**УДК 004.056.53:519.17**

**Балалаєва О. Ю., Кочукова А. В.**

# МОДЕЛЮВАННЯ І РЕІНЖИНІРИНГ ПРОЦЕСІВ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ТЕОРІЇ ГРАФІВ І МЕТОДОЛОГІЇ IDEF

*У роботі розглянуто основні категорії загроз інформаційній безпеці підприємства, а також теорії, які можуть бути покладені в основу системи захисту інформації. Побудовано контекстну і функціональну діаграми процесів забезпечення інформаційної системи підприємства в нотаціях IDEF0, IDEF3, DFD, а також діаграми окремих підпроцесів, виконано їхню декомпозицію за методологією IDEF. Виявлено, що найбільше питань викликав підпроцес «Усунення загроз», обґрунтовано доцільність побудови математичної моделі системи захисту інформації. Наведено формальний опис системи захисту інформації як моделі з повним перекриттям, а також наведено її удосконалений варіант із урахуванням вразливостей і бар'єрів системи. Запропоновано використовувати величину захищеності для оцінки проектованої системи. Визначено основні заходи реінжинірингу процесу розробки системи захисту інформації. Виконано порівняльний аналіз діаграм для варіантів AS-IS та TO-BE. Проаналізовано діаграму підпроцесу розробки системи захисту інформації в нотації IDEF0 з урахуванням удосконаленої математичної моделі системи захисту інформації підприємства. Обґрунтовано доцільність застосування принципу «розумної достатності», який дозволяє зберегти баланс між витратами на захист і одержуваним ефектом. Визначено перспективу використання ризик-орієнтованої моделі для усунення недоліків моделі безпеки з повним перекриттям при моделюванні процесів функціонування системи захисту інформації. Зроблено висновок про необхідність дослідження ефективності реінжинірингу із використанням ризик-орієнтованої моделі, що дозволить оцінити ризики від реалізації загроз інформаційній безпеці і прийняти оптимальне рішення щодо мінімізації ризиків і впровадження нових засобів захисту інформаційної безпеки підприємства.*

***Ключові слова:*** *система захисту інформації, загрози інформаційній безпеці, моделювання процесів, реінжиніринг, теорія графів, модель із повним перекриттям, вразливість системи, ризик-орієнтована модель, принципу «розумної достатності», методологія IDEF, нотації IDEF0, IDEF3, DFD*

**Постановка проблеми.** Серед найпоширеніших загроз інформаційній безпеці виділяють: небажаний контент, несанкціонований доступ, витік інформації, втрату даних, шахрайство тощо. При цьому найбільшу загрозу представляє крадіжка інформації, що вимагає впровадження системи безпеки інформації на підприємстві.

**Аналіз останніх досліджень і публікацій.** В основу створення системи захисту інформації можуть бути покладені такі теорії: теорії ймовірностей і випадкових процесів; теорії графів, автоматів та мереж Петрі; теорія нечітких множин; теорії ігор та конфліктів; теорія катастроф; еволюційне моделювання; формально-евристичний підхід; ентропійний підхід тощо. Також перспективним напрямом є використання методів моделювання, заснованих на неформальній теорії систем, таких як методи структурування, методи оцінювання та методи пошуку оптимальних рішень [1].

Згідно з джерелом [2] система захисту інформації може бути представлена у вигляді орієнтованого графа, де вершинам відповідають компоненти інформаційної системи, а ребрам – інформаційні потоки між ними. При цьому використовують опис трактів проходження, де послідовно вказується джерело інформації, проміжна апаратура і одержувач

інформації, а також вид переданої інформації. Побудова матриць суміжності та інцидентності дозволяє визначити компоненти інформаційної системи, які обробляють інформацію різних рівнів конфіденційності з метою подальшого посилення захисту від потенційних загроз інформаційній безпеці.

Аналіз літературних джерел показав. що для формального опису системи захисту інформації зручно використовувати модель з повним перекриттям, яка базується на теорії графів і розглядає системи інформаційної безпеки як взаємодію множини загроз, множини об'єктів захисту та множини механізмів захисту [3].

Для моделювання системи захисту інформації з точки зору поточного опису процесів доцільно використовувати методології IDEF [4] – технологію опису бізнес-процесів в цілому як множини взаємозалежних дій або функцій. Такий підхід дозволяє провести глибоке передпроектне дослідження процесів системи з необхідним рівнем деталізації для подальшого виявлення «вузьких» місць і розробки заходів для реінжинірингу відповідних процесів.

**Мета дослідження.** Метою роботи є моделювання та реінжиніринг процесів захисту інформації із використанням теорії графів та методології побудови бізнес-процесів IDEF.

**Основний матеріал дослідження.** Процес забезпечення інформаційної безпеки можна розбити на наступні підпроцеси: аналіз вхідних даних, розподіл за рівнями захисту інформації, усунення загроз, обробка інформації засобами для захисту інформації. У рамках методології IDEF функціонування системи захисту інформації зручно зобразити як в нотації IDEF0, що дозволяє описати логічні відносини між окремими процесами системи (рис. 1).

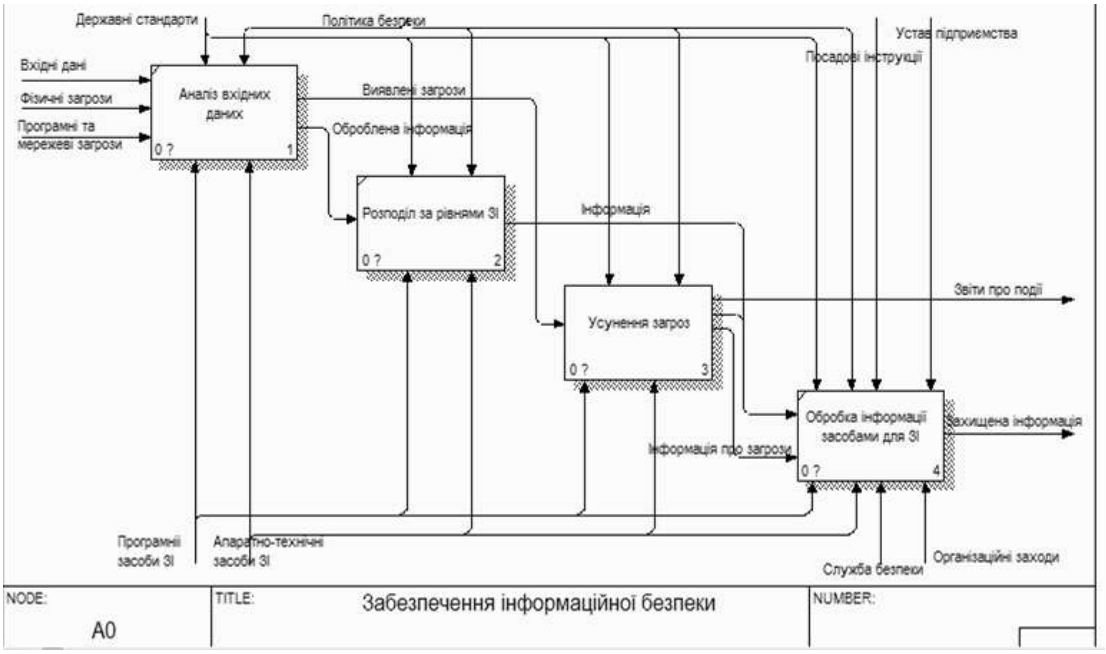


Рисунок 1 – Діаграма IDEF0 «Забезпечення інформаційної безпеки»

З точки зору розробки системи захисту інформації найбільш проблемним є процес «Усунення загроз», який можна розбити на наступні підпроцеси: класифікація загроз за категоріями, розробка системи захисту інформації, реалізація системи захисту інформації, планові перевірки для виявлення загроз (рис. 2).

Розглянемо декомпозицію процесу «Розробка системи захисту інформації» із використанням теорії графів, а саме моделі системи захисту з повним перекриттям.

Модель системи захисту з повним перекриттям може бути представлена у вигляді трьох множин: множини загроз $T = \{t_i\}$, множини об'єктів захисту $O = \{o_j\}$, множини механізмів захисту $M = \{m_k\}$. Тобто систему захисту інформації можна зобразити як тридольний граф {T,O,M} [3].

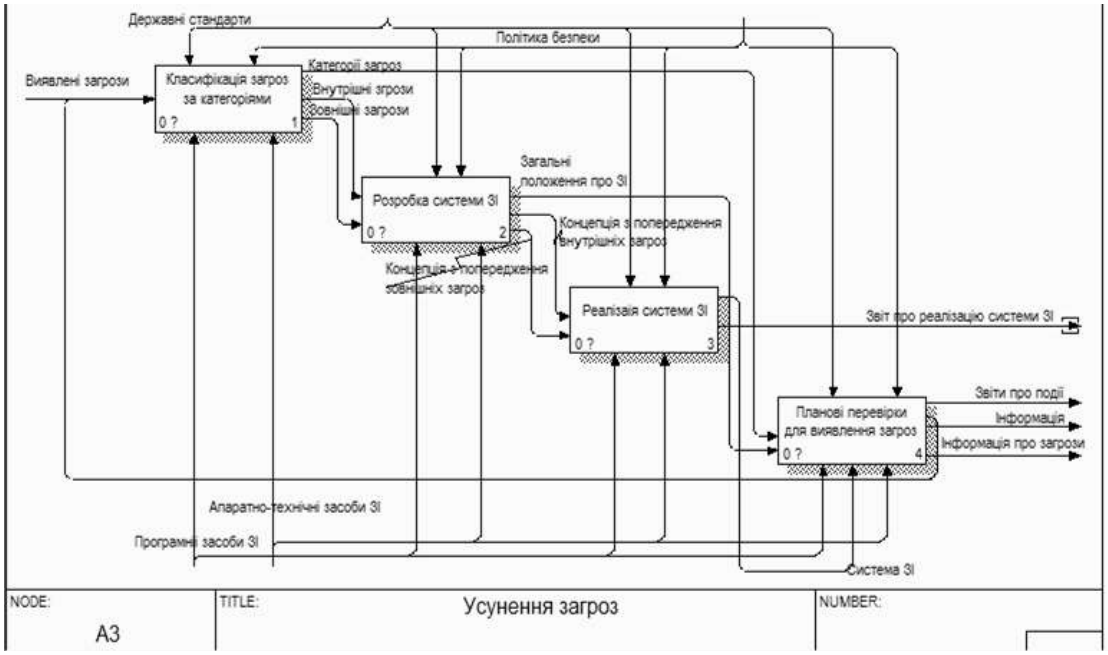


Рисунок 2 – Діаграма IDEF0 «Усунення загроз»

Згідно із наведеною математичною моделлю розіб'ємо процес «Розробка системи захисту інформації» на наступні підпроцеси (рис. 3):

– визначення актуальних загроз – на виході отримуємо множину загроз $T = \{t_i\}$;

– визначення інформаційних ресурсів для захисту – на виході отримуємо множину об'єктів захисту $O = \{o_j\}$;

– визначення механізмів захисту інформації – на виході отримуємо механізмів захисту $M = \{m_k\}$;

– розробка документів, регламентуючих захист інформації;

– створення цілісної системи захисту інформації.

Однак така модель системи захисту інформації не враховує можливостей здійснення загроз для системи і шляхів захисту від них.

Аналіз літературних джерел показав, що модель із повним перекриття отримала подальший розвиток [3], який полягає у введенні двох нових елементів.

Першим елементом є набір вразливостей $V = \{v_r\}$, що визначають можливість здійснення загрози T щодо об'єкту захисту O; визначається як $\{T \cdot O\}$: $v_r = <t_i,o_j>$.

Другим елементом є набір бар'єрів $B = \{b_l\}$, що визначають шлях здійснення загрози T, перекритий механізмом захисту M; визначається як $\{V \cdot M\}$: $b_l = <t_i,o_j,m_k>$.

Виходячи із вищезазначеного і згідно із джерелом [3] система захисту інформації може бути представлена моделлю, що складається з п'яти елементів: {T,O,M,V,B}. У такій системі для будь-якої уразливості існує бар'єр, який її усуває, тобто для всіх можливих загроз безпеці існують механізми захисту, що перешкоджають здійсненню цих загроз.

Також необхідно враховувати, що реальна система захисту інформації може забезпечити лише певний ступінь опірності загрозам безпеки. Тому було запропоновано кожному елементу множини бар'єрів $b_l$ поставити у відповідність набір $<P_l,L_l,R_l>$, де $P_l$ – ймовірність появи загрози; $L_l$ – величина збитку при вдалому здійсненні загрози щодо

об'єктів захисту; $R_l$ – ступінь опірності механізму захисту $m_k$, що характеризується ймовірністю його подолання [3].

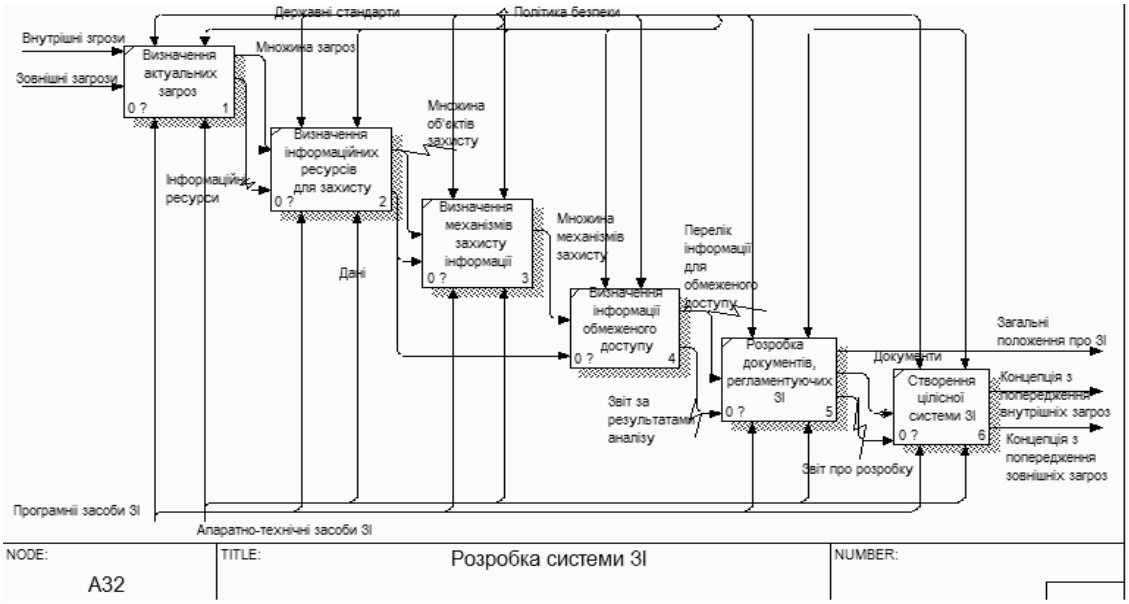


Рисунок 3 – Діаграма IDEF0 «Розробка системи захисту інформації» (AS-IS)

Для оцінки проектованої системи пропонується використовувати величину захищеності S, яка згідно з [3] розраховується за формулою: $S = 1/Risk_0$, де $Risk_0$ – сума всіх залишкових ризиків ($0<[P_k,L_k]<1$; $0<[R_k]<1$). Залишкові ризики характеризують надійність кожного бар'єра і пов'язані з можливістю виконання загрози $t_i$ щодо об'єкта захисту $o_j$ при використанні механізму захисту $m_k$: $Risk_l = P_kL_k(1 – R_k)$.

На основі наведеної математичної моделі визначено наступні заходи з реінжинірингу процесів системи захисту інформації, а саме процесу «Розробка системи захисту інформації»:

– визначити вразливість системи, тобто можливість здійснення кожної загрози щодо кожного об'єкту захисту;

– визначити бар'єри системи. тобто всі шляхи здійснення загрози, перекриті одним з механізмів захисту;

– проаналізувати захищеність системи із урахуванням залишкових ризиків кожного бар'єру та їхньої сумарної величини.

Запропоновані заходи з реінжинірингу системи відображено на діаграма IDEF0 «Розробка системи захисту інформації» для варіанта «ТО-ВЕ» (рис. 4).

Перспективним напрямом удосконалення запропонованої моделі системи захисту інформації є використання принципу «розумної достатності», суть якого полягає у збереженні балансу між витратами на захист і одержуваним ефектом [1].

Для досягнення такого балансу доцільно розглянути варіант ризик-орієнтованої моделі, що використовує теорію графів, згідно з якою система захисту інформації представляється у вигляді орієнтованого графа, де вершинами є загрози активам, а дугами – їхні зв'язки. Спочатку за допомогою формул розрахунку вартості ризику згідно з джерелом [1] обчислюються ймовірні втрати від реалізації окремих загроз і загроз, що реалізуються один за одним по деякому шляху. Потім проводиться порівняння вартості ризику з витратами на забезпечення інформаційної безпеки і приймається рішення щодо цього ризику.

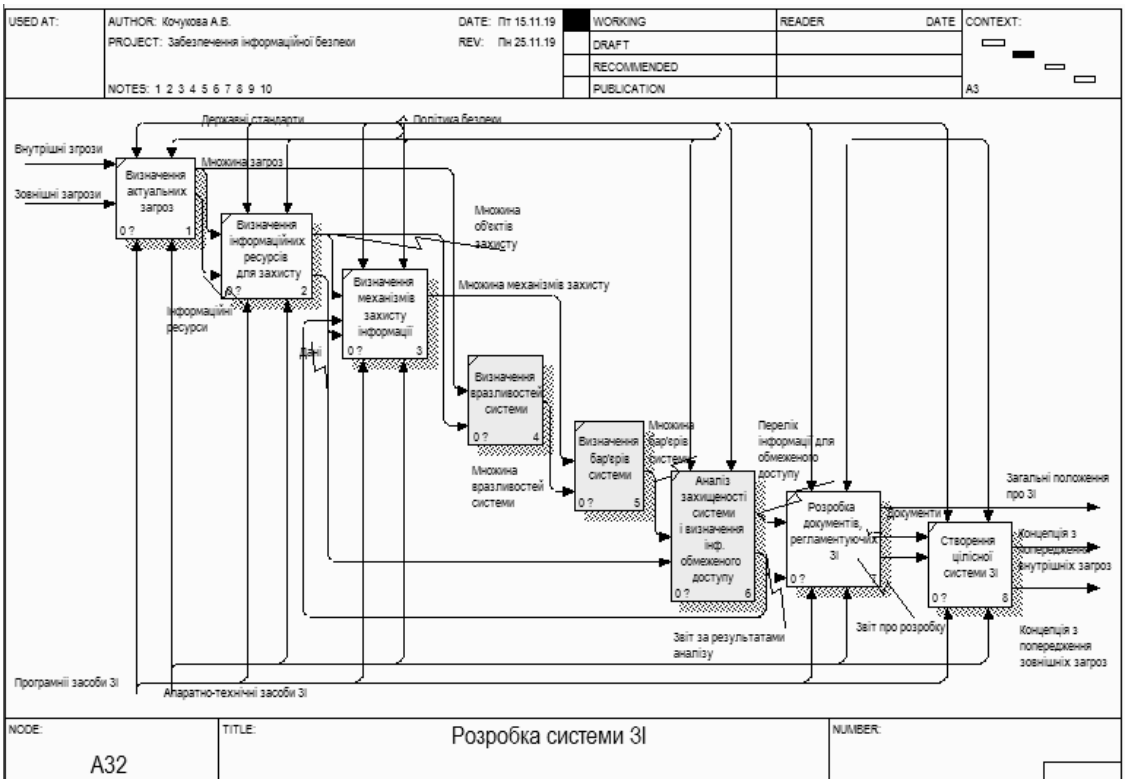


Рисунок 4 – Діаграма IDEF0 «Розробка системи захисту інформації» (TO-BE)

,

Таким чином, на основі використання теорії графів, а саме комбінації моделі системи захисту із повним перекриттям та ризик-орієнтованої моделі, було побудовано ефективну модель системи захисту інформації з використанням методології IDEF.

## ВИСНОВКИ

На основі математичної моделі системи захисту з повним перекриттям проведено моделювання системи захисту інформації. Наведено удосконалену математичну модель, яка враховує вразливості та бар'єри системи, надані рекомендації з оцінки захищеності проектованої системи.

Запропоновано основні заходи з реінжинірингу процесів системи захисту інформації, які базуються на удосконаленій математичній моделі. Побудовано діаграму забезпечення інформаційної безпеки та виконано її декомпозицію із використанням методології IDEF. Виконано порівняльний аналіз діаграм для варіантів AS-IS та TO-BE.

Проаналізовано доцільність застосування принципу «розумної достатності», який дозволяє зберегти баланс між витратами на захист і одержуваним ефектом. Визначено перспективу використання ризик-орієнтованої моделі для усунення недоліків моделі безпеки з повним перекриттям при моделюванні процесів функціонування системи захисту інформації.

*Список використаних джерел*

1. *Курилов, Ф. М.* Моделирование систем защиты информации. Приложение теории графов / *М. Ф. Курилов* // Технические науки: теория и практика: материалы III Междунар. науч. конф. – Чита: Издательство Молодой ученый, 2016. – С. 6–9.

2. *Попова, М. С.* Применение теории графов при выявлении потенциальных угроз безопасности информации / *М. С. Попова, А. П. Карпов* // Проблемы современной науки и образования. – 2016. – № 35 (77). – Режим доступа: https://ipi1.ru/s/05-00-00-tekhnicheskie-nauki/1233-primenenie-teorii-grafov.html.

3. Методология анализа защищенности информационной системы. – Режим доступа: https://studme.org/97431/informatika/metodologiya_analiza_zaschischennosti_informatsionnoy_sistemy.

4. *Черемных, С. В.* Структурный анализ систем. IDEF-технологии / С. В. Черемных, И. О.Семенов, В. С. Ручкин. – Финансы и статистика, 2003. — 208 с.

**Балалаева Е. Ю., Кочукова А. В.**

## МОДЕЛИРОВАНИЕ И РЕИНЖИНИРИНГ ПРОЦЕССОВ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ТЕОРИИ ГРАФОВ И МЕТОДОЛОГИИ IDEF

*В работе рассмотрены основные категории угроз информационной безопасности предприятия, а также теории, которые могут быть положены в основу системы защиты информации. Построены контекстна и функциональна диаграммы процессов обеспечения информационной системы предприятия в нотациях IDEF0, IDEF3, DFD, а также диаграммы отдельных подпроцессов, выполнена их декомпозиции по методологии IDEF. Выявлено, что больше всего вопросов вызвал подпроцесс «Устранение угроз», обоснована целесообразность построения математической модели системы защиты информации. Приведены формальное описание системы защиты информации как модели с полным перекрытием, а также приведен ее усовершенствованный вариант с учетом уязвимостей и барьеров системы. Предложено использовать величину защищенности для оценки проектируемой системы. Определены основные мероприятия реинжиниринга процесса разработки системы защиты информации. Выполнен сравнительный анализ диаграмм для вариантов AS-IS и TO-BE. Проанализирована диаграмма подпроцесса разработки системы защиты информации в нотации IDEF0 с учетом усовершенствованной математической модели системы защиты информации предприятия. Обоснована целесообразность применения принципа «разумной достаточности», который позволяет сохранить баланс между затратами на защиту и получаемым эффектом. Определена перспектива использования риск-ориентированной модели для устранения недостатков модели безопасности с полным перекрытием при моделировании процессов функционирования системы защиты информации. Сделан вывод о необходимости исследования эффективности реинжиниринга с использованием риск-ориентированной модели, что позволит оценить риски от реализации угроз информационной безопасности и принять оптимальное решение по минимизации рисков и внедрения новых средств защиты информационной безопасности предприятия.*

***Ключевые слова:*** *система защиты информации, угрозы информационной безопасности, моделирование процессов, реинжиниринг, теория графов, модель с полным перекрытием, уязвимость системы, риск-ориентированная модель, принципа «разумной достаточности», методология IDEF, нотации IDEF0, IDEF3, DFD.*

**Balalayeva E. Yu., Kochukova A. V.**

## MODELING AND RE-ENGINEERING OF INFORMATION PROTECTION PROCESSES BASED ON GRAPHIC THEORY AND IDEF METHODOLOGY

*The main categories of information security threats for an enterprise and theories that can form the basis of an information security system are considered in the work. Contextual and functional diagrams of the processes for ensuring the information system of an enterprise in notations IDEF0, IDEF3, DFD, as well as diagrams of individual subprocesses are constructed, their decomposition according to the IDEF methodology is performed. It was revealed that the sub-process "Elimination of threats" caused the most questions, and the feasibility of constructing a mathematical model of the information protection system was substantiated. A formal description of the information protection system as a model with full overlap is given, as well as its improved version is given taking into account vulnerabilities and system barriers. It is proposed to use the security value to evaluate the designed system. The main measures of reengineering the process of developing an information security system are identified. A comparative analysis of the diagrams for the AS-IS and TO-BE options has been performed. The diagram of the subprocess of developing an information security system in the IDEF0 notation is analyzed, taking into account the improved mathematical model of an enterprise information security system. The expediency of applying the principle of "reasonable sufficiency", which allows you to maintain a balance between the cost of protection and the resulting effect, is substantiated. The prospect of using a risk-oriented model to eliminate the shortcomings of the security model with complete overlap in modeling the processes of functioning of the information protection system is determined. It is concluded that it is necessary to study the effectiveness of reengineering using a risk-based model, which will allow us to assess the risks from the implementation of information security threats and make the best decision to minimize risks and introduce new means of protecting the information security of the enterprise.*

***Keywords:*** *information security system, threats to information security, process modeling, reengineering, graph theory, a model with complete overlap, system vulnerability, risk-based model, the principle of «reasonable sufficiency», IDEF methodology, IDEF0, IDEF3, DFD notations*

**УДК 004:65.012.23**

**Балалаєва О. Ю., Саєнко Є. О.**

## МОДЕЛЮВАННЯ І РЕІНЖИНІРИНГ БІЗНЕС-ПРОЦЕСІВ МАГАЗИНУ КАНЦЕЛЯРСЬКИХ ТОВАРІВ НА ОСНОВІ МЕТОДУ ЕКСПЕРТНИХ ОЦІНОК ТА АЛГОРИТМУ ВИЗНАЧЕННЯ НАДІЙНОСТІ ПОСТАЧАЛЬНИКІВ

*У роботі розглянуто сегментацію ринку канцелярських товарів, проаналізовано попит, основні тенденції, перспективи розвитку та наявні проблеми. Встановлено, що основними двома сегментами протягом останніх років залишаються товари для діловодства і товари для освіти. Проведено моделювання бізнес-процесів торгівельної мережі магазинів канцелярських товарів, побудовано діаграми IDEF0, DFD, IDEF3 із використанням методології IDEF для варіанту «AS-IS». Зроблено висновок, що реінжинірингу потребують бізнес-процеси оптової торгівлі, пов'язані з оцінкою постачальників, що на теперішній час обумовлюється суб'єктивним судження про їхню діяльності директора магазину. Проаналізовано основні критерії для оцінки постачальників магазину канцелярських товарів, наведено їхню класифікацію. Визначено основні критерії*