УДК 658.336.8

О.Г. Тімінський *к.т.н. доцент.*
Київський національний університет будівництва і архітектури

ІНФОРМАЦІЙНИЙ ЗАХИСТ УПРАВЛІНСЬКИХ ТА ТЕХНОЛОГІЧНИХ СИСТЕМ ВІД ЗОВНІШНІХ НЕГАТИВНИХ ВПЛИВІВ В СУЧАНОСМУ СЕРЕДОВИЩІ

Постановка проблеми. Сучасні системи управління в будівництві та інших технологічно орієнтованих галузях, як правило, інтегрують управлінську (АСУ, управління проектами) і технологічну (АСУТП) складову. Основою їх інтеграції є сучасні комп'ютеризовані інформаційно-аналітичні системи підтримки прийняття рішень (КІАС ППР). І якщо в технологічних підсистемах інформаційна складова все більше зміщується у бік звільнення людини від управління, а також від прийняття рішень, заміни її автоматичними системами, то у системах організаційного управління навпаки, інформаційні системи, вдосконалюючись, все більше підкреслюють роль людини у прийнятті остаточних рішень і у аналітичній обробці запропонованої системою інформації.

Управлінські рішення на основі варіантів, які розробляє КІАС ППР, є помірно чутливими до самих запропонованих варіантів, корелюють зі ступенем технологічно-управлінської підготовки особи, що приймає рішення (ОПР), і надчутливі до вихідних даних, на основі яких робляться подальші технологічно-управлінські висновки.

А отже, актуальною видається задача забезпечення адекватності і оновлення цих даних, яка може бути забезпечена двома функціями – ефективним моніторингом і надійним захистом систем від зовнішніх атак. В цій статті ми зупинимося на другій функції.

Невирішена раніше частина проблеми. В науковому і практичному аспекті організаційні і технологічні інформаційні системи, до яких входить і КІАС ППР, розглядаються, як правило окремо [1-3], тому що належать до компетенції різних наукових напрямків, і, в той же час, практично зовсім не розглядається можливість і не розробляється відповідний методологічний інструментарій інтеграції цих систем в єдину управлінсько-технологічну інформаційну систему управління. Цьому питанню і буде присвячена стаття.

Мета роботи. Запропонувати підхід до аналізу комбінованих управлінсько-технологічних систем і розробки відповідних систем захисту.

Основний матеріал дослідження. Інформаційний простір виробничої організації, що має два рівні – технологічний і управлінський, має передбачати вирішення наступних задач:

1) інтеграцію технологічної і управлінської компоненти у систему вищого рівня – об'єднану інформаційну систему управління (ОІСУ);
2) розробку інтегрованих процесів управління;
3) організаційну трансформацію виробничої організації;
4) захист ОІСУ;
5) розробку напрямків і методик розвитку ОІСУ.

Етапи життєвого шляху системи захисту інформації згідно [2] включають чотири етапи, що наведені нижче.

Етап 1. Визначення вимог і проектування системи захисту інформації.

Етап 2. Експлуатація системи захисту інформації

Етап 3. Супровід системи захисту інформації.

Етап 4. Парирування інцидентів.

З цього переліку можна зробити висновок, що етап 1 можна віднести до фази планування, етапи 2-4 – до фази реалізації захисту. Враховуючи це, а також інтеграційну складову ОІСУ, можна запропонувати концептуальну схему реалізації системи захисту ОІСУ (рис. 1).

Слід зазначити, що згідно такого підходу етапи фази реалізації захисту здійснюються паралельно.

Аналізуючи запропонований підхід, можна зробити висновок, що методологічно найбільш важливим етапом є етап 1, оскільки реалізація етапів 2-3 потребує *не науково-методологічної бази*, яку якраз закладає етап 1, *а виконавської дисципліни і кваліфікованості персоналу*, що буде реалізовувати захист, експлуатуючи і супроводжуючи систему, при цьому парируючи інциденти – тобто реалізуючи діяльність по втіленню принципів, законів, моделей, методів і методологій захисту у конкретній ОІСУ, що розроблюються на етапі 1.

Отже, розглянемо детальніше перший етап. Для здійснення ефективного захисту необхідно розробити адекватну його концепцію, що б полягала у максимальному врахуванні усіх можливіх ризиків, передбачаючих впливи оточення на ОІСУ.

Оскільки ОІСУ поєднує управлінську і технологічну складові, логічно розраховувати ризики кожної підсистеми, визначаючи технологічну і управлінську складові ризиків.

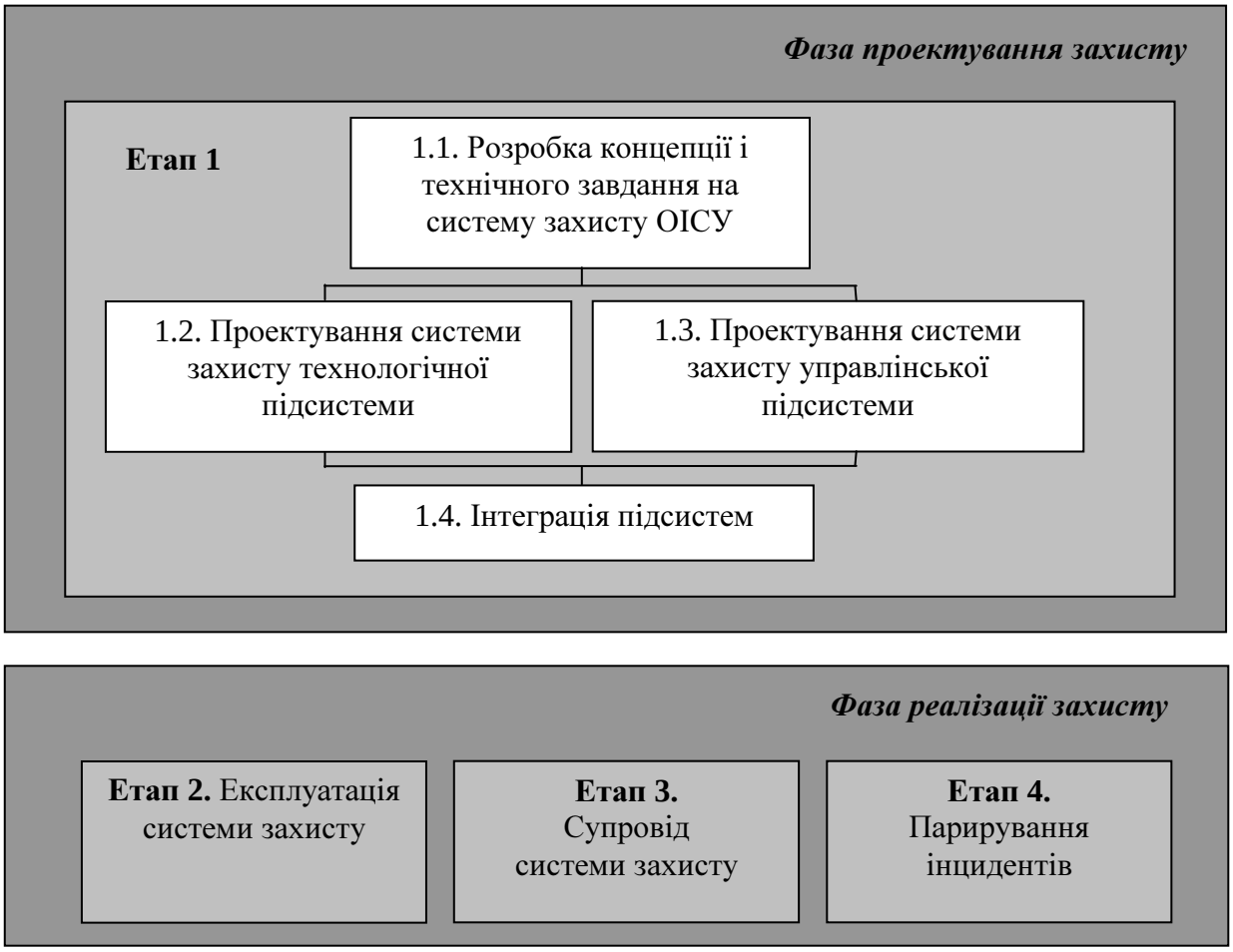

Рис. 1. Життєвий цикл системи захисту ОІСУ

Технологічну складову загального ризику пропонується розраховувати наступним чином:

$$R_t = P_t^{загр} \cdot P_t^{враз} \cdot C^{втрат},$$

де R_t - технологічний ризик;

$P_t^{загр}$ - ймовірність загрози технологічній підсистемі;

$P_t^{враз}$ - ймовірність виникнення вразливості системи відповідній загрозі;

$C^{втрат}$ - рівень втрат від ризику.

При цьому ***загрозою*** вважатимемо сукупність умов, що можуть стати чинником порушення цілісності, доступності або конфіденційності технологічної підсистеми, а ***вразливістю*** – слабкі сторони у системі захисту, що робить можливою реалізацію загрози.

Управлінська складова R_m загального ризику вираховується аналогічно:

$$R_m = P_m^{загр} \cdot P_m^{враз} \cdot C^{втрат}.$$

В інтегрованій системі кожен технологічний ризик викликає певний визначенний управлінський ризик таким чином, що їх взаємозалежність може носити функціональний характер. Але, разом з тим, існують взаємовпливи цих ризиків таким чином, що при спільному виникненні пари таких ризиків вони можуть утворювати деяку нову якість впливу з причини синергетичної взаємодії.

Отже, можемо визначити, що сумарний ризик ОІСУ складатиме:

$$R^{\Sigma} = F^{h}(\sum_{i} f_i^1(R_i^t, R_i^m) + f_j^2 \sum_{j} (R_j^{t,m}))\,,$$

де f_i^1 - функція синергетизму споріднених пар ризиків;

f_j^2 - функція синергетизму окремих ризиків;

F^h - функція синергетизму множини ризиків;

R^{Σ} - загальний ризик ОІСУ.

На основі аналізу ризиків розроблюється концептуальна схема захисту і далі формується технічне завдання (ТЗ) на проектування системи захисту.

Важливо також передбачати різні джерела ризиків та різні їх типи, а також типи елементів оточення, що можуть нейтрально, позитивно або негативно впливати на ОІСУ [4,5].

Інші підетапи етапу 1, як і етапи 2-4 полягають у реалізації концепції захисту. Однак, ефективна реалізація концепції неможлива без планування, формування графіку, бюджету, залучення ресурсів, моніторингу, і, особливо – без команди професіоналів в управлінні і технологічних процесах. А отже, формування концепції захисту вимагає розробки методологічної бази, тоді як реалізація захисту вимагає використання проектного підходу для успішного функціонування ОІСУ.

Отже, задачі 1 і 4, що визначені вище (інтеграція і захист), реалізовуватиме інформаціна система захисту. Задачі розробки інтегрованих процесів управління і організаційної трансформації виробничої організації (задачі 2 і 3) здатна вирішити команда управлінців, що компетентна в управлінні відповідними проектами, а задачу 5 щодо розробки напрямків і методик розвитку ОІСУ повинна вирішувати наука управління проектами.

Висновки і перспективи подальших досліджень. Втілення систем захисту ОІСУ у конкретних організаціях вимагатиме:

1) реалізації проектного підходу;
2) визначення специфічних характеристик об’єднаного управлінсько-технологічного об’єкту управління;

3) формулювання особливостей захисту для систем різної топології, походження, призначення;
4) віднайдення загальних закономірностей і тенденцій поведінки джерел негативного впливу, її розвитку і вдосконалення – з метою актуалізації системи захисту і забезпечення її можливості більшість атак на ОІСУ відводити з використанням принципу проактивності, тобто реалізуючи упереджуючи дії, не допускаючи перетворення ризиків (тобто потенційних проблем) на реальні проблеми.

Саме ці напрямки можна вважати перспективними для розвитку і побудови ефективних, актуалізуємих, сучасних, надійних і гнучких систем захисту об'єднаних інформаційних систем управління. Отже, ці напрямки потребують розробки відповідної методологічної бази і можуть розглядатися як перспективні з точки зору подальших досліджень систем захисту ОІСУ.

Список літератури:

1. *Бушуева Н.С.* Модели и методы проактивного управления программами организационного развития. Монография. – К.: Наук. світ, 2007. – 199 с.

2. *Петренко С.А., Симонов С.В.* Управление информационными рисками. Экономически оправданная безопасность. – М.: Компания АйТи; ДМК Пресс, 2005. – 384 с.

3. *Microsoft* Solutions Framework: Дисциплина управления рисками MSF. Версия 1.1 / Пер. на рус. язык под ред. В.Павлова. – М.: eLine Software, Inc, 2002. – 46 с.

4. *Тімінський О.Г.* «Дієвий» підхід до класифікації проектного оточення // Управління проектами та розвиток виробництва: Зб.наук.пр. – Луганськ: Вид-во СНУ ім. В.Даля, 2007. – №2(22). – С.74-79.

5. *Тімінський О.Г., Бондарчук О.В.* Системне бачення зовнішніх проектних взаємодій // Управління проектами та розвиток виробництва: Зб.наук.пр. – Луганськ: Вид-во СНУ ім. В.Даля, 2008. – №1(25). – С.12-18.