилення під час ПЗІ керівника СЗІ; 7 – засоби розробки оперативних управлінських рішень керівником СЗІ; 8 – засоби аналізу зрілості ПЗІ керівником СЗІ; 9 – засоби розробки заходів з удосконалення ПЗІ керівника СЗІ; 10 – засоби аналізу оперативної інформації про відхилення у ДЗІ керівником організації; 11 – засоби розробки оперативних управлінських рішень керівником організації; 12 – засоби аналізу інформації щодо діяльності із захисту інформації керівником організації; 13 – засоби розробки заходів з удосконалення ДЗІ та приведення її у відповідність до стратегічних цілей організації; 14 – засоби аналізу середовища безпеки.

Рисунок 1 – Структура системи управління захистом інформації в рамках процесного підходу

Після формування стратегії захисту, керівництво формує цільові значення показників безпеки $Y_{Ö}$, яким мають відповідати результати процесів захисту інформації (ПЗІ) та власно самі процеси (показники результативності, економічності, оперативності, зрілості тощо). Інформація щодо значень цільових показників безпеки $Y_{Ц}$ доводиться до керівників підрозділів, начальника служби захисту інформації та власників ПЗІ.

Начальник служби захисту інформації та власники ПЗІ, у свою чергу, здійснюють більш детальне планування своєї діяльності, зокрема визначають детальні показники для своїх ПЗІ та результатів захисту інформації – множину показників результативності та зрілості $R_{Ц}, Z_{Ц}$.

Протягом виконання ПЗІ власник процесу отримує оперативну інформацію про результати захисту інформації $I_{ОП}\left(R(u)\right)$ (блок 1) та проводить її аналіз (блок 2), під час якого формується показник результативності $Э\left(U_R\right) = f\left(R(u), R_{Ц}\right)$. У разі виникнення відхилень, рішення за якими знаходяться в рамках його компетенції, власник ПЗІ розробляє відповідне оперативне управлінське рішення $C_{ОП}^{ВПЗІ}\left(Э\left(U_R\right)\right)$ (блок 3). Якщо рішення з управління ПЗІ не може бути прийнято безпосередньо власником процесу (перевищення повноважень), то оперативна інформація про результати виконання ПЗІ та відхилення $I_{ОП}^{\Sigma}\left(R^{\Sigma}(u)\right)$ надаються керівнику вищого рівня (начальник служби захисту інформації).

Власник ПЗІ періодично виконує аналіз зрілості процесу захисту інформації на основі інформації про стан процесу $I_{ОП}\left(Z(u)\right)$ (блок 1*). Шляхом порівняння поточного профілю зрілості $Z(u)$ з цільовим $Z_{Ц}$ власник ПЗІ отримає показник зрілості $Э\left(U_Z\right) = f\left(Z(u), Z_{Ц}\right)$ (блок 4) та розробляє заходи щодо його вдосконалення $C_{ОП}^{ВПЗІ}\left(Z\left(U_Z\right)\right)$ (блок 5). У разі, якщо для виконання заходів достатньо ресурсів та повноважень, які надано власникові ПЗІ, заходи, що розроблені, виконуються у встановлені ним терміни. Якщо для виконання заходів потрібні додаткові ресурси та повноваження, то документально оформлені, економічно обґрунтовані описи заходів $I_{ОП}^{\Sigma}\left(Z^{\Sigma}(u)\right)$, що плануються, доповідаються власником ПЗІ керівникам вищих рівнів. Під час розрахунку економічної ефективності заходів власник ПЗІ має оцінити можливі втрати та рівень ризиків для організації у разі невиконання заходів.

Начальник СЗІ є власником декількох процесів. Це означає, що він здійснює управління декількома ПЗІ, для кожного з яких призначений свій власник.

Кількість ланок управління залежить від масштабів та специфіки основної діяльності організації. Виділення ПЗІ та призначення власників ПЗІ здійснюється на основі аналізу організаційної структури служби захисту інформації, організаційної структури організації в цілому та специфіки діяльності організації. Начальник СЗІ здійснює аналіз результатів виконання ПЗІ (блок 6) на основі наданої інформації $I_{ОП}^{\Sigma}\left(R^{\Sigma}(u)\right)$ та формує узагальнений показник результативності $Э^{\Sigma}\left(U_R\right) = f\left(R^{\Sigma}(u), R_{Ц}\right)$. На основі цього показника він розробляє та приймає оперативні управлінські рішення $C^{НСЗІ}\left(Э^{\Sigma}\left(U_R\right)\right)$ з управління ПЗІ з урахуванням своїх повноважень та відповідальності (блок 7). Ці рішення носять також і координаційний характер.

Періодично начальник СЗІ здійснює аналіз зрілості ПЗІ (блок 8) на основі комплекту звітних документів (довідки, протоколи, звіти тощо), які він отримує від власників кожного ПЗІ, а також іншої необхідної інформації – $I_{ОП}^{\Sigma}\left(Z^{\Sigma}(u)\right)$. На основі цих даних начальник СЗІ формує узагальнений показник зрілості діяльності із захисту інформації $Э^{\Sigma}\left(U_Z\right) = f\left(Z^{\Sigma}(u), Z_{Ц}\right)$.

Начальник СЗІ розглядає заходи з удосконалення ПЗІ (напрямку діяльності), що вимагають виділення додаткових ресурсів та визначає доцільність їх виконання. У разі наявності достатніх повноважень та ресурсів, начальник СЗІ приймає рішення про впровадження відповідних заходів $C^{НСЗІ}\left(Э^{\Sigma}\left(U_Z\right)\right)$ та проводить відповідну роботу (). У іншому випадку, начальник СЗІ подає опис заходів $I^{\Sigma}\left(Z^{\Sigma}(u)\right)$ на розгляд керівнику організації.

Керівник організації на основі даних щодо результативності $I^{\Sigma}\left(R^{\Sigma}(u)\right)$ та зрілості $I^{\Sigma}\left(Z^{\Sigma}(u)\right)$ діяльності із захисту інформації формує узагальнені показники результативності захисту інформації

$\Theta^{\Sigma}(U_R) = f(R^{\Sigma}(u), R_{Ц})$ та функціональних можливостей організації в сфері захисту інформації $Z^{\Sigma}(U_Z) = f(Z^{\Sigma}(u), Z_{Ц})$. На основі цих показників вище керівництво формує відповідні стратегічні рішення $K_{St}(\Theta^{\Sigma}(U_R))$ та $K_{St}(\Theta^{\Sigma}(U_Z))$, які носять здебільшого координаційній характер та впливають на стратегічні цілі в сфері забезпечення інформаційної безпеки.

Таким чином, у системі управління захистом інформації формується два контури управління. Перший контур управління – це управління за результатами захисту інформації. Рішення у цьому контурі управління приймаються на основі аналізу результативності процесів захисту інформації. Критерії прийняття рішення спираються на порівняння поточних результатів захисту інформації $R(u)$ з тими, що вимагаються $R_{Ц}$. Другий контур управління – це управління зрілістю процесів захисту інформації, діяльності із захисту інформації в цілому. Рішення в цьому контурі управління приймається на основі аналізу та порівняння поточного профілю зрілості процесів захисту інформації $Z(u)$ з цільовим профілем зрілості $Z_{Ц}$.

III Модель управління процесом захисту інформації

На рис. 2 наведено блок-схему моделі управління процесом захисту інформації, що розроблена з урахування вимог міжнародного стандарту ISO/IEC 27001 [2]. Систему управління ПЗІ, яку наведено на рис. 2, можна розглядати як дворівневу багатоцільову систему (за класифікацією Месаровича-Мако-Такахара [9]). Спираючись на основні положення теорії багаторівневих ієрархічних систем надамо формалізацію системи управління ПЗІ.

На рис. 3 наведено блок-схему дворівневої системи управління ПЗІ, що відповідає моделі (рис. 2) з деяким узагальненням.

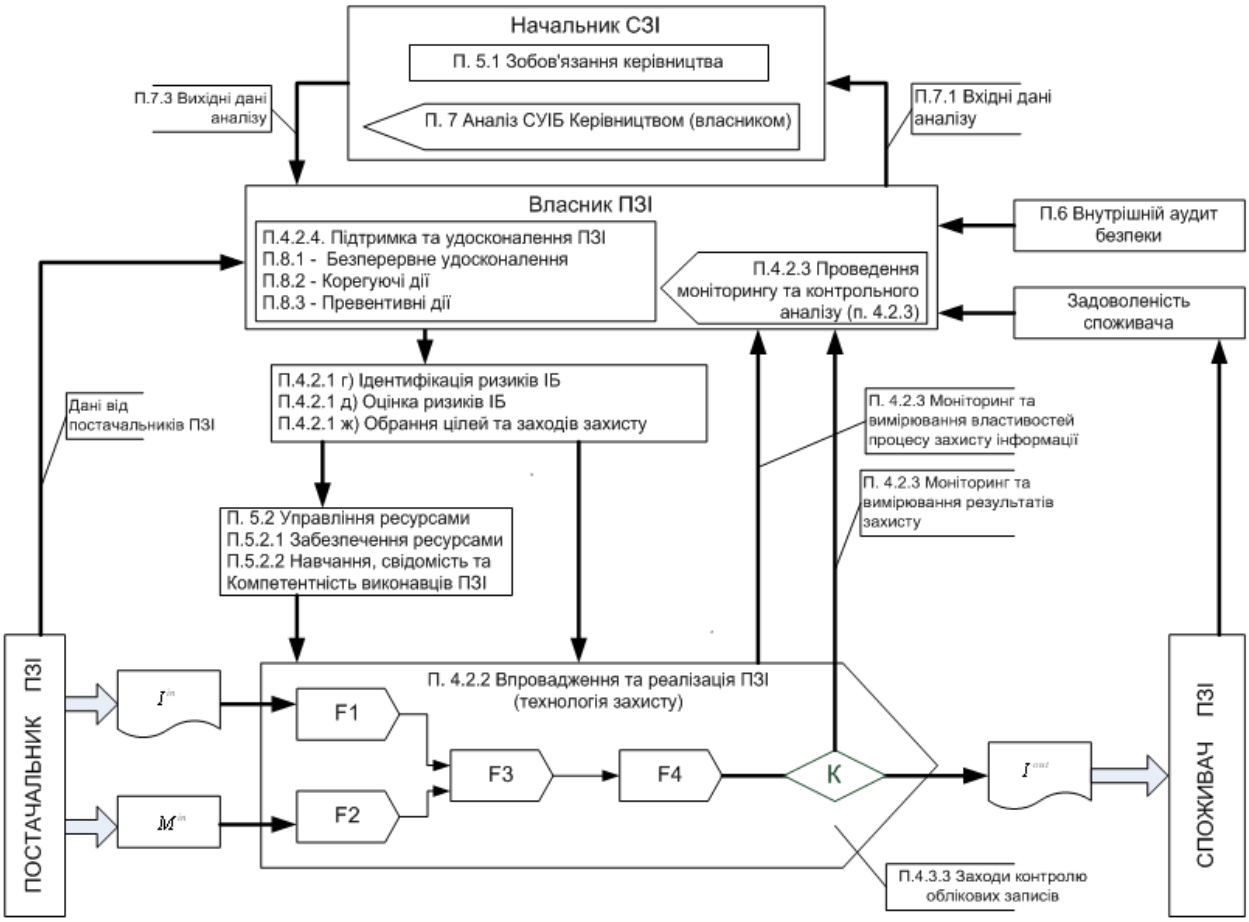


Рисунок 2 – Блок-схема системи управління ПЗІ (з урахуванням вимог міжнародного стандарту ISO/IEC 27001)

Окремі блоки зображують підсистеми, а їх взаємне розташування відображує ієрархічну структуру управління. Система управління, що наведена на рис. 3, складається з таких підсистем:

– система управління вищої ланки C_0 (координуюча система або координатор) – система, яка є сферою повноважень вищого керівництва (начальник служби захисту або керівник організації);

– локальні системи управління (системи управління нижчої ланки управління) $C_1, C_2, ..., C_n$, які є сферою повноважень власника (власників) ПЗІ. Такими системами можуть бути система планування ПЗІ, система управління зрілістю, система управління ризиками, система удосконалення ПЗІ, система управління ресурсами ПЗІ, система управління якістю робіт тощо;

– процес захисту інформації P, що управляється.

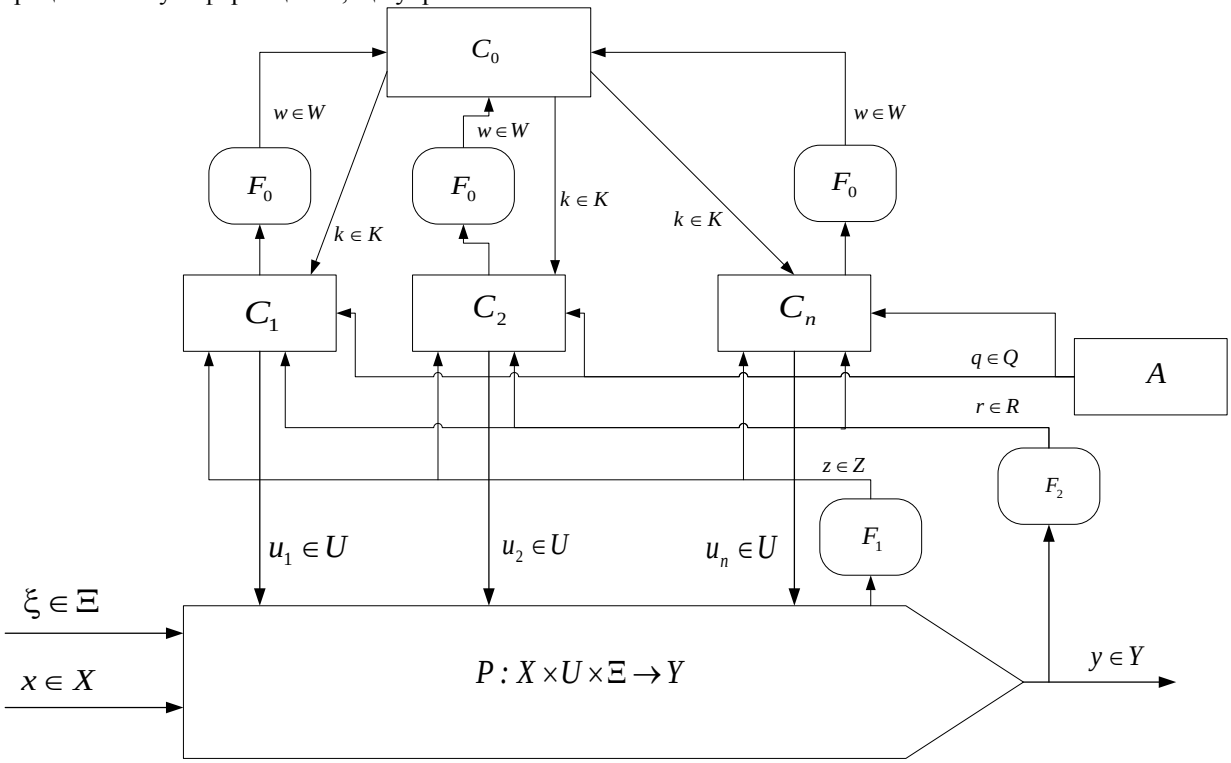


Рисунок 3 – Модель системи управління процесом захисту інформації

Між підсистемами визначено два види вертикальної взаємодії. Перший вид – це передача до низу командних сигналів:

– сигналів управління u – сигнали від локальних систем управління $C_1, C_2, ..., C_n$ власника процесу безпосередньо до процесу P;

– сигналів координації k - сигнали від координатора C_0 до локальних систем управління $C_1, C_2, ..., C_n$.

Другий вид взаємодії – це передача інформаційних сигналів зворотного зв'язку від об'єкта управління до підсистем управління, а саме:

– інформаційних сигналів z та r від процесу P до локальних систем управління $C_1, C_2, ..., C_n$;

– інформаційних сигналів w від локальних систем управління $C_1, C_2, ..., C_n$ до координатора C_0.

Процес захисту інформації P розглядатимемо як функціональну систему, на вхід якої поступають такі сигнали:

– сигнал управління $u \in U$, де U – множина сигналів управління;

– вхідний інформаційний потік $x \in X$, де X – множина вхідних інформаційних об'єктів, що підлягають перетворенню під час виконання процесу (входи процесу);

– сигнали зовнішніх впливів ξ, $\xi \in \Xi$.

На виході процесу формується потік вихідних інформаційних об'єктів $y, y \in Y$ (вихід процесу). Тоді процес P можна подати у вигляді відображення:

$$P : X \times U \times \Xi \to Y . \quad (1)$$

Множину сигналів управління U доцільно подати у вигляді декартового добутку n множин $U = U_1 \times U_2 \times ... \times U_n$, оскільки кожна локальна система управління $C_i, i = \overline{1,n}$ має повноваження обирати *i*-ту компоненту $u_i \in U_i$ сигналу управління і, таким чином, впливати на процес захисту інформації.

Кожну локальну систему управління $C_i, i = \overline{1,n}$ розглядатимемо як систему типу «вхід-вихід». До системи C_i поступають такі сигнали:

– командний сигнал координації $k, k \in K$ від координатора C_0;

– інформаційні сигнали $z, z \in Z$ та $r, r \in R$ (сигнали зворотного зв'язку) від P;

– інформаційний сигнал $q, q \in Q$ – результати аналізу задоволеності зацікавлених у безпеці сторін та результати зовнішнього аудиту безпеки.

Виходом локальної системи управління C_i є командний сигнал управління u_i, що обирається з множини $U_i \in U$. Таким чином, система C_i реалізує відображення:

$$C_i : K \times Z \times Q \times R \to U_i . \quad (2)$$

Якщо відображення (2) подати у функціональному вигляді, то ми отримаємо модель управління ПЗІ та критерії управління.

Координатор C_0 здійснює функцію координації. Координація – це сфера діяльності або задача системи управління вищої ланки, яка здійснюється з метою забезпечення узгодженого функціонування систем управління нижчої ланки [9]. На вхід координатора C_0 поступає інформаційний сигнал $w, w \in W$ від локальних систем управління $C_1, C_2, ..., C_n$ та використовується для формування сигналів координації $k, k \in K$. За допомогою сигналів координації координатор C_0 впливає на локальні системи управління $C_1, C_2, ..., C_n$ та координує їх функціонування. Таким чином, координатор C_0 реалізує відображення:

$$C_0 : W \to K . \quad (3)$$

Уточнимо характер інформаційних сигналів у системі управління. Сигнали зворотного зв'язку z_i, що поступають на вхід локальних систем управління $C_1, C_2, ..., C_n$, містять інформацію про стан процесу захисту інформації P. У сукупності сигнали z_i – це параметри, що характеризують зрілість процесу. Ці сигнали пов'язані функціональною залежністю з сигналом управління u, факторами зовнішнього впливу ξ та факторами внутрішнього впливу на зрілість процесу φ (більш детально у роботі [10]). Цю залежність подаватимемо у вигляді відображення:

$$F_1 : U \times \Xi \times \Phi \to Z . \quad (4)$$

Сигнал зворотного зв'язку $r \in R$ містить інформацію відносно результатів процесу захисту інформації P. Ці сигнали пов'язані функціональною залежністю з сигналом управління $u \in U$, станом процесу $z \in Z$, входом $x \in X$ та виходом $y \in Y$ процесу. Цю залежність подаватимемо відображенням:

$$F_2 : U \times X \times Z \times Y \to R . \quad (5)$$

Інформаційний сигнал $w \in W$, що поступає каналами зворотного зв'язку від локальних систем управління $C_1, C_2, ..., C_n$ до координатора C_0, містить інформацію відносно поведінки локальних систем управління. Цей сигнал задається відображенням

$$F_0 : Z \times U \times R \times K \to W . \quad (6)$$

тобто w є функцією від сигналу координації $k \in K$, інформаційних сигналів зворотного зв'язку $z \in Z$ та $r \in R$, сигналу управління $u \in U$.

Вирази (1) – (6) по суті складають математичну модель управління процесом захисту інформації. Математична модель є заданою, якщо визначено всі її елементи, тобто всі множини командних та інформаційних сигналів – X, Y, Z, R, W, U, фактори впливу – Ξ, Φ, та оператори відображень (функціональних перетворень) – $P, C_0, C_i, F_0, F_1, F_2$. В цій моделі, з точки зору її реалізації, значна увага приділяється експертним судженням та оцінкам. У такому контексті виникають такі задачі.

1. Прийняття управлінських рішень на рівні локальних систем управління $C_1, C_2, ..., C_n$ (формування сигналу управління $u \in U$) та на рівні координатора C_0 (формування сигналу координації $k \in K$).

2. Вироблення узгодженої оцінки результативності захисту інформації $\hat{r} = G_R(u, x, z, y)$ та зрілості процесу захисту інформації $\hat{z} = G_Z(u, \xi, \varphi)$.

3. Оцінювання вагомості показників зрілості z та результативності r.

4. Побудова та ідентифікація моделей походження даних для оцінювання зрілості $G_Z(\bullet)$ та результативності $G_R(\bullet)$.

5. Оцінка ефективності управління ПЗІ.

IV Висновок

Впровадження вимог сучасних міжнародних стандартів з управління інформаційною безпекою вимагає розроблення та дослідження моделей системи управління. Модель системи управління, що запропонована в роботі, може виступати основою для впровадження в практику захисту інформації вимог стандарту ISO/IEC 27001. Відмінною рисою моделі є виділення двох контурів управління – контуру управління за результативністю та контуру управління за зрілістю. Така структура управління дозволяє контролювати як результати виконання заходів захисту, так і якість (ефективність) досягнення цих результатів. Система управління процесом захисту інформації може розглядатися як дворівнева багатоцільова система, формалізацію якої надано вище. Розроблення моделі дало змогу сформулювати задачі управління, які мають розв'язуватися під час прийняття управлінських рішень.

Отримані моделі є розвитком теорії захисту інформації у напрямку моделювання управління інформаційною безпекою.

Перспективними напрямками досліджень є вирішення задач вироблення узгодженої оцінки результативності захисту інформації на різних ланках управління, а також оцінки рівня зрілості процесів захисту інформації, що спирається на сукупність кількісних показників зрілості.

Література: ***1.*** *ISO 9001:2008. Quality management systems – Requirements* ***2.*** *ISO/IEC 27001:2005. Information technology. Security techniques. Information security management systems. Requirements* ***3.*** *Деминг В. Едвард. Выход из кризиса. – Тверь: Альба. 1994.* ***4.*** *Москвин В. А. Управление качеством в бизнесе: Рекомендации для руководителей предприятий, банков и риск-менеджеров. – М.:Финансы и статистика, 2006. – 384 с.* ***5.*** *Бинкин Б. А. Эффективность управления: наука и практика. – М.:Наука, 1982.* ***6.*** *Теория систем и методы системного анализа в управлении и связи/ В. Н. Волкова, В. А. Воронков, А. А. Денисов и др.- М.: Радио и связь, 1983.* ***7.*** *Клиланд Д., Кинг В. Системный анализ и целевое управление. – М.: Сов. радио, 1974.* ***8.*** *В. Г. Елиферов, В. В. Репин. Бизнесс-процессы. Регламентация и управление. – М. Инфра-М, 2005. – 319 с.* ***9.*** *М. Месарович, Д. Мако, И. Такахара. Теория иерархических многоуровневих систем – М.:Мир, 1973. – 344 с.* ***10.*** *Потій О. В. Сутність категорії „зрілість" та змістовна модель зрілості процесів захисту інформації//Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. Т.5, 2006. - № 1. – С. 139-147.*

УДК 621.327.12

СИНЕРГЕТИЧЕСКИЙ ПРОЦЕСС ПЕРЕДАЧИ ЭНЕРГИИ РЕЧЕВОГО СИГНАЛА

Владимир Журавлёв
Запорожский национальный технический университет

Анотація: **Запропонована математична модель генерації та прийому мовного сигналу (МС), яка пояснює протиріччя адекватності сучасних теорій мовнослухового процесу. Модель базується на**