Міністерство освіти і науки України
Державний вищий навчальний заклад
«Національний гірничий університет»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
дипломної роботи

магістра
(ступінь підготовки)

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

напрям підготовки (спеціальність) *125 Кібербезпека*
(код і назва напряму підготовки)

спеціалізація (освітня програма) *Кібербезпека*
(код і назва спеціальності)

ступінь підготовки *магістр*
(назва освітнього рівня)

кваліфікація *професіонал із організації інформаційної безпеки*
(код і назва кваліфікації)

на тему: ***Архітектури управління інформаційною та кібербезпекою для підприємств середнього бізнесу***

Виконавець: студент ***6*** **курсу, групи** ***125м-16-1***

_____ ***Лимарчук-Яциковська Тетяна Олександрівна***
(підпис) (прізвище ім'я по-батькові)

Керівники	Прізвище, ініціали	Оцінка	Підпис
роботи	д.ф.-м.н., проф. Кагадій Т.С.		
розділів:			
спеціальний	ас. Мілінчук Ю.А.		
економічний	к.е.н., доц. Волотковська Ю.О.		

Рецензент			

Нормоконтроль			

Дніпро
2018

Міністерство освіти і науки України
Державний вищий навчальний заклад
«Національний гірничий університет»

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
д.т.н., доц. _____Корнієнко В.И

«_____»_____201_ року

ЗАВДАННЯ
на виконання кваліфікаційної роботи магістра

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

студенту ***125м-16-1*** ***Лимарчук-Яциковській Тетяні Олександрівні***
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи ***Архітектурні методи управління інформаційною та кібербезпекою для середнього бізнесу***

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора Державного ВНЗ «НГУ» _____

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень *особливості застосування архітектурного методу для управління інформаційною безпекою в умовах середнього бізнесу.*

Предмет досліджень *Управління інформаційною та кібербезпекою на підприємствах середнього бізнесу за домогою архітектурних методів*

Мета НДР *забезпечення спостереженості інформації та зручності масштабування інформаційних систем на підприємствах середнього бізнесу*

Вихідні дані для проведення роботи *законодавство України та міжнародні стандарти у сфері інформаційної безпеки, наукові публікації вітчизняних та іноземних авторів, показники діяльності підприємства.*

3 ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна	*полягає в розробці архітектурної моделі, яка базується на існуючих методиках та пристосовує методологію до властивостей середнього бізнесу*
Практична цінність	*полягає в розробці адаптованої архітектурної моделі, яка покращує забезпечення спостереженості інформації та зручність масштабування інформаційних систем.*

4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Результати роботи мають відповідати вимогам чинного законодавства України та бути поданим у вигляді, що дозволяє безпосереднє використання при прийнятті

рішення із моделювання архітектури підприємства з урахуванням потреб інформаційної безпеки на підприємствах середнього бізнесу

5 ЕТАПИ ВИКОНАННЯ РОБІТ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Ознайомлення з існуючими архітектурними моделями, порівняння моделей управління інформаційної безпеки	30 жовтня 2017 – 20 листопада 2017
Дослідження додаткових інструментів розширення існуючих архітектур, відповідності архітектур кібербезпеки національним нормативним актам	20 листопада 2017– 4 грудня 2017
Розробка архітектурної моделі з урахуванням вимог інформаційної безпеки	4 грудня 2017 – 4 січня 2018
Визначення витрат на реалізацію запропонованих рекомендацій, щодо впровадження архітектурного методу управління ІБ та довести економічну ефективність цих рекомендацій	4 січня 2017 – 15 січня 2018
Оформлення технічної документації	15 січня 2018 – 23 січня 2018

6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект *від реалізації результатів роботи очікується позитивним завдяки оптимізації витрат на інформаційну безпеку через застосування запропонованої у дипломній роботі методики управління ІБ.*

Соціальний ефект *дипломної роботи, як наслідок підвищення спостереженості інформації зменшуються ризики помилкових звинуваченнь співробітків у інцидентах підприємства у його надійності.*

7 ДОДАТКОВІ ВИМОГИ

Відповідність оформлення пояснювальної записки:
ДСТУ 3008-95. «Документація. Звіти у сфері науки і техніки. Структура і правила оформлення».
Бабенко Т.В. Методичні вимоги до підготовки та захисту дипломної роботи (проекту) для студентів галузей знань 1701 «Інформаційна безпека» та спеціальності 125 «Кібербезпека» / Бабенко Т.В., Корнєєв М.В., Кручінін О.В., Тимофєєв Д.С.; Нац. гірн. ун-т. – Д: НГУ, 2016. – 45 с.
Бабенко Т.В. Методичні вимоги до підготовки та захисту дипломної роботи

Завдання видала _____ д.ф.-м.н., проф. Кагадій Т.С.
(підпис) (прізвище, ініціали)

Завдання прийняла до виконання _____ Лимарчук-Яциковська Т.О.
(підпис) (прізвище, ініціали)

Дата видачі завдання: 30.10.2017
Термін подання дипломної роботи до ДЕК 23.01.2017

ЗМІСТ

РЕФЕРАТ

Пояснювальна записка ___с., ___рис.,___табл.,___ додатків, ___джерел.

Об’єкт дослідження: особливості застосування архітектурного методу для управління інформаційною безпекою в умовах середнього бізнесу.

Мета роботи: забезпечення спостереженості інформації та зручності масштабування інформаційних систем на підприємствах середнього бізнесу.

Методи дослідження: морфологічний аналіз; спостереження; порівняння; аналіз та синтез; системний підхід; історичний метод; абстрагування.

У спеціальній частині було проаналізовано особливості застосування архітектурного методу для управління інформаційною безпекою в умовах середнього бізнесу. Досліджено різноманіття архітектурних моделей. У роботі проаналізовано архітектурні методи управління ІБ та кібербезпеки. Розроблено та запропоновано адаптовану для вимог середнього бізнесу архітектурну модель В економічному розділі визначено що, архітектурний метод управління інформаційною та кібербезпекою заощаджує витрати та покриває потреби ІБ підприємств середнього бізнесу. Практичне значення роботи полягає в розробці адаптованої архітектурної моделі. Запропонована нова модель покращує забезпечення спостереженості інформації та зручність масштабування інформаційних систем. Результати здійснених у дипломній роботі досліджень можуть бути впровадженні на підприємствах середнього бізнесу.

Наукова новизна одержаних результатів: Вперше розроблено архітектурну модель, яка базується на методиках TOGAF і SABSA. Запропонована архітектурна модель відрізняється від існуючих тим, що вона забезпечує спільну рівноправну роботу фахівців ІТ та ІБ та об’єднує орієнтованість на інфраструктуру та додатки і на безпеку.

Напрямки подальших досліджень. Необхідна апробація нової моделі архітектури та подальше удосконалення даної моделі.

АРХІТЕКТУРНИЙ ПІДХІД, СПОСТЕРЕЖЕННІСТЬ, МАСШТАБУВАННЯ

РЕФЕРАТ

Пояснительная записка___с.,___рис.,___табл.,____ прил., _ __ источников.

Объект исследования: особенности применения архитектурного метода для управления информационной безопасностью в условиях среднего бизнеса.

Цель работы: обеспечение наблюдаемости информации и удобства масштабирования информационных систем на предприятиях среднего бизнеса.

Методы исследовании: морфологический анализ; наблюдения; сравнения; анализ и синтез; системный подход; исторический метод; абстрагирования.

В специальной части были проанализированы особенности применения архитектурного метода для управления ИБ в условиях среднего бизнеса. Исследовано многообразие архитектурных моделей. В работе проанализированы архитектурные методы управления ИБ и кибербезопасности. Разработано и предложено адаптированную, для среднего бизнеса, архитектурную модель. В экономическом разделе определено, что архитектурный метод управления информационной и кибербезопасностью экономит расходы и покрывает потребности ИБ предприятий среднего бизнеса.

Практическое значение работы состоит в разработке адаптированной архитектурной модели, которая отличается от существующих тем, что улучшает обеспечение наблюдаемости информации и удобство масштабирования информационных систем. Результаты проведенных в дипломной работе исследований могут быть внедрены на предприятиях среднего бизнеса. Научная новизна полученных результатов: впервые разработан архитектурной модель, основанная на методиках TOGAF и SABSA. Предложенная архитектурная модель отличается от существующих тем, что она обеспечивает совместную равноправную работу специалистов ИТ и ИБ и объединяет ориентированность на инфраструктуру и приложения и на безопасность.

Направления дальнейших исследований. Необходима апробация новой модели архитектуры и дальнейшее совершенствование данной модели.

АРХИТЕКТУРНЫЙ ПОДХОД, НАБЛЮДАЕМОСТЬ, МАСШТАБИРУЕМОСТЬ

ABSTRACT

Explanatory note __ p., __ pic., __ tables., __ applications, __ sources.

Object of research: features of the application of architectural method for information security management in a medium-sized business.

Objective: ensuring observability of information and convenience of scaling information systems at medium-sized enterprises.

Research methods: analysis, synthesis, induction, deduction, maximum likelihood method, system analysis, structural analysis, comparison and observation methods.

In the special chapter, the features of the application of the architectural method for information security management in the conditions of medium business were analyzed.

The diversity of architectural models was investigated. The work analyzes the architectural methods of management of information security and cybersecurity. An architectural model adapted to the requirements of a medium-sized business has been developed and proposed within the work.

In the economic section it was determined that the architectural method of information and cyber security management saves costs and covers the needs of information security of medium-sized businesses.

The practical value of the work is in development of an adapted architectural model. The proposed new model differs from existing ones by improving the provision of information observability and the convenience of scaling information systems. The results of the thesis research can be implemented at medium-sized enterprises.

The scientific novelty of the work is the following: For the first time an architectural model based on TOGAF and SABSA techniques was developed. The proposed architectural model is different from the existing ones because it provides equal and cooperative work of the IT and information security professionals and combines infrastructure and application focus with security focus.

ARCHITECTURAL APPROACH, OBSERVABILITY, SCALING

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ДСТУ – державний стандарт України;

ІБ – інформаційна безпека;

ІТ – інформаційні технології;

ІС – інформаційна система;

НД – нормативний документ;

НД ТЗІ – нормативний документ технічного захисту інформації;

ПЗ – програмне забезпечення;

АЗ – апаратне забезпечення;

ПБ – політика безпеки;

КЗЗ – комплекс засобів захисту;

КС – комп’ютерна система;

ІР – інформаційний ресурс;

ТЗ – технічне завдання;

DLP – Data Leak Prevention;

IPS – Intrusion prevention system;

IDS – Intrusion detection system;

SIEM – security information & event management;

ADM – architecture develop method;

КПЕ – ключові показники ефективності.

ВСТУП

У наш час більшість підприємств вже замислюється над тим, що їм треба захищати свою інформацію та інформаційні ресурси. Після нечуваної для України кібератаки 27 червня 2017 року, майже всі зрозуміли, що їм потрібен фахівець з кібербезпеки. Фахівцеві з кібербезпеки в більшості випадків в структурах середнього бізнесу необхідно створювати систему управління інформаційною безпекою. Складність реалізації даної задачі полягає в тому, що середній бізнес – це дуже динамічна система, яка потребує оперативного втручання, прийняття рішень, змінення механізмів та цілей обробки інформації і всі ці аспекти повинні бути реалізовані при мінімальному фінансуванні.

В наш час все більше уваги приділяється новому напрямку – архітектурі підприємства. Даний напрямок, спочатку, призначався для вирішення двох основних проблем у сфері IT. Перша проблема полягає в постійному збільшенні складності IT-систем, що призводить до збільшення витрат на їх побудову. Друга – викликана тим, що с часом отримати реальну віддачу від IT-систем стає важче. Тобто, не зважаючи на дедалі зростаючу вартість IT-систем, підприємствам з великими труднощами вдається підтримувати відповідність вимогам бізнесу.

Очевидно, ці проблеми взаємопов’язані. Чим складніша система, тим важче нею управляти. Чим краще вдається впоратись зі складністю системи, тим вище ймовірність отримати від неї реальні вигоди.

Метою дипломної роботи є забезпечення спостереженості інформації та зручності масштабування інформаційних систем на підприємствах середнього бізнесу.

Для досягнення зазначеної мети дипломної роботи поставлені окремі завдання:

— визначитися з понятійним полем;

— ознайомитися з архітектурним методом управління;

— провести аналіз деяких існуючих архітектурних моделей;

— провести дослідження додаткових інструментів розширення існуючих архітектур;
— перевірити сумісність обраних архітектур з національнам законодавством;
— розробити архітектурну модель, яка враховує вимоги середнього бізнесу до ІБ;
— обґрунтування доцільності впровадження розробленої архітектури.

Об’єкт дослідження – особливості застосування архітектурного методу для управління інформаційною безпекою в умовах середнього бізнесу.

Предмет дослідження – управління інформаційною та кібербезпекою на підприємствах середнього бізнесу за допомогою архітектурних методів.

Методи дослідження: морфологічний аналіз (для визначення поняття «архітектура підприємства», «архітектура інформаційних систем», «архітектура кібербезпеки»); спостереження (виявлення актуального «лінійного» підходу до ІБ на підприємствах середнього бізнесу); порівняння (відповідність архітектурних моделей з національною нормативною базою); аналіз та синтез; системний підхід; історичний метод; абстрагування.

Наукова новизна досліджень – Вперше розроблено архітектурну модель, яка базується на методиці описи архітектури Open Group (TOGAF) і Шервудській прикладній архітектурі безпеки бізнесу (SABSA). Запропонована архітектурна модель відрізняється від існуючих тим, що вона забезпечує спільну рівноправну роботу фахівців ІТ та ІБ та об’єднує орієнтованість на інфраструктуру та додатки і на безпеку.

Практичне значення одержаних результатів полягає в розробці адаптованої архітектурної моделі. Запропонована нова модель відрізняється від існуючих тим, що покращує забезпечення спостереженості інформації та зручність масштабування інформаційних систем. Результати здійснених у дипломній роботі досліджень можуть бути впровадженні на підприємствах середнього бізнесу

Питання архітектурних методів ґрунтовно розглядаються у роботах таких авторів, як Дж. Захман, Телемтаєв М.М., Мартиросян С.Т., Козлов Ю.І. та ін.

Основні наукові положення доповідалися та обговорювалися на п’ятій всеукраїнській науково-технічній конференції студентів, аспірантів і молодих учених «Молодь: наука та інновації», а також викладені у збірнику праць цієї конференції.

РОЗДІЛ 1.

АНАЛІЗ НОРМАТИВНОЇ БАЗИ ТА МЕТОДИЧНИХ МАТЕРІАЛІВ У СФЕРІ АРХІТЕКТУРНИХ МЕТОДІВ УПРАВЛІННЯ

1.1 Терміни та визначення

Згідно Закону України «Про інформацію» захист інформації – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї [1].

Згідно Закону України «Про основні засади забезпечення кібербезпеки України» [2]:

1 кібербезпека - захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;

2 інформація про інцидент кібербезпеки - відомості про обставини кіберінциденту, зокрема про те, які об’єкти кіберзахисту і за яких умов зазнали кібератаки, які з них успішно виявлені, нейтралізовані, яким запобігли за допомогою яких засобів кіберзахисту, у тому числі з використанням яких індикаторів кіберзагроз;

3 інцидент кібербезпеки (далі - кіберінцидент) - подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів;

4 кібератака - спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту;

5 кіберзагроза - наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об’єктів;

6 кіберзахист - сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем;

7 кіберпростір - середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з’єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних;

8 критична інформаційна інфраструктура - сукупність об’єктів критичної інформаційної інфраструктури;

9 критично важливі об’єкти інфраструктури (далі - об’єкти критичної інфраструктури) - підприємства, установи та організації незалежно від форми

власності, діяльність яких безпосередньо пов’язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров’я людей.

1.2 Архітектурний підхід управління

Всі знають, що світ змінюється швидше, ніж раніше, і що інформаційні системи повинні встигати за цими змінами. Але відомо і інше. Впроваджену та реально використовувану систему важко (довго, дорого, часто нездійсненно) змінити. В результаті ІС може стати або стає гальмом розвитку підприємства. Причини можуть бути різними, але джерела проблем - завжди в трансформації підприємства. Рівень розвитку сучасних технологій настільки високий, що дозволяє побудувати інформаційну систему будь-якого масштабу, складності й функціональності. Однак, з огляду на вимоги бізнесу, засновані на показниках різних бізнес-оцінок, виникають додаткові складності, вирішення яких зводиться до забезпечення раціонального підходу до процесу проектування, реалізації й подальшій експлуатації інформаційних систем. Виходячи із цього, можна однозначно вважати обрану архітектуру одним з основних показників ефективності створюваної інформаційної системи, а, отже, і успішності бізнесу.

Архітектура підприємства являє собою процес збору та поширення інформації про те, як організація використовує і повинна використовувати ІТ в своїй діяльності. По суті, архітектура підприємства являє собою інформаційну основу корпоративної структури компанії. Безпосередньо архітектура підприємства не описує конкретні технічні рішення окремих інформаційних систем, але дозволяє отримати істотну вигоду для бізнесу організації в цілому, що пов'язано з підвищенням ступеня використання та ефективності інформаційних систем і програмних продуктів, стандартизацією і повторним використанням ІТ-ресурсів, а також зниженням ризиків інвестицій в ІТ-сфері.

Визначити поняття "архітектура інформаційної системи" можна безліччю способів.

Загалом архітектуру інформаційної системи можна описати як концепцію, що визначає модель, структуру, виконувані функції й взаємозв’язок компонентів інформаційної системи.

Концепція архітектури інформаційної системи повинна формуватися ще на етапі техніко-економічного обґрунтування й вибиратися такою, щоб вартість володіння нею була мінімальною.

Для того щоб конструктивно визначити архітектуру, необхідно відповісти на ряд питань:

— Що робить система?

— На які складові частина вона розділена?

— Яким чином відбувається взаємодія цих частин?

— Як і де ці частини розміщені?

Таким чином, можна вважати архітектуру інформаційної системи моделлю, що визначає вартість володіння через наявну в даній системі інфраструктуру.

Чому питання формування IT-архітектури стають особливо актуальними саме зараз? Пояснення може грунтуватися на цілій сукупності факторів, основні з яких пов'язані з:

— змінами в самому бізнесі і індустріальному суспільстві;

— зміною ролі інформаційних технологій в бізнесі і суспільстві;

— зміною корпоративної культури та стилю управління в бізнесі;

— а також з об'єктивним збільшенням IT-бюджетів компаній.

До числа характерних змін бізнесу, які мають істотний вплив на використання інформаційних технологій, відносяться перш за все:

— глобалізація бізнесу, пов'язана з необхідністю об'єднання різних національних процесів, даних і персоналу;

—динаміка злиттів і поглинань, що призводить до об'єктивно необхідної інтеграції різних інформаційних систем, об'єднання IT-служб і, що є найбільш складним, інтеграції різних корпоративних культур;

—поява адаптивного стилю бізнесу - перехід від моделі, заснованої на наявній лінійці продуктів (т.зв. "make-and-sell"), до моделі, заснованої на гнучкому реагуванні на потреби ринку - ("sense-and-respond"). Цей стиль пов'язаний з визнанням неминучості і непередбачуваності змін у зовнішньому середовищі. Компанії, які взяли таку модель, пов'язують досягнення успіху зі здійсненням таких перетворень в бізнес-процесах і організаційній структурі, які могли б оперативно і адекватно підлаштовуватися під зміни, що відбуваються;

—скорочення характерних тривалостей бізнес-процесів і віртуалізація бізнесу.

Методика є інструментом для створення широкого спектра різних архітектур. Вона, як правило, включає в себе опис методів проектування архітектури, опис того, як різні ланки проектування пов'язані між собою, набір інструментів для опису елементів архітектури, загальний словник використовуваних термінів. Методики також можуть містити список рекомендованих стандартів і сумісних продуктів, які можуть використовуватися для реалізації різних елементів архітектури. Важливо розуміти, що методики не тільки задають набір документів і планів, необхідних для опису підприємства, а й визначають, як всі ці елементи опису пов'язані між собою.

Методики описують, як визначаються і документуються основні елементи архітектури підприємства. Вони дозволяють вирішити проблему поганого взаєморозуміння між залученими в цей процес людьми, оскільки задають якийсь загальний, однаково зрозумілий набір понять і моделей для опису елементів архітектури в інтересах різних категорій зацікавлених сторін. Розробка одних методик була ініційована державними структурами, інших - приватним сектором та представниками індустрії. Різні методики, як правило, орієнтовані на різні аудиторії потенційних користувачів і відрізняються

широтою охоплення проблеми, увагою до певних галузей, хоча тенденція полягає в поступовій уніфікації визначень, пов'язаних з архітектурою. Деякі з методик концентруються на певних секторах індустрії, переваги інших підходів полягають у більш чіткому документуванні, а треті приділяють більшу увагу процесу переходу від сьогоднішнього в майбутній стан архітектури.

Існують індустріальні стандарти на опис архітектури підприємства, прийняті такими організаціями, як Інститут інженерів електрики і електроніки (IEEE - Institute of Electrical and Electronics Engineers), міжнародна організація стандартизації (ISO - International Organization for Standardization), The Open Group і т.д. Але жоден з цих стандартів не займає домінуючого положення. Більш того, жоден з них, взятий окремо, не дає групам, відповідальним за розробку архітектури, всіх інструментів, необхідних з методичної точки зору і з точки зору шаблонів, які використовуються для опису архітектури. Однак цей накопичений арсенал методик і стандартів надає архітекторам широкі можливості вибору архітектурних моделей, прикладів і досвіду різних індустрій.

При цьому треба чітко розуміти, по-перше, відмінність методики опису архітектури від самої архітектури як такої, а по-друге те, що використання однієї і тієї ж методики може призводити до створення абсолютно несхожих між собою архітектур підприємства через відмінності в бізнесі і області діяльності організації, наявності певного набору успадкованих систем і т.д.

Важливим для розуміння методик є використовувані в них моделі, різні уявлення (view) або домени архітектури.

Опис IT-архітектури служить детальним керівництвом, яке визначає основні, стандартні або типові елементи IT-систем, їх взаємозв'язку, а також процеси управління інформаційними системами. Що хотілося б отримати від такого документа? Можна сформулювати такі, частково суперечливі, вимоги:

— досить високий рівень деталізації для практичного використання фахівцями в області інформаційних технологій при розробці нових систем;

— простоту для розуміння бізнес-аудиторією;

— динаміку розгляду (тобто "Архітектура як є" - "Короткострокові та середньострокові завдання" - "Стратегічні плани");

— можливість адаптації за новими вимогами бізнесу та врахування можливостей реалізації незапланованих проектів.

Для формалізованого опису IT-архітектури організації можуть використовувати різні формати. Важливо, щоб організація використовувала такий формат опису, який би забезпечував легкий для розуміння спосіб керівництва щодо розвитку всіх аспектів IT в організації. Тому закономірно виникає питання з приводу "оптимального" формату, який може використовуватися для опису IT-архітектури саме як підмножини Архітектури підприємства.

Нижче представлена модель (рис 1.1), яка є відображенням того факту, що існують два взаємодоповнюючих визначення архітектури: "архітектура як опис" і "архітектура як процес".

<table>
<tr><th colspan="2" rowspan="2">Зміст (предмет) Архітектури підприємства</th><th colspan="4">Визначення архітектури</th></tr>
<tr><th colspan="2">Опис систем</th><th colspan="2" rowspan="2">Політики, правила та стандарти</th></tr>
<tr><th>Як є</th><th>Як повинно бути</th></tr>
<tr><td rowspan="4">Бізнес архітектура</td><td>Зв'язки між бізнес-процесами</td><td></td><td></td><td colspan="2" rowspan="4">Принципы (система ценностей и постулатов)
Новые требования</td></tr>
<tr><td>Бизнес-функции</td><td></td><td></td></tr>
<tr><td>Подфункции</td><td></td><td></td></tr>
<tr><td>Новые функции</td><td></td><td></td></tr>
<tr><td>Архитектура информации</td><td>Информация</td><td></td><td></td><td>Шаблоны, Правила (политики), Сервисы</td><td>Модели технологической архитектуры (список стандартных технологий и продуктов)</td></tr>
<tr><td rowspan="3">Архитектура приложений</td><td>Приложения</td><td></td><td></td><td rowspan="9"></td><td rowspan="9"></td></tr>
<tr><td>Точки доступа</td><td></td><td></td></tr>
<tr><td>Интеграция</td><td></td><td></td></tr>
<tr><td rowspan="6">Технологическая архитектура</td><td>Инфраструктура</td><td></td><td></td></tr>
<tr><td>Платформы</td><td></td><td></td></tr>
<tr><td>Системы хранения</td><td></td><td></td></tr>
<tr><td>Сети</td><td></td><td></td></tr>
<tr><td>Безопасность</td><td></td><td></td></tr>
<tr><td>Системное управление</td><td></td><td></td></tr>
<tr><td colspan="2">Описание текущей среды ИТ</td><td colspan="4">Область управления и контроля архитектуры</td></tr>
<tr><td colspan="6">Движущие силы с точки зрения бизнеса и стратегии</td></tr>
</table>

Рисунок 1.1 – Архітектура, як процес та як опис

Перше визначення говорить про те, що "архітектура - це опис деякої складної системи в певний момент часу". Воно аналогічно схемам опису і кресленням будівлі, міста, саду або комп'ютерної мережі. Цьому визначенню архітектури відповідає центральна секція таблиці. Дана частина таблиці описує два уявлення архітектури: існуючий і майбутній стан.

Друге визначення говорить, що "архітектура - це процес, тобто набір посібників, правил і / або стандартів, які застосовуються в процесі побудови нових систем" (права секція таблиці). Тобто другий сенс архітектури - в створенні системи правил, що забезпечують спрямований перехід з поточного стану інформаційних систем в майбутні. Одним з елементів архітектури при цьому є модель технологічної архітектури, яка задає список затверджених для закупівлі технологій. Вибір цих правил, узаконених архітектурою, визначається принципами, які повинні бути сформульовані як частина всього архітектурного процесу.

Наявність цієї моделі не означає, що весь опис архітектури підприємства можна помістити в одну просту таблицю. Однак ця таблиця наочно відображає основні аспекти архітектури і зв'язок між ними.

Корпоративна архітектура безпеки (enterprise security architecture) визначає стратегію інформаційної безпеки, яка складається з рівнів політики, стандартів, рішень, процедур і способів, якими вони з'єднані стратегічно, тактично і операційно. Це відрізняється від архітектури інфраструктури. Інфраструктура - це технології і апаратне забезпечення, що лежать в основі та необхідні для підтримки корпоративної архітектури безпеки. Просто мати інфраструктуру (комутатори, кабелі, маршрутизатори, вузли і т.п.) недостатньо. Щоб мати корпоративну архітектуру безпеки необхідно забезпечити спільну роботу всіх елементів інфраструктури взаємопов'язаним і безпечним чином, для чого потрібне програмне забезпечення, люди і процеси. Крім безпеки, цей тип архітектури дозволяє компаніям досягати кращої сумісності, інтеграції, легкості використання, стандартизації та керованості.

1.3 Стратегія ІБ

Стратегія ІБ - документ, який визначає цілі ІБ, і служить засобом підтримки стратегії бізнесу, а також є підставою для складання програми ІБ.

Метою стратегії ІБ є досягнення бажаного рівня ІБ, певне керівництвом компанії. Як правило, можна визначити шість цілей стратегії ІБ:

— Узгодження з цілями бізнесу;

— Ефективне управління ризиками компанії;

— Оптимізація інвестицій в ІБ;

— Управління ресурсами;

— Вимірювання продуктивності;

— Інтеграція всіх функцій управління ІБ.

У стратегії потрібно врахувати кожну із зазначених цілей, визначити що вони значать для компанії, яким чином досягати їх, за допомогою яких ресурсів і в які терміни. Крім чітко визначених цілей, стратегія ІБ повинна містити і кількісні показники, які дозволять визначити рівень успіху в досягненні бажаного результату.

Архітектура ІБ відображає стан інформаційної безпеки в певний момент часу. І хоча складно собі уявити повністю застиглу систему, в якій не відбувається ніяких змін, все ж архітектура грає велику роль в діяльності будь-якої служби ІБ. Але як досягти цього стану? Як з поточного стану перейти в нове, більш досконале і відповідне цілям бізнесу? Для цього існує стратегія, тобто напрямок руху для досягнення поставлених цілей.

Стратегія - це структурований і взаємопов'язаний набір дій, націлених на поліпшення в довгостроковому плані благополуччя підприємства. А для того щоб забезпечення безпеки здійснювалося найбільш ефективним чином, треба розробити стратегію ІБ, що дозволяє не тільки оцінити поточний рівень захищеності, але і розробити оптимальну схему переходу до розробленої архітектури ІБ з урахуванням як кращих міжнародних практик, так і національного законодавства в області захисту інформаційних ресурсів.

Багато в чому, метою процесу забезпечення безпеки є забезпечення безперервності бізнесу. Замість того щоб ставати жертвою, інфраструктура повинна бути здатна «поглинати» атаки і зберігати працездатність, подібно імунній системі людини, що дозволяє організму функціонувати при наявності в ньому вірусів і бактеріальних інфекцій. [10]

1.4 Огляд існуючих архітектурних моделей

1.4.1 Модель Дж. Захмана

Є класична архітектурна модель – модель Захмана (рис. 2). Вона гарна своєю простотою та універсальністю. З моменту публікації "Модель Захмана для опису архітектури підприємства" пройшла певну еволюцію в своєму розвитку і стала основою, на базі якої багато організацій створювали свої власні методики опису інформаційної інфраструктури підприємства. Отже, у своїй роботі Дж. Захман визначив архітектуру підприємства як "набір описових уявлень (моделей), які можуть застосовуватися для опису підприємства відповідно до вимог управлінського персоналу (якість) і які можуть розвиватися протягом певного періоду (динамічність)".

Для зручності опису Дж. Захман запропонував так звану Модель архітектури підприємства (Zachman Framework for EnterpriseArchitecture). Модель має дві основні мети - з одного боку, логічно розбити всі описи Архітектури на окремі розділи для спрощення їх формування і сприйняття, з іншого - забезпечити можливість розгляду цілісної Архітектури з виділених точок зору або відповідних рівнів абстракції.

Модель забезпечує можливість послідовного опису кожного окремого аспекту системи в координації з іншими. Модель Захмана складається з таблиці, що налічує п’ять строк (планувальник, менеджер, архітектор, проектувальник, розробник) та шість стовпців (дані (що?), функції (як?), мережа (де?), люди (хто?), час (коли?), мотивація (навіщо?)). Перспективи (строки в таблиці) можуть відповідати рівню управління підприємством: сфера дій (контекст), модель підприємства, модель системи, технологічна (фізична)

модель, деталі реалізації, працююче підприємство (організація). Дві перші строки (бізнес-керівники) відповідають найбільш загальним представленням та досить у загальному сенсі описують існуючі плани та цілі. Наступний рівень (IT-менеджери та розробники) – рівень логічної моделі, який є більш конкретним, але залишається абстрактним. Аналогічно, згідно з діяльністю організації, верхній рядок “Контекст” – відповідає рівню інтересів вищого керівництва; другий рівень – інтересам бізнес-менеджерів та власників процесів; третій рівень – рівень, де бізнес-менеджери, бізнес-аналітики та спеціалісти з IT працюють разом; четвертий рівень – описує деталі та сферу інтересів проектувальників та розробників системи.

Модель Захмана не є методологією, оскільки вона не передбачає конкретних методів. Коректно визначити модель Закман як онтологію, схему організації архітектурних артефактів (проектних документів, специфікацій, моделей). На схемі одночасно представлені цільової користувач артефакту (наприклад, власник бізнесу) і проблемна область (наприклад, робота з даними).

Модель названа в честь її творця Джона Захмана, який розробив першу редакцію онтології в 1980-х роках, будучи співробітником IBM. З тих пір було опубліковано ще кілька редакцій

		Дані	Функції	Дислокація, мережа	Люди	Час	Мотивація	
		Що?	**Як?**	**Де?**	**Хто?**	**Коли?**	**Чому?**	
Бізнес-керівники	Планувальник	Список важливих понять та обєктів	Список ключових бізнес-процесів	Теріторіальне розташування	Ключові організації	Найважливіші події	Бізнес-цілі та стратегії	Сфера дії (контекст)
	Власник, менеджер	Концептуальна модель даних	Модель бізнес-процесів	Схема логістики	Модель потока робіт (workflow)	Мастер-план реалізації	Бізнес-план	Модель підприємства
ІТ-менеджери та розробники	Конструктор, архитектор	Логічні моделі даних	Архітектура додатків	Модель розподіленої архітектури	Архітектура інтерфейса користувача	Структура процесів	Ролі та моделі бізнес правил	Модель системи
	Проектувальник	Фізична модель даних	Системний проект	Технологічна архітектура	Архітектура презентації	Структура керування	Опис бізнес-правил	Технологічна (фізична) модель
	Розробник	Опис структури даних	Программний код	Мережева архітектура	Архітектура безпеки	Визначення часових привязок	Реалізація бізнес-логіки	Деталі ралізації
	-	Дані	Працюючі программи	Мережа	Реальні люди, організації	Бізнес-події	Працюючі бізнес-стратегії	Працююче підприємство
		Інформація	Функції, процеси	Мережа, розташування систем	Люди, організації	Час, розклади	Мотивація	

Рисунок 1.2 – Модель Захмана

1.4.2 Методика опису архітектури Open Group

Open Group Architecture Framework (TOGAF) - це основа архітектури підприємства, яка забезпечує підхід до проектування, планування, впровадження та управління корпоративної інформаційної технологічної архітектури. Прихильники TOGAF часто використовують фреймворк для вивчення архітектурних проблем і тому, що він дає розумні рекомендації щодо того, як контролювати розробку і реалізацію, хоча це не гнучкий метод розробки або метод управління проектами, це не допомогає розробляти або керувати інформацією, необхідної в програмних додатках, як її слід підтримувати, використовувати, отримувати або зберігати.

TOGAF підкреслює модульність і стандартизацію, обидва з цих напрямків розвитку є відмінними бажаними концепціями, які також добре підходять до дизайну інформаційних послуг. Адже, чим більш модульними і стандартними стають речі, тим легше автоматизувати їх; проте реальність полягає в тому, що багато аспектів проектування інформаційних послуг, особливо на рівні зацікавлених сторін, є випадковими і не можуть бути стандартизовані. У міру розвитку дизайну джерела інформації можуть бути відкриті для стандартизації (назва та адресна інформація), а при розробці програмного коду код може бути стандартизований (і повторно використаний). Елементи процесів типу ITIL (іншими словами, процедури) також будуть відкриті для механізації, але буде помилково вважати що, наприклад, управління інцидентами може бути повністю автоматизовано.

Те ж саме стосується управління пропускною спроможністю, фінансового управління або будь-якого іншого великого процесу. До тих пір, поки штучний інтелект не буде доступний для всіх і який буде гарантовано безпомилковий.

Документація TOGAF є вільно доступною для перегляду в Інтернеті без ліцензії. Позаяк, повна документація TOGAF може бути завантажена та збережена за ліцензією, яка оформляється на інформаційному веб-сайті TOGAF.

У будь-якому випадку документація TOGAF може бути вільно використана будь-якою організацією, яка бажає це зробити, для розробки архітектури для використання в цій організації. Open Group працює як неприбутковий консорціум, який прагне забезпечити більшу ділову ефективність, шляхом спільного використання покупцями та постачальниками інформаційних систем з метою зниження бар'єрів інтеграції новітніх технологій через підприємство.

Тому Open Group публікує TOGAF на своєму загальнодоступному веб-сервері, а також дозволяє і заохочує його відтворення та безоплатне використання будь-якою організацією, яка бажає використовувати її для розробки власної архітектури.

Наразі, однією з найактуальніших є саме модель архітектури TOGAF запропонована The Open group. Основним полем для застосування TOGAF є, перш за все, програмна інфраструктура інформаційної системи (на противагу таким типам архітектур, як бізнес-архітектура, архітектура даних і додатків). Таким чином, вона в найкращій мірі підходить для опису інтеграційних компонент, що використовуються для підтримки широкого спектра корпоративних додатків, перш за все, критичних для бізнесу (mission-critical). Оскільки ця інтеграційна архітектура сильно залежить від прийнятих рішень в інших областях, то в рамках TOGAF в необхідній мірі розглядаються і ці суміжні області.

До складу моделі TOGAF входять дві основні компоненти - методика ADM (Architecture Development Method), яка визначає процес розробки архітектури, і Базова Архітектура (Foundation Architecture). Вона доповнюється відповідною базою даних ресурсів, що включає описи архітектурних принципів, прикладів реалізації, а також спеціалізований мову ADML (Рис 1.3).

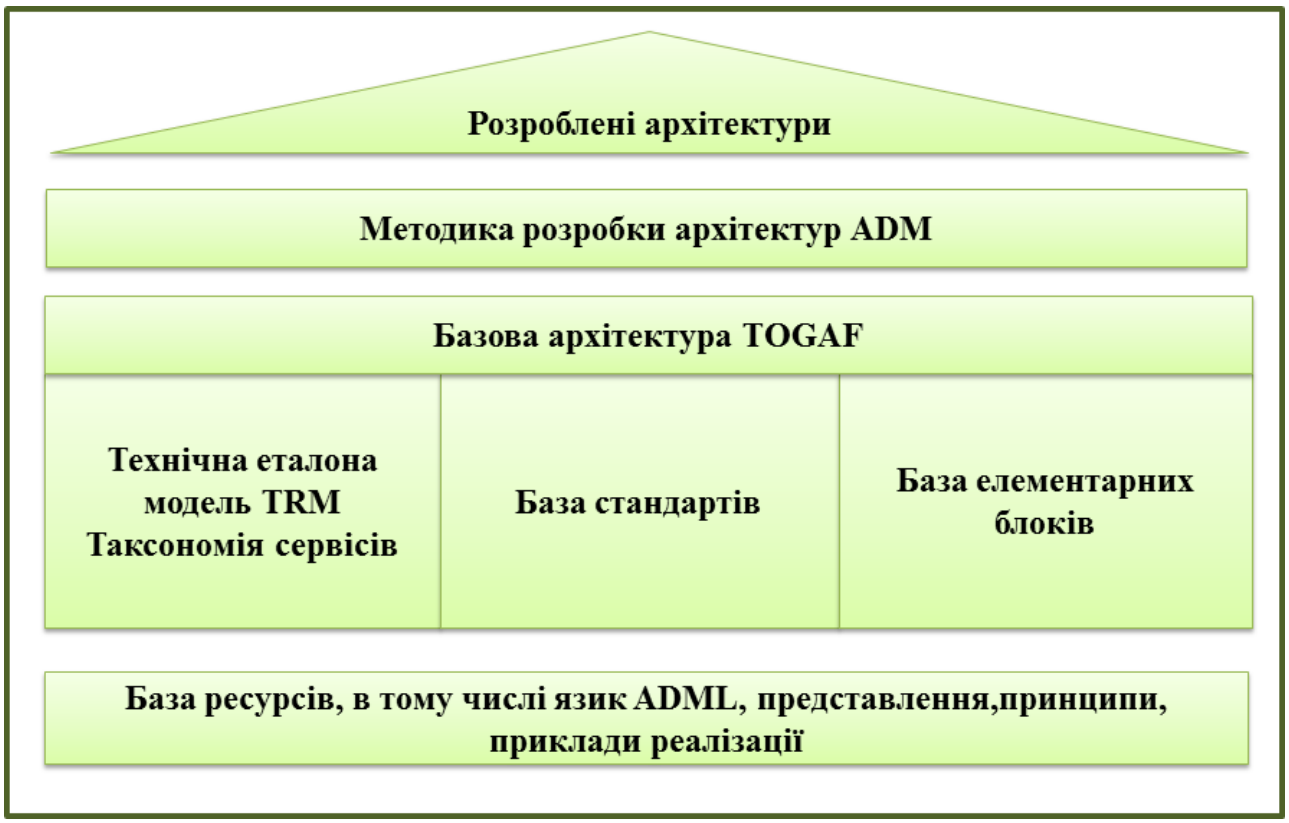


Рисунок 1.3 - Склад моделі SABSA

Відповідно до методики ADM, процес розробки архітектури включає наступні фази (рис. 1.4):

Підготовка: уточнення моделі під особливості організації, визначення принципів реалізації проекту.

Фаза A: визначення меж проекту, розробка загального уявлення (Vision) архітектури; затвердження плану робіт і підходу керівництвом.

Фаза B: розробка бізнес-архітектури підприємства.

Фаза C: розробка архітектури даних і архітектури додатків.

Фаза D: розробка технологічної архітектури.

Фаза E: перевірка можливості реалізації запропонованих рішень.

Фаза F: планування переходу до нової системи.

Фаза G: формування системи управління перетвореннями.

Фаза H: управління зміною архітектури.

Рисунок 1.4 – ADM

Діаграма високого рівня має десять кіл, хоча ADM описується як чотириступеневий процес:

—Підготовка TOGAF для обраного підприємства вимагає: до прийняття TOGAF наголошується на тому, що ця діяльність лише один раз виконується, перш ніж почати приймати TOGAF для підприємства. Рекомендація зроблена для того, щоб ніхто не робив припущення "підійшло одного разу - підходить всім"

— Визначається обсяг робіт, для підприємства, для якого є намір використати структуру та підготувати план впровадження (TOGAF описує шість кроків для цього процесу)

— Нагляд за розробкою та впровадженням: механізм того, як здійснюється фактичний розвиток та впровадження, які не входять в сферу діяльності TOGAF

—Керування змінами після впровадження: будь-які серйозні зміни спричинять інший цикл управління архітектурним розвитком.

Коло в центрі на рисунку представляє сховище знань. TOGAF має конкретні рекомендації щодо організації сховища та представляє покрокову інструкцію використання (табл. 1.1).

Таблиця 1.1 – Управління вимогами

Кроки управління вимогами	**Кроки фази ADM**
Дія 1	Ідентифікація/документування вимог з використанням бізнес-сценаріїв
Вимоги базової лінії: 1. Визначення пріоритетів виходячи з результатів поточної фази ADM 2. Підтвердження згоди зацікавлених осіб з результуючими пріоритетами 3. Документування пріоритетних вимог та їх включення до репозиторію вимог	**Дія 2**
Моніторинг вимог базової лінії	**Дія 3**
Дія 4	Ідентифікація змін вимог: 1. Видалення або переоцінка пріоритетів 2. Додавання вимог і переоцінка пріоритети 3. Модифікація існуючих вимог
Ідентифікація змінених вимог та запис пріоритетів: 1. Ідентифікуйте змінені вимоги та гарантуйте, що вимоги розміщені по пріоритетам архітектором, відповідальним за перебіг поточної фази, та відповідними зацікавленими особами. 2. Запис нових пріоритетів. 3. Гарантування того, що всі конфлікти ідентифіковані та управляються для досягнення успішних результатів і встановлення пріоритетів.	**Дія 5**

4. Генерування оцінки впливу вимог, щоб управлять архітектурною групою.	
Дія 6	1. Оцінка впливу змінених вимог на поточну (активну) фазу 2. Оцінка впливу змінених вимог на попередні фази 3. Визначення потреб або реалізація змін зараз; або виконання циклуADM та реалізація змін пізніше; якщо вирішено реалізувати зараз – оцініть витрати часу для реалізації управління змінами . 4. Оновлення оцінки впливу вимог до версії n+1
Дія 7	Реалізація вимог, які є результатом фази H Архітектура може бути змінена протягом життєвого циклу у фазі «Управління змінами архітектури (фаза H)». Процес управління потреб гарантує, що нові або змінені потреби , отримані с фази H, управляються коректно.
Оновлення репозиторію потреб інформації, стосовно змін, включаючи представлення зацікавлених осіб, на яких впливають ці зміни	**Дія 8**
Дія 9	Реалізація змін у поточній фазі
Дія10	Оцінка та огляд аналізу розбіжностей протягом попередніх фаз. Аналіз розбіжностей у фазах B – D. ADM виявляє розриви міх архітектурами базової лінії та цільової. Певні типи розбіжностей можуть давати початок потреб розбіжностей. ADM висвітлює два типа розбіжностей: • Щось, що присутнє у базовій лінії, але відсутнє у цільовій (тобто виключене, випадково або свідомо) • Щось, чого немає у базовій , але є у цільовій (тобто , щось нове) «Вимоги розбіжностей» це будь-яка річ, яка була виключена випадково і тому

	потребує зміни цільової архітектури. Якщо аналіз розбіжностей виявляє вимоги розбіжностей, то цей крок гарантує, що вони прийняті, задокументовані та записані у репозиторій вимог, і що цільова архітектура відповідно розглянута.

Кожна фаза, в свою чергу розбивається на підпроцеси (етапи), окремі роботи і так далі. Наприклад, фаза D включає наступні основні підпроцеси:

—Опис існуючої технологічної архітектури.

—Огляд бізнес-архітектури, архітектури даних і додатків для визначення початкових даних і необхідного ступеня деталізації.

—Опис існуючої системи з необхідним ступенем деталізації, яка вибирається для того, щоб можна було виявити необхідні зміни при формуванні цільової архітектури.

—Формування реєстру використовуваних платформ програмного і апаратного забезпечення.

—Виявлення та опис елементарних архітектурних блоків - кандидатів на використання в новій архітектурі.

Фактично, мова йде про можливі архітектурні шаблони.

Розробку чернетки технічного звіту, яка резюмує основні результати вивчення існуючого стану і можливості використання типових блоків. Направлення чернетки звіту на рецензування, аналіз коментарів та внесення, при необхідності, поправок.

— Формування цільової технологічної архітектури.

А саме опис існуючої системи в термінах TOGAF: Визначення перспектив (подань) архітектури; формування моделі цільової архітектури; визначення IT-служб (сервісів), підтвердження обліку бізнес-вимог; визначення архітектури і використовуваних блоків (шаблонів); проведення аналізу розбіжностей (gap analysis).

Для кожного такого підпроцесу визначаються завдання, які вирішуються на його етапі, вхідні і вихідні документи. Важливо відзначити, що процес передбачає не обов'язкову, але можливу адаптацію самого методу до умов конкретного підприємства, яка здійснюється на попередній фазі. Це може бути викликано як необхідністю врахування інших існуючих стандартів підприємства, так і залученням аутсорсингових компаній до розробки архітектури.

Особливо корисним інструментом TOGAF є те, що як самостійну модель архітектури корпоративної архітектури, можна адаптувати "свою" модель для кожного підприємства, наприклад, коли підприємства злилися та інтегровують інформаційні технології. Підтримка IT-послуг (для конкретних загальних IT-послуг), таких як білінгові системи, SAP, сервісні бюро тощо, буде відрізнятися і повинна бути інтегрована. В іншому випадку внутрішня підтримка та зовнішня діяльність, що стоять перед клієнтами, веявиться великою проблемою. Злиття та поглинання включають складні технологічні, процеси та поліпшення людей . Початкова точка зору архітектури підприємства може бути дуже корисною, але це далеко не "модель бізнесу та IT-узгодження" або хороша практика.

1.4.3 Шервудська прикладна архітектура безпеки бізнесу SABSA

SABSA є методологією розробки інформаційної безпеки та обробки інформації, орієнтовної на ризики забезпечення архітектури та надання рішень для безпеки інфраструктури, які підтримують критичні бізнес-ініціативи. Це відкритий стандарт, який включає в себе безліч принципів, моделей, методів та процесів для використання всіма, без ліцензування, необхідного для кінцевих організацій, які використовують стандарт в розробці та впровадженні архітектур та рішень. SABSA - це бізнес-результат. Основна ідея SABSA полягає в тому, що архітектура безпеки є, щоб полегшити бізнес. Це відповідає концепціям TOGAF. В основі методології SABSA - модель SABSA, підхід зверху донизу, яким керує SABSA-Процес розробки (Рис 1.5).

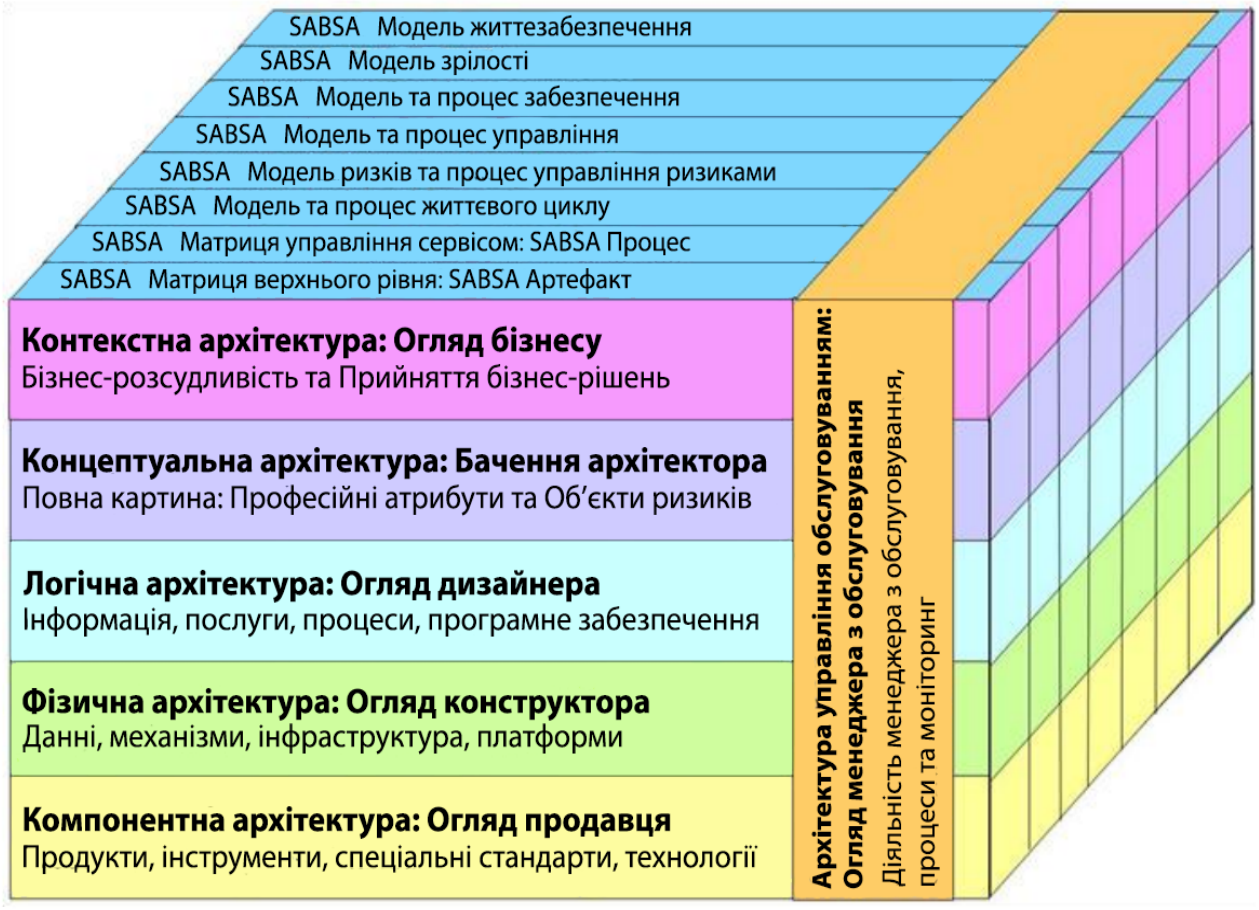


Рисунок 1.5 – Модель SABSA

Цей процес спочатку аналізує бізнес-вимоги і створює ланцюг простежування через етапи життєвого циклу SABSA стратегії та планування, проектування, впровадження та поточного управління та заходів для забезпечення збереження бізнес-мандату. SABSA містить рамки інструментів, створених з практичного досвіду, включаючи Матрицю SABSA та SABSA Business Attribute Profile, який надалі підтримуватиме всю методологію

Управління складністю. Однією з ключових функцій "архітектури" як інструменту архітектора є створення структури, в рамках якої Складністю можна успішно управляти. Малі, ізольовані, окремі проекти не потребують "архітектури", тому що їх рівень складності обмежений і головний дизайнер може керувати загальним дизайном одними руками. Однак, оскільки зростає розмір та складність проекту, то зрозуміло, що для цього потрібні багато дизайнерів працюючих як команда, щоб створити те, що має зовнішній вигляд, розроблений єдиним "дизайнерським авторитетом". Крім того, якщо

індивідуальний проект не є ізольованим, він має на меті гармонійно вписатись у набагато ширший, вищій рівень комплексу інших проектів, то архітектура необхідна, щоб виступати в якості "дорожньої мапи", в межах якої всі ці проекти можуть бути об'єднані в єдине ціле. Результат має бути таким, ніби вони дійсно були частиною єдиного, великого, складного проекту. Це стосується того, чи розробляються та впроваджуються окремі проекти одночасно, чи вони розроблені та впроваджені незалежно протягом тривалого періоду часу. З огляду на збільшення складності, потрібна система, в рамках якої кожен розробник може працювати над своїм завданням, яке сприятиме будівництву загального проекту. Кожен учасник проекту також повинен бути впевненим, що його робота буде в гармонії з роботами колег, і що загальна цілісність дизайну не буде загрожувати роботі, яка розділяється на велику команда дизайнерів. Роль "архітектури" полягає в тому, щоб забезпечити структурою, яка розбиває складність на очевидні прості речі. Це досягається методами накладання - зосереджуючи увагу на конкретних концептуальних рівнях мислення, і шляхом модульності - розбиття загального дизайну на керовані частини, в яких визначені функціональність і інтерфейси. Цей процес також відомий як "системна інженерія"

Архітектура безпеки підприємств Загальним досвідом багатьох корпоративних організацій є частота рішень з інформаційної безпеки розроблений, придбаний і встановлений на тактичній основі. Визначено вимогу, розроблена специфікація та для вирішення цієї ситуації потрібно знайти рішення. У цьому процесі немає можливості розглядати стратегічний і це означає, що організація створює суміш технічних рішень на спеціальній основі, кожен незалежно спроектований і конкретизований і без гарантії, що вони будуть сумісними та між собою дієздатний. Часто немає аналізу довгострокових витрат, особливо операційних витрат, які складають а велика частка загальної вартості володіння, і не існує стратегії, яку можна було би точно визначити, щоб підтримати цілі бізнесу. Підхід, який уникає цих частих проблем, - це розробка архітектури безпеки підприємства який керується

бізнесом і який описує структуровану взаємозв'язок між технічними та процесуальні рішення для підтримки довгострокових потреб бізнесу. Якщо архітектура повинна бути успішною, то вона повинен забезпечити раціональну основу, в рамках якої можна приймати рішення щодо вибору рішень з безпеки.

Критерії прийняття рішення повинні виходити з глибокого розуміння бізнес-вимог, включаючи:

— Необхідність скорочення витрат;

— Модульність;

— Масштабованість;

— Зручність повторного використання компонентів;

— Корисність;

— Працездатність;

— Взаємодія з внутрішнім та із зовнішнім середовищем;

— Інтеграція з корпоративною IT-архітектурою та її застарілими системами.

Крім того, безпека інформаційних систем є лише незначною частиною інформаційної безпеки, забезпечення інформацією або Управління інформаційними ризиками (ці умови мають певну мінливість), що у свою чергу є лише однією частиною більш широкої теми: безпека бізнесу. Безпека бізнесу охоплює три основні сфери: інформаційна безпека; безперервність бізнесу; фізична та екологічна безпека. Тільки завдяки комплексному підходу до цих широких аспектів безпеки бізнесу, стане можливим для підприємства зробити найбільш рентабельним та корисним рішення стосовно управління операційним ризиком. Тому архітектура безпеки підприємства та процес управління безпекою повинен охоплювати всі ці сфери. Основна характеристика моделі SABSA полягає в тому, що все повинно бути отримано з аналізу бізнес-вимоги до безпеки та управління ризиками. Управління ризиками SABSA тримає фокус та охоплює як поняття можливості, так і поняття загрози, а також баланс, який повинен існувати між цими двома поняттями. Модель є багатошаровою структурою, з верхнім шаром - етапом визначення бізнес-вимог. На кожному нижчому шарі розробляється новий рівень абстракції, що проходить через

визначення понятійного контексту архітектури, логіки архітектури, фізичної архітектури і, нарешті, на найнижчому шарі, вибір технологій і продуктів (архітектура компонентів) - іншими словами, список покупок. У цьому відношенні SABSA тісно узгоджується з ITIL v3. Сама модель SABSA є загальною і може бути відправною точкою для будь-якої організації, але з шляхом проходження через процес аналізу та прийняття рішень, передбачений його структурою, вихід стає специфічним для кожного підприємства, і, нарешті, дуже налаштований на унікальну бізнес-модель. Насправді це становить безпеку архітектури підприємства, і це є ключовим елементом успіху стратегічної програми управління інформаційною безпекою в організації. Але потрібно відзначити, що SABSA не покрокова інструкція, а методологія і основа, за допомогою якої можна розробити унікальні та індивідуальні рішення.

Таблиця 2.1 – Модель рівнів SABSA

	Активи (Що?)	Мотивація (Чому?)	Процеси (Як?)	Люди (Хто?)	Дислокація (Де?)	Час (Коли?)
Контекстна архітектура	Бізнес рішення	Бізнес ризик	Бізнес процеси	Керівництво бізнесу	Географія бизнесу	Залежність бизнесу від часу
	Таксономія бізнес активів, включаючи цілі та завдання	Ряд можливостей і загроз	Ряд операційних процесів	Організаційна структура і розширене підприємство	Ряд будівель, майданчиків, територій, юрисдикцій і т.д.	Тимчасові залежності бізнес завдань
Концептуальна архітектура	Знання бізнесу і стратегія ризику	Завдання управління ризиками	Стратегії забезпечення процесів	Ролі та відповідальності	Структура домену	Структура управління часом
	Профіль бізнес атрибутів	Завдання щодо запровадження і контролю; архітектура політики	Структура зіставлення процесів; Архітектурні стратегії для інформаційних і комунікаційних технологій	Власники, розпорядники та користувачі; Провайдери послуг і клієнти	Концепт і структура домена безпеки	Структура безперервного управління ризиками
Логічна архітектура	Інформаційні активи	Політики управління ризиками	Карти процесів та сервісів	Структура организації та довіри	Карти доменів	Календар і розклад
	Ряд информаційних активів	Доменні політики	Информаційні потоки; Функциональні трансформації; Сервис-ориентирована архітектура	Схема организації; Моделі довіри; Привілегійовані профілі	Доменні визначення; Внутрішні доменні взаємодії	Час початку, жизни и крайні терміни
Физична архітектура	Активи даних	Практики управління	Механізми процессів	Інтерфейс користувача	Інфраструктура інформаційних та	Графік управління

		ризиками			коммунікаційних технологій	
	Запас данных и словарь данных	Правила и процедуры управления рисками	Приложения; Промежуточные системы; Механизмы безопасности	Системы интерфейсов пользователя для информационных и коммуникационных технологий; Системы контроля доступа	Хост платформы, инфраструктура и сеть	Регулировки времени и последовательности процессов и сессий
Компонентная архитектура	Компоненты информационных и коммуникационных технологий	Инструменты и стандарты управления рисками	Инструменты и стандарты процессов	Инструменты и стандарты управления персоналом	Инструменты и стандарты локализации	Инструменты пошаговых заданий и последовательностей
	Продукты информационных и коммуникационных технологий включая репозитории данных и процессоры	Инструменты анализа рисков; Регистры рисков; Инструменты мониторинга и отчетности по рискам	Инструменты и протоколы предоставления процессов	Идентификаторы; Описания должностей; Роли; Функции; Списки контроля действий и доступов	Узлы, адреса и другие идентификаторы	Расписания времени; Часы, таймеры и прерывания
Архитектура управления обслуживанием	Управление предоставлением сервисов	Управление операционными рисками	Управление предоставлением процессов	Управление персоналом	Управление окружением	Управление временем
	Контроль непрерывности и качества операций	Оценка рисков; Мониторинг и отчетность по рискам; Обработка рисков	Управление и поддержка систем, приложений и сервисов	Управление учетными записями: Управление поддержкой пользователей	Управление постройками, площадками, платформами и сетями	Управление календарем и расписанием

1.5 Властивості середнього бізнесу

Згідно з визначенням Державної фіскальної служби України до суб'єктів середнього підприємництва відносяться суб'єкти господарювання будь-якої організаційно-правової форми та форми власності, у яких середня кількість працівників за звітний період (календарний рік) не перевищує 250 та не менше 50 осіб, балансова вартість активів не перевищує суму, еквівалентну 20 мільйонам євро і не менше 4 мільйонів євро, а також чистий дохід від реалізації продукції (товарів, робіт, послуг) не менше 8 мільйонів євро та не більше 40 мільйонам євро визначену за середньорічним курсом Національного банку України. [4]

Чим він характерний? Бізнес процеси компанії, які між собою погано налагоджені, протікають у різних середовищах (через різне не пов'язане між собою ПЗ або вирішення задач лише на паперових носіях), а також вони швидко змінюються тому, що на цьому етапі перебирають усі можливі варіанти ведення бізнесу. Це відбувається тому, що на етапі малого бізнесу усе працює більш-менш просто і достатньо вирішення ситуативних проблем, а чим більше структура, тим складніше нею керувати, а вирішувати проблеми, не торкнувшись інших процесів, виходить все рідше. У той час коли у великому бізнесі все налагоджено, а зміни впроваджуються більш обережно та обґрунтовано.

Малий і середній бізнес в Україні має певні риси, які істотно відрізняють його від підприємництва більшості зарубіжних країн, а саме:

• низький рівень технічної озброєності при значному інноваційному потенціалі;

• низький управлінський рівень, бракує знань, досвіду і культури ринкових відносин;

• прагнення до максимальної самостійності (більшість малих зарубіжних підприємств працює за умов франчайзингу і тому подібне, а у нас це майже відсутнє);

• поєднання в межах одного малого підприємства декількох видів діяльності, неможливість в більшості випадків орієнтуватися на однопродуктову модель розвитку;

• відсутність системи самоорганізації і недостатня інфраструктура підтримки малого підприємництва. [5]

Отже, вище було перераховано відмінності, які більш за все стосуються економістів чи менеджерів. Але фахівець з інформаційної безпеки дивиться на речі під іншим кутом. Для того, хто забезпечує захист інформації, на перший план виходять інші проблеми, які можуть заважати виконанню службових обов'язків, а саме:

1 Відсутність технічного завдання. При створенні СУІБ або введенні деяких окремих поодиноких засобів захисту інформації, фахівець може втрачати час на опис всіх видів інформації, а потім виявляється, керівництво перщ за все хоче захистити щось конкретне.

2 Швидкі зміни. При активному зрості ведеться форсований пошук нових рішень тих чи інших процесів

Коли фахівцеві треба розробляти СУІБ, писати модель порушника та модель загроз, розробляти політику безпеки та ін., що треба робити для виконання своїх функцій, представники бізнесу цікавляться, що саме планується зробити для забезпечення інформаційної безпеки. Та коли між технічними фахівцями та керівниками бізнесу немає стандартизованого посередника, можуть виникати ситуації, коли фахівець ІБ вигадує якісь етапи своєї діяльності, щоб керівники побачили якийсь алгоритм, навіть якщо там все залежить від експертної думки (рис 1.6).

Але навіть покроковий алгоритм не допоможе, якщо він не пристосований до середнього бізнесу

Це той сегмент організацій, у котрому найтяжче вибудовувати інформаційний захист тому, що підприємці вже розуміють, що їм потрібні послуги з ІБ, але не розуміють які саме і не можуть сформувати ТЗ. Тому все лягає на плечі фахівця з інформаційної безпеки. І коли він розбереться в усіх

процесах компанії напише політику безпеки та інші документи з ІБ, він побачить, що все вже змінилося, а його про це не сповістили.

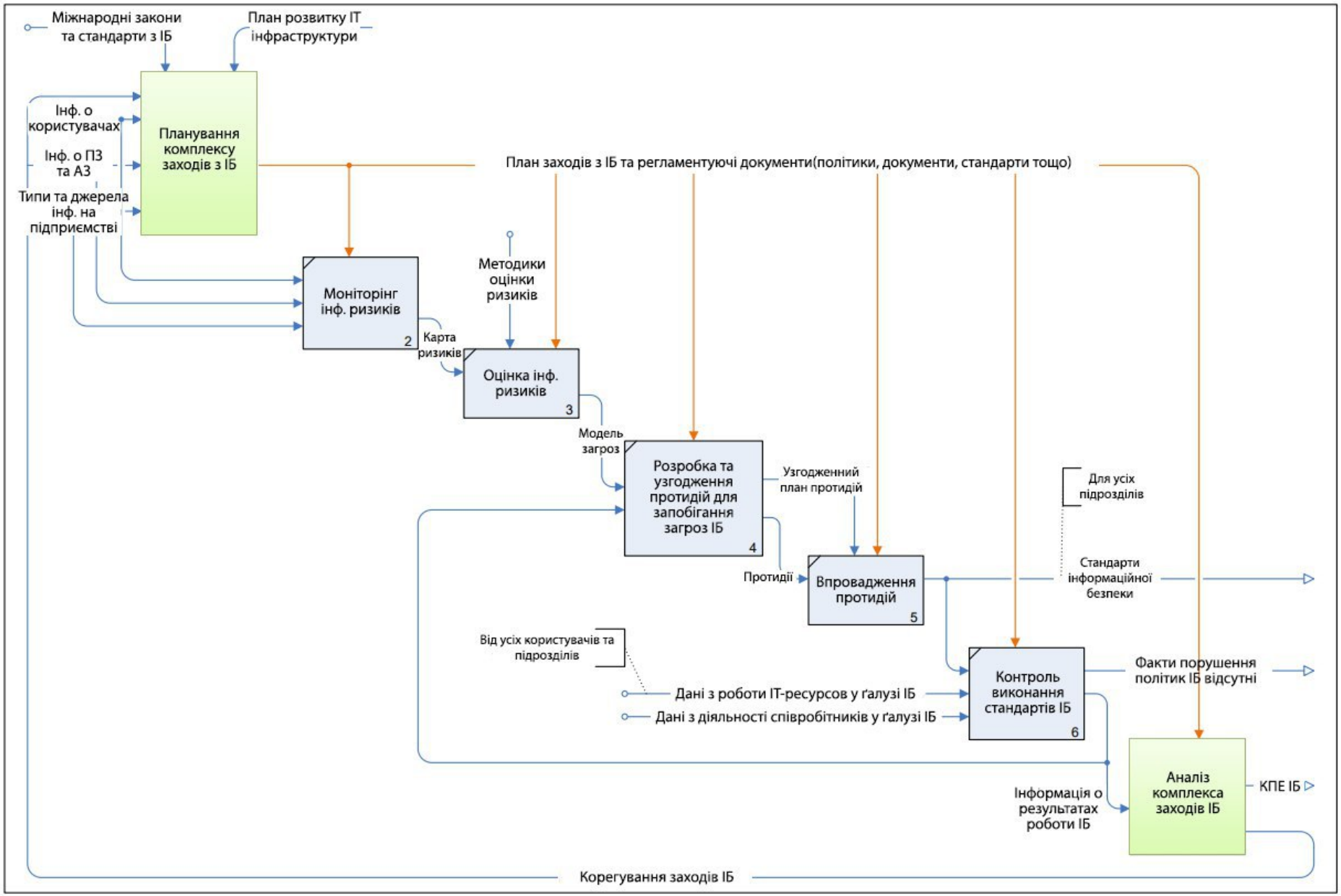


Рисунок 1.6 – алгоритм дій фахівця ІБ

Висновки до розділу 1

В сучасних умовах просто неможливо розвиватися без використання інформації та інформаційних технологій, які повинні не тільки підтримувати будь-які зміни в бізнесі, але і передбачати їх, готуватися до них заздалегідь, а в ряді випадків і сприяти появі нових бізнес-можливостей. Однак не завжди бізнес розвивається передбачуваним чином. Ризики різної природи можуть порушити зростання і розвиток підприємства і поставити його на грань вимирання. Чималу роль в цьому відіграють інформаційні та операційні ризики, пов'язані з витоками даних, виведенням з ладу елементів IT-інфраструктури і т. п. Для того щоб підготувати себе до ризиків сьогодення і майбутнього та налогодити співпрацю ІБ та представників бізнес-керівництва необхідна архітектура інформаційної безпеки, що пронизує всі інші архітектури підприємства. У розділі розглянута нормативна база, а саме фахова термінологія, концепції архітектур та відмінності середнього бізнесу.

РОЗДІЛ 2

АНАЛІЗ ІСНУЮЧИХ АРХІТЕКТУР ТА ЇХ АДАПТАЦІЯ ДЛЯ ЗАДАНИХ ПОТРЕБ

2.1 Відповідність архітектур кібербезпеки національним нормативним актам

Для застосування архітектурних методів в управлінні кібербезпекою в Україні, потрібно зважати чи не конфліктують вимоги до розробки та використання архітектур вимогам українського законодавства у сфері кібербезпеки та сфері захисту інформації.

Більш за все це стосується **НД ТЗИ 2.5-004** «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу». Адже у цьому документі надаються:

- Порівняльна шкала для оцінки надійності механізмів захисту інформації від несанкціонованого доступу, реалізованих в комп'ютерних системах.
- База (орієнтири) для розробки комп'ютерних систем, в яких мають бути реалізовані функції захисту інформації.[6]

У цьому документі розглянуті ключові питання кібербезпеки:

Конфіденційності

- Хто і в якій мірі забезпечує конфіденційність. Покладений цей обв'язок на власника IP (довірча конфіденційність) чи на адміністратора IC (адміністративна конфіденційність)
- Як налаштоване повторне використання об'єктів?
- Аналіз прихованих каналів
- Конфіденційність при обміні

Цілісності

- Хто і в якій мірі забезпечує цілісність. Покладений цей обов'язок на власника IP (довірча цілісність) чи на адміністратора IC (адміністративна цілісність)

— Відкат. Чи налагоджена автоматизована послуга повернення попереднього стану.

— Цілісність при обміні

Доступності

— Використання ресурсів

— Стійкість до відмов

— Гаряча заміна

— Відновлення після збоїв

Спостереженості

— Реєстрація

— Ідентифікація

— Автентифікація

— Достовірний канал

— Розподіл обов'язків

— Цілісність КЗЗ

— Самотестування

— Ідентифікація та автентиифікація при обміні

— Автентифікація відправника

— Автентифікація одержувача

Також даний нормативний документ встановлює вимоги до КС, а саме до її архітектури, середовища розробки, послідовності розробки, документації та випробовувань КЗЗ.

Отже, хоча НД ТЗІ 2.5-004 і розглядає питання кібербезпеки комплексно, та це стосується лише КС та не зважає на цілі бізнесу.

Білий документ SABSA роз'яснює що, основні бізнес-вимоги до інформаційної безпеки є специфічними для бізнесу. Вони, як правило, виражаються з точки зору захисту доступності, цілісності, автентичності та конфіденційності ділової інформації, і забезпечення відповідальності та перевірки в інформаційних системах. Щоб зрозуміти ці вимоги, докладно необхідний Аналіз бізнес-процесів, використовуючи як вихідну інформацію,

отриману шляхом прямого інтерв'ю з оперативними бізнес-менеджерами. Проте бізнес-вимоги набагато ширші, ніж просто "безпека та контроль". Інформаційна безпека забезпечує впевнене використання інформації в комерційних цілях на всій території організації.

Загальні бізнес-вимоги до рішення щодо захисту інформації часто включають наступне:

- Придатність до використання. Чи рішення відповідає технічній компетенції призначених користувачів і чи буде це ергономічно прийнятно для цих користувачів?
- Взаємодія. Чи буде рішення забезпечувати довгострокові вимоги до взаємодії між передачею інформації системи та програми?
- Інтеграція. Чи буде рішення інтегруватися з широким спектром комп'ютерних додатків і платформ, для яких це може бути потрібно в довгостроковій перспективі?
- Підтримка. Чи зможе рішення отримувати підтримку у середовищі в якому вона була розроблена та використовується?
- Низька вартість розвитку. Це рішення модульної конструкції і, отже, здатне бути інтегроване в програму розвитку на мінімальна вартість?
- Короткий час до запуску у роботу. Це рішення може бути інтегроване в програму розвитку з мінімальною затримкою, щоб відповідати часовим рамкам, пов'язаним з вікнами бізнес-можливостей?
- Масштабованість платформ. Чи буде рішення відповідати діапазоном обчислювальних платформ з якими може знадобитися інтеграція?
- Масштабованість витрат. Чи вартість початкового рівня відповідає діапазону бізнес-додатків, для яких рішення призначене?
- Масштабованість рівня безпеки. Чи підтримує цей варіант криптографічні та інші методи, які будуть потрібні для реалізації необхідного діапазону надійності та рівня забезпечення?
- Масштабованість використання. Чи рішення можна масштабувати, щоб відповідати майбутнім числу ділових користувачів та / або потенціалу

майбутніх вимог до пропускної спроможності, зберігання інформації та обсягів транзакцій?

— Повторне використання. Чи рішення можна використовувати в самих різних ситуаціях, щоб отримати найкращий прибуток від своїх інвестицій придбання та розвиток?

— Операційні витрати. Чи буде мінімізувати вплив вартості на операції системи?

Архітектура TOGAF заснована на визначенні ряді архітектурних блоків в архітектурних каталогах, що визначають взаємозв'язок між цими будівельними блоками в матрицях архітектури, а потім представляють схеми зв'язку, які показують, зрозуміло і стисло, що таке архітектура.

Роль TOGAF полягає в тому, щоб забезпечити відкритий стандарт для архітектури, який застосовується у багатьох сценаріях та ситуаціях. Для того, щоб задовольнити це бачення, необхідно мати повнофункціональну метамоделю входу до премії для вмісту, а також забезпечити можливість уникнути проведення ненужної діяльності шляхом посилення адаптації.

Метамоделі повинні забезпечити базову модель із мінімальним набором функцій, а потім підтримувати включення додаткових розширень під час пошиття одягу.

Основні метамоделі

Метамоделі контенту використовують термінологію, яка обговорюється в TOGAF ADM, як основна для офіційної метамоделі. Використовуються наступні основні терміни:

—діяч: персона, організація або система, яка не враховує архітектурну модель, але взаємодіє з нею;

—компонент програми: інкапсуляція функціональності додатків, яка узгоджується зі структурою впровадження;

—бізнес-сервіс: підтримує ділові можливості через явно визначений інтерфейс і явно регулюється організацією;

—об'єкт даних: інкапсуляція даних, яка визнана експертом бізнесу як дискретна концепція. Суб'єкти даних можуть бути прив'язані до програм, репозитаріїв та служб, і можуть бути об'єднані відповідно до міркувань впровадження;

—функція: забезпечує ділові можливості, тісно пов'язані з організацією, але явно не керуються організацією;

—служба інформаційної системи: автоматизовані елементи бізнес-сервісу. Служба інформаційної системи може надавати або підтримувати або всі одні або декілька бізнес-сервісів;

—організаційний підрозділ: самодостатня одиниця ресурсів з цілями, завданнями та заходами. Організаційні підрозділи можуть включати зовнішні установи та організації ділових партнерів;

—сервіс платформи: технічні можливості, необхідні для забезпечення інфраструктури, яка підтримує доставку додатків;

—роль: діяч бере на себе роль для виконання звіту;

—компонент технології: інкапсуляція технологічної інфраструктури, яка представляє собою клас технологічного продукту або спеціального технологічного продукту.

Нижче описано деякі **концепції ключових відносин**, пов'язані з основними об'єктами метамоделі:

— Процес повинен звичайно використовуватися для опису потоку. Процес - це взаємодія між функціями та службами і не може бути фізично розгорнута. Всі процеси повинні описувати виконання функції і тому розгортання процесу відбувається за допомогою функції, яку він підтримує; наприклад, програма реалізує функцію, яка має процес, а не програма, яка реалізує процес.

— Функція описує одиниці ділової спроможності на всіх рівнях деталізації

— Термін "функція' 'використовується для опису одиниці ділової здатності на всіх рівнях гранулярності, що включає такі терміни, як ланцюжок

вартості, область обробки, можливості, бізнес-функції і т. Д. Передбачувана одиниця бізнес-функції повинна бути описана як функція .

— Бізнес-послуги підтримують організаційні цілі та визначаються на рівні деталізації, що відповідає рівню необхідного управління

2.2. Супутні документи TOGAF

Для вирішення завдань кібербезпеки Open Group разом з іншими спеціалізованими організаціями (інститут SABSA, Міжнародна електротехнічна комісія (IEC), Міжнародна організація по стандартизації (ISO) та ін.) виробили супутні документи, які допомагають інтегрувати стандарти ІБ до архітектури підприємства побудованої за стандартом TOGAF.

Інтеграція безпеки та ризику в стандарт TOGAF: цей проект працює над тим, щоб майбутні версії стандарту TOGAF комплексно відповідали на безпеку та ризики. Проект включає в себе інтеграцію з архітектурою "Шервудська архітектура прикладної безпеки бізнесу" (SABSA).

Серія керівництв з практики архітектур безпеки. Цей проект закріплений для розробки Теорії знань, яка визначає роль, методи та найкращі практики архітектора безпеки, а також програму сертифікації. Він має на меті мати зміст на основі принципу, а не є обов'язковим, і буде застосовуватися незалежно від архітектурної структури, у будь-якій галузі, національному контексті або культурі підприємства. Таксономія навчальних цілей Блума стане основою для формування професійних компетенцій та критеріїв професійної сертифікації.

Каталог послуг із забезпечення безпеки. Метою проекту є реалізація спільного розвитку каталогу служб безпеки, щоб його могли використовувати архітектори підприємств (безпеки). Просто доступний каталог дозволяє архітекторам Enterprise (Security) швидко встановити чітку зв'язок між вимогами високого рівня та відповідними рішеннями.

Стандартна модель стабільності управління інформаційною безпекою (O-ISM3) Стандарт: Включення найкращих практик для зв'язку

безпеки з бізнес-потребами, використання підходу, що ґрунтується на процесі, надання рекомендацій щодо впровадження та використання специфічних показників, при цьому зберігається сумісність із поточним управлінням інформацією та безпекою стандарти Цей проект розвиває стандарт O-ISM3. • Стандарти управління ризиками, керівництва та сертифікація. Наша робота з ризику включає в себе два стандарти (O-RA та O-RT), які разом називають знаком Open FAIR ™, і базуються на факторному аналізі інформаційного ризику (FAIR) метод Ми також створили декілька посібників та білих документів з питань аналізу ризиків, у тому числі щодо використання аналізу ризику Open FAIR з ISO / IEC 27005, STIX та NIST Cybersecurity Framework. Активні проекти включають в себе Відкритий FAIR Process Guide та розробку інструменту аналізу кількісного ризику Open FAIR. Форум також забезпечує нагляд та керівництво програмою відкритої FAIR сертифікації

2.3 Інтеграція TOGAF-SABSA

Архітектура підприємства (включаючи архітектуру безпеки) полягає у вирівнюванні бізнес-систем та підтримці ефективності інформаційних систем (системи є поєднання процесів, людей і технологій) та ефективно реалізувати бізнес-цілі. Один з важливих аспектів якості архітектури підприємства - це ризик інформаційної безпеки та способи управління ними. Занадто довго, інформаційна безпека розглядалась як окрема дисципліна, ізольована від архітектури підприємства. Зараз вже існує підхід до покращення методології архітектури підприємства, TOGAF з SABSA створили новий підхід до архітектури безпеки і таким чином створили одну цілісну методологію архітектури. Бачення полягає в тому, щоб підтримати корпоративних архітекторів, яким необхідно враховувати операційне управління ризиками надаючи рекомендації, що описують, як TOGAF та SABSA можуть бути об'єднані таким чином, щоб бізнес-підхід SABSA до архітектури безпеки через ризики та можливості могли бути інтегрованим у TOGAF бізнес-стратегічний підхід до розробки більш повної архітектури підприємства. В цій Білій книзі з інтеграції є два головних координаційних пункти. Перше - описати, як

найкраще використовувати SABSA на TOGAF-основі архітектурних завдань. На відміну від безпеки як окремого продукту, це Біла книга дає практичний підхід, що робить вимоги та послуги безпеки SABSA доступними як загальні Артефакти TOGAF. Другий координатор - показати, як процеси управління вимогами в TOGAF можуть бути інтегровані в найширший загальний зміст (тобто, не тільки з точки зору архітектури безпеки) за допомогою застосування SABSA-Концепції створення профілю атрибутів до всього процесу ADM.

2.4 Моделювання нової архітектури для середнього бізнесу

Крок перший. Якщо розглядати подібності та відмінності моделей TOGAF та Дж. Захмана, то може здаватися, що їх нічого не поєднує. У той час як TOGAF являє собою методологією на 700 сторінок, модель Захмана являє собою лише одну таблицю. Але саме через модель Захмана керівники краще зрозуміють, чого від них вимагають при описі бізнес процесів. Тому треба залишити цю модель як основу. Для більш точного опису усіх бізнес процесів з точки зору керівників. Зважаючи на те, що у моделі Захана та в архітектурній методології TOGAF, не акцентується увага на питаннях безпеки та не відводяться задачі для фахівців з інформаційної безпеки та кібербезпеки, треба ввести підрозділ інформаційної безпеки у проекту группу з опису бізнес-процесів, написання IT-стратегії, формування, впровадження та підтримки архітектури підприємства. Пропонується наступна схема описану на прикладі моделі Захмана з використання фаз моделі TOGAF та доопрацюванням з точки зору ІБ (Рис. 2.1). У цій схемі об’єднано Фази C та D в одну та об’єднано виконавців реалізації, тобто майже за весь етап будівництва та підтримки архітектури відповідають керівник підрозділу інформаційних технологій та керівник підрозділу інформаційної безпеки. Фазу А реалізують керівник ІБ та організаційний директор, з можливістю залучення інших топ-менеджерів, для більш детального розгляду цілей та бізнес-процесів підпорядкованих їм напрямків.

	Що?	**Як?**	**Де?**	**Хто?**	**Чому?**	
Керівник ІБ та оргдиректор	Критичні обекти	Модель загроз; розрахунок економічних ризиків	Географічне розташування; юридична подпорядкованність	Организація; партнери	Бізнес-целі	A
Керівники ІТ та ІБ та керівники підрозділів	Концептуальна модель даних	Модель бізнес-процесів; врахування економіко-політичної обстановки	-	ІТ та ІБ керівники	Бізнес-план	B
	Логична модель; політики ІБ	Врахування бюджету	Модель розподіленої архітектури	Адміністратори	Ролі та моделі бізнес правил	C, D
Керівники підрозділів та системні адміністратори	Физична модель; ІБ інструкції	Врахування сумісності ПЗ та АЗ	Мережева архітектура	Користувачі	Зручність; дотримання ІБ користувачами	
	Структура даних	Працюючі программи	Директорії	Програми	Стандартизація запитиів та зберігання, перевірка реалізації	E
	F					

Рисунок 2.1 – перша ступінь адаптованої моделі

Крок другий. Окрім долучення до будівництва фахівців, які знають цілі інформаційної безпеки та засоби їх досягнення, треба ще найбільш адаптовані для архітектурного підходу вимоги до інформаційної безпеки. Адже, як розглянуто у першому розділі, «лінійний» підхід до ІБ, через нерозуміння може ігноруватися власниками бізнесу. А якщо власники та вище керівництво ігнорує ІБ, тоді і більш нижчі ланки не будуть дотримуватись принципів інформаційної безпеки.

Для налаштування інформаційної безпеки для архітектурного підходу, краще за все взяти керівництва до ІБ з методології SABSA. Адже ця методологія направлена на вирішення питань інформаційних та операційних ризиків та їх усунення.

Тому при налаштуванні треба звертатися до Білої та Синьої книг SABSA. І виглядати запропонавана модель буде вже інакше.

Крок третій. Враховуючи, що модель розробляється для підприємств середнього бізнесу, потрібно виключити модель зрілості та не виділяти, як обов'язкову вимогу часові критерії тому, що український середній бізнес поки що не відповідає вимогам «зрілих» компаній та не навчився розпоряджатися часом.

SABSA процесс

SABSA артефакт

Модель та процесс життєвого циклу

Модель ризиків та процесс управління ризиками

Модель та процесс управління

Модель життєзабезпечення

	Що?	Як?	Де?	Хто?	Чому?	
Керівник ІБ та оргдиректор	Критичні обекти; таксономія бізнес активів, включаючи цілі та завдання	Модель загроз; розрахунок економічних ризиків; Ряд можливостей і загроз	Географічне розташування; юридична подпорядкованність	Організація; партнери	Бізнес-цілі	A
	Концептуальна модель даних	Модель бізнес-процесів; врахування економіко-політичної обстановки;Завдання щодо запровадження і контролю; архітектура політики	Концепт і структура домена безпеки	ІТ та ІБ керівники	Бізнес-план	B
Керівники ІТ та ІБ	Логична модель; політики ІБ	Врахування бюджету, Информаційні потоки; Функциональні трансформації; Сервис-ориентирована архітектура	Модель розподіленої архітектури	Адміністратори	Ролі та моделі бізнес правил	C, D
Керівники підрозділів та системні адміністратори	Физична модель; ІБ інструкції	Врахування сумісності ПЗ та АЗ, Оцінка ризиків; Моніторинг и звітність по ризикам; оброблення ризиків	Мережева архітектура	Користувачі	Зручність; дотримання ІБ користувачами	
	Структура даних	Працюючі программи	Директорії	Програми	Стандартизація запитиів та зберігання, перевірка реалізації	E
	F					

Висновки за розділом 2

В сучасних умовах просто неможливо розвиватися без використання інформації та інформаційних технологій, які повинні не тільки підтримувати будь-які зміни в бізнесі, але і передбачати їх, готуватися до них заздалегідь, а в ряді випадків і сприяти появі нових бізнес-можливостей. Однак не завжди бізнес розвивається передбачуваним чином. Ризики різної природи можуть порушити зростання і розвиток підприємства і поставити його на грань вимирання. Чималу роль в цьому відіграють інформаційні та операційні ризики, пов'язані з витоками даних, виведенням з ладу елементів IT-інфраструктури і т. п. Для того щоб підготувати себе до ризиків сьогодення і майбутнього необхідна архітектура інформаційної безпеки, що пронизує всі інші архітектури підприємства.

В розділі розглянуті відповідність архітектурного підходу державним нормативним документам, стандарти, які можуть допоїти у налаштуванні архітектури підприємства та разроблена нова адаптована модель.

РОЗДІЛ 3

ЕКОНОМІЧНИЙ РОЗДІЛ

3.1. Опис підприємства

Організація являється мережею роздрібних магазинів продуктів харчування (близько 60 магазинів) з одним офісом. У Додатку показана організаційна структура компанії, за винятком одного підрозділу (його робота віднесена до комерційної таємниці), який складають близько 25 осіб. Співробітники цього підрозділу використовують лише дві специфічні програми та контактують лише з одним іншим підрозділом.

Офіс, підприємства знаходиться на середньому поверсі банківської будівлі. Тому загрози витоку інформації, технічними каналами, далі самого банку дуже низькі, а сам банк (будучи орендодавцем, а не конкурентом) не зацікавлений в розголошенні інформації суб'єкту.

В компанії є затверджена керівництвом ПБ, але немає реальних механізмів реалізації контролю та протидії порушенням ПБ. Є домен контролер, та не усі пристрої та користувачі введені до його бази. Керівництво департаменту ІТ, без огляду на ризики, створює списки користувачів, яких не стосуються політики.

Враховуючи все це, пропонується розглянути архітектурний підхід ІТ-систем, як інструмент для «вбудовування» ІБ у процеси компанії на всіх рівнях.

3.2. Постановка економічної задачі

Сьогодні більшість успішних українських підприємств відчувають кризу росту і при постійному збільшенні кількості реалізованих проектів вже не можуть використовувати звичні методи і технології управління. Керівництву підприємств складно визначати поточний стан розвитку проектів, контролювати їх виконання, приймати адекватні управлінські рішення та налогоджувати взаємодію між підрозділами. Зазвичай 75% проектних ризиків – це внутрішні ризики, пов'язані з некоректним плануванням, недисциплінованістю і низькою кваліфікацією персоналу, відсутністю

стандартизованих робіт, безконтрольним використанням дефіцитних ресурсів проекту, несвоєчасним прийняттям рішень. Тому для вирішення цих проблем потрібен більш коплексний підхід, а саме розробка архітектури.

3.4 Обґрунтування економічної ефективності

При впровадженні архітектурного підходу можна виділити декілька варіантів заощадження коштів, а саме:

Коли здійснено перехід до архітектурного управління кібербезпекою, тоді звісно визначена IT-стратегія компанії, на основі котрої можна прописувати проект на довгостроковий період (від декількох місяців до декількох років) та презентувати його обраному вендору (постачальнику від виробника). У таких випадках зазвичай нараховується знижка, її розмір іноді досягає 20% та залежить від об'єму закупівель програмного чи апаратного забезпечення та строку на який розписується проект.

— Великі компанії все частіше впроваджують інтелектуальні системі, які самі будуть інформувати про небезпеку, що зменшує ризики пов'язані з людським фактором . Це, наприклад, SIEM системи. Вони визначають яка інформація важлива та відстежують її оброблення в ІС. Їх середня ціна для 250 користувачів щонайменш 1 млн.грн [8,9]. З архітектурним підходом фахівці ІБ сумісно з фахівцями ІТ визначають ключову інформацію, навіть новостворену. Навчальні курси з Архітектури підприємства коштують від 6 тис. грн [7]

Точно вирахувати які втрати будуть у підприємства у випадку реалізації загроз майже неймовірно , але можна вирахувати, скільки втрачає компанія, якщо при розширенні компанії та, як наслідок, масштабуванні системи, яке не було спланованo, втрачається така властивість інформації, як доступність.

$$Y = \frac{\sum ЗП_{нал}}{t_р} \times (t_{простою} + t_{відновлення}) \quad (3.1)$$

Где $ЗП_{нал}$ – заробітна платня з урахуванням податків

$$Y_{min} = \frac{(5000 + 1100)}{160} \times 1 = 38{,}125$$

Наразі, є змога розрахувати лише мінімальні втрати. У нашому випадку це порушення доступності для одного співробітника на одну годину, без втрати його напрацювань. Але з кожною хвилиною, з кожним постраждалим працівником, з кожним втраченим документом ці втрати зростають з арифметичною прогресією. А якщо через недогляд в нас буде порушена ще й конфіденціальність, тоді втрати будуть зростати у геометричній прогресії.

Висновки до розділу 3

У розділі на прикладі підприємства розглянуті найменші можливі втрати,при відсутності реалізації архітектурного підходу, відсоткова економія на закупівлі обладнання, а також обґрунтовано впровадження архітектури, як заміна SIEM систем для середніх підприємств.

ВИСНОВКИ

У дипломній роботі розв’язано актуальне наукове завдання щодо використання архітектурних методів в управлінні інформаційною та кібербезпекою на підприємствах середнього бізнесу.

Вирішені наступні завдання:

1. Ознайомлення з існуючими архітектурними моделями;
2. Дослідження додаткових інструментів, розширення існуючих архітектур, відповіддності архітектур кібербезпеки національним нормативним актам;
3. Розробка архітектурної моделі з урахуванням вимог середнього бізнесу до ІБ
4. Визначення витрат на реалізацію запропонованих рекомендацій щодо впровадження архітектурного методу управління ІБ

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1 Про інформацію [Електронний ресурс] : закон України від 02.10.1992 № 2657-XII – Режим доступу : http://zakon2.rada.gov.ua/

2 Про основні засади забезпечення кібербезпеки України [Електронний ресурс] : закон України від 05.10.2017 № 2163-VIII

3 "3D-предприятие" - модель стратегии трансформирующейся системы. Е. З. Зиндер, директор фирмы "Группа 24" http://citforum.ru/seminars/cbd2000/cbd_day2_01.shtml

4 Про внесення змін до Закону України "Про бухгалтерський облік та фінансову звітність в Україні" щодо удосконалення деяких положень [Електронний ресурс] : Відомості Верховної Ради (ВВР), 2017, № 44, ст.397

5 Розвиток інфраструктури малого і середнього бізнесу в Україні. Ольвінська Ю.О., Самотоєнкова О.В. УДК 336.77:334.012.64

6 НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу

7 Архитектура ИТ-предприятия (IT_ARCH) [Електронний ресурс] – Режим доступу : https://www.flane.com.ua/course/itil-it_arch#schedule

8 Выбираем DLP-систему для средней организации [Електронний ресурс] – Режим доступу : https://habrahabr.ru/post/141000/

9 Сравнение SIEM систем [Електронний ресурс] – Режим доступу : http://siem.su/compare_SIEM_systems.php

10 Архитектура безопасности [Електронний ресурс] – Режим доступу https://www.cisco.com/c/dam/global/ru_ru/downloads/broch/Cisco_Security_Architecture.pdf

11 IBS. E-Government. Современные технологии государственного управления

12 Meta Group. Enterprise Architecture Desk Reference 2002

13 Steven Overby. The Future of Jobs and Innovation. Issue of CIO Magazine. December 15 2003

14 Stack C. Managing Enterprise Architecture Artifacts and Assets, presentation for Enterprise Architect Summit June, 2004

15 P. Helland. Metropolis. Microsoft Architects Journal April 2004

16 Preparing for the Upswing: The 2004 CIO Agenda. March 2004 Gartner EXP Premier Report

17 Giovinazzo M. Business Architecture: Aligning business and IT Strategies l 2003

18 Driving Enterprise Agility with enterprise IT Architecture Gartner COM-19-4566, 2003

19 Drobik et al The Gartner definition for the Real-Time enterprisecGartner Research Note COM-18-3057, 2002

20 T. Friedman. Data Warehouse Infrastructure: Providing Flexibility for Inevitable Change Gartner Business Intelligence Conference, Amsterdam 2003

21 SABSA – in 3 minutes [Електронний ресурс] – Режим доступу : https://www.vanharen.net/blog/enterprise-architecture/sabsa-in-3-minutes/

22 Б. Позин ИТ-катализатор успешности бизнеса. Сетевой журнал 7'2003

23 E-Government Architecture: Development and Governance Gartner, 2002

24 Strategy of Acceleration: Time to Change Culture and Architecture Gartner, 2002

25 Коллинз Джим. «От хорошего к великому. Почему одни компании совершают прорыв, а другие нет...» Стокгольмская школа экономики в Санкт-Петербурге, 2001

26 Enterprise Architecture: Fart Too Important to Be Left to the IT Team Gartner, 2002

27 C.K. and Krishnan, M.S, Prahalad The Dynamic Synchronization of Strategy and Information Technology An article from MIT Sloan Management Review Summer 2002, Volume 43, Number 4

28 Microsoft Technology Strategy Consulting. Benefits Driven Approach to Strategy Building on Benefits Management to Address the Challenges of IS/IT Strategy and Planning, 2000

29 M.E, Porter. Competitive Strategy: Techniques for Analyzing Industries and Competitors New York: Free Press, 1980

30 M. Treacy and F. Wiersema. The Discipline of Market Leaders: Choose Your Customers, narrow Your Focus, Dominate Your Market Addison Wesley Longman, 1994

31 The Business Executive's Guide to IT Architecture

32 Beath, C., J., M, Ross, Subramani. Synchronizing IT Management Practices for Business Value, Sloan School of Management Massachusetts Institute of Technology Research Briefing, July 2002 Ross, J., Beath, C., Subramani, M

33 Farell D The Real New Economy Harvard Business Review, 2003 October

34 Curtis G., Goyal D and Holtschke B. Paradox lost. Accenture Information Technology Outlook, 2004, Number 2

35 IT Forecasts: Spending Recovery in Most Vertical –Markets. Gartner Dataquest Alert ITSV-WW-DA-0178, 2003

36 Elsa Opitz, Kevin White, Stephen Minton. Global IT Economic Outlook, 2Q04. Study #31738 IDC, August 2004

37 Vertical Markets Gain Momentum in 2004 IT Spending Gartner Dataquest, 2004

38 Eastern Europe: Country Segmentation Gartner HARD-WW-DP-0146, 2001

39 2002 IT Spending and Staffing Survey Results Gartner R-18-6281, 2002

40 Broadbent M, Weill P. Leveraging the Infrastructure. How Market Leaders Capitilize on Information technologies. Harvard Business School Press, 1998

41 Federal Enterprise Architecture: realigning IT to Efficiently Achieve Agency Goals 2004

42 B. Gomolski 2003 IT Spending and Staffing Survey Results Gartner Strategic Analysis Report R-21-2290, 2003

43 L.A. Sechrest CIO Update: Use Creative Cost containment Gartner IGG-10012003-01

44 [Електронний ресурс] – Режим доступу : http://lab18.ipu.ru/projects/conf2012/1/5.htm

45 http://www.sworld.com.ua/simpoz6/29.pdf

46

47 Журнал «Финансовый директор» №7, 2003
48 Carr, Nicholas G. IT Doesn’t Matter. Harvard Business Review, May 2003
49 Curtis G., Page S. and Kaltenmark K. Thinking bigger. Accenture Information Technology Outlook 2003, Number 2
50 Mark D. and Monnoyer E. Next Generation CIOs. The MvcKinsey Quarterly Web exclusive, Kuly 2004
51 Three Laws of IT Converge to Define the Future of Business. Gartner G2 Report, 2003
52 Understanding Gartner Hype Cycles
53 B. Kirwin et al Enterprise Personality Profile: How Did We Get Here? Gartner COM-22-3093, 2004
54 D. Morello et al Introducing the Enterprise Personality Profile. Gartner AV-22-2193, 2004
55 GAO. Information Technology. Leadership Remains Key to Agencies making Progress on Enterprise Architecture Efforts 2003.
56 J, Schekkerman. Strategic Governance & Enterprise Architecture Be Enterprising EA Survey 2003
57 Return on Investment Methodology for Evaluating E-Business Infrastructure Giga, 2001
58 Hype Cycle Shows E-Government Overcoming Disillusionment Gartner, 2004
59 Structure Architecture to Win Business Buy-In/Compliance Gartner, 2004
60 E. Rechtin System Architecting: Creating and building complex systems Prentice-Hall, 1991
61 Buliding the enterpise architecture: The Popkin proces
62 Data Architecture 101 Giga, 2000
63 G. Muller Architectural reasoning; balancing genericity and Specificity Embedded Systems Institute
64 S.Haeckel Adaptive Enterprise: creating and leading sense-and-respond organizations Harvard Business School Press, 1999

ДОДАТОК А

Перелік документів на оптичному носії

1 Дипломний проект Лимарчук-Яциковської Т.О. 125м-16-1.doc – Пояснювальна записка.

2 Лимарчук-Яциковська Т.О.ptt – Презентація

ДОДАТОК Б

ВІДГУК КЕРІВНИКА ЕКОНОМІЧНОГО РОЗДІЛУ

Керівник розділу
доц. Волотковська Ю.О.

(підпис) (ініціали, прізвище)

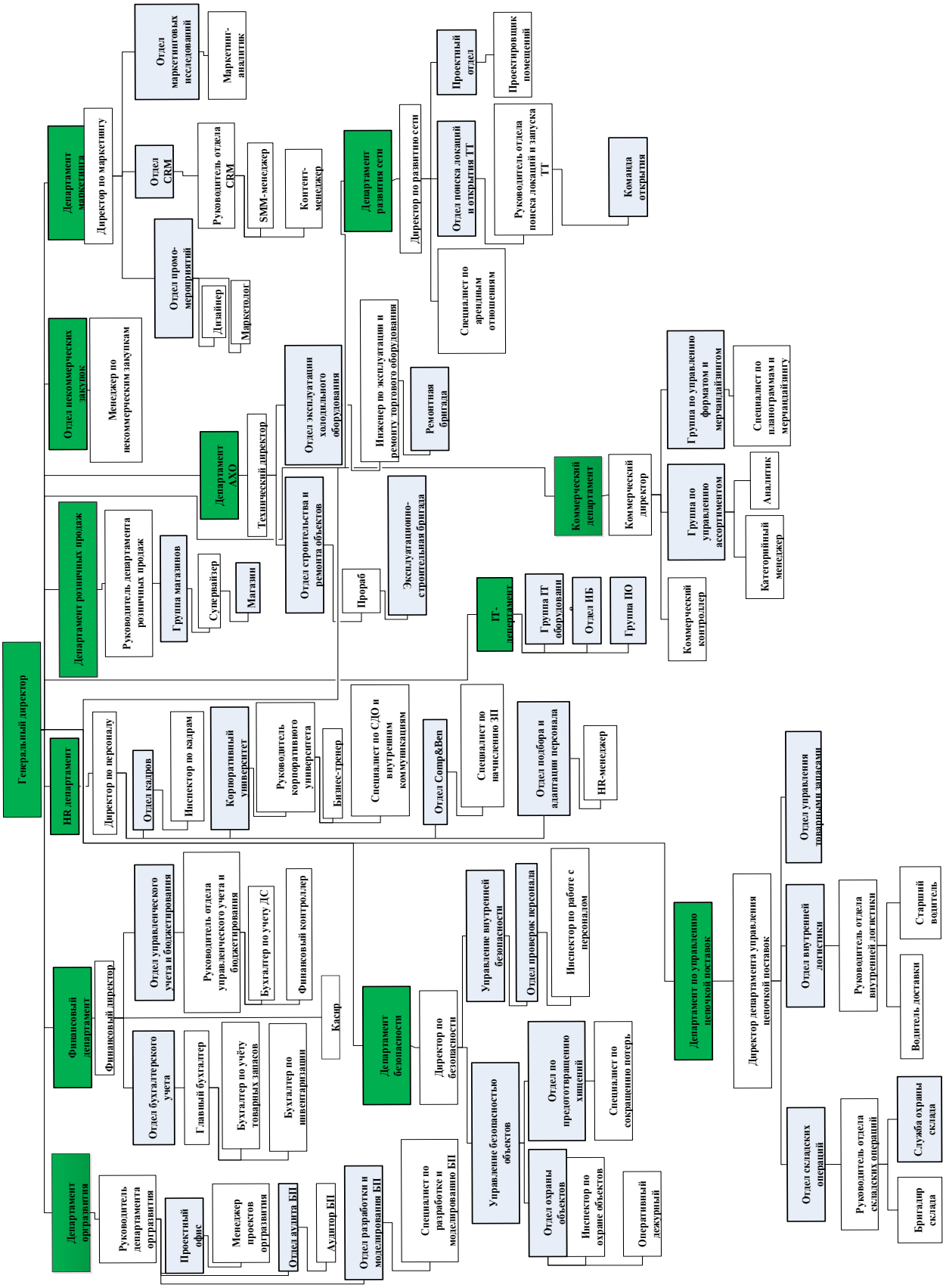
ДОДАТОК Г

Заробітна платня співробітників

Посада	Заробітна платня	Премія
Інспектор з охорони об'єктів	7000,00	
Оперативний черговий	5000,00	
Фахівець зі скорочення розкрадань	10000,00	
Бригадир складу	7500,00	
Охорона складу	7000,00	
Керівник відділу складських операцій	15000,00	
Керівник відділу внутрішньої логістики	15000,00	
Водій доставки товару	8000,00	+ %
Старший водій	8500,00	+ %
Інспектор по роботі з персоналом	7000,00	
Директор з персоналу	18000,00	
Фахівець з нормування праці	7200,00	
Фахівець ситеми дистанційного навчання	7200,00	
Бізнес-тренер	12000,00	
Керівник корпоративного університету	15000,00	
Інспектор з кадрів	7000,00	
Керівник департаменту роздрібної торгівлі	20000,00	+ %
Супервайзер	15000,00	+ %
Продавець	6000,00	
Виконроб	9000,00	
Робітник з ремонту обладнання	7600,00	
Інженер з експлуатації та ремонту торгівельного обладнання	10400,00	
Фахівець з некомерційних закупівель	7400,00	
Фахівець з маркетингу	10000,00	
Контент-менеджер	7500,00	
Дизайнер	7100,00	
smm-менеджер	7500,00	
Аналітик з маркетингу	6000,00	
Директор з маркетингу	18000,00	
Керівник відділу відкриття та розвитку торгівельних точок	15000,00	+ %
Фахівець по роботі з нерухомістю	10300,00	
Інженер- роетувальник	11000,00	
Категорийный менеджер	18000,00	+ %
Аналітик групи управління асортиментом	10000,00	
Фахівець з планограм	9500,00	
Системний адміністратор	10000,00	
Інженер з розробки ПЗ	15000,00	
Фахівець з технічної підтримки РКВ	8500,00	
Диспетчер з підримки користувачів	7000,00	
Фахівець з підбору персоналу	8000,00	
Директор департаменту з організаційного розвитку	20000,00	
Фахівець з розробки та моделювання бізнес-процесів	10000,00	
Аудитор бізнес-процесів	9000,00	

ДОДАТОК Д

Організаційна структура підприємства



Оргструктура відображена без змін відносно отриманої від організаційного директора компанії.