SIC enter
System
Integrations
Center

Практический опыт реализации проектов по построению Системы Управления Информационной Безопасностью (СУИБ) Банка в соответствии с требованиями постановления №474 и стандартов Национального банка Украины.

Дмитрий Зарахович
Ирина Ивченко

Требования регулятора

- Відповідно до статті 7 Закону України “Про Національний банк України”, статті 10 Закону України “Про захист інформації в інформаційно-телекомунікаційних системах” і статті 10 Закону України “Про стандартизацію”, з метою підвищення рівня інформаційної безпеки в банківській системі України Правління Національного банку України видало Постанову №474 від 28 жовтня 2010р. “Про набрання чинності стандартами з управління інформаційною безпекою в банківській системі України” http://bank.gov.ua/B_zakon/Acts/2010/28102010_474.pdf

- З дня опублікування цієї постанови набирають чинності такі стандарти НБУ:
  - **СОУ Н НБУ 65.1 СУІБ 1.0:2010 “Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги” (ISO/IEC 27001:2005, MOD);**
  - **СОУ Н НБУ 65.1 СУІБ 2.0:2010 “Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою” (ISO/IEC 27002:2005, MOD).**
- **Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України.**

Наш опыт - Нам доверили

SIC enter
System
Integrations
Center

UniCredit Bank

ДЕЛЬТА БАНК

БМБанк

GlobalMoney

UKR EXIM BANK

Банк Национальные инвестиции

Этапность работ по создании системы Менеджмента

Подготовительный этап

- Назначение ответственных
- Анализ документации

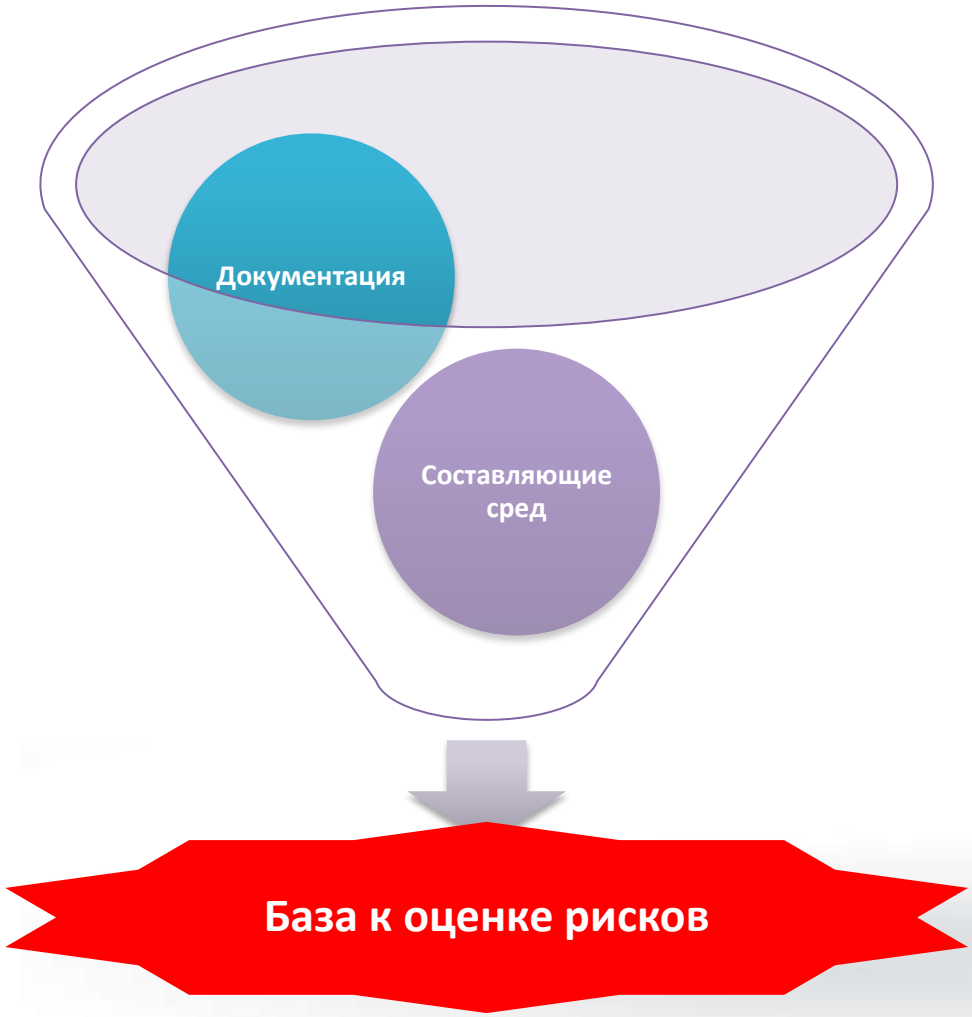
Назначение ответственных

Анализ документации

Экспертная оценка

- Существующая у Заказчика документация
- Составляющие инвентаризации:
  - Информационная среда
  - Технологическая среда
  - Физическая среда
  - Среда пользователей

Экспертная оценка



Возникающие вопросы

- Чему должно отвечать описание структуры и сети. Состав этих документов – ответ дает п.4.4 методики

Банк повинен мати внутрішнє положення про мережу банку, у якому надається така інформація:

- принципи побудови мережі з описом принципів резервування мережевого обладнання;
- принципи розподілу мережі на сегменти (підмережі) – за наявності;
- принципи розподілу адресного простору;
- система управління мережею;
- побудова вузла доступу до ресурсів мережі Інтернет;
- принципи доступу до мереж інших організацій – за наявності;
- наявність та правила роботи через канали зв'язку зовнішніх провайдерів телекомунікаційних послуг, у тому числі опис принципів резервування каналів зв'язку;
- засоби захисту мережі від зовнішнього та внутрішнього несанкціонованого доступу, у тому числі антивірусного захисту;
- принципи надання доступу працівникам банку до мережі та ресурсів мережі Інтернет;
- принципи та процедура надання віддаленого доступу працівникам банку до мережі банку – за наявності;
- принципи та процедура надання бездротового доступу до мережі банку – за наявності;
- принципи резервного копіювання інформації.

Возникающие вопросы

- Какие документы описывают физическую среду - ответ дает п.4.5 методики

Банк повинен мати такі документи:

- опис географічного та територіального розташування приміщень банку, включаючи відокремлені підрозділи банку (обласні дирекції, філії, відділення тощо) для визначення загроз з боку навколишнього середовища;
- опис принципів пропускного режиму;
- наказ із визначення приміщень з обмеженим доступом та опис відповідного захисту цих приміщень із забезпеченням контролю доступу до таких приміщень;
- опис принципів побудови систем відео спостереження;
- опис системи електроживлення та заземлення;
- опис охоронної та пожежної сигналізації;
- опис умов зберігання магнітних, оптомагнітних, паперових та інших носіїв інформації, у тому числі електронних архівів.

Оценка рисков

- Перечень бизнес-процессов
- Выделение критических бизнес-процессов
- Описание бизнес-процессов согласно методике НБУ

Возникающие вопросы

- Какие критичные бизнес-процессы выбирать для области применения и как их описывать - ответ дает п.4.2 методики

  – Відповідно до Положення про організацію операційної діяльності в банках України, затвердженого постановою Правління Національного банку України від 18.06.2006 N254 **банківський продукт - це стандартизовані процедури, що забезпечують виконання банками операцій, згрупованих за відповідними типами та ознаками.**

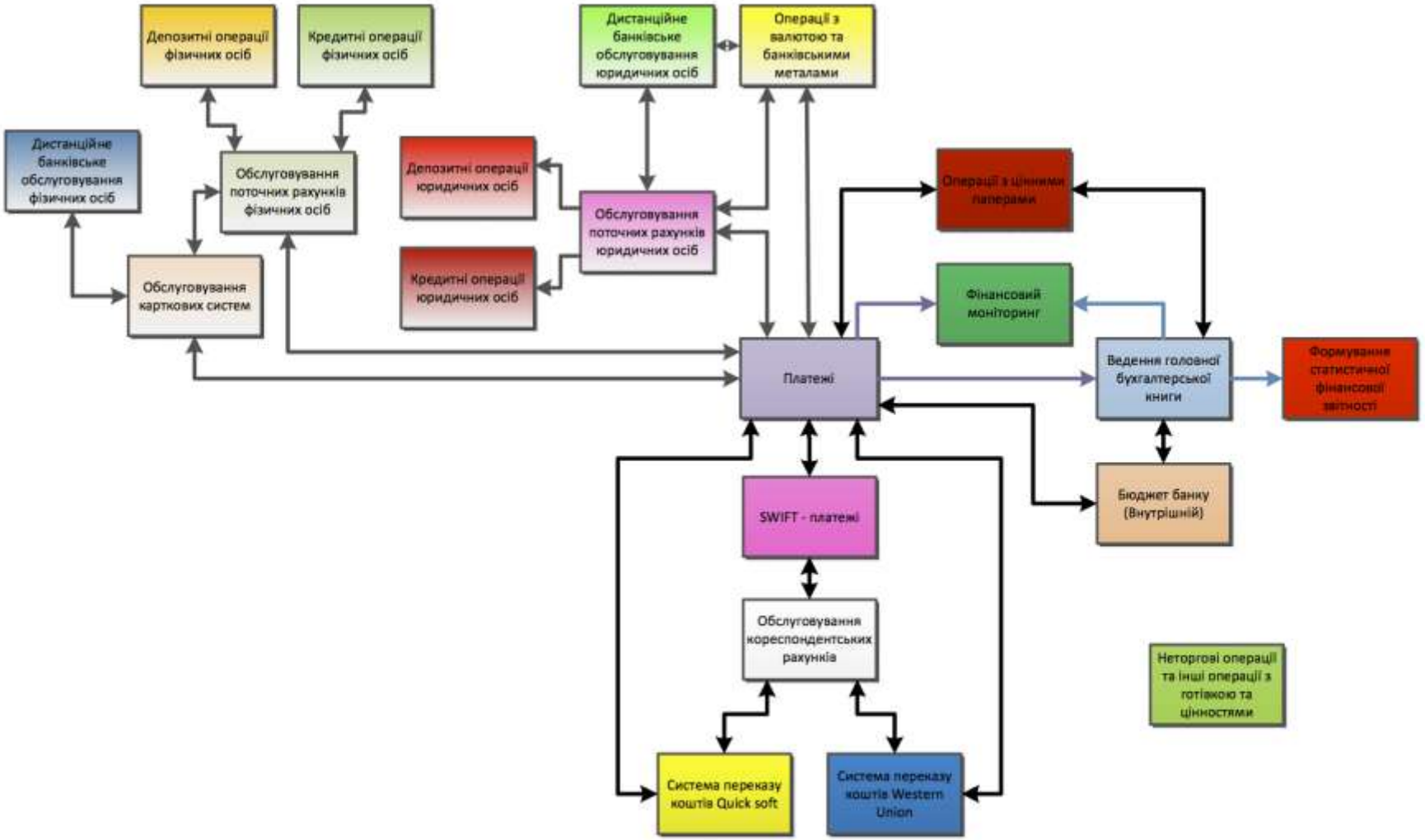
  – **Не існує стандартного набору бізнес-процесів/банківських продуктів для будь-якого банку.** Тому банк має самостійно визначити відповідні бізнес-процеси/банківські продукти, які використовуються всередині банку.

Возникающие вопросы

- Какие критичные бизнес-процессы выбирать для области применения и как их описывать - ответ дает п.4.2 методики

  – Для визначення бізнес-процесів/банківських продуктів, які має охоплювати СУІБ, необхідно проаналізувати всі бізнес-процеси/банківські продукти банку та **створити перелік критичних процесів, функціонування яких має великий вплив на успішну роботу банку.** Оскільки в банку бізнес-процеси/банківські продукти взаємопов'язані, то рекомендується **створити їх блок-схему з визначенням усіх взаємозв'язків. Така візуалізація значно спростить розуміння всього обсягу робіт, що виконуються банком.**

Пример блок-схемы критичных бизнес-процессов



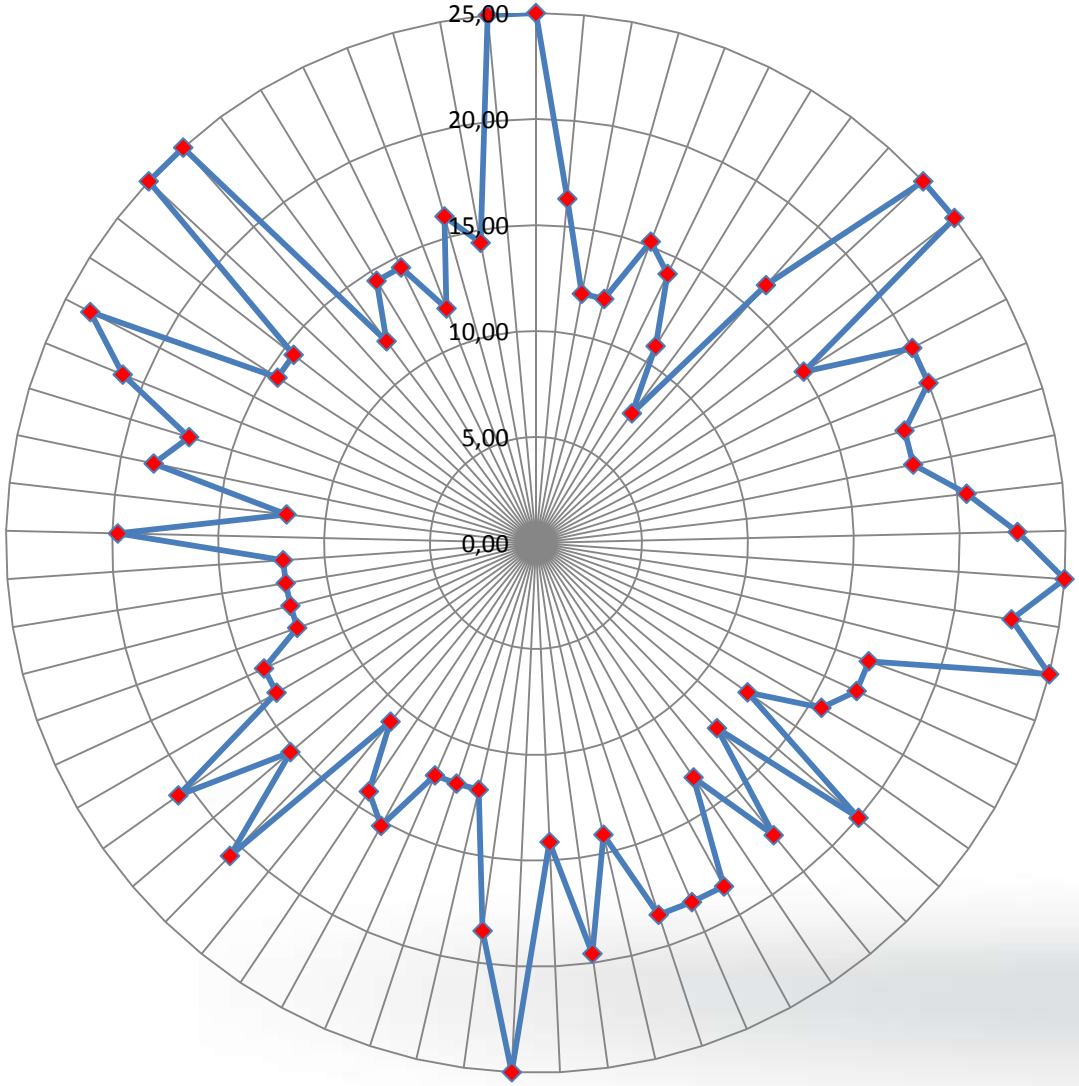
Возникающие вопросы

- Какие критичные бизнес-процессы выбирать для области применения и как их описывать - ответ дает п.4.2 методики
  - Банк повинен створити **перелік критичних бізнес-процесів/банківських продуктів, які обробляють інформацію з обмеженим доступом, розголошення якої може нанести шкоду банку**. До цього переліку повинні бути включеними всі бізнес-процеси/банківські продукти, що обробляють:
    - платіжні документи,
    - внутрішні платіжні документи,
    - кредитні документи,
    - документи на грошові перекази,
    - персональні дані клієнтів та працівників банку,
    - статистичні звіти,
    - інші документи, які містять інформацію з обмеженим доступом.

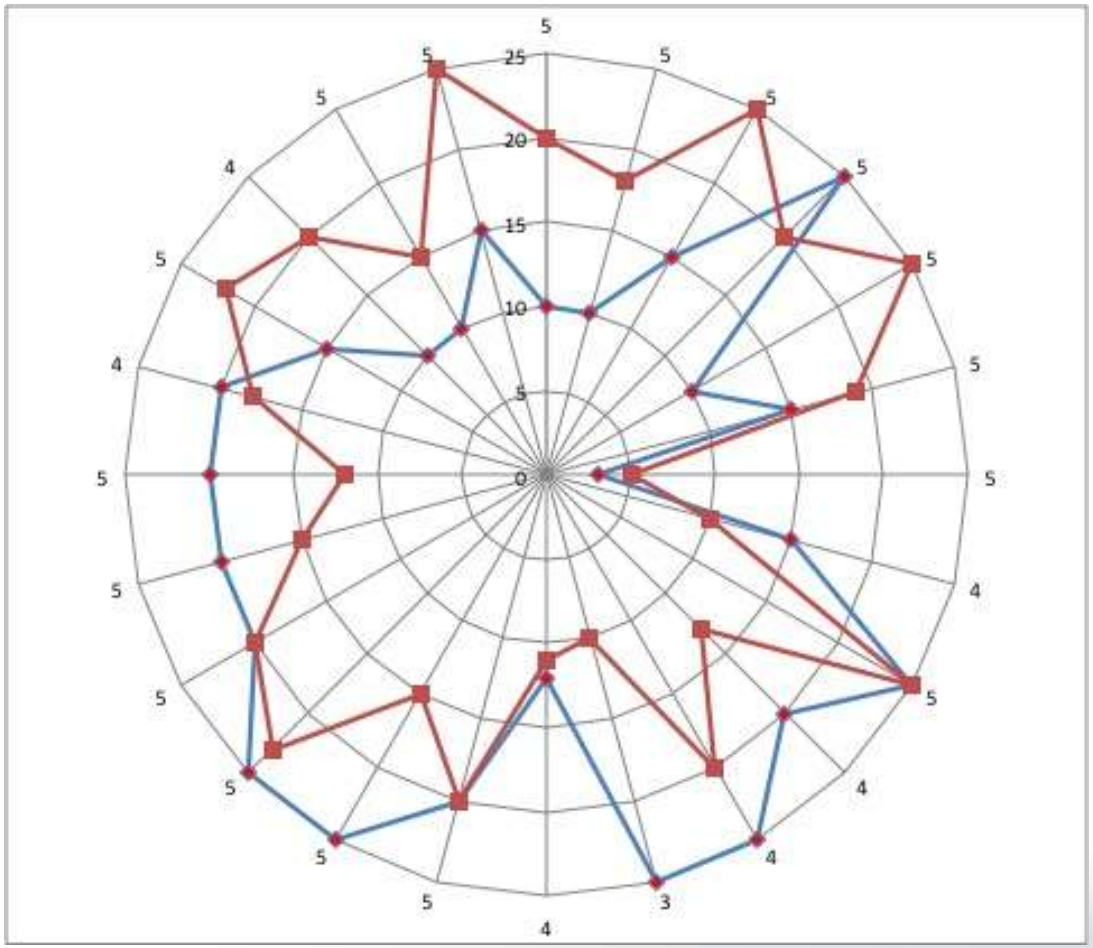
Возникающие вопросы

- Какие критичные бизнес-процессы выбирать для области применения и как их описывать - ответ дает п.4.2 методики
  - назва бізнес-процесу/банківського продукту;
  - цілі бізнес-процесу/банківського продукту;
  - гриф інформації з обмеженим доступом, яка обробляється бізнес-процесом/банківським продуктом;
  - власник бізнес-процесу/банківського продукту;
  - підрозділи банку, які забезпечують функціонування бізнес-процесу/банківського продукту;
  - наявність зобов'язань перед третіми сторонами (угоди на розроблення, доопрацювання, супроводження та технічне обслуговування);
  - вхідні та вихідні дані бізнес-процесу/банківського продукту;
  - перелік процедур бізнес-процесу та блок-схема послідовності їх виконання з визначенням взаємозв'язків (у тому числі додаткової вхідної інформації з інших бізнес-процесів);
  - вимоги щодо забезпечення безперервності бізнес-процесу/ банківського продукту (максимально допустимий час простою);
  - типи ролей(груп) для бізнес-процесу/банківського продукту;
  - існування забороненого суміщення типів ролей;
  - програмно-технічний(ні) комплекс(и), що забезпечує(ють) функціонування бізнес-процесу;
  - кількість користувачів програмно-технічного комплексу;
  - архітектура і технологія роботи (зокрема, файловий обмін або режим реального часу, в тому числі й для обміну інформацією з іншими програмно-технічними комплексами в разі наявності);
  - операційна система та тип бази даних програмно-технічного комплексу, які використовуються для функціонування бізнес-процесу/банківського продукту;
  - географічне розміщення (серверів та робочих місць) програмно-технічного комплексу;
  - засоби захисту, які вже існують у програмно-технічному комплексі;
  - взаємодія з іншими програмно-технічними комплексами;
  - принципи резервування обладнання та інформації програмно-технічного комплексу (за наявності окремих принципів для цього

«Облако рисков» для пар угроза/уязвимость



«Облако рисков» и их устранение



Дмитрий Зарахович
Dmitry.Zarakhovych@sicenter.net
+380 98 124-0-126
Ирина Ивченко
Irina.Ivchenko@sicenter.net
+380 67 715-13-69

SICenter (ООО «Центр Системных Интеграций»)
Оболонская набережная, 7
корпус 3, офис 1
04210, Киев, Украина

тел.: +380 44 581-86-14/15
e-mail: ukraine@sicenter.net
http://sicenter.net

SICenter (ООО «Центр Системных Интеграций»)
ул. Нахимова, 12, офис 110
220033, Минск, Беларусь

тел.: +375 17 298-13-84
e-mail: belarus@sicenter.net
http://sicenter.net