Collective Monograph

Theoretical and Practical Aspects of Development of Legal Knowledge, National Security and Physical Education of Citizens

Edition 1

2021-2022 | Primedia eLaunch

ISBN 978-1-63848-595-7
DOI 10.36074/tpadlknspec.ed-1

THEORETICAL AND PRACTICAL ASPECTS OF DEVELOPMENT OF LEGAL KNOWLEDGE, NATIONAL SECURITY AND PHYSICAL EDUCATION OF CITIZENS

Collective Scientific Monograph

EDITION 1

Dallas
2021-2022

Primedia eLaunch
E-book conversion, distribution & marketing

UDC 370.15+371.302.81+613
T 44

Primedia eLaunch
in collaboration with European Scientific Platform

Compilers: NGO European Scientific Platform (Ukraine)
21037, Ukraine, Vinnytsia, Zodchykh str. 18/81

Publisher: Primedia eLaunch LLC (USA)
TX 75001, United States, Texas, Dallas

Authors of the monograph:
Brzezicki T. – Dr. Hab.
Demenko M. – Ph.D (Military Sciences)
Doska O. – Ph.D (Engineering)
Fomenko D. – Ph.D (Engineering)
Holubnychyi D. – Ph.D (Engineering)
Kalmykov V.G. – Ph.D (Engineering)
Kobziev V. – Ph.D (Engineering)
Kornieiev P.
Kryvtsov A.
Kryvtsov O.
Lukianchuk V. – Dr.S (Engineering)
Malyshev O.V. – Ph.D (Engineering)
Nikolaiev I. – Ph.D (Engineering)
Novichenko S. – Ph.D (Military Sciences)
Onishchenko N. – Dr.S (Law)
Onishchuk V.
Saveliev A.
Suniehin S. – Ph.D (Law)
Tkachenko P.
Tretiak V. – Ph.D (Engineering)
Tsarenko O. – Ph.D (Politics)
Vasyliev V. – Ph.D (Engineering)
Voitko O. – Ph.D (Military Sciences)
Zapara D.

In the collective scientific monograph, researchers consider issues of implementation of the state information police and ensuring information security of Ukraine, tax systems in Polish tax law and the capabilities of Ukraine and USA defense planning. Gender relations are discussed as a factor of development of civil society. Scientists analyze criminal legal and criminological characteristics of violation between military services and a functional model of information security control system. The question of the description model of the problem of justification is being also discussed as long as the reflection of transport aircraft.

T 44 **Theoretical and practical aspects of development of legal knowledge, national security and physical education of citizens**: Collective Scientific Monograph (1st edition). Tomkins R. (ed.). Dallas, USA: Primedia eLaunch LLC, 2022. 100 p.

ISBN 978-1-63848-595-7
DOI 10.36074/tpadlknspec.ed-1

UDC 370.15+371.302.81+613

ISBN 978-1-63848-595-7

CONTENT

UDC 342.95 (477) *DOI 10.36074/tpadlknspec.ed-1.07*

Published online ahead of print (August 26, 2022)

Голубничий Д.Ю.[1], Третяк В.Ф.[2], Запара Д.М.[3], Деменко М.П.[4],
Holubnychyi D., Tretiak V., Zapara D., Demenko M.,
Новіченко С.В.[5], Доска О.М.[6], Савельєв А.М.[7]
Novichenko S., Doska O., Saveliev A.

ФУНКЦІОНАЛЬНА МОДЕЛЬ УПРАВЛІННЯ СИСТЕМОЮ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

FUNCTIONAL MODEL OF INFORMATION SECURITY CONTROL SYSTEM

АНОТАЦІЯ:

Використовуючи методологію функціонального моделювання IDEF0 була розроблена функціональна модель основних процесів управління системою інформаційної безпеки. Основна мета цієї моделі – відображення процесів управління системою інформаційної безпеки в організації. Показано, що можливо проведення декомпозиції процесу управління системою інформаційної безпеки у вигляді восьми підпроцесів. Основна увага приділена розгляданню вимог до адміністрування комп'ютерних систем і обчислювальних мереж.

ВСТУП

В якості об’єкта системи будемо розглядати функціонування комп’ютерної мережі організації, як частини загальної інформаційної системи. Для такого аналізу застосуємо середовище моделювання процесів – BPWin.

[1] кандидат технічних наук, доцент, доцент кафедри Інформаційних систем
Харківський національний економічний університет імені Семена Кузнеця, Україна

[2] кандидат технічних наук, доцент, науковий співробітник наукового центру Повітряних Сил
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Україна

[3] начальник науково-дослідного відділу наукового центру Повітряних Сил
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Україна

[4] кандидат воєнних наук, доцент, провідний науковий співробітник наукового центру Повітряних Сил
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Україна

[5] кандидат воєнних наук, доцент, провідний науковий співробітник наукового центру Повітряних Сил
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Україна

[6] кандидат технічних наук, старший науковий співробітник науково-дослідного відділу наукового центру Повітряних Сил
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Україна

[7] науковий співробітник науково-дослідного відділу наукового центру Повітряних Сил
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Україна

This work has been republished [without change]. First publication: Голубничий, Д., Третяк, В., Запара, Д., Деменко, М., Новіченко, С., Доска, О., & Савельєв, А. (2021). ФУНКЦІОНАЛЬНА МОДЕЛЬ УПРАВЛІННЯ СИСТЕМОЮ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. *Грааль Науки*, (2-3), 175-186. DOI 10.36074/grail-of-science.02.04.2021.035.

Мета інформаційної системи – забезпечити безперебійну роботу організації та звести до мінімуму збиток від подій, що містять загрозу безпеці, за допомогою їхнього запобігання й зведення наслідків до мінімуму.

Управління інформаційною безпекою дозволяє колективно використати інформацію, забезпечуючи при цьому її захист і захист обчислювальних ресурсів. Інформаційна безпека складається із трьох основних компонентів:

– конфіденційність: захист конфіденційної інформації від несанкціонованого розкриття або перехоплення;

– цілісність: забезпечення точності й повноти інформації та комп'ютерних програм;

– доступність: забезпечення доступності інформації та життєво важливих сервісів для користувачів, коли це потрібно.

ОСНОВНА ЧАСТИНА

Інформація існує в різних формах. Її можна зберігати на комп'ютерах, передавати по обчислювальних мережах, роздруковувати або записувати на папері, а також озвучувати в розмовах. З погляду безпеки всі види інформації, включаючи паперову документацію, бази даних, плівки, мікрофільми, моделі, магнітні стрічки, дискети, розмови й інші способи, які використовуються для передачі знань і ідей, вимагають належного захисту [1-5].

Таким чином, використовуючи нотацію стандарту IDEF0 розробимо функціональну модель основних процесів управління системою інформаційної безпеки (рис. 1.).

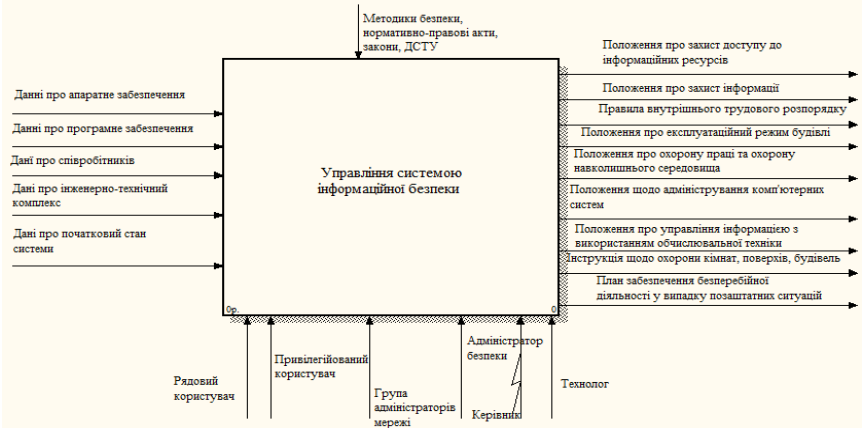

Рис. 1. **Контекстна діаграма комплексу завдань "Управління системою інформаційної безпеки" (методологія IDEF0)**

Основна мета моделі – відобразити процеси управління системою інформаційної безпеки в організації. Щоб ініціювати й контролювати процес забезпечення інформаційної безпеки, необхідно створити в організації відповідну структуру управління. Такою структурою в термінах IDF0 може бути структура, яка показана на рис. 2.

Таким чином, використовуючи декомпозицію процесу управління системою інформаційної безпеки отримуємо:

1. Формування засобів контролю (рівень А1);
2. Захист немашинних інформаційних ресурсів (рівень А2);
3. Забезпечення безпеки персоналу (рівень А3);
4. Забезпечення фізичної безпеки (рівень А4);
5. Забезпечення безпеки навколишнього середовища (рівень А5);
6. Адміністрування комп'ютерних систем і обчислювальних мереж (рівень А6);
7. Додаткові засоби охорони системи (рівень А7);
8. Планування забезпечення безперервної діяльності у випадку позаштатних ситуацій (рівень А8).

Кожен з рівнів має мету, особисте призначення та також декомпозицію.

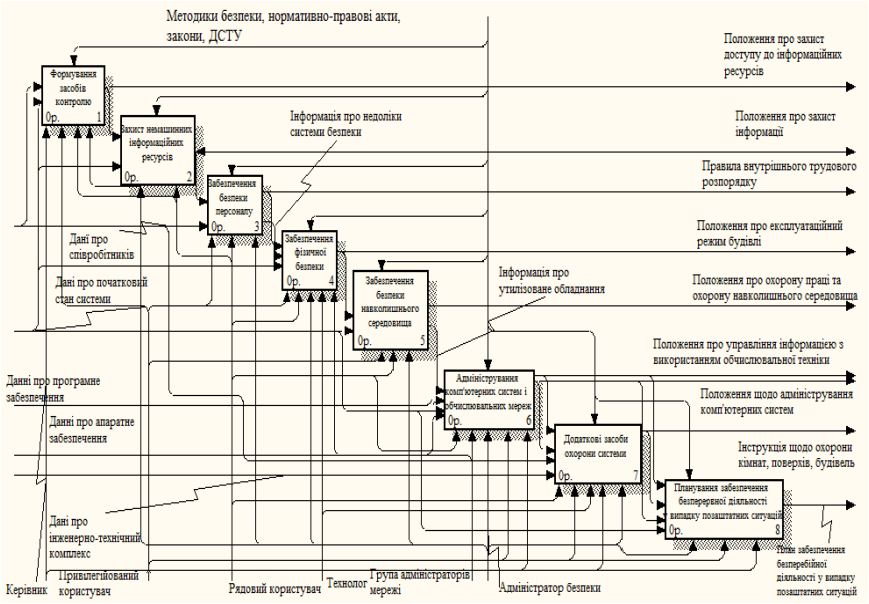

Рис. 2. **Діаграма функціональної декомпозиції процесу управління системою інформаційної безпеки**

Декомпозиція процесу формування засобів контролю (рис. 3) визначає такі процеси, як виявлення загроз інформаційної безпеки; аналіз причин необхідності використання системи інформаційної безпеки; розробка стратегії усунення погроз інформаційної безпеки; формування засобів контролю системи; створення документа про політику інформаційної безпеки.

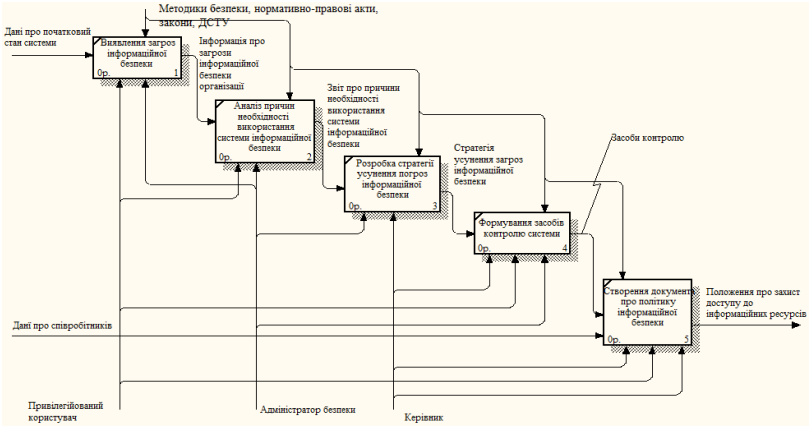

Рис. 3. **Декомпозиція рівня роботи "Формування засобів контролю"**

Декомпозиція процесу захисту немашинних інформаційних ресурсів (рис. 4) визначає такі процеси, як: інвентаризацію інформаційних ресурсів; присвоєння грифів таємності; забезпечення належного рівня захисту інформаційних ресурсів.

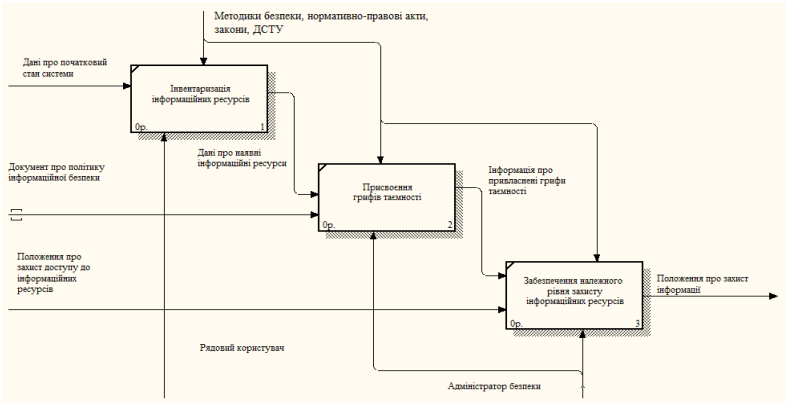

Рис. 4. **Декомпозиція роботи "Захист немашинних інформаційних ресурсів"**

Декомпозиція процесу забезпечення безпеки персоналу (рис. 5) визначає такі процеси, як : запобігання несанкціонованого доступу до інформаційних сервісів; контроль доступу в приміщення; захист центрів даних і комп'ютерних залів; визначення фізичних периметрів безпеки; захист обладнання.

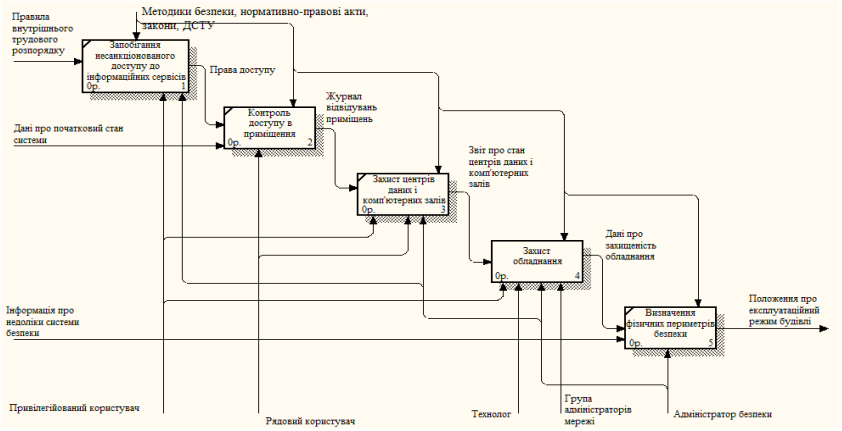

Рис. 5. **Декомпозиція роботи "Забезпечення фізичної безпеки"**

Декомпозиція процесу забезпечення безпеки персоналу (рис. 6) визначає такі процеси, як: складання посадових інструкцій; перевірка прийнятих на роботу; укладення угоди про конфіденційність; підвищення кваліфікації персоналу; повідомлення про слабкі місця в системі безпеки; повідомлення про інциденти у системі безпеки.

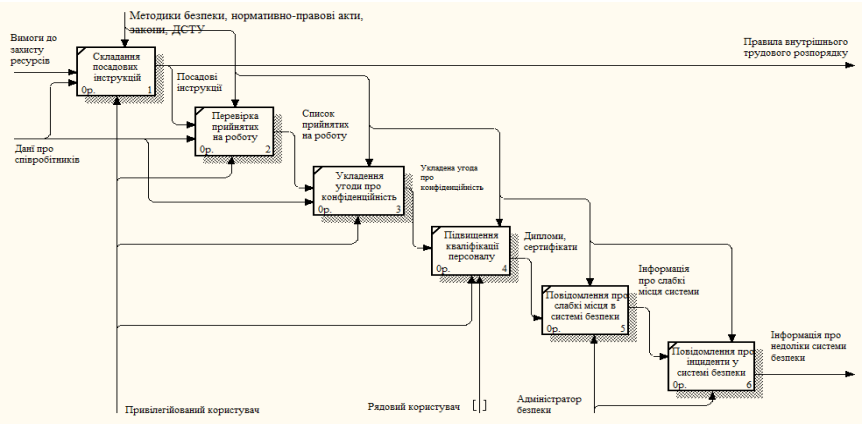

Рис. 6. **Декомпозиція роботи "Забезпечення безпеки персоналу"**

Декомпозиція процесу захисту обладнання (рис. 7) визначає такі процеси, як: розміщення обладнання; технічне обслуговування обладнання; захист обладнання, що використовується за межами організації; захист кабельного розведення.

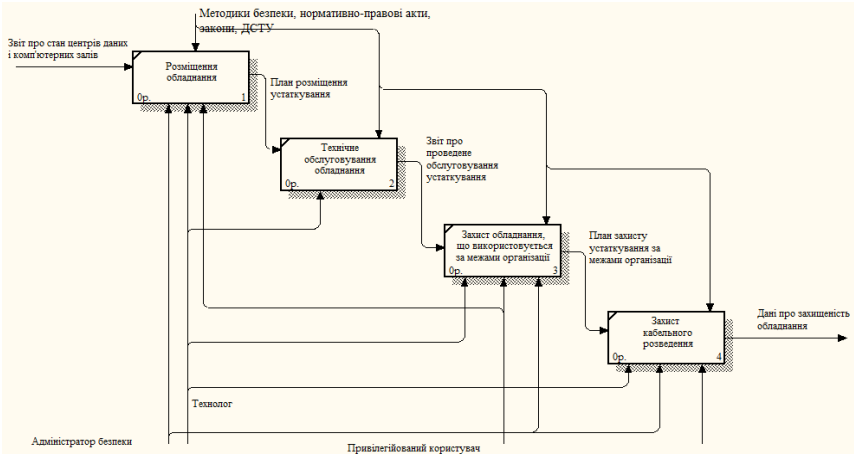

Рис. 7. **Декомпозиція роботи "Захист обладнання"**

Декомпозиція процесу забезпечення безпеки навколишнього середовища (рис. 8) визначає такі процеси: контроль джерел електроживлення; утилізація обладнання.

Рис. 8. **Декомпозиція роботи "Забезпечення безпеки навколишнього середовища"**

Декомпозиція процесу адміністрування комп'ютерних систем і обчислювальних мереж (рис. 9) визначає такі процеси, як: визначення процедур; визначення вимог до програмного забезпечення (ПЗ); визначення вимог до планування комп'ютерних систем; захист внутрішньомашинних інформаційних ресурсів; управління безпекою обчислювальних мереж.

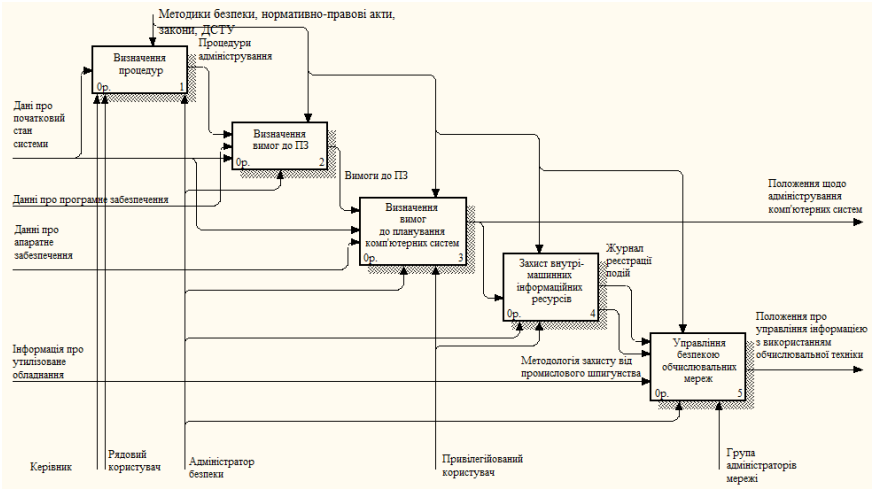

Рис. 9. **Декомпозиція роботи "Адміністрування комп'ютерних систем і обчислювальних мереж"**

На рис. 10 представлена декомпозиція процесу "Визначення процедур".

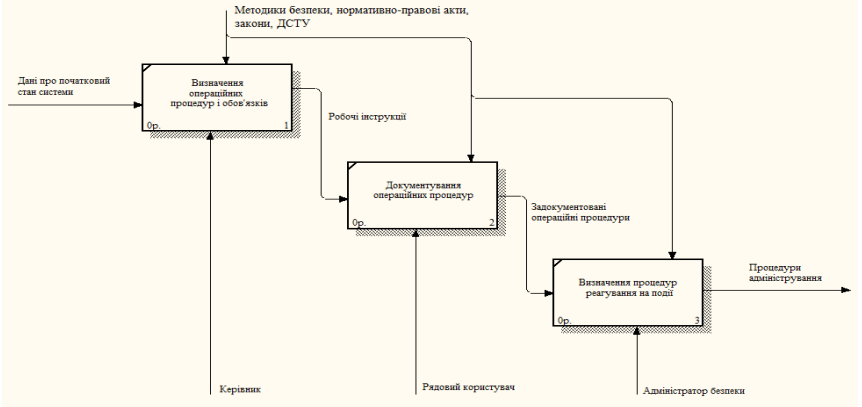

Рис. 10. **Декомпозиція роботи "Визначення процедур"**

Декомпозиція процесу визначення процедур (рис. 11) містить такі процеси, як (рис.А.11 додатку А): класифікація програмних засобів розробки та робочих програм; захист від шкідливого ПЗ.

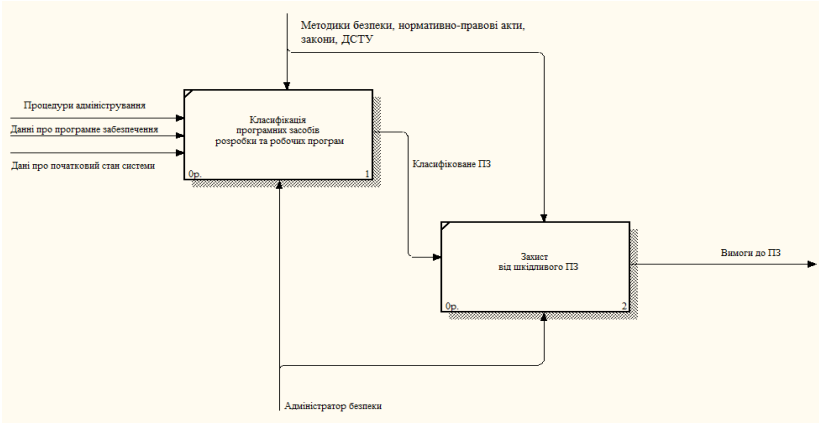

Рис. 11. **Декомпозиція роботи "Визначення вимог до ПЗ"**

Декомпозиція процесу визначення вимог до планування комп'ютерних систем (рис. 12) містить такі процеси, як: планування навантаження комп'ютерних систем; приймання комп'ютерних систем; реєстрація збоїв у комп'ютерних системах; керування процесом внесення змін у робочі системи; обслуговування комп'ютерних систем.

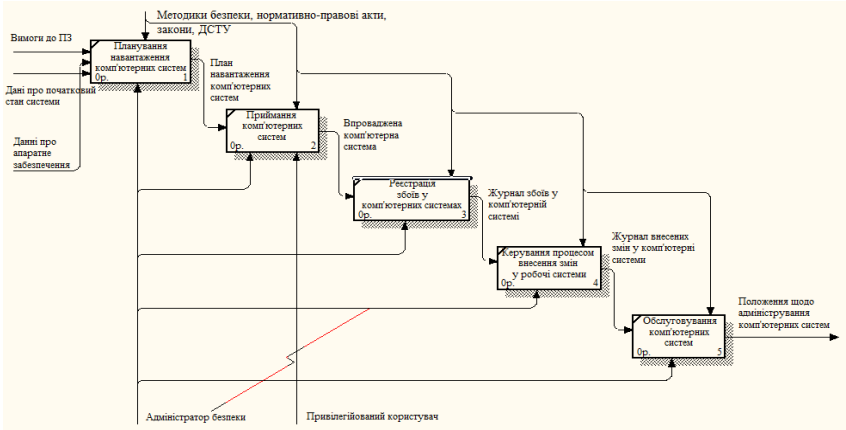

Рис. 12. **Декомпозиція роботи "Визначення вимог до планування комп'ютерних систем"**

Декомпозиція процесу захист внутрішньомашинних інформаційних ресурсів (рис. 13) містить такі процеси, як: створення резервних копій даних; ведення журналу реєстрації подій; захист від промислового шпигунства.

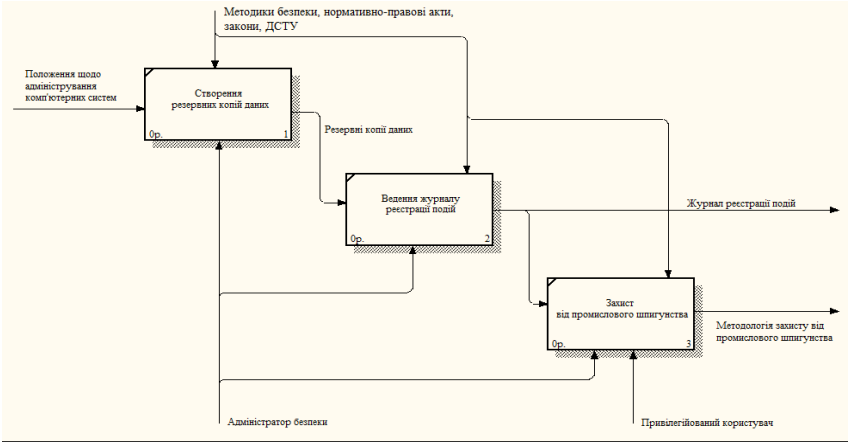

Рис. 13. **Декомпозиція роботи "Захист внутрішньомашинних інформаційних ресурсів"**

На рис. 14 представлена декомпозиція процесу "Управління безпекою обчислювальних систем".

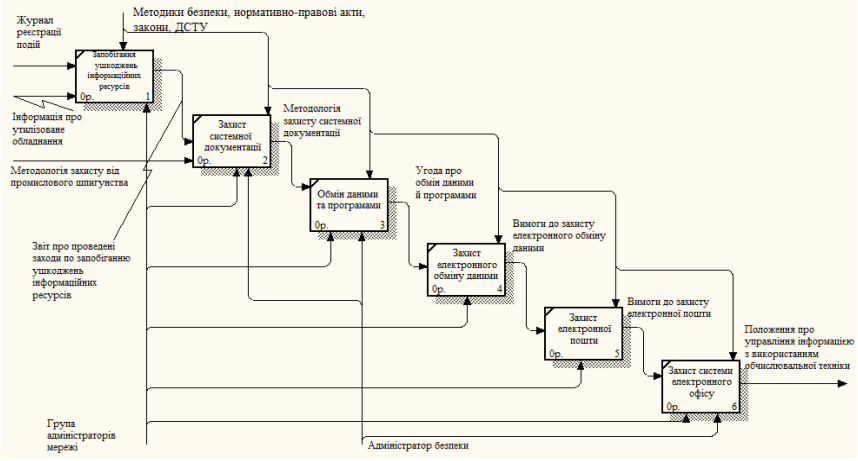

Рис. 14. **Декомпозиція роботи "Управління безпекою обчислювальних систем"**

Так декомпозиція процесу забезпечення додатковими засобами охорони (рис. 15) системи визначає такі процеси, як: зміцнення інженерно-технічних об'єктів; біологічні засоби захисту; керування системою охоронного телебачення; забезпечення охоронно-пожежної сигналізації.

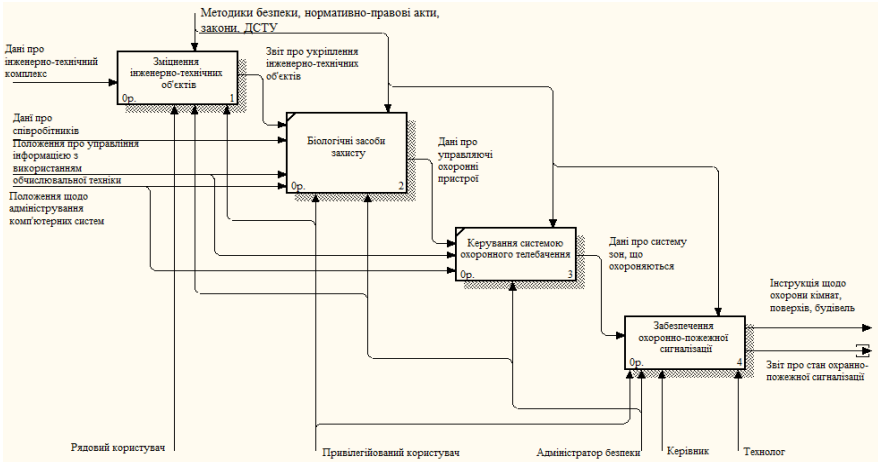

Рис. 15. **Декомпозиція роботи "Додаткові засоби охорони системи"**

На рис. 16 представлена декомпозиція процесу "Забезпечення охоронно-пожежної сигналізації".

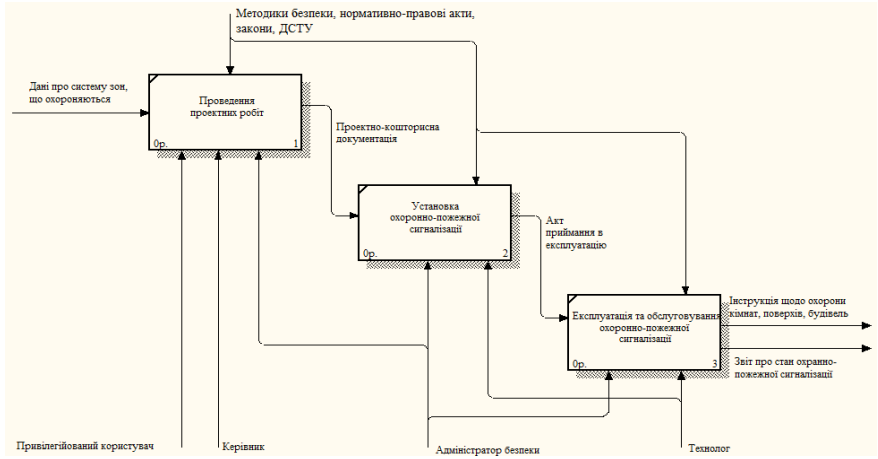

Рис. 16. **Декомпозиція роботи "Забезпечення охоронно-пожежної сигналізації"**

На рис. 17 представлена декомпозиція процесу "Планування забезпечення безперервної діяльності в разі позаштатних ситуацій". Діаграма дерева рішень представлена на рис. 18.

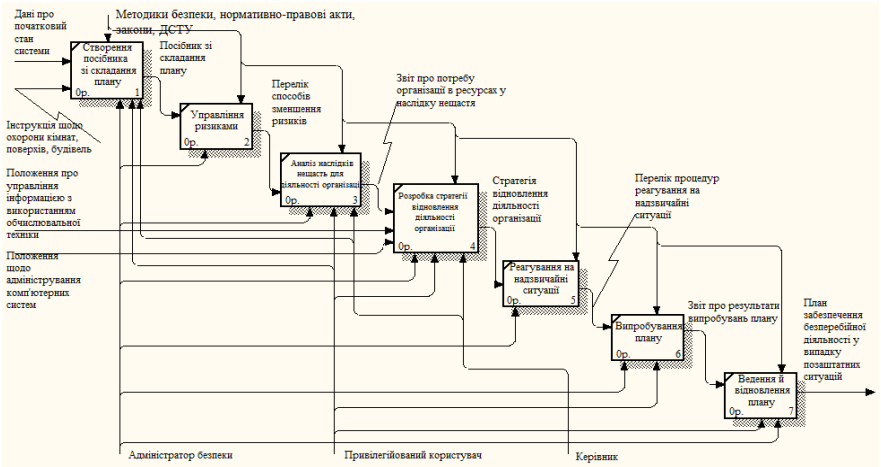

Рис. 17. **Декомпозиція роботи "Планування забезпечення безпосередньої діяльності в разі нештатних ситуацій"**

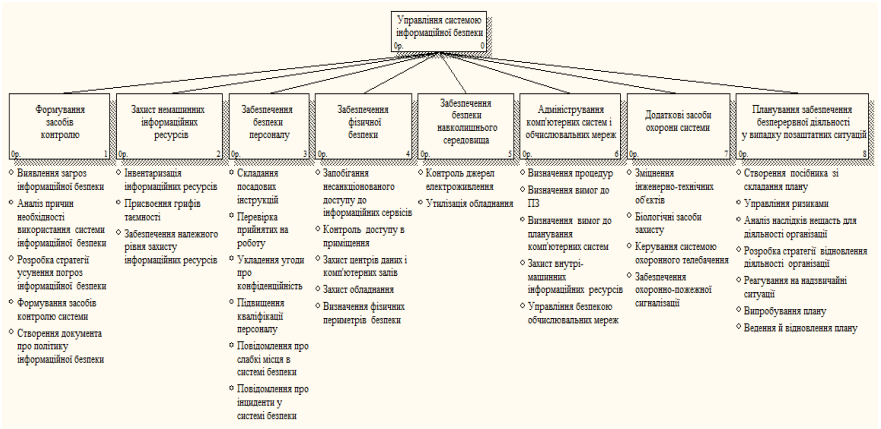

Рис. 18. **Діаграма дерева рішень**

ВИСНОВКИ.

Використовуючи нотацію стандарту IDEF0 була розроблена функціональна модель основних процесів управління системою

інформаційної безпеки. Основна мета цієї моделі – відображення процесів управління системою інформаційної безпеки в організації. Показано, що можливо проведення декомпозиції процесу управління системою інформаційної безпеки у вигляді восьми підпроцесів. Основна увага була приділена розгляданню вимог до адміністрування комп'ютерних систем і обчислювальних мереж.

REFERENCES:

[1] Коломійцев, О., Голубничий, Д., Коц, Г., Третяк, В., Євстрат, Д., & Лисиця, А. (2020). Задачі дискретної оптимізації та їх постановка для розміщення засобів захисту в розподіленій системі. Збірник наукових праць ΛΌГОΣ, 36-41. https://doi.org/10.36074/20.11.2020.v5.12.

[2] Третяк, В., Голубничий, Д., Коломійцев, О., Мегельбей, Г., Возний, О., & Філіпенков, О. (2020). Математична модель рангового підходу. Збірник наукових праць ΛΌГОΣ, 116-122. https://doi.org/10.36074/25.12.2020.v1.40.

[3] Третяк, В., & Пашнєва, А. (2017) Оптимізація структури сховища даних у вузлах інфокомунікаційної мережі хмарного середовища. Системи управління, навігації та зв'язку. № 4 (44). – С. 122-128.

[4] Голубничий Д., Коломійцев О., Запара Д., Новіченко С. & Євстрат Д.І. (2020). Визначення фаз проведення аудиту та категорії порушників кібербезпеки. Scientific Collection «InterConf», (38): with the Proceedings of the 1st International Scientific and Practical Conference «Science, Education, Innovation: Topical Issues and Modern Aspects» (December 16-18, 2020) in Tallinn, Estonia; pp. PP. 1367-1375. Вилучено із: https://www.interconf.top/archive.html.

[5] Голубничий Д., Сєвєрінов О., Коломійцев О., Місюра О., Третяк В., Власов А. & Крук Б. (2021). Аналіз сучасних загроз в інформаційних системах за складовими загроз: кібербезпеки, інформаційної безпеки та безпеки інформації. InterConf, (45), 21-27. Вилучено із https://ojs.ukrlogos.in.ua/index.php/interconf/issue/archive.