УДК 004.056.53(045)

Тупкало В. М.
д-р техн. наук, проф.,
професор кафедри кібербезпеки, інформаційних технологій та економіки
Київський університет інтелектуальної власності та права
Київ, Україна
ORCID: 0000-0002-6594-530X

МЕТОДОЛОГІЧНІ ЗАСАДИ СИНТЕЗУ СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Сучасний етап розвитку інформаційної безпеки потребує комплексного підходу до розробки та впровадження методів і засобів захисту ресурсів підприємств критичної інфраструктури (ПКІ) держави як на технічному, так і організаційному рівні. Для сучасних ПКІ актуальною стає розробка методологічних засад системного впровадження системи менеджменту інформаційної безпеки підприємств критичної інфраструктури (СМІБП) на основі системних процесно-орієнтованого та ризик-орієнтованого підходів шляхом комплексного об'єднання вимог двох міжнародних стандартів ДСТУ 9001 «Системи управління якістю. Вимоги» та ДСТУ ISO/IEC 27001 «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги». Тому можна стверджувати, що інжиніринговий синтез СМІБП – це не лише технічна, але й організаційно-управлінська задача, що вимагає застосування системного підходу, заснованого на управлінні ризиками на циклах постійного поліпшення згідно вимог стандарту ДСТУ ISO/IEC 27001. В першу чергу це стосується розв'язання задачі виявлення множини об'єктів інформаційної безпеки у системі управлінських та технологічних процесів загальної системи менеджменту підприємства (СМП) [1].

Стосовно створення СМІБП на засадах системного процесно-орієнтованого підходу пропонується в першу чергу керуватися двома логічно пов'язаними концептуальними твердженнями.

Твердження 1. СМІБП є невід'ємною складовою частиною загальної системи СМП і тому базовою основою створення СМІБП повинна бути структурно – логічне взаємовідношення між пірамідами менеджменту СМП та СМІБП згідно моделі рис. 1).

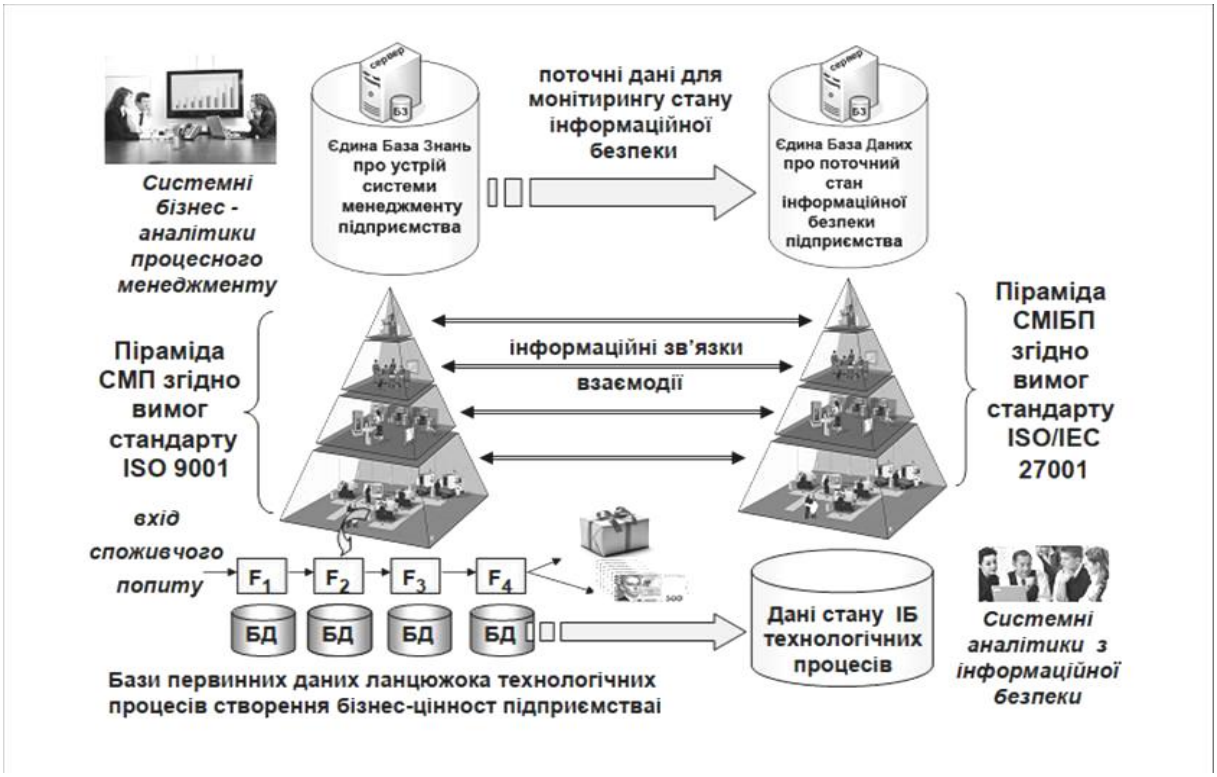

Рисунок 1 – Концептуальна модель створення СМІБП (авторська модель)

Твердження 2. Основна мета створення СМІБП – це не просто «захистити комп'ютери», а забезпечити безперервність бізнесу та мінімізувати збитки шляхом запобігання інцидентам безпеки або зменшення їхнього впливу на всіх рівнях загальної СМП щодо захисту шістьох ключових властивостей інформації (модель безпеки інформації «Гексада Дона Паркера» [2, с. 13])

Доведено, що в СМП, насамперед, критичним є кортеж з чотирьох технологічних бізнес-процесів F_1, F_2, F_3, F_4 ланцюжка створення споживчої цінності (товар / послуга – виручка). Тому на основі інформаційної сутності цих бізнес-процесів пропонується насамперед формувати перелік (модель) первинних дій з інформаційної безпеки щодо ланцюжків створення цінності первинних облікових даних за видами операційної діяльності, а потім – створення моделі управлінської інформаційної цінності для ланцюжка прийняття управлінських рішень підприємства згідно рівнів піраміди менеджменту підприємства [3, с.24]. Наступним етапом рішення задачі синтезу СМІБП є аналітичні дослідження з ідентифікації інформаційних активів (ІТ- активів) щодо рівнів піраміди менеджменту СМП та аналіз їх можливих видів загроз (формування матриці «ІТ- активи - види ризиків») з використанням кількісних методів оцінки ризиків інформаційної безпеки (вартість збитків, частота реалізації загрози для точного розрахунку ризику) на всіх рівнях СМП. У контексті сутності поняття «вартість засобів інформаційного захисту» в доповіді зазначено, що ця вартість не повинна перевищувати вартості інформації, що захищається або інших ресурсів захисту- апаратних та програмних. Із цього приводу запропоновано наступне уточнююче твердження.

Твердження 3. Сукупні витрати на функціонування СМІБП у частині її невід'ємної інженерно-технологічної складової «система захисту інформації» (СЗІ) повинна бути нижче вартості ІТ- ресурсів інформаційного поля підприємства, що захищаються. Це дає підставу у методологічному плані відрізнити між собою сутності понять СМІБП та СЗІ, хоча вони тісно пов'язані. Тобто не коректно вважати ці поняття синонімами в інтересах забезпечення якості синтезу СМІБП у цілому. Цьому є просте пояснення: система захисту інформації (СЗІ) – це «що» і «як» ми захищаємо (технічна сторона), а система менеджменту інформаційної безпеки підприємства (СМІБП) – це «навіщо», «хто» і «як цим керувати» (управлінська сторона).

З метою детального тлумачення різниці понять СМІБП та СЗІ пропонуються наступні визначення**.**

Визначення 1. Система захисту інформації (СЗІ) – це сукупність технічних, програмних та криптографічних засобів (технології та інженерія), спрямованих на безпосередній захист даних з метою побудови «стіни захисту», яка не дозволить зловмиснику викрасти або знищити дані.

Визначення 2. Інжиніринг системи менеджменту інформаційної безпеки (СМІБ) – це комплексний процес проектування, впровадження та супроводу механізмів захисту даних, що базується на міжнародних стандартах (зокрема ISO/IEC 27001). Тобто, це не просто встановлення комп'ютерних антивірусних програм, а створення живої екосистеми, де технології, процеси та люди працюють злагоджено для мінімізації інформаційних ризиків (кіберризиків).

Тобто відносно взаємодії СМІБП та СЗІ можна зазначити, що СМІБП – це «мозок» всієї діяльності підприємства з інформаційної безпеки (кібербезпеки). Вона визначає, які дані є найціннішими і які загрози для них існують. На основі цього СМІБП «дає команду» побудувати СЗІ певного рівня інформаційного захисту. При цьому не відкидається ситуація: можна мати чудову СЗІ (наприклад, найкращі фаєрволи), але без СМІБП вона буде неефективною. Наприклад, якщо працівник запише пароль від суперзахищеної системи на стікері та наклеїть його на свій монітор ПК – це провал СМІБП незважаючи на ідеальну технічну систему СЗІ.

У контексті наведеного вище принципу побудови СМІБП «адекватність (розумна достатність) витрат» у разі реалізації стратегії ризик - орієнтованого проактивного підходу до захисту інформації необхідно мати механізм проведення економічного обґрунтування (оцінювання) витрат на інвестиції у систему СЗІ. Для цього пропонується використовувати методику економічного обґрунтування витрат (інвестицій) у систему СЗІ за показником окупності інвестицій у інформаційну безпеку ROSI (Return on Security Investment) [4].

Список використаних джерел

1. Тупкало В. М. Бізнес - інжиніринг сучасних процесно- орієнтованих підприємств: монографія. Київ. ДУТ, 2016. 281 с.

2. Комплексна безпека інформаційних мережевих систем: навчальний посібник / Укладачі: А.Г. Микитишин, М.М. Митник, О.С. Голотенко, В.В. Карташов. Тернопіль: ФОП Паляниця В.А., 2023. 324 с.

3. Тупкало В. М. Системний підхід і нотація TBPN опису бізнес- процесів об'єктів критичної інфраструктури: монографія. Київ: КУІВтаП НУ «ОЮА», 2024. 91 с.

4. Тупкало В. М. Побудова механізму процесно – орієнтованого контролінгу економічної стійкості підприємства: Київ; . Зб. наук. пр. Державного економіко-технологічного університету транспорту. Серія «Економіка і управління». Вип. 31, 2015. С. 295-306.