DOI 10.15276/imms.v11.no3.239
УДК 004.056

Informatics and Mathematical Methods in Simulation
Vol. 11 (2021), No. 3, pp. 239-246

МОДЕЛЮВАННЯ ОРГАНІЗАЦІЙНИХ ЗАХОДІВ ДЛЯ СТВОРЕННЯ ПОЛІТИКИ БЕЗПЕКИ ОРГАНІЗАЦІЇ З ВИКОРИСТАННЯМ БІЗНЕС-ПРОЦЕСІВ

В.В. Радуш, О.Ю. Лебедєва, Н.І. Кушніренко, В.В. Зоріло

Національний університет «Одеська політехніка», пр. Шевченко, 1, Одеса, 65044, Україна; e-mail: o.y.lebedieva@opu.ua,kushnirenko@op.edu.ua, v.v.zorilo@op.edu.ua

Фундаментальним поняттям захисту інформації є політика безпеки, або політика захисту. Важливість цього поняття важко переоцінити – існують ситуації, коли правильно сформульована політика є чи не єдиним механізмом захисту від несанкціонованого доступу. Під поняттям політика безпеки інформації розуміється організована сукупність документованих керівних рішень, спрямованих на захист інформації й асоційованих з нею ресурсів системи. Політика безпеки викладає систему поглядів, основних принципів, практичних рекомендацій і вимог, що закладаються в основу реалізованого в системі комплексу заходів із захисту інформації. Формування політик безпеки є дуже складним аналітичним процесом, який важко формалізувати. У роботі наводяться організаційних заходів для створення політики безпеки підприємства. Для опису цих заходів використовуються нотації бізнес-процесів. Моделювання бізнес-процесу це процес відображення суб'єктивного бачення потоку робіт у вигляді формальної моделі, що складається з взаємопов'язаних операцій. В даний час найбільший розвиток і застосування при описі бізнес-процесів отримують графічні підходи та методи. Найбільш широко використовувана методологія опису бізнес-процесів це стандарт IDEF0.Нотація IDEF0 призначена для високорівневого опису бізнесу-процесу у функціональному аспекті. Було розроблено декомпозицію діаграм A-0 та A0. IDEF0 не використовують для побудови процесів нижнього рівня, які деталізують докладне виконання робіт персоналом для підвищення розуміння функціонування розробленого процесу було прийнято рішення показати взаємодію між механізмами, які використовувались у нотація IDEF0. Для опису взаємодії між механізмами була обрана нотація BPMN, яка орієнтована на детальний опис потоків робіт, і якнайкраще підходить для моделювання процесів на нижньому рівні.

Ключові слова: захист інформацій, політика безпеки, організаційні заходи для створення політики безпеки, бізнес-процес, нотації бізнес-процесу, IDEF0, BPMN.

Вступ

Сучасне суспільство характеризується бурхливим розвитком інформаційних технологій, які займають дедалі міцніше місце на підприємствах різного профілю, допомагаючи вирішувати нагальні завдання управління та функціонування підприємств. В умовах безперервно змінюваних та вдосконалюваних загроз, реалізація яких може призвести до зриву функціонування підприємства на перше місце виходять завдання забезпечення інформаційної безпеки.

У міру того, як процес інформатизації більшості сфер діяльності в Україні, промисловості, соціальній сфері, бізнесу тощо розвивається бурхливими темпами. Постає питання про комплексний підхід до захисту інформації. Політика інформаційної безпеки спрямована на вирішення цієї проблеми. Коректне розроблена та актуальна політика безпеки відображає думку керівництва з питання інформаційної безпеки, пов'язує докупи всі методи захисту інформації, регламентує роботу співробітників. Політики інформаційної безпеки є основою подальшої розробки документів із забезпечення безпеки процедур, регламентів, посадових інструкцій тощо.

Актуальність розробки політик інформаційної безпеки для компаній пояснюється необхідністю створення механізму управління та планування інформаційної безпеки.

Також політики інформаційної безпеки дозволяють удосконалювати такі напрями діяльності компанії, як залучення інвестицій, підтримка безперервності бізнесу, мінімізація ризиків, підвищення рівня довіри до компанії тощо. Удосконалення напрямів діяльності організації залежить від грамотності упорядкування політики інформаційної безпеки. Тому тема даної роботи э актуальною.

Метою роботи є розробка бізнес-процесу організаційних заходів для створення політики безпеки підприємства шляхом використання різних нотацій опису бізнес-процесів.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

- Провести аналіз організаційних заходів для створення політики безпеки підприємства;
- Проаналізувати та обрати нотації моделювання бізнес-процесів для опису організаційних заходів для створення політики безпеки підприємства;
- Розробити бізнес-процес з використанням обраних нотацій.

Основна частина

Забезпечення інформаційної безпеки – це комплексна проблема, розв'язання якої на практиці вимагає ефективного сполучення нормативно-правових заходів (законодавчий рівень), організаційних заходів, інженерно-технічних методів і засобів, блокування та нейтралізації технічних каналів витоку інформації (адміністративний і процедурний рівень), методів і засобів криптографічного та технічного і захисту (програмно-технічний рівень)[1].

Основу заходів адміністративного рівня, тобто заходів, що реалізуються керівництвом організації, становить політика безпеки.

Під політикою безпеки розуміється сукупність документованих управлінських рішень, спрямованих на захист інформації й асоційованих з нею ресурсів. Політика безпеки визначає стратегію організації в галузі інформаційної безпеки, а також ресурси, які керівництво вважає за можливе виділити для реалізації її завдань. На підставі політики безпеки будується програма безпеки, яка реалізується на процедурному й програмно-технічному рівнях.

Політикою інформаційної безпеки (ІБ) називається комплекс заходів, правил та принципів, якими у своїй повсякденній практиці керуються співробітники підприємства/організації з метою захисту інформаційних ресурсів.

За час, що минув із виникнення самого поняття ІБ, напрацьовано чимало подібних політик – у кожній компанії керівництво саме вирішує, яким чином та яку саме інформацію захищати.

Політика безпеки є обов'язковою складовою певних місцевих або міжнародних стандартів (ISO/IEC 17799, ISO/IEC 27001 тощо). Необхідна відповідність конкретним вимогам, які зазвичай висувають зовнішні аудитори, що вивчають діяльність організації. Відсутність безпекової політики породжує негативні відгуки, а подібні оцінки негативно впливають на такі показники організації, як рейтинг, рівень надійності, інвестиційна привабливість тощо.

Узгодження політики безпеки з керівництвом підприємства, це спосіб донести до керівників цілі та завдання безпеки компанії. Затверджена безпекова політика, по суті, є формалізованою думкою керівництва компанії з питань забезпечення захисту інформації, на яку можна посилатися при обговоренні поточних питань, пов'язаних з безпекою.

Ще одне призначення політики інформаційної безпеки підприємства – доведення до рядових працівників основних принципів та правил захисту інформації, прийнятих у компанії. Зазвичай прості користувачі не будуть вдумливо читати насичені технічними термінами документи, наприклад, інструкції з роботи з електронною поштою або регламент антивірусного захисту. Політика безпеки, будучи верхньорівневим документом,

повинна у простій та зрозумілій формі доносити до кожного працівника позицію компанії щодо питань, пов'язаних з інформаційною безпекою.

Методологія моделювання, включає послідовність дій, які необхідно виконати для побудови моделі (процедуру моделювання), і нотацію (мова). Мова моделювання має свій синтаксис (умовні позначення різних елементів та правила їх поєднання) та семантику (правила тлумачення моделей та їх елементів).

Бізнес-процес являє собою систему послідовних, цілеспрямованих і регламентованих видів діяльності, в якій за допомогою керуючого впливу і за допомогою ресурсів входи процесу перетворюються в виходи, результати процесу, що представляють цінність для споживачів.

Ключовими властивостями бізнес-процесу є те, що це кінцева і взаємопов'язана сукупність дій, що визначається відносинами, мотивами, обмеженнями і ресурсами всередині кінцевої множини суб'єктів і об'єктів, які об'єднуються в систему заради спільних інтересів з метою отримання конкретного результату.

Моделлю бізнес-процесу називається його формалізований (графічний, табличний, текстовий, символьний) опис, що відображає реально існуючу або передбачувану діяльність підприємства[2].

Модель, як правило, містить такі відомості про бізнес-процес:

1) набір складових процесів кроків – бізнес-функцій;
2) порядок виконання бізнес-функцій;
3) механізми контролю та управління в рамках бізнес-процесу;
4) виконавців кожної бізнес-функції;
5) вхідні документи/інформацію, що використовуються кожною бізнес-функцією;
6) вихідні документи/інформацію, що генеруються кожною бізнес-функцією;
7) ресурси, необхідні для виконання кожної бізнес-функції;
8) документацію/умови, що регламентують виконання кожної бізнес-функції;
9) параметри, що характеризують виконання бізнес-функцій та процесу в цілому.

Метою моделювання є систематизація знань про компанію та її бізнес-процеси в наочній графічній формі з тим, щоб в подальшому дані процеси можна було аналізувати і вдосконалювати. Моделювання бізнес-процесів дозволяє проаналізувати не тільки, як працює підприємство в цілому, як воно взаємодіє із зовнішніми організаціями, замовниками та постачальниками, але і як організована діяльність на кожному окремо взятому робочому місці.

Текстовий спосіб опису бізнес-процесу це такий спосіб, що являє собою простий текстовий послідовний опис процесів.

Табличний спосіб опису бізнес-процесу є більш формалізованим і передбачає розбиття бізнес-процесу по осередках структурованої таблиці, в якій кожен стовпець і рядок мають деякий певне значення.

В даний час найбільший розвиток і застосування при описі бізнес-процесів отримують графічні підходи та методи. Вони мають найбільшу результативністю при вирішенні задач по опису, аналізу та раціоналізації діяльності підприємства.

Нотація – це набір знаків і правил, які використовуються для графічного опису, моделювання бізнес-процесів. Нотація визначає як ми позначаємо на схемі процеси, операції, події та тощо, і за якими правилами з'єднуємо їх між собою.

Найбільш широко використовувана методологія опису бізнес-процесів – стандарт IDEF0. Моделі у нотації IDEF0 призначені для високорівневого опису бізнесу компанії у функціональному аспекті. За допомогою наочної графічної мови IDEF0 система, що вивчається, постає перед розробниками та аналітиками у вигляді набору взаємопов'язаних функцій (функціональних блоків – у термінах IDEF0). Як правило, моделювання засобами IDEF0 є першим етапом вивчення будь-якої системи.

Розглянемо основні елементи нотації IDEF0, такі як результат, власник, виконавець, вхід, управління та механізми процесу.

В нашій роботі головний процес, що описується – це створення політики безпеки.

Результат бізнес-процесу – те, заради чого здійснюється бізнес-процес, тобто діяльність завжди розглядається разом з метою цієї діяльності – отримання на виході деякого результату, що задовольняє заданим вимогам. Результати бізнес-процесу часто згадуються як виходи бізнес-процесу. В нашій роботі результатом опису організаційних заходів для створення політики безпеки підприємства є документ з описаною політикою безпеки.

Власник бізнес-процесу – посадова особа, яка несе відповідальність за отримання результату процесу і володіє повноваженнями для розпорядження ресурсами, необхідними для виконання процесу. В нашій роботі власником бізнес-процесу є начальник відділу ІБ.

Виконавці бізнес-процесу – команда фахівців з різних функціональних областей (крос-функціональна команда), що виконують дії процесу. В нашій роботі виконавці – це спеціаліст з відділу ІБ та експертна група.

Входи бізнес-процесу – ресурси (матеріальні, інформаційні), необхідні для виконання і отримання результату процесу, які споживаються або перетворюються при виконанні процесу. В нашій роботі входи це відомості про організацію, для якої створюється політика безпеки.

Під відомостями про організацію будемо розуміти: структуру організації, модель ієрархії засобів обчислювальної техніки, ресурси інформаційної системи, що підлягають захисту, технологію обробки інформації.

Управління процесу – як правило інформація, яка визначає правила перетворення входів в вихід. В нашій роботі під управлінням процесу будемо розуміти стандарти, які використовуються для створення політики безпеки.

Механізм процесу – то, що перетворює вхід у вихід. Механізмами, як правило, є співробітники (в роботі це начальник відділу ІБ, спеціаліст з відділу ІБ, експертна група, керівники відділів) організації та техніка, на якій вони працюють (в роботі це програмне забезпечення для створення документу з політика безпеки).

Для опису процесу в нотації IDEF0 використовується такий принцип, як декомпозиція. Використання декомпозиції дозволяє розділити кожен блок, який розуміється як єдине ціле, на свої складові, що описуються на більш детальній діаграмі. Процес декомпозиції проводиться до досягнення необхідного рівня подробиці опису. Кожний рівень опису оформлюється як контекстна діаграма.

Перша діаграма в ієрархії діаграм IDEF0 завжди зображує функціонування системи в цілому. Такі діаграми позначаються А-0 (А мінус нуль). На рисунку 1 зображена діаграма А-0.

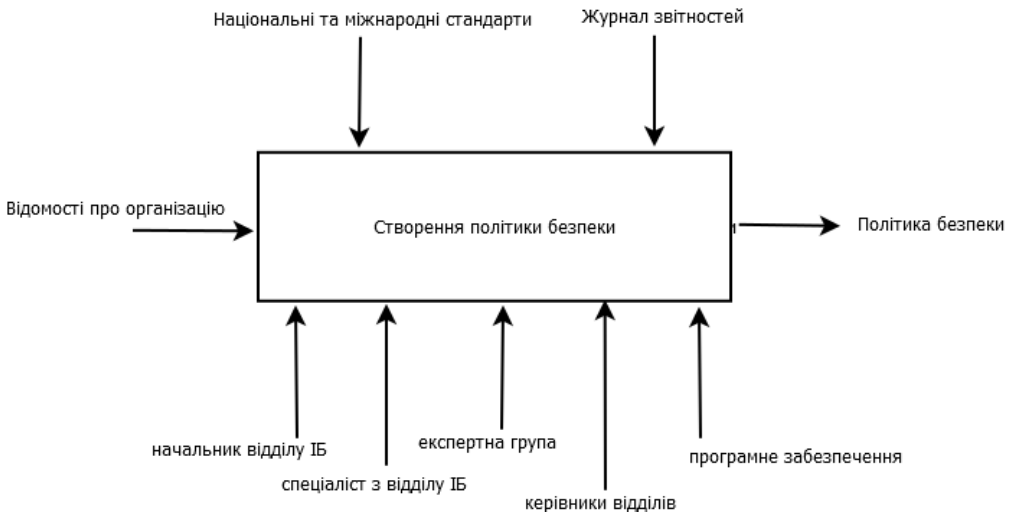

Рис. 1. Діаграма А-0

Процес «Створення політики безпеки» можна поділити на такі підпроцеси:

- Аудит інформаційної безпеки;
- Оцінювання ризиків;
- Опис правил інформаційного обміну з урахуванням ризиків і інцидентів, що виникали раніше.

Аудит інформаційної безпеки підприємства – процес отримання об'єктивних якісних та кількісних оцінок про поточний стан інформаційної безпеки організації відповідно до певних критеріїв, стандартів та показників.

Аудит ІБ передбачає реалізацію наступних етапів:

- проведення аудиту об’єкту інформаційної діяльності.
- створення моделі загроз.

Результатом аудиту будуть ризики, пов’язані з вразливостями в ІБ.

Другий процес при створенні політики безпеки це оцінка ризиків. Спочатку встановлюється зв’язок між ресурсами, втратами, загрозами і вразливими місцями, виділеними на процесі «Аудит ІБ».

Оцінка ризиків на цьому кроці здійснюється шляхом:

- з’ясування наслідків для ресурсів в разі реалізації ризиків в плані конфіденційності, цілісності та доступності;
- оцінки імовірності реалізації ризиків;
- встановлення рівня ризиків.

Ціль оцінки ризиків полягає у визначенні характеристик ризиків для інформаційної системи і її ресурсів. На основі таких даних можуть бути обрані необхідні засоби керування ІБ. Діаграма другого рівня (A0) зображена на рисунку 2.

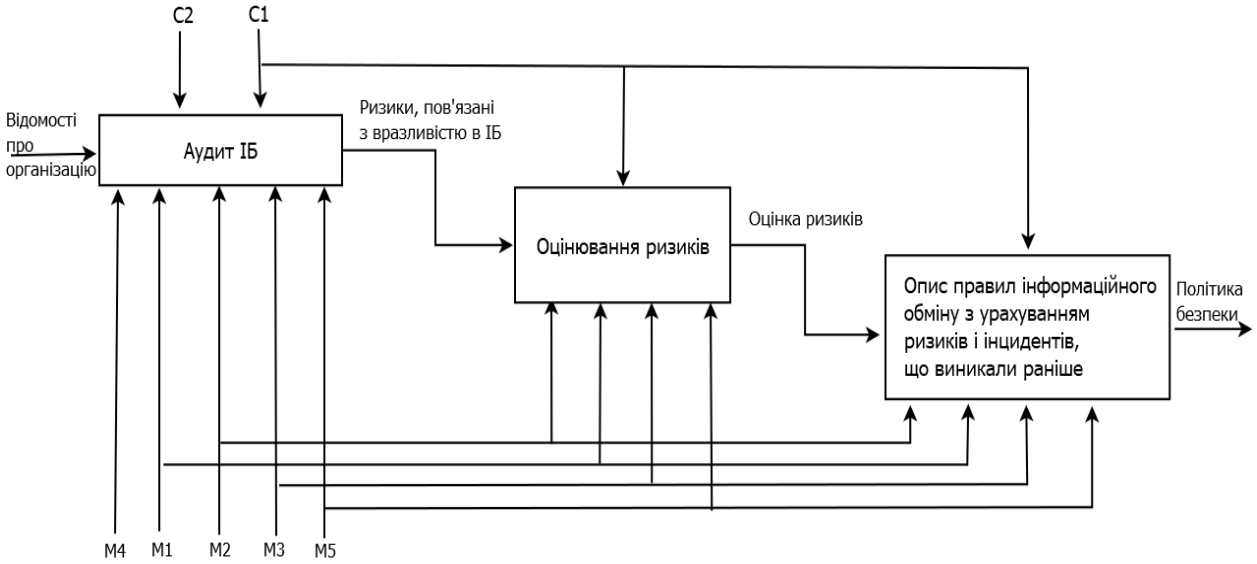

Рис. 2. Діаграма A0

За всіх переваг IDEF0 її не використовують для побудови процесів нижнього рівня, то що вона не деталізує докладне виконання робіт персоналом. По-перше, нотація IDEF0 не здатна відобразити тимчасову послідовність виконання робіт, а по-друге, не містить блоків умовного переходу, тому всі процеси описуватимуть роботи лише лінійно і недостатньо деталізовано.

При описі процесу «Створення політики безпеки» в нотації IDEF0 були запропоновані такі механізми, як начальник відділу ІБ, спеціаліст з відділу ІБ, експертна група, керівники відділів. Для підвищення розуміння функціонування процесу «Створення політики безпеки» бажано показати взаємодію між цими механізмами. Для цієї задачі підійде нотація BPMN.

BPMN (Business Process Management Notation) – це мова моделювання бізнес-процесів, яка є проміжною ланкою між формалізацією/візуалізацією та втіленням бізнес-процесу. Нотація є описом графічних елементів, що використовуються для побудови схеми протікання бізнес-процесу.

Розроблений процес «Створення політики безпеки» в нотації BPMN зображено на рисунку 3.

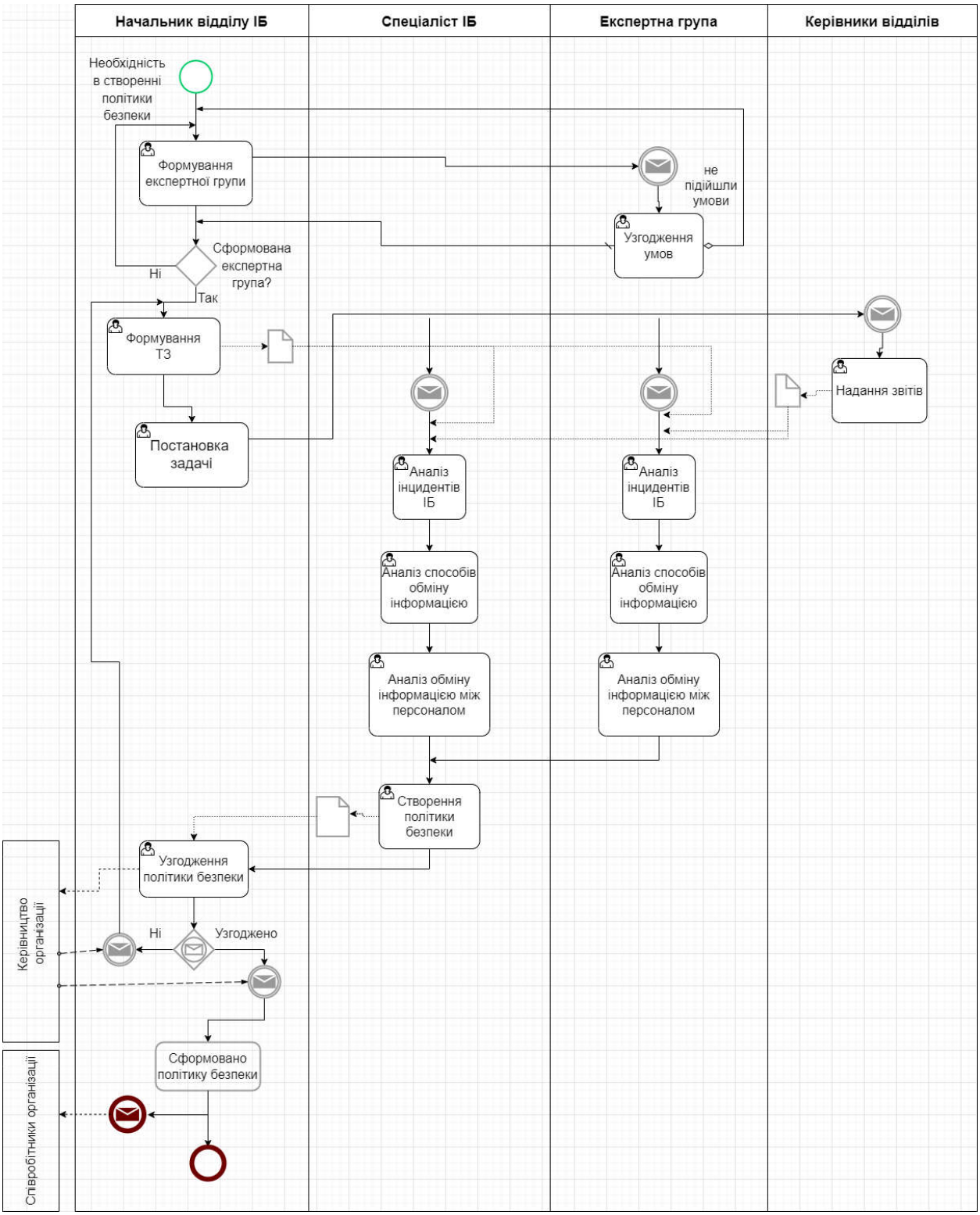

Рис. 3. Розроблений процес в нотації BPMN

Для відображення взаємодії між учасниками бізнес-процесу в нотації BPMN використовуються елементи Пул та Доріжка. Елемент Доріжка часто використовують як внутрішні ролі (зони відповідальності), що є розподілом обов'язків серед учасників процесу. Для процесу «Створення політики безпеки» в якості доріжок виступають начальник відділу ІБ, спеціаліст з відділу ІБ, експертна група, керівники відділів.

Доріжка фактично є зоною відповідальності учасника: будь-який елемент, вміщений у доріжку, виконується виконавцем, прописаним у заголовку доріжки.

Під дією або завданням у нотації BPMN розуміється одиниця роботи, що виконується під час виконання бізнес-процесу.

Подія є одним із головних елементів BPMN і служить для опису того, що має статися (на відміну від завдання, коли щось має бути зроблено). Залежно від стану події на схемі процесу діляться на: початкова подія (що ініціює бізнес-процес), проміжна подія, кінцева подія (що закінчує бізнес-процес).

Потік – це послідовність дій, що позначається стрілкою. Елемент потік показує яку дію після якої потрібно зробити.

Під артефактами в BPMN розуміють об'єкти, які безпосередньо не впливають на виконання бізнес-процесу. Це може бути документи, дані, інформація.

Висновки

Було проведено аналіз організаційних заходів для створення політики безпеки підприємства. Були розглянуті сучасні нотації моделювання бізнес-процесів. Для опису організаційних заходів для створення політики безпеки підприємстваобрано нотації IDEF0 та BPMN. Було розроблено процес «Створення політики безпеки» з використанням обраних нотацій.

Список літератури

1. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. К.: Видавництво НА СБ України, 2020. 256 с.
2. Гадецька З.М., Холопова М.О. Моделювання бізнес-процесів діяльності підприємства. *Ефективна економіка*. 2016. № 5. URL: http://www.economy.nayka.com.ua/?op=1&z=4950

MODELING ORGANIZATIONAL ACTIVITIES TO CREATE AN ORGANIZATION'S SECURITY POLICY USING BUSINESS PROCESSES

V.V. Radush, O.Yu. Lebedieva, N.I. Kushnirenko, V.V. Zorilo

National Odessa Polytechnic University

The fundamental concept of information security is security policy. The importance of this concept is difficult to overestimate - there are situations where a well-formulated policy is almost the only mechanism to protect against unauthorized access. The concept of information security policy means an organized set of documented management decisions aimed at protecting information and associated system resources. The security policy sets out a system of views, basic principles, practical recommendations and requirements that underlie the set of information protection measures implemented in the system. Security policy-making is a very complex analytical process that is difficult to formalize. The paper presents organizational measures to create a security policy of the enterprise. Business process notations are used to describe these activities. Business process modeling is the process of reflecting a subjective vision of the workflow in the form of a formal model consisting of interrelated operations. Currently, the greatest development and application in the description of business processes are graphical approaches and methods. The most widely used business process description methodology is the IDEF0 standard.IDEF0 notation is intended for a high-level description of the business process in functional terms. Decomposition of diagrams A-0 and A0 was developed. IDEF0 is not used to build lower-level processes that detail the detailed work performed by staff. To increase the understanding of the functioning of the developed process, it was decided to show the interaction between the mechanisms used in the IDEF0 notation. To describe the interaction between the mechanisms, the BPMN notation was chosen, which focuses on a detailed description of workflows and is best suited for modeling lower-level processes.

Keywords: information protection, security policy, organizational measures for creating security policy, business process, business process notation, IDEF0, BPMN.