УДК 659.4:327.88

Дячков Д. В.,
E-mail: dmiraf@ukr.net, ORCID ID: 0000-0002-2637-0099,
Researcher ID: Q-6394-2016,
к е.н., доц., доцент кафедри менеджменту, Полтавська державна аграрна академія, м. Полтава

ФОРМУВАННЯ МОДЕЛІ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОСНОВІ КОНЦЕПЦІЙ “ГЛИБИННОГО ЗАХИСТУ”

Анотація. *В статті обґрунтовано важливість на необхідність побудови ефективної політики інформаційної безпеки суб’єктів макро- та макрорівнів в умовах інформатизації світових економічних процесів. Метою статті є аналіз існуючих моделей формування політики інформаційної безпеки та розробка моделі політики інформаційної безпеки на основі поєднання концепції “глибинного захисту” та “mind map”. Вирішення поставлених у статті завдань здійснено за допомогою таких загальнонаукових і спеціальних методів дослідження: аналізу та синтезу, систематизації та узагальнення, діалектичного підходу. Розглянуто традиційні та новітні моделі формування політики інформаційної безпеки, основними серед яких є: модель Bell-LaPadula, модель Biba, модель Clark-Wilson, дискреційна (матрична) модель, модель Адепт-50, модель “MITER ATT & CK ™”, модель “Diamond model”, модель “The pyramid of pain”. Визначено їх переваги на недоліки. Запропоновано модель формування політики інформаційної безпеки на основі концепцій “глибинного захисту” та “mind map”. Концепція “глибинного захисту” полягає в тому, що механізми інформаційної безпеки розшаровані і тим самим підвищують безпеку системи в цілому. Концепція “глибинного захисту” визначає три рівні організації інформаційного захисту: фізичний, технічний, адміністративний. Водночас ця модель включає безліч компонентів: персонал (людей), технологію, операційну систему, моніторинг та різні аспекти захисту як ключові компоненти забезпечення інформаційного захисту. Пропонована модель формалізована у вигляді “карти розуму”, яка впорядковує основні категорії як з організаційного, так і технічного аспектів захисту та водночас враховує функціонал ключових елементів: людей, політику, моніторинг та показники безпеки. Модель політики інформаційної безпеки на основі концепції “глибинного захисту” рекомендує зосередитися на всіх рівнях та напрямах захисту інформаційних ресурсів, а використання “*mind map*” дозволить визначити та обрати той набір процедур, правил та інструментів, які забезпечать реалізацію найбільш відповідної та оптимальної політики інформаційної безпеки.*

Ключові слова: загрози, захист інформації, інформаційна безпека, концепція mind map, концепція глибинного захисту, модель формування політики інформаційної безпеки, політика інформаційної безпеки.

Diachkov D. V.,
dmiraf@ukr.net, ORCID ID: 0000-0002-2637-0099,
Researcher ID: Q-6394-2016,
Ph.D., Associate Professor, Associate Professor of the Department of Management, Poltava State Agrarian Academy, Poltava

FORMATION OF A MODEL OF INFORMATION SECURITY POLICY BASED ON THE “DEFENSE-IN-DEPTH” CONCEPTS

Abstract. *The article substantiates the importance of building an effective information security policy for the subjects of makro- and micro levels in the context of informatization of world economic processes. The purpose of the article was to analyze the existing models of information security policy formulation and to develop the model of information security policy based on the combination of the " defense-in-depth " and "mind map" concept . The tasks of the article were solved using the following general scientific and special methods of research: analysis and synthesis, systematization and generalization, dialectical approach. The traditional and the latest models of information security policy formation were considered, the main ones being: Bell-LaPadula model, Biba model, Clark-Wilson model, discretionary (matrix) model, Adept-50 model, MITER ATT & CK ™ model, " Diamond model ", model" The pyramid of pain ". Their advantages to disadvantages were determined. A model of information security policy formation based on the "defense-in-depth" and "mind map" concepts was proposed. The concept of "defense-in-depth" is that information security mechanisms are stratified and thus increase the security of the system as a whole.The concept was proposed that information security mechanisms were stratified, and thus increase the security of the system as a whole. The "defense-in-depth" concept defines three levels of information security organization: physical, technical, administrative. At the same time, this model includes many components: personnel (people), technology, operating system, monitoring and various aspects of security as key components of information security. The proposed model was formalized in the form of a "mind map", which organizes the main categories from both organizational and technical aspects of protection and, at the same time, takes into account the functionality of key elements: people, policy, monitoring and security indicators. The model of*

information security policy, based on the concept of "defense-in-depth", recommends focusing on all levels and areas of information resources protection, and the use of "mind map" will allow to define and select that set of procedures, rules and tools that will provide the most appropriate and optimal information security policy.

Keywords: concept of "defense-in-depth", concept of "mind map", information protection, information security policy, information security, model of formation of information security policy, threats.

JEL Classification: M15, F52, G14
DOI: https://doi.org/10.36477/2522-1256-2019-25-17

Постановка проблеми. В умовах глобалізації економіки успішне ведення бізнесу передбачає наявність інформації про ринкову кон'юнктуру, фінансове становище конкурентів, новітні розробки, тенденції розвитку в конкретних галузях науки і виробництва. Водночас практика діяльності господарюючих суб'єктів повсякденно свідчить про їх підвищену вразливість від незаконних та інших посягань злочинних організацій та окремих осіб з метою викрадення інформаційних ресурсів, псування програмного та техніко-технологічного забезпечення, розкриття комерційної таємниці тощо. Тому забезпечення інформаційної безпеки, збереження конкурентних переваг стає важливою необхідністю, одним із базових принципів функціонування сучасних суб'єктів як на макро-, так і на макрорівні.

Побудова ефективної системи захисту інформації вимагає реалізації комплексного підходу, найважливішим елементом якого є формування і реалізація політики інформаційної безпеки, що, в свою чергу, передбачає пошук оптимальної моделі формування політики інформаційної безпеки суб'єктів різних рівнів.

Аналіз останніх досліджень і публікацій. Важливу роль у забезпеченні інформаційної безпеки суб'єкта будь-якого рівня відіграє політика безпеки. Визначивши політику інформаційної безпеки, потрібно вирішити питання стосовно технології, що буде використана для її реалізації, що потребує формування релевантної моделі формування політики інформаційної безпеки.

Проблематика забезпечення інформаційної безпеки, зокрема в аспектах формування моделі політики інформаційної безпеки, знайшла своє відображення в працях Богомолова С. А., Зегджи Д. П., Івашко А. М., Мельника М. О., Нікітина Г. Д., Мезенцевої К. О., Мілославської Н. Г., Толстої А. І., Петрова А. А., Степанова В. Ю., Чуруброві С. М. та інших.

Найбільша увага науковців приділяється визначенню складових політики забезпечення інформаційної безпеки, яка в основному ґрунтується на використанні апаратних, програмних та криптографічних засобів захисту. Водночас залишаються недостатньо вивченими питання, пов'язані з моделлю реалізації політики інформаційної безпеки з позиції досягнення мети бізнесу та застосування економічних методів управління інформаційними ризиками.

Постановка завдання – аналіз існуючих моделей формування політики інформаційної безпеки та розробка моделі політики інформаційної безпеки на основі поєднання концепції "глибинного захисту" та "mind map".

Виклад основного матеріалу дослідження. Інформаційні операції можуть проводитися на різних рівнях управління інформаційною безпекою: рівні окремої особи (групи осіб), одного підприємства, групи підприємств, галузі промисловості, регіону та держави в цілому. Ефективність здійснення інформаційних операцій та функціонування інформаційної системи загалом, від якої, в свою чергу, залежить соціо-економіко-технічний стан діяльності окремого об'єкта, обґрунтовано вимагає формування не тільки системи інформаційної безпеки, а формування дієвої та прийнятної політики забезпечення роботи із захистом інформації. Тому розробка моделі управління політикою інформаційної безпеки є актуальним завданням.

Формування такої моделі обґрунтовує необхідність характеристики існуючих моделей.

Найбільш відомою є модель політики інформаційної безпеки Bell-LaPadula (BLP) [3]. Вона базується на політиці конфіденційності і визначає поняття захищеного стану. В цілому BLP стала першою визначною моделлю політики безпеки, яка застосовується для інформаційних технологій і до сьогодні в зміненому вигляді використовується. Модель математично повністю формалізована. Її основу складає конфіденційність [6].

Далі розглянемо "модель Biba" [4]. Вона є першою спробою створення інтегрованої моделі. Основні відмінності від попередньої полягають у наявності рівнів інтеграції та додаткової властивості – вик-лику, що відповідає за можливість суб'єкта надсилати сервісні запити. Інші властивості схожі з попередньою моделлю, проте зазначена має прив'язку до рівня інтеграції, на якому знаходиться об'єкт і суб'єкт (у попередній моделі рівні класифікації) [6].

Набір правил моделі Clark-Wilson (CW) [2] розроблений таким чином, щоб в повній мірі забезпечувати безпеку та підзвітність переходів у системі за рахунок вибору необхідного для такої ситуації режиму роботи з даними. Головне досягнення цих правил в порівнянні з моделлю Biba – поділ процедур з перевірки цілісності та процедур зміни, що дозволяє запобігти або виправити більшість нелегальних дій, що здійснюються зсередини організації [6].

Дискреційна (матрична) модель [10] вже має більш практичне спрямування, оскільки стан системи захисту можна описати тріадою (на основі термінів матричної моделі):

$$\{S, O, M\}, \quad (1)$$

де S – безліч суб'єктів, які є активними структурними елементами моделі;

O – безліч об'єктів доступу, є пасивними захищеними елементами моделі;

M – матриця доступу.

Для визначення права доступу суб'єкта до об'єкта використовується значення елемента матриці M. Звернення до різних типів об'єктів доступу з боку суб'єкта необхідно здійснювати, керуючись правами доступу, в яких описані способи такого звернення. Зазвичай права доступу суб'єктів до файлових об'єктів визначають як читання (R), запис (W) і виконання (E).

Аналіз ряду матриці доступу за зверненням суб'єкта до об'єкта береться за основу реалізації управління доступом. Він проводиться наступним чином: для перевірки обирається відповідний до об'єкта рядок матриці. Під час перевірки визначається наявність необхідних прав доступу для суб'єкта. За результатами перевірки здійснюється надання чи заборона доступу. Наочність і гнучкість налаштувань політики доступу до ресурсів у матричних моделях є їх великою перевагою, на противагу якій постає ряд недоліків, до них можна віднести зайвий деталізований рівень опису відносин суб'єктів та об'єктів. Він призводить до підвищення складності адміністрування системи захисту під час задання параметрів і їх підтримки в актуальному стані при включенні до схеми розмежування доступу нових елементів (об'єктів чи суб'єктів або ж і тих, і інших одночасно), через що виникає ризик допустити багато помилок при адмініструванні. Виходячи з цього, такий недолік можна назвати основним для дискреційної моделі. Коли мова йде про велику кількість користувачів, то традиційні підсистеми управління доступом потрібно адмініструвати, використовуючи об'єктно-орієнтовані рішення, що дозволяють знизити складність адміністрування. Це необхідний захід, тому що число зв'язків пропорційне добутку кількості користувачів на кількість об'єктів, що робить процес адміністрування надскладним завданням. Є кілька різновидів об'єктно-орієнтованих рішень. Наприклад, це рольове управління доступом. Реалізується воно шляхом додавання проміжних сутностей (ролей) між користувачами та їх привілеями. Це дозволяє в різні проміжки часу мати різні права, за рахунок зміни ролі. Один користувач може мати кілька ролей. При використанні рольового доступу можна спростити процес адміністрування системи, оскільки збільшення його складності при зростанні кількості користувачів відбувається значно повільніше. Досягається це за рахунок абстрагування від конкретних видів і способів перевірки прав користувачів та встановлення зв'язків між ролями. Ролей в такому випадку потрібно значно менше, ніж користувачів. Відповідно, число зв'язків, які потрібно адмініструвати, стає пропорційним сумі, а не добутку кількості користувачів та об'єктів [6].

Адепт-50 – одна з перших моделей безпеки, яка розглядає 4 групи об'єктів безпеки: користувачі, завдання, термінали та файли. Кожен об'єкт безпеки описується вектором (A, C, F, M), що включає наступні параметри безпеки:

- компетенція A – елемент з набору впорядкованих універсальних положень безпеки, які включають апріорно задані можливі в інформаційній системі характеристики об'єкта безпеки, наприклад категорії конфіденційності об'єкта: нетаємно, конфіденційно, таємно, цілком таємно;
- категорія C – рубрикатор (тематична класифікація). Рубрики не залежать від рівня компетенції. Приклад набору рубрик: фінансовий, політичний, банківський;
- повноваження F – перелік користувачів, які мають право на доступ до даного об'єкта;
- режим M – набір видів доступу, дозволених для певного об'єкта або здійснюваних об'єктом. Приклад: читати дані, записувати дані, виконати програму (виконання програм розуміється як породження активної компоненти з деякого об'єкта – як правило, виконуваного файлу) [1, 8].

Достатньо своєрідною є модель "MITER ATT & CK ™", яка являє собою доступну у всьому світі базу знань про тактики та методи формування інформаційної політики, базовані на реальних спостереженнях. База знань ATT & CK використовується як основа для розробки конкретних моделей та методологій загроз, для приватного сектора користувачів та уряду.

Дана модель передбачає використання матриці, яка формується на основі використання показників: ступінь доступу, система реалізації програмних додатків, наполегливість, ескалація привілеїв, ухилення від захисту, доступ до довірених даних, відкриття, додатків дії, збір, управління та адміністрування, ексфільтрація, вплив [5, 9].

Досить оригінальною для формування політики інформаційної безпеки є "модель алмазу" "Diamond Model". Вона визначає політику інформаційної безпеки об'єкта на основі аналізу чотирьох ознак: зловмисника (супротивника), інформаційної інфраструктури, можливостей (здатностей персоналу) та об'єкта впливу (жертви) [7]. Зазначені елементи розташовані у формі ромба, що і визначає назву моделі, а також додаткові мета-функції для підтримки конструкцій вищого рівня, таких як пов'язання подій разом у потоки діяльності та подальше злиття подій потоків у групи інформаційної активності (рис. 1).

Ця модель встановлює формальний метод, який застосовує наукові принципи аналізу вторгнень або загроз, методів їх вимірювання, встановлення достовірності та повторюваності, забезпечуючи комплексний метод синтезу та кореляції діяльності відносно забезпечення інформаційної безпеки об'єкта [5].

Ця проста діаграма показує взаємозв'язок між типами показників, які використовуються для виявлення діяльності порушника інформаційної безпеки, і ступінь "болю", який він їм заподіє.

Ще однією, незвичною моделлю формування політики інформаційної безпеки є застосування "піраміди болю" ("The Pyramid of Pain") (рис. 2).

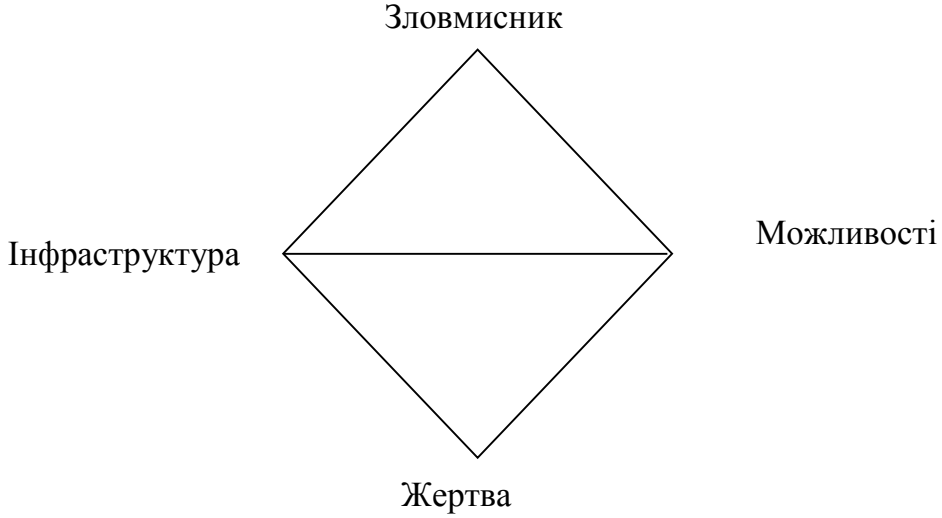

Рис. 1. Формування політики інформаційної безпеки на основі моделі “Алмаз” [5]

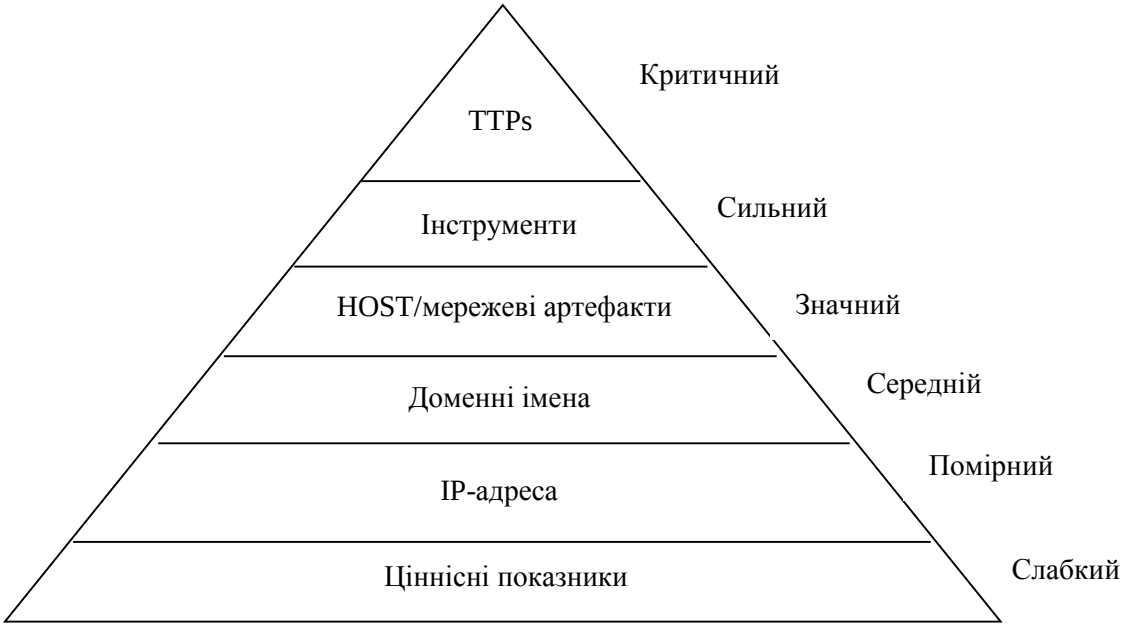

Рис. 2. Формування політики інформаційної безпеки на основі моделі “Піраміди болю” [5, 11]

Існуюча література зосереджується на описі структури та змісту політики безпеки, але, як правило, не в змозі детально описати процеси розробки політики. Зважаючи на відсутність настанов, розробники часто використовують політику, розроблену іншими організаціями, доступні джерела або шаблони. Проте політика інформаційної безпеки, отримана в результаті таких методів, не надасть належного спрямування для захисту інформації [12].

Враховуючи зазначене, пропонується модель формування політики інформаційної безпеки на основі концепції “глибинного захисту”.

Вона полягає в тому, що механізми інформаційної безпеки розшаровані і тим самим підвищують безпеку системи в цілому. Якщо атака спричиняє збій одного механізму захисту, інші механізми все ще можуть забезпечити необхідний рівень безпечності для захисту системи [12]. Водночас ця модель включає безліч компонентів: персонал (людей), технологію, операційну систему, моніторинг та різні аспекти захисту як ключові компоненти забезпечення інформаційного захисту. Ці організаційні шари важко перевести в конкретні технологічні шари захисту, і вони залишають такі сфери, як моніторинг безпеки та показники. На рис. 3 зображена пропонована модель формування політики інформаційної безпеки на основі концепції “глибинного захисту” у вигляді “карти розуму”, що впорядковує основні категорії як з організаційного, так і технічного аспектів захисту та водночас враховує функціонал ключових елементів: людей, політику, моніторинг та показники безпеки.

Концепція “глибинного захисту” визначає три рівні організації інформаційного захисту:

1. Фізичний рівень: включає заходи щодо обмеження фізичного доступу до IT-інфраструктури неавторизованих осіб: охоронець офісу, системи

СКУД, камери відеоспостереження, сигналізація, телекомунікаційні шафи тощо.

2. Технічний рівень: включає всі хардверні та софтові засоби захисту інформації, призначені контролювати мережевий доступ до об'єктів інформаційної системи, міжмережевий екран, засоби антивірусного захисту робочих станцій, проксі-сервери, системи аутентифікації та авторизації.

3. Адміністративний рівень: сюди відносяться всі політики та процедури інформаційної безпеки. Документи покликані регулювати управління захистом, розподілом і обробкою критичної інформації, використання програмних і технічних засобів, а також взаємодію співробітників з інформаційною системою, сторонніми організаціями та іншими зовнішніми суб'єктами.

Хоча концепція "глибинного захисту" при формуванні моделі інформаційної безпеки передбачає створення і реалізацію вичерпного плану захисту, проте буде неправильним вважати, що застосовування цієї концепції здійснюється за принципом "все або нічого". Насправді для досягнення швидких результатів з мінімальними витратами доцільно дотримуватися покрокового підходу при її побудові.

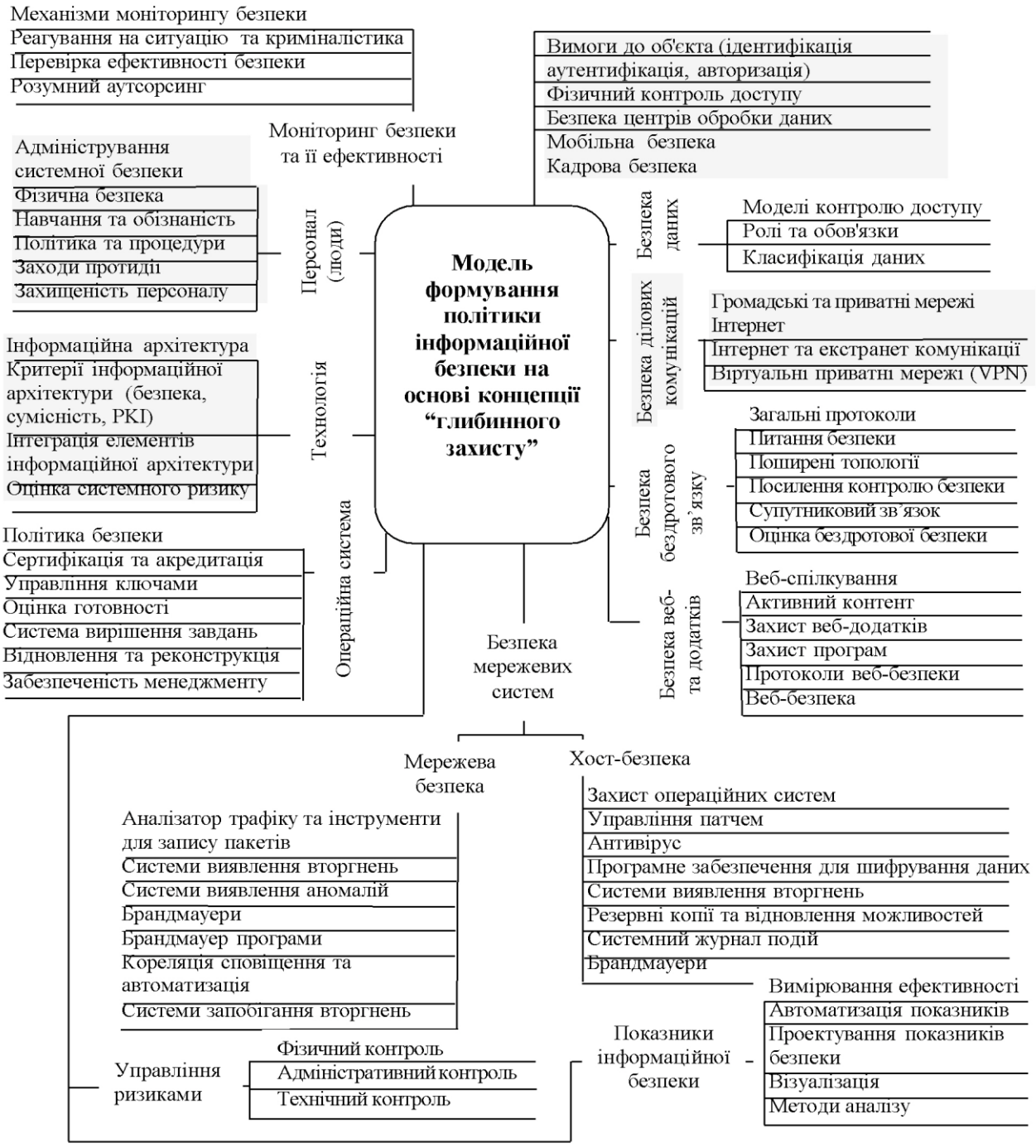

Рис. 3. Формування моделі політики інформаційної безпеки на основі концепцій "глибинного захисту" та "mind map" [розроблено на основі 11, 12]

Висновки і перспективи подальших досліджень у даному напрямі. Проаналізовані моделі формування політики інформаційної безпеки у межах політики інформаційної безпеки в цілому призводить до результатів, які у багатьох відношеннях корелюють з тим, на що пропонується звернути увагу при використанні концепцій "глибинного захисту" та "mind map". Відмінність полягає в тому, що модель політики інформаційної безпеки на основі концепції "глибинного захисту" рекомендує зосередитися на всіх рівнях та напрямах захисту інформаційних ресурсів, а використання "mind map" дозволить визначити та обрати той набір процедур, правил та інструментів, які забезпечать реалізацію найбільш відповідної та оптимальної політики інформаційної безпеки.

ЛІТЕРАТУРА

1. Богомолов С. А. Модели типовых политик безопасности. - 2016 URL: https://infourok.ru/lekciya-po-zaschite-informacii-modeli-bezopasnosti-927637.html (дата звернення 12.12.2019 р.).
2. Зегджа Д. П. Основы безопасности информационных систем / Зегджа Д. П., Ивашко А. М. - М. : Горячая линия – Телеком, 2000. – 452 с.
3. Мельник М. О. Аналіз побудови моделі політики інформаційної безпеки підприємства / Мельник М. О., Нікітин Г. Д., Мезенцева К. О. // Системи обробки інформації. – 2017. – Вип. 2(148). – С. 126-128.
4. Милославская Н. Г. Интрасети: доступ в Internet, защита : учебное пособие для вузов / Милославская Н. Г., Толстой А. И. – М. : ЮНИТИ – ДАНА, 2000. – 527 с.
5. Модели в информационной безопасности. URL: https://habr.com/ru/post/467269/(дата звернення 19.12.2019 р.).
6. Петров А. А. Компьютерная безопасность. Криптографические методы защиты информации / Петров А. А. – М. : ДМК, 2000. – 448 с.
7. Ревнивых А. В. Обзор политик информационной безопасности / Ревнивых А. В., Федотов А. М. // Вестник НГУ. Серия: Информационные технологии. – 2012. – №3. URL: https://cyberleninka.ru/article/n/obzor-politik-informatsionnoy-bezopasnosti (дата звернення 15.12.2019 р.).
8. Степанов В. Ю. Інформаційна безпека як складова державної інформаційної політики / Степанов В. Ю. // Державне будівництво. – 2016. – № 2. URL: http://www.kbuapa.kharkov.ua/e-book/db/2016-2/doc/1/02.pdf (дата звернення 15.12.2019 р.).
9. Чуруброва С. М. Політика інформаційної безпеки в системах інформаційно-аналітичного забезпечення підтримки прийняття організаційних рішень / Чуруброва С. М. // Проблеми програмування. –2016. – № 4. – С. 97-103.
10. Ярочкин В. И. Служба безопасности коммерческого предприятия / Ярочкин В. И. – М. : Ось-89, 1995. – 144 с.
11. Caballero A. Information security essentials for it managers: protecting mission-critical systems. Syngress, 2013. URL : https://booksite.elsevier.com/samplechapters/9781597495332/02~Chapter_1.pdf (дата звернення 19.12.2019 р.).
12. Defense in Depth: A Practical Strategy for Achieving Information Assurance in Today's Highly Networked Environments. National Security Agency, Information Assurance Solutions Group – STE 6737.

REFERENCES

1. Bohomolov, S. A. (2016), Modely typovykh polytyk bezopasnosty, available at: https://infourok.ru/lekciya-po-zaschite-informacii-modeli-bezopasnosti-927637.html (data zvernennia 12.12.2019 r.).
2. Zehdzha, D. P. and Yvashko, A. M. (2000), Osnovy bezopasnosty ynformatsyonnykh system, Horiachaia lynyia – Telekom, M., 452 s.
3. Mel'nyk, M. O. Nikityn, H. D. and Mezentseva, K. O. (2017), Analiz pobudovy modeli polityky informatsijnoi bezpeky pidpryiemstva, *Systemy obrobky informatsii*, vyp. 2(148), s. 126-128.
4. Myloslavskaia, N. H. and Tolstoj, A. Y. (2000), Yntrasety: dostup v Internet, zaschyta : uchebnoe posobye dlia vuzov, YuNYTY – DANA, M., 527 s.
5. Modely v ynformatsyonnoj bezopasnosty, available at: https://habr.com/ru/post/467269/(data zvernennia 19.12.2019 r.).
6. Petrov, A. A. (2000), Komp'iuternaia bezopasnost'. Kryptohrafycheskye metody zaschyty ynformatsyy, DMK, M., 448 s.
7. Revnyvykh, A. V. and Fedotov, A. M. (2012), Obzor polytyk ynformatsyonnoj bezopasnosty, *Vestnyk NHU. Seryia: Ynformatsyonnye tekhnolohyy*, №3, available at: https://cyberleninka.ru/article/n/obzor-politik-informatsionnoy-bezopasnosti (data zvernennia 15.12.2019 r.).
8. Stepanov, V. Yu. (2016), Informatsijna bezpeka iak skladova derzhavnoi informatsijnoi polityky, *Derzhavne budivnytstvo*, № 2, available at: http://www.kbuapa.kharkov.ua/e-book/db/2016-2/doc/1/02.pdf (data zvernennia 15.12.2019 r.).
9. Churubrova, S. M. (2016), Polityka informatsijnoi bezpeky v systemakh informatsijno-analitychnoho zabezpechennia pidtrymky pryjniattia orhanizatsijnykh rishen', *Problemy prohramuvannia*, № 4, s. 97-103.
10. Yarochkyn, V. Y. (1995), Sluzhba bezopasnosty kommercheskoho predpryiatyia, Os'-89, M., 144 s.
11. Caballero A. (2013), Information security essentials for it managers: protecting mission-critical systems. Syngress, available at : https://booksite.elsevier.com/samplechapters/9781597495332/02~Chapter_1.pdf (data zvernennia 19.12.2019 r.).
12. Defense in Depth: A Practical Strategy for Achieving Information Assurance in Today's Highly Networked Environments. National Security Agency, Information Assurance Solutions Group – STE 6737.

Стаття надійшла до редакції 3 липня 2019 р