vsRisk

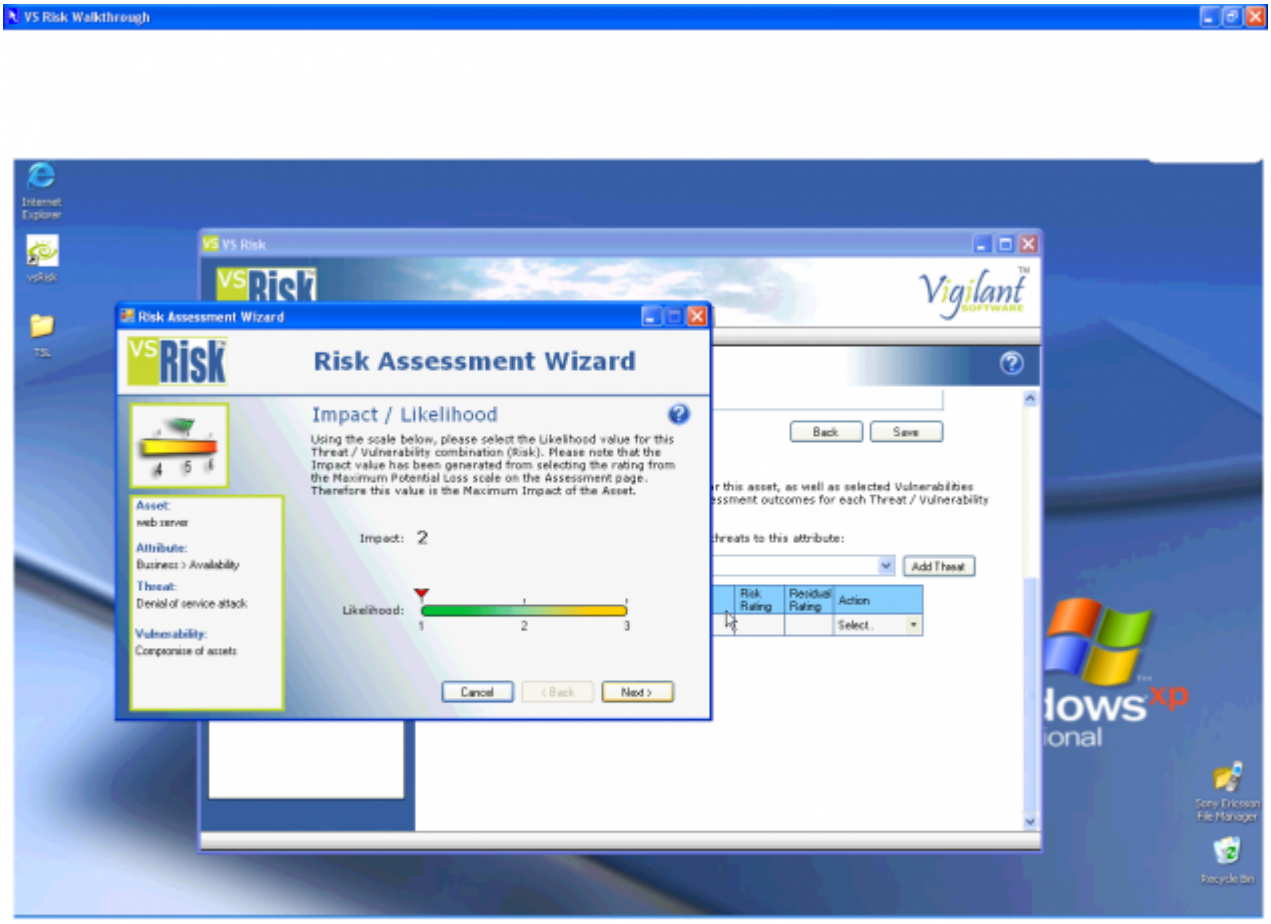
написано Александр Астахов | 11 июня, 2023
Разработанный британской компаний IT Governance совместно с Vigilant Software программный продукт *vsRisk Risk Assessment Tool* является современным средством оценки рисков, так же как и RA2, полностью базирующемся на международном стандарте ISO 27001.

Программный продукт vsRisk предоставляет простой и понятный пользовательский интерфейс на основе визардов и обладает следующими полезными свойствами:

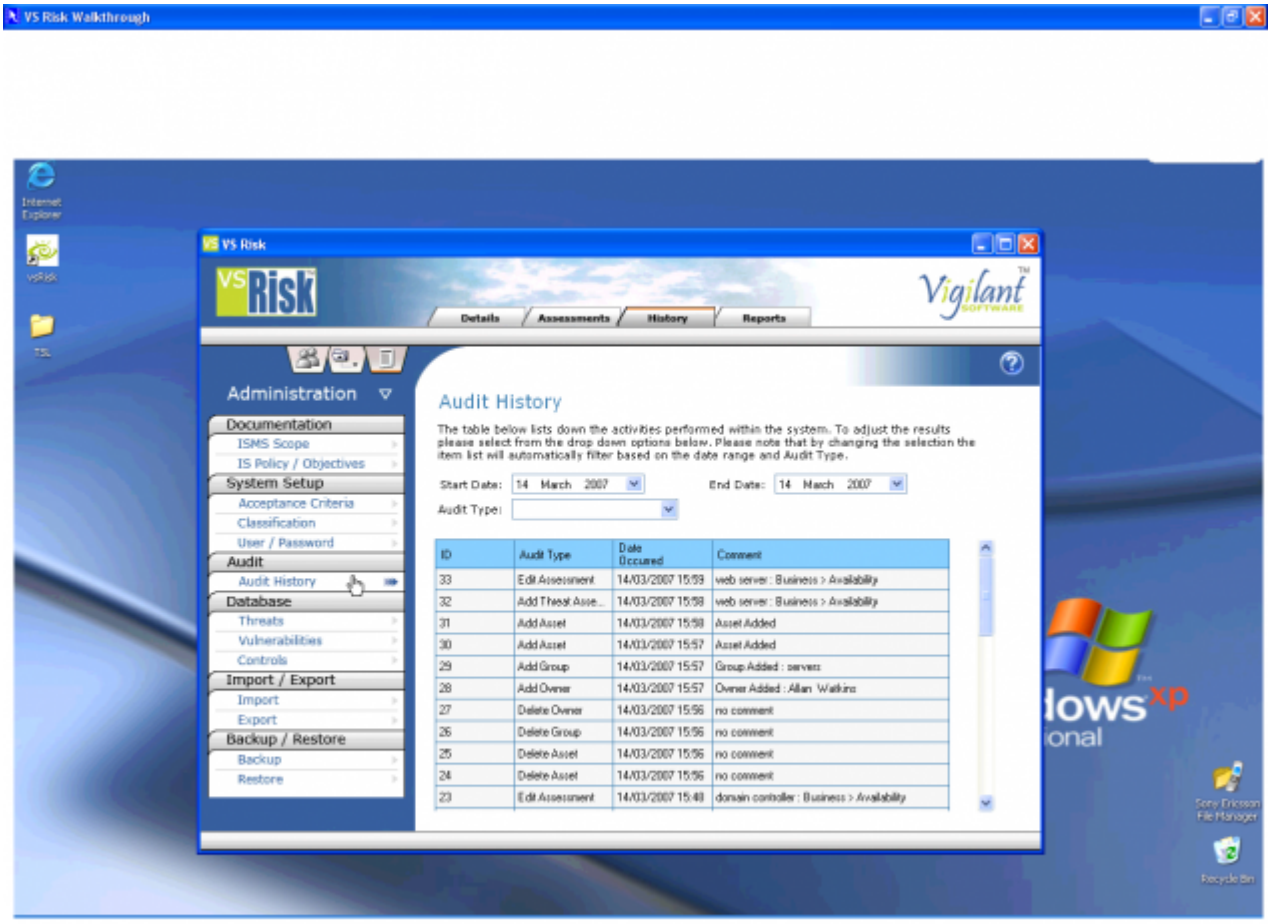
- позволяет оценивать риски нарушения конфиденциальности, целостности и доступности информации для бизнеса, а также с точки зрения соблюдения законодательства и контрактных обязательств в четком соответствии с ISO 27001;
- поддерживает следующие стандарты: ISO/IEC 27002, BS7799-3:2006, ISO/IEC TR 13335-3:1998, NIST SP 800-30;
- содержит интегрированную, регулярно обновляемую базу знаний по угрозам и уязвимостям.

Создатели vsRisk относятся к числу ведущих британских экспертов в области управления информационной безопасностью, которые готовили первые британские компании к сертификации по требованиям стандарта BS 7799, поэтому с концептуальной точки зрения продукт хорошо проработан. К сожалению, он не содержит средств для количественной оценки величины риска, ограничиваясь только качественными шкалами, настраиваемыми пользователем. Все прочие недостатки, скорее, лежат в области реализации.

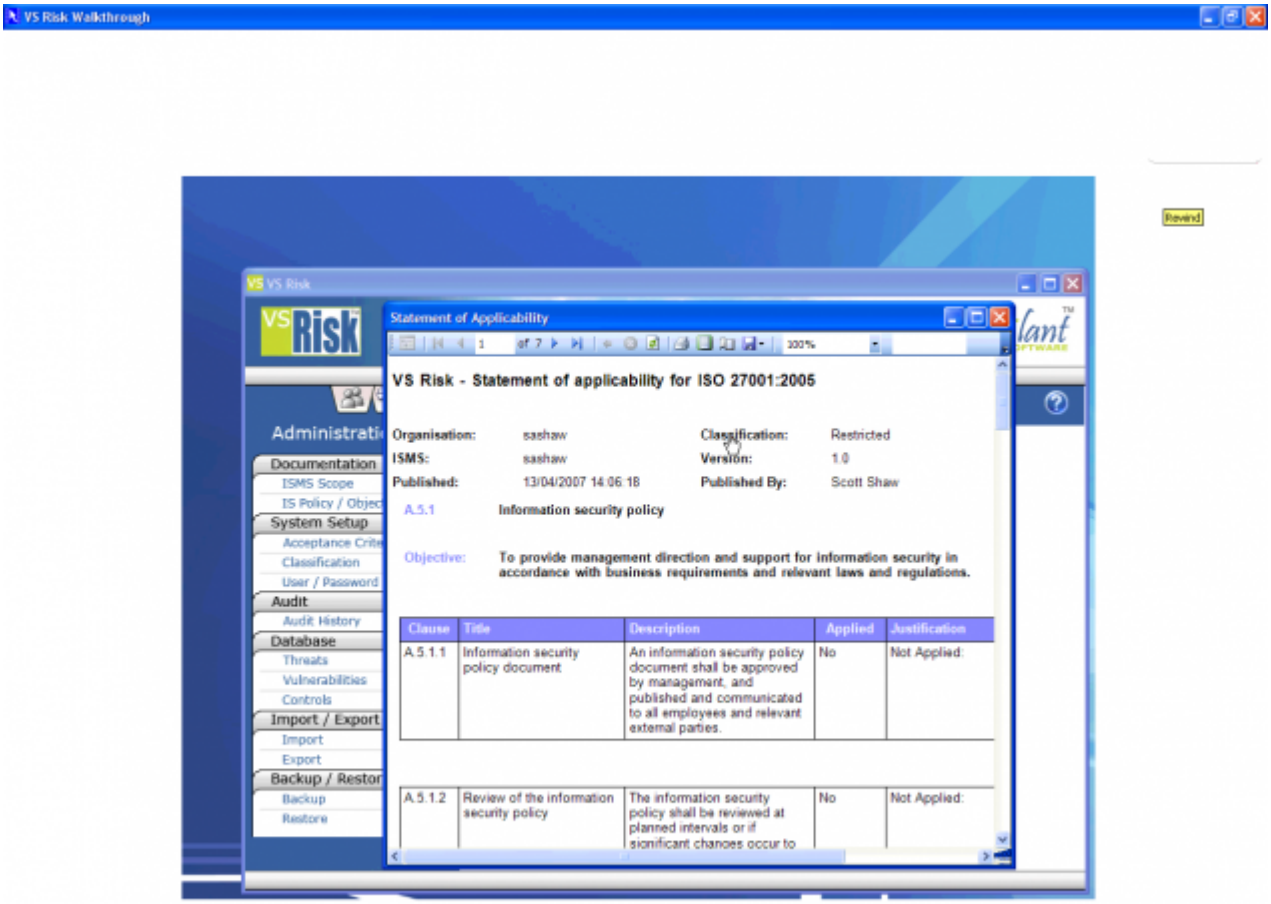
Программный продукт vsRisk предоставляет средства для качественной оценки всех факторов рисков, включая угрозы, уязвимости, активы и механизмы контроля.



Все изменения, вносимые в базу данных продукта по ходу работы, подробным образом фиксируются в журнале аудита.



vsRisk позволяет по результатам оценки рисков формировать Декларации о применимости механизмов контроля и План обработки рисков в соответствии с требованиями стандарта ISO 27001.



vsRisk достаточно прост в использовании, его интерфейс снабжен всеми необходимыми пояснениями и он полностью соответствует требованиям международного стандарта ISO 27001, предъявляемым к оценке рисков.

В то же время существует ряд проблем, характерных не только для vsRisk, но и для многих других импортных продуктов. Приведем здесь перечень этих проблем, который был направлен разработчикам для устранения:

- *Проблема с отображением символов кириллицы*. Встречается в том или ином виде в большинстве импортных продуктов, специально не позиционируемых для российского рынка.Комментарии здесь излишни.
- *Отсутствие средств для построения модели активов*(такие средства предусмотрены, например, в CRAMM). В vsRisk активы не связаны между собой. Серверы не связаны с установленными на них приложениями или хранящимися на

них данными, а также с помещениями, в которых они расположены. В результате при оценке рисков для правильной оценки ущерба, связанного, скажем, с техническими неполадками сервера, пользователь должен «держать в голове» все эти связи между сервером, приложениями, данными и помещениями, чтобы учитывать последствия данного сбоя для других активов. Затем, при оценке рисков для приложений и данных, мы вынуждены снова оценивать эти ущербы.

- *Угрозы не связаны с соответствующими типами уязвимостей и категориямиактивов.*В результате в vsRisk для каждого рассматриваемого актива мы должны выбирать применимые к нему угрозы из полного списка угроз, который включает в себя множество угроз, заведомо неприменимых к данной категории активов. Затем для каждой угрозы необходимо выбрать связанные с ней уязвимости, опять же из полного списка уязвимостей, многие из которых не могут иметь отношения к данной угрозе. Мы находим этот процесс слишком трудоемким.
- *Невозможность добавления пояснений и обоснований выбора тех или иных значений вероятности угрозы и величины уязвимости.*В результате чего при анализе результатов оценки рисков невозможно определить, почему были выбраны те или иные значения.
- *Описание механизмов контроля включает в себя только название и цели*. В то же время нам требуется подробное описание каждого механизма контроля в соответствии со стандартом ISO 27002, а также возможность добавлять наши собственные описания.

Следует учитывать, что мы тестировали самую первую версию продукта, от которой сложно было бы ожидать идеальной проработанности функционала. Остается лишь подождать, когда данный продукт будет «доведен до ума». По крайней мере, разработчики обещали нам приложить определенные усилия в этом направлении.