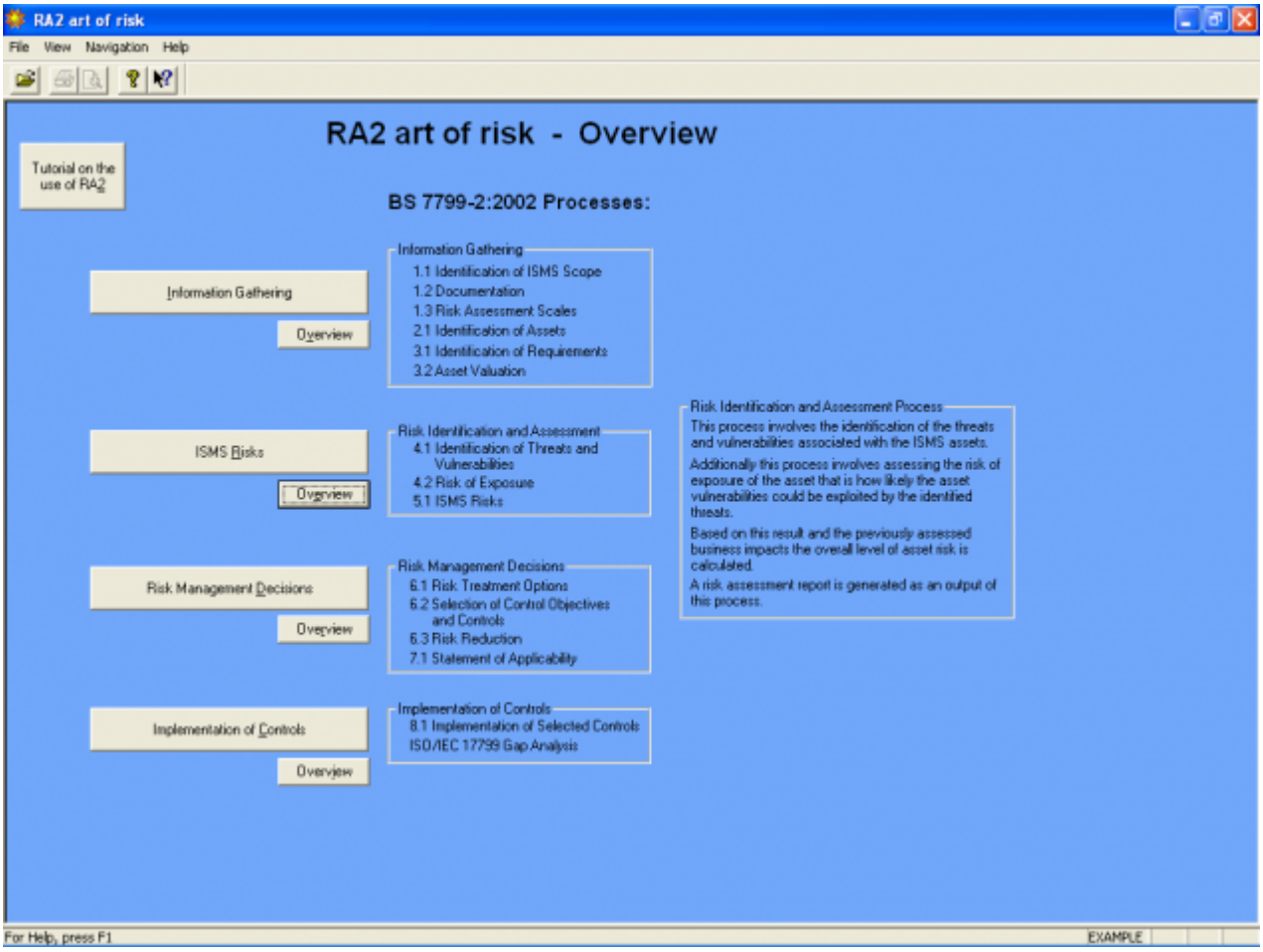
RA2 the art of risk

написано Александр Астахов | 11 июня, 2023
Совместно разработанный AEXIS Security Consultants и XiSEC Consultants Ltd инструментарий для оценки и управления информационными рисками *RA2 the art of risk* предназначен в первую очередь для того, чтобы облегчить создание СУИБ в соответствии с требованиями международного стандарта ISO 27001. В RA2 реализован достаточно простой для понимания процессный подход, общие требования к которому определены в ISO 27001 и более подробно описаны в стандарте BS 7799-3.

Наш особый интерес к этому программному продукту обусловлен в первую очередь тем, что его разработчики Тэд Хамфриз (Ted Humphreys) и Анжелика Плейт (Angelika Plate) – известные личности в области управления безопасностью. Они являются редакторами британского стандарта BS 7799 и международных стандартов ISO 27001 и ISO 17799, а также авторами серии книг BIP 0071-0074, являющихся официальными руководствами Британского Института Стандартов по внедрению стандартов серии 27000.

Процесс создания СУИБ в RA2 разделен на четыре этапа:

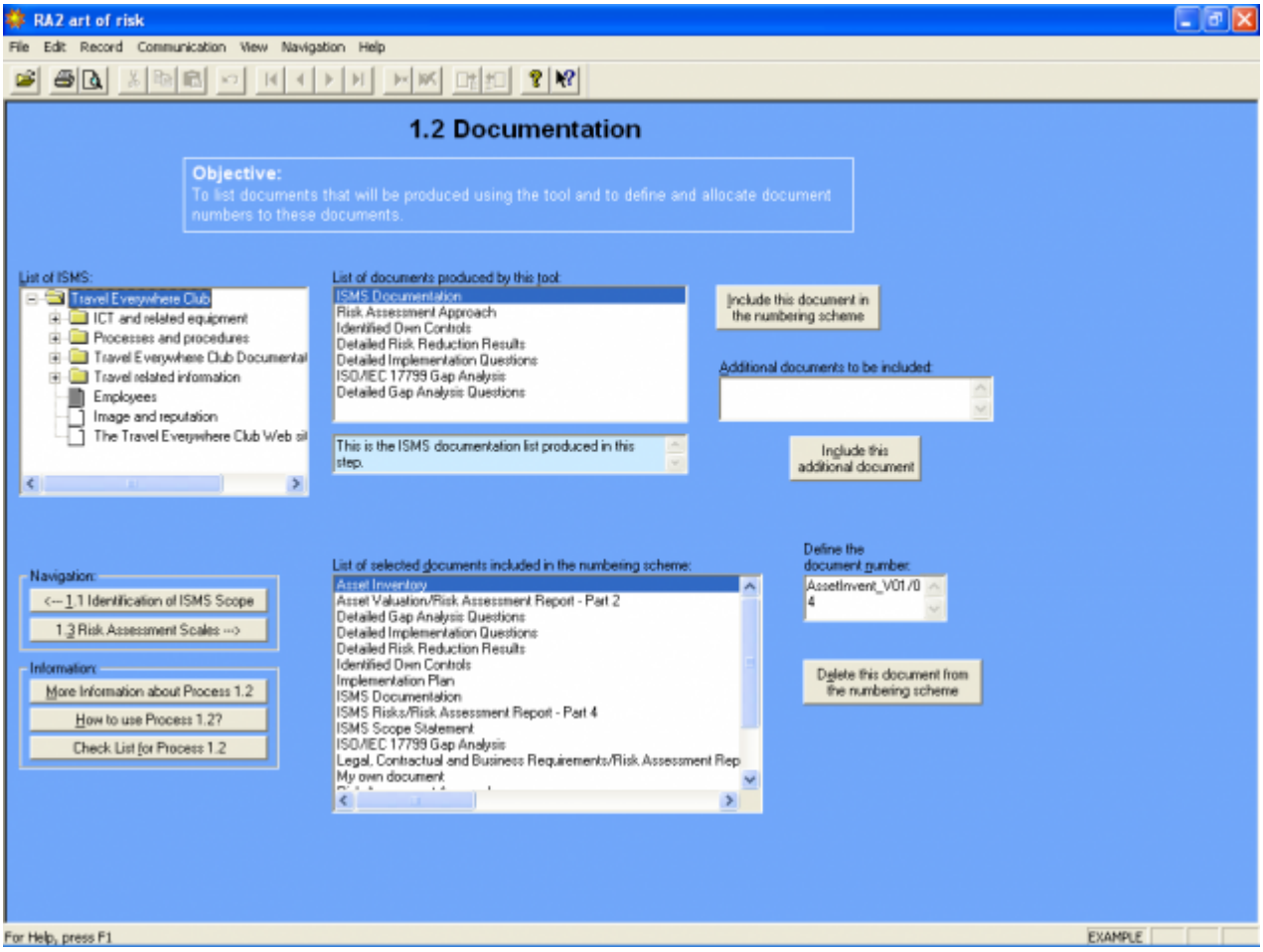
1. Сборинформации(Information Gathering).
2. Оценка рисков (ISMS Risks).
3. Обработкарисков(Risk Management Decisions).
4. Внедрениемеханизмовконтроля(Implementation of Controls).



Каждый шаг программы снабжен подробными пояснениями в полном соответствии со стандартом BS 7799.

Программный продукт RA2 включает в себя средства для решения следующих задач:

- определения области действия, бизнес-требований, политики и целей СУИБ;
- разработки реестра активов СУИБ;
- оценки рисков СУИБ;
- принятия решения по обработке рисков путем выбора подходящих контрмер из приложения А к стандарту BS 7799-2;
- анализа расхождений со стандартом ISO 27002;
- формирования Декларации о применимости и других документов СУИБ.



На наш взгляд, RA2 является хорошим средством для демонстрации концепции процессного построения СУИБ, выраженной в BS 7799-2 (ISO 27001), а также полезным инструментом для обучения внедрению СУИБ. Его практическое использование в организации в качестве средства для управления рисками затрудняется недостаточной проработанностью пользовательского интерфейса (неудобные средства ввода и редактирования текстовой информации), примитивностью средств, предоставляемых для работы с моделью активов, угрозами и уязвимостями, а также определенными огрехами по части отображения кириллицы в отчетах.