І.А. Маркіна
д.е.н., проф., завідувач кафедри, Полтавська державна аграрна академія
Д.В. Дячков
к.е.н., доц., докторант, Полтавська державна аграрна академія

ТЕХНОЛОГІЯ ВДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОСНОВІ ПРОЦЕСІВ ГНУЧКОГО РЕІНЖИНІРИНГУ

Забезпечення інформаційної безпеки як і будь-який інший об'єкт потребує постійного адаптування до умов зовнішнього середовища та вимог внутрішньої системи організації. Оскільки норми та принципи складних процесів використовуються для концептуальної їх перебудови, в тому числі, і для забезпечення ефективності процесів інформаційної безпеки, то для останньої можливе її вдосконалення на основі проведення реінжинірингу.

Інформаційна безпека організації передбачає рівень розвитку інформаційної діяльності організації, таким чином, щоб забезпечити безперебійне й стабільне функціонування, а також оптимальне використання наявних інформаційних ресурсів при мінімізації впливів загроз. Тому, головною причиною реінжинірингу системи інформаційної безпеки є розбіжність між вимогами до даної системи з боку користувачів та її дійсними характеристиками. З часом, ситуація з розбіжністю між вимогами до інформаційної безпеки та її характеристиками стає критичною, що потребує втручання в зазначену систему. Причиною реінжинірингу інформаційної безпеки є реінжиніринг бізнес-процесів. І навпаки, реінжиніринг інформаційної безпеки часто призводить до реінжинірингу бізнес-процесів. Тому процес реінжинірингу інформаційної

безпеки слід розглядати як розробку нових методів оптимізації процесів забезпечення інформаційної безпеки, бізнес-процесів, способів організації забезпечення безпеки підприємства, нових рішень в галузі архітектури системи інформаційної безпеки; апаратних і технічних засобів з більш високою продуктивністю; нових носіїв інформації, програмного забезпечення

Технології забезпечення інформаційної безпеки постійно вдосконалюються, а отже вдосконалюються й методи їх реінжинірингу та оптимізації. Існуючі відмінності в основному знаходяться в організаційних сферах застосування даних технологій [14, 17, 37, 38].

Критеріями якісного розвитку, перепроектування систем з 90-х років XX століття займалися Thomas H. Davenport і James E. Short (Sloan Manadement Review), Martinez Ervin, Braithwaite Timothy, Hammer Michael [13], Davenport T. H., Jacobson I., Зіндер Е. З. Петров Ю. К. та інші [1, 2, 5, 7]. В основному, поняття «реінжиніринг» відносилося до бізнес-процесів і означало стрибкоподібний перехід до нових методів функціонування компанії.

Проект з реінжинірингу в класичному розумінні складається з наступних етапів:

– моделювання та аналіз існуючих бізнес-процесів;

– переосмислення і розробка принципових нових бізнес-процесів;

– впровадження нових бізнес-процесів [10].

Серед найбільш розповсюджених методів реінжинірингу інформаційної безпеки доцільно виділити:

модернізація – відносно незначне поліпшення системи інформаційної безпеки, виправлення критичних помилок, при відсутності кардинальних змін в системі;

рефакторинг – повне або часткове перетворення внутрішньої структури програмного забезпечення системи інформаційної безпеки (тільки програмного) при

збереженні зовнішньої поведінки; перехід на більш сучасну мову програмування;

редизайн – вдосконалення користувальницького інтерфейсу без істотного втручання в її функціонування;

реверс-інжиніринг дослідження, відновлення (побудова) структурних моделей інформаційної безпеки;

реінжиніринг бізнес-процесів – фундаментальне переосмислення і радикальне перепроектування бізнес-процесів для досягнення істотних поліпшень в ключових показниках результативності;

організаційний реінжиніринг – принципово новий підхід до здійснення процесів забезпечення інформаційної безпеки [9].

Існуючі дослідження в галузі вдосконалення інформаційної безпеки, в основному, стосувалися оцінок часу ефективного функціонування в рамках життєвого циклу. Передбачалося, що після закінчення життєвого циклу систем інформаційної безпеки замінюється новою, або проводиться її відновлення. В сучасних умовах розвитку інформаційних технологій необхідно і можливо гнучке вдосконалення: або поступове, протягом нормального функціонування системи інформаційної безпеки, або інтенсивне (реінжиніринг), після значного зниження її ефективності.

На відміну від відомих методологій, пропонована технологія гнучкого реінжинірингу являє собою процес побудови і послідовного перетворення узгоджених моделей на всіх етапах життєвого циклу (причому ці моделі в більшості випадків зберігаються й накопичуються в репозитарії проекту), пропонована методологія формує важелі управління розвитком системи інформаційної безпеки на основі планування часу початку процедур революційного вдосконалення.

Це дозволить, по-перше, розширити період життєвого циклу системи інформаційної безпеки і, по-друге, на початковому етапі погіршення властивостей інформаційної безпеки запропонувати конкретні шляхи її модернізації. Більш того, поєднання двох типів вдосконалення інформаційної безпеки дозволить управляти параметрами модернізації: часом початку вдосконалення, в тому числі окремих підсистем, об'ємом матеріальних вкладень на поступове вдосконалення і визначати рівень модернізації (рис. 1).

Рис. 1. Концептуальні положення технології вдосконалення інформаційної безпеки на основі процесів гнучкого реінжинірингу

Особливість пропонованої технології полягає в варіативності процедур реінжинірингу інформаційної безпеки по горизонтально-вертикальним схемам, що забезпечують можливість реалізації вимог на різних ступенях перепроектування, в тому числі: структурному, програмному, організаційному, функціональному та комплексному їх поєднанні (рис. 2).

Рис. 2. Специфіка вимог до реінжинірингу системи інформаційної безпеки підприємства [розроблено на основі 3, 4]

Таким чином, пропонується ідея специфікації вимог, які містить три рівні: програмний, функціональний та організаційний і чотири категорії: I – вимоги характеристики, II – малоресурсні, III - ресурсоємні, IV – аналітико-проектні.

За типами вимог для проведення реінжинірингу інформаційної безпеки, їх доцільно класифікувати наступним чином:

характерні вимоги зі списку вимог до системи інформаційної безпеки;

нестандартні вимоги, що потребують залучення мінімуму ресурсів;

нестандартні вимоги, які визначаються зниженням ефективності системи інформаційної безпеки;

нестандартні вимоги, які визначаються значним зниження ефективності системи інформаційної безпеки або вимоги, пов'язані з необхідністю розширення цілей системи.

Система специфікації вимог являє собою матричну структуру, що охоплює основні рівні вимог, класифіковані за групами. Належність вимоги певної групі визначає його категорію (I-IV), які дозволяють попередньо оцінити час, потрібний для реалізації цього запиту.

На рис. 3 зображено матрицю визначення специфікації вимоги до реінжинірингу інформаційної безпеки відповідно до карти класифікації вимог [3].

У загальному випадку до матриці специфікації вимог додається проектний рівень, який надає можливість врахувати як початкове проектування та побудову системи інформаційної безпеки, так і необхідність повернення до проектних процедур на етапах перепроектування та реінжинірингу.

У репозитарій проекту в загальному випадку потрапляє безліч застарілих моделей або версій систем, які можуть вважатися такими в разі онлайн-проектування систем з безперервним циклом функціонування.

Таким чином, в процесі специфікації вимог до інформаційної безпеки виділені особливі категорії вимог, вирішення яких передбачає проведення функціонально-організаційного аудиту або реінжинірингу системи, що відноситься до процесів аналізу і вдосконалення систем даного класу.

Організаційний рівень	Планова процедура	Позапланована молоресусна процедура	Аналіз можливостей наявних організаційних процедур	Реорганізація планів
Функціональний рівень	Стандартна функція системи моніторингу	Мінімально ресурсна процедура	Аналіз функціонального покриття вимог	Функціональна реструктуризація і репроектування
Програмний рівень	Характерний запит СУБД, аналіз стандартного ПО	Нехарактерний SQL-запит СУБД, аналіз на прикладному ПО	Модифікація прикладного ПО, міграція версій ПО	Модульне і системне проектування
Проектний рівень	Ідентифікація вимог до проектування	Тестування та незначне репроектування	Адаптація та значне репроектування	Репроектування та інжиніринг
	I категорія вимог: вимоги характеристики	II категорія вимог: малоресурсні	III категорія вимог: ресурсоємні	IV категорія вимог: аналітико-проектні

Рис .3. Матриця специфікації вимоги до інформаційної безпеки відповідно до мапи класифікації вимог [3, 6, 10]

Інформаційна безпека здійснює перетворення:

$$Y_t = F(X_t, A_t), \quad (1)$$

де X_t – поточний стан вхідного об'єкта системи інформаційної безпеки;

Y_t – поточний стан вихідного об'єкта системи інформаційної безпеки;

A – поточний стан вихідної системи інформаційної безпеки;

F – функції перетворення вихідної системи інформаційної безпеки.

Ефективність функціонування даної системи інформаційної безпеки матиме вигляд:

$$U_{n=1}^{N}\left\{X_i^{(n)}\middle|(\delta_i \le \delta^{Xi})\right\} \xrightarrow{a_l \in A, l=\overline{1,n_H}} U_{n=1}^{N}\left\{Y_j^{(k)}\middle|(\theta_j \le \theta^{Yj})\right\}, n=\overline{1,N} \quad (2)$$

$$Y_j^{(k)} = R(X_i^{(n)}, A_i \middle| \delta_i \le \delta^{Xi}, \theta_j \le \theta^{Yj}, t_i \le T, e_i \ge e^*),$$
$$e^* = \sup(W)\middle| e_i \in E_{w,} \forall s \in E_{w,} : e^* \le s, \quad (3)$$

де R – оператор відображення вектора вхідних станів системи в вектор вихідних станів;

δ_i – якість вхідних даних;

δ^{Xi} – допустима якість вхідних даних;

θ_j – якість вихідних даних;

θ^{Yj} – допустима якість вихідних даних;

ti – час функціонування системи в і-м циклі;

T – допустимий час на цикл функціонування системи;

a_i – внутрішній стан вихідної системи;

e_i – і-а вимога до системи;

e^* – необхідний стан системи після реалізації і-ої вимоги до системи;

E_w – сукупність верхніх граней множини W, рівних або більших всіх елементів W [3, 6, 8, 12].

Множина вхідних станів інформаційної безпеки відображається в множині вихідних станів з обмеженнями

на якість вихідних і результуючих параметрів, а також наявності зовнішніх впливів середовища. В процесі функціонування системи інформаційної безпеки виникає конфлікт між існуючим перетворенням вхідного стану об'єкта вихідної системи і забезпеченням максимуму нижньої межі вимог до вихідної системи. Тобто, при виникненні комплексу вимог передбачається, що хоча б мінімальні результати, які забезпечують дозвіл, що виникли в процесі функціонування системи завдань, повинні бути дозволені. На рис. 4 показані варіанти співвідношення часу реалізації вимог до системи t_{wi} і часу циклу її функціонування, T_c.

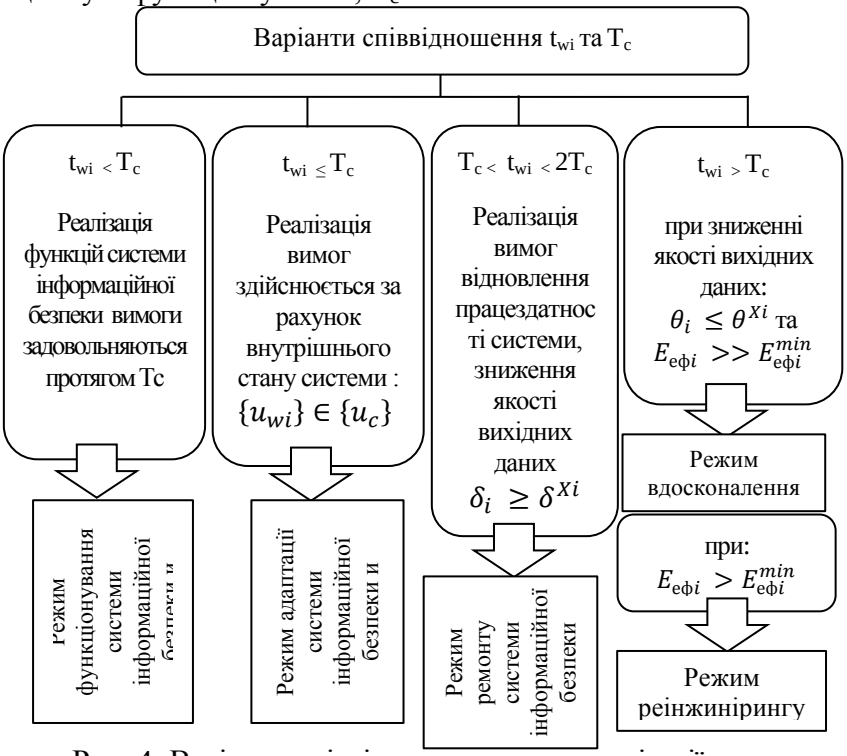

Рис. 4. Варіанти співвідношення часу реалізації вимог до системи інформаційної безпеки і часу циклу її функціонування

Отже, для сучасної системи інформаційної безпеки притаманні процеси постійного вдосконалення та реінжинірингу, які методологічно справедливо в базових метопроцедурах взаємно визначають один одного. Проте, умови сьогодення визначають необхідність пошуку новітніх технологій модифікації систем та процесів. З цією метою запропоновано технологію вдосконалення інформаційної безпеки на основі процесів гнучкого реінжинірингу, яка передбачає поєднання горизонтально-вертикальним схем, які забезпечують можливість реалізації вимог на різних ступенях перепроектування, в тому числі: структурному, програмному, організаційному, функціональному та комплексному їх поєднанні та враховують життєвий цикл системи інформаційної безпеки.

Список використаних джерел:

1. Davenport T. H. Process Innovation: Reengineering Work / T. H. Davenport. // Through Information Technology. – Boston: Harvard Business School Press, 1993.

2. Jacobson I. The Object Advantage. Business Process Reengineering with Object Technology / Jacobson I., Ericsson M., Jacobson A. // N-Y: Addison-Wesley Publishing Company, 1995.

3. Доронина Ю. В. Реинжиниринг информационных систем: [монограф.] / Ю. В. Доронина. – М.: Издательство «Спутник +», 2015. – 170 с.

4. Доронина Ю. В. Реинжиниринг мониторинговых информационных систем циклического типа / Ю. В. Доронина // Східно-європейський журнал передових технологій. – Харків, 2012. – 1/2(55). – С. 12-14.

5. Зиндер Е. З. Бизнес-реинжиниринг и технологии системного проектирования: [учеб. пособ.] / Е.З. Зиндер. – М.: Центр Информационных Технологий, 1996. – 236 с.

6. Литвинская О.С. Обощенная структура принятия решения для метода выбора средств реализации проектируемой информационной технической системы / О.С. Литвинская, И.И. Сальников// «Искусственный интеллект». – Пенза.: ПГТУ, 2010. – №4. – С.404-414.

7. Петров Ю. К. JAM-инструментальное средство разработки приложений в информационных системах архитектуры «клиент/сервер», построенных на базе РСУБД [Электронный ресурс] / Ю.К. Петров//CitForum. – «СУБД», 1995. – Режим доступа: http://citforum.ru/database /kbd96/612.shtml.

8. Резник А. Развивающиеся системы [Электронный ресурс] / А. Резник// International Conference «Knowledge-Dialogue-Solutions», 2007. – Режим доступа: http://www. foibg.com/conf/ITA2007/KDS2007/PDF/KDS07-Reznik1.pdf.

9. Реинжиниринг информационных систем [Электронный ресурс]. – Режим доступа: http://5fan.ru/ wievjob.php?id=19283

10. Схиртладзе А. Основные принципы и приемы реинжиниринга бизнес-процессов [Электронный ресурс] / Схиртладзе А. // Режим доступа: https://www.cfin.ru/ management/strategy/change/foundations.shtml

11. Тельнов Ю. Ф. Реинжиниринг бизнес-процессов: компонентная методология. / Ю. Ф. Тельнов. – М.: Финансы и статистика, 2004. – 320 с.

12. Унижаев Н.В. Модель формирования или реинжиниринга принципов системы обеспечения экономической безопасности организации / Н.В. Унижаев // Экономика: проблемы, решения и перспективы. Вестник университета. – 2016. – №3. – С. 107-112.

13. Хаммер, М. Не автоматизируйте-уничтожайте. Reengineering Work: Don't Automate, Obliterate [Электронный ресурс] / Корпоративный менеджмент. – Режим доступа : http://www.cfin.ru/chuvakhin/bpr.shtml/.