# Callio Secura 17799

написано Александр Астахов | 11 июня, 2023
Компания Callio Technologies была основана в 2001 году двумя канадскими академиками и специализируется в области разработки программных продуктов для анализа информационных рисков и управления информационной безопасностью в соответствии с требованиями стандартов BS 7799 и ISO 17799. *Callio Secura 17799* представляет собой комплексную систему для разработки, внедрения, эксплуатации и сертификации Системы управления информационной безопасностью (СУИБ) на основе стандарта BS 7799.

Также разработчик предлагает инструментальный комплект Callio Toolkit Pro 17799, который представляет собой серию документов и утилит, объединенных с целью помочь в понимании стандарта и приведении СУИБ в соответствие с его базовыми требованиями.

Callio Secura 17799 предоставляет следующие основные возможности:

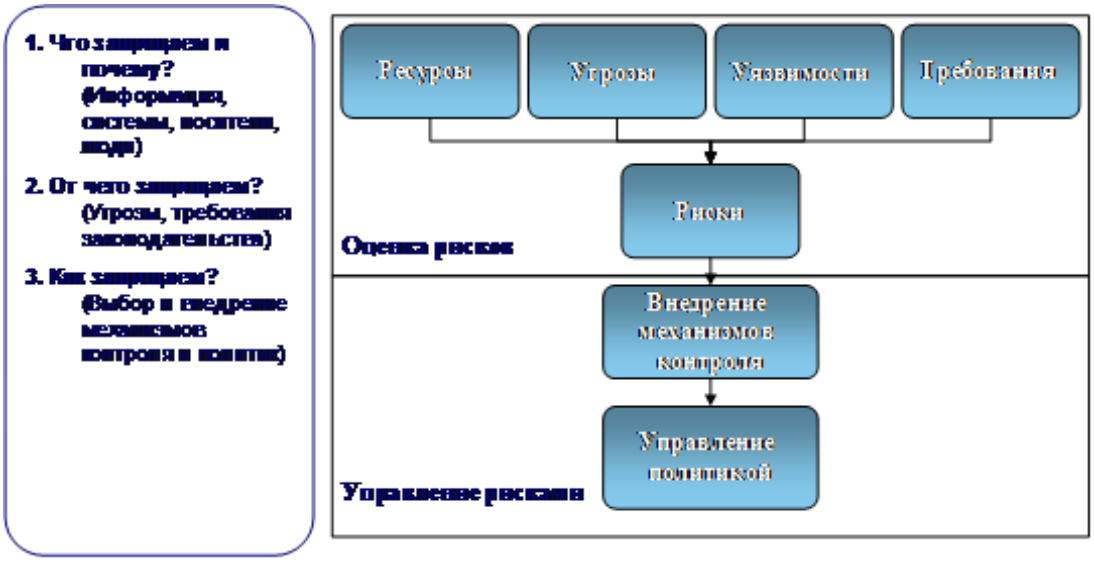
- оценку соответствия стандарту ISO 17799;
- инвентаризацию активов;
- описание структуры и процессов СУИБ;
- оценку и обработку рисков;
- разработку планов внедрения механизмов контроля;
- шаблоны политик безопасности (свыше 50 примеров);
- управление документами;
- управление опросными листами;
- оценку готовности к сертификации СУИБ по требованиям международного стандарта ISO 27001.

Процесс управления рисками по Callio состоит из двух этапов.

*На первом этапе*производится идентификация активов, угроз, уязвимостей и требований безопасности, оценивается величина уязвимостей, вероятность угроз и ценность активов. На

основании этих данных вычисляются значения рисков.

*На втором этапе*принимается решение относительно способов обработки рисков, приемлемого уровня остаточных рисков, разрабатывается план обработки рисков, производится внедрение механизмов контроля и разработка политик безопасности и других организационно-распорядительных документов.




Callio Secura 17799 предоставляет Web-интерфейс, механизмы коллективной работы, распределения ролей и полномочий между участниками процессов управления ИБ – рабочими группами, реализует управление документами, предоставляет шаблоны документов и опросники, а также методологию анализа и управления рисками. Система реализует рабочий процесс (workflow), который используется при внедрении СУИБ и подготовке к сертификации.

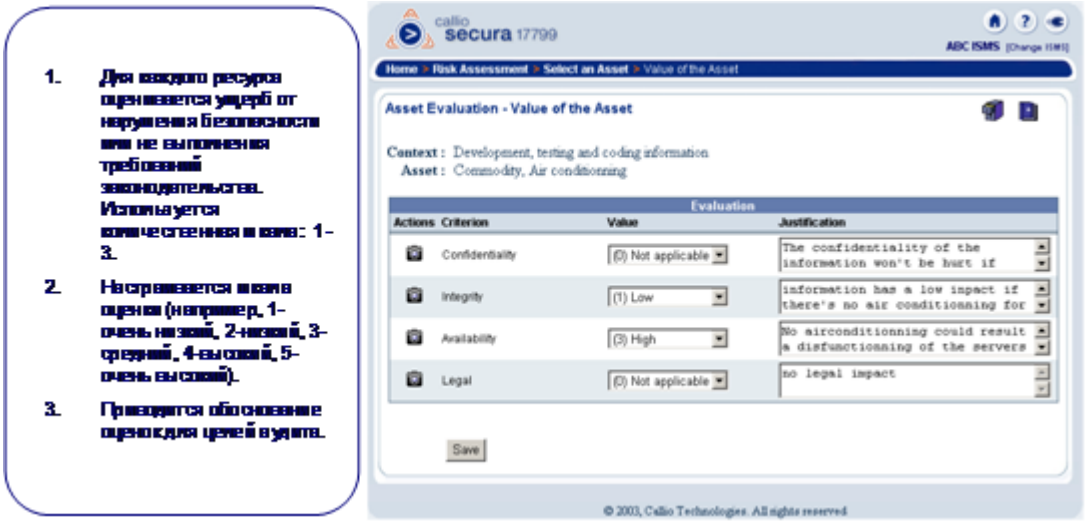
Процесс подготовки к сертификации начинается с первоначальной диагностики, в ходе которой выполняется оценка соответствия текущего состояния ИБ требованиям стандарта (gap analysis).

1. Заполнение опросника (127 вопросов) для оценки состояния системы управления безопасностью, на основе механизмов контроля, процедур и политик, описанных в ISO 17799.
2. Изучение каждого из 127 механизмов контроля, описанных в Стандарте, в соответствии с Руководством.
3. Идентификация существующих мер защиты. Проверка механизмов контроля, которые были полностью или частично реализованы, являются неправильными, либо отсутствуют.


На следующем этапе производится оценка рисков. Процесс оценки рисков начинается с инвентаризации активов. Он включает в себя идентификацию и категорирование ресурсов, составление перечня сведений ограниченного распространения и реестра информационных активов.


Далее для каждого актива оценивается его ценность для организации, которая определяется ущербом в результате

нарушения его конфиденциальности, целостности, доступности или невыполнения требований при осуществлении угроз безопасности.



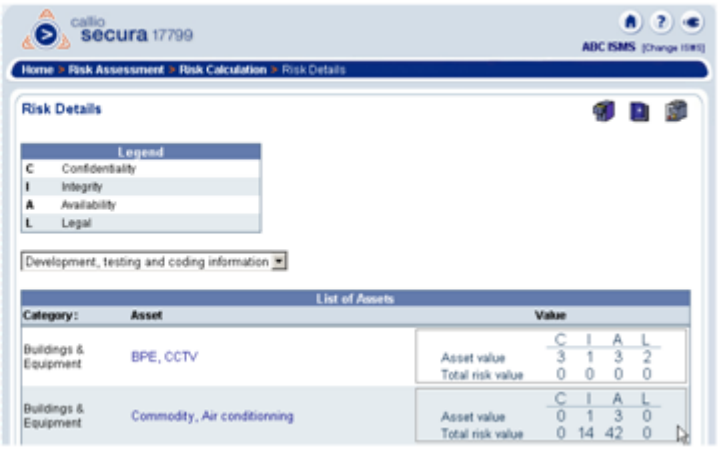

Идентификация рисков предполагает установку взаимосвязей между активами, уязвимостями и угрозами безопасности. Эта задача была бы очень непростой, т.к. для обычной организации таких взаимосвязей насчитывается несколько тысяч. Используемый инструментарий облегчает нам эту задачу, предлагая установки по умолчанию.


Далее для вычисления рисков определяются вероятности реализации угроз. Для каждой угрозы указывается вид ущерба.

1. Используйте собственную вероятностную шкалу для каждой СУИБ.
2. Оцените количественно вероятность реализации угроз, использующих идентифицированные для каждого ресурса уязвимости.
3. Определите, с чем связан ущерб: нарушение конфиденциальности, целостности, доступности или нарушение требований законодательства.


Базируясь на информации о ценности активов и вероятности угроз, система автоматически вычисляет значения рисков и производит их упорядочивание по приоритетам.

1. Просмотр рисков в порядке приоритета.
2. Риск = ущерб х вероятность реализации угрозы или нарушения требований законодательства или бизнеса.
3. Просмотрите отчет об анализе рисков, чтобы принять правильное решение о том, что с ними делать (уменьшить, принять, избежать или передать).




Когда оценка рисков завершена, можно переходить к выбору и внедрению механизмов контроля, необходимых для минимизации рисков. CallioSecuraна основании результатов оценки рисков автоматически формирует набор рекомендуемых механизмов контроля из числа описанных в стандарте. Для каждого механизма контроля проставляется его текущий статус.

По завершении этого этапа формируется план создания СУИБ. После этого можно переходить к разработке и внедрению политик безопасности.

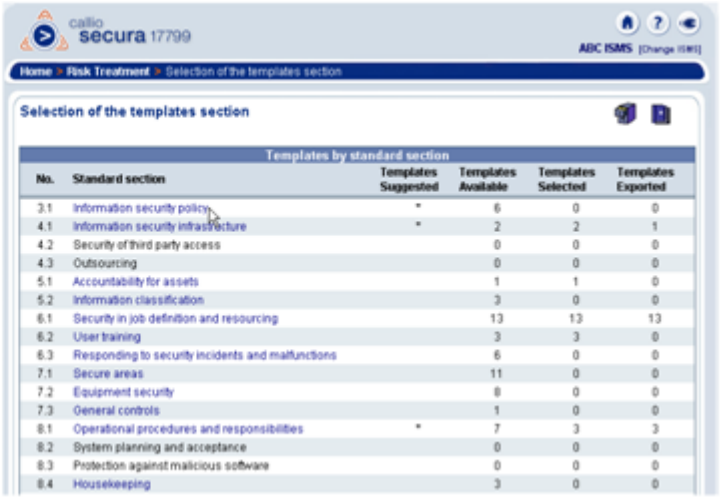
1. На основании результатов анализа рисков Callio Secura 17799 предлагает административные, технические и физические механизмы контроля.
2. Выбор из предложенных механизмов контроля и обоснование принятых решений по каждому механизму.
3. Чтобы правильно понимать смысл механизма контроля, используйте руководство. Используйте инструкции по внедрению, интерпретации рекомендаций стандарта, цели контроля, а также словарь терминов.


Для разработка политик безопасности используются шаблоны типовых документов. Базируясь на результатах анализа рисков, система автоматически формирует набор необходимых шаблонов. Готовые политики экспортируются в модуль управления документами, который позволяет производить их ревизию, согласование и публикацию на Web-портале.

1. Создание политики безопасности с использованием шаблонов, предоставляемых Callio Secura 17799 (35 политик и более 500 разъяснений положений ISO 17799).
2. На основании результатов анализа рисков автоматически появляется набор политик в модуле «Policy Generator».
3. Выбирайте, добавляйте, удаляйте и изменяйте набор политик.
4. Набор политик экспортируется в модуль «document manager» для согласования и публикации.

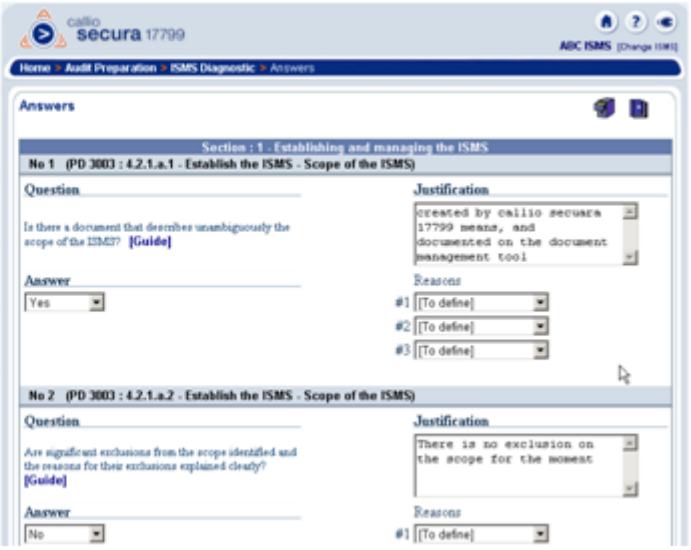

Всего имеется более 100 различных документов, которые используются при реализации механизмов контроля СУИБ. Если предложенных системой шаблонов недостаточно, мы можем выбрать дополнительные документы и экспортировать их в модуль управления документами.

1. Около 100 документов, включая модели, списки проверок, примеры, дополнительная информация и утилиты используются для реализации механизмов контроля СУИБ в соответствии с ISO 17799.
2. Выберите нужные шаблоны и экспортируйте их в модуль «Документооборот».

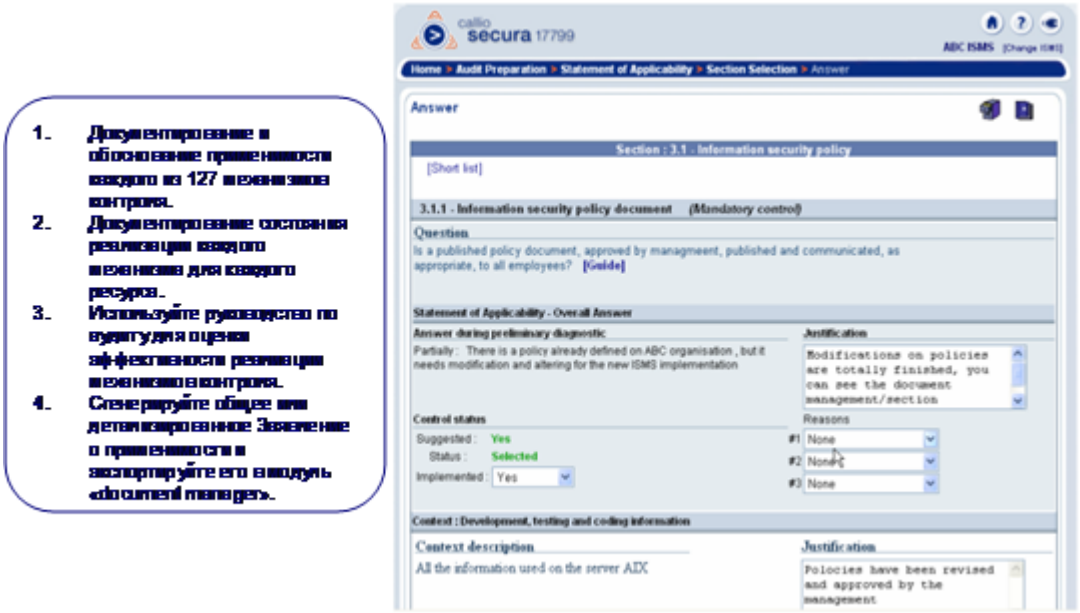



После того как создание СУИБ завершено – люди обучены, политики разработаны и внедрены, а функционирование механизмов контроля подтверждается документированными свидетельствами, – производится диагностика СУИБ с целью определения степени ее готовности к сертификации. Для этого используются специальный опросник и сопроводительные инструкции, предоставляемые системой.

1. Проверьте что СУИБ готова к сертификации по BS 7799-2.
2. Ответьте на 81 вопрос, которые помогут проверить что СУИБ позволяет устанавливать, контролировать, проверять, сопровождать и совершенствовать существующую структуру управления.
3. Проверьте что в организации правильно осуществляется управление документацией и правильно распределены ответственность и обязанности.
4. Изучайте инструкции, интерпретирующие каждый вопрос.




Декларация о применимости является последним разрабатываемым документом и обязательным условием для сертификации. В нем для каждого механизма контроля, описанного в стандарте, указывается его применимость, текущий статус, степень реализации и обоснование его использования. Это первый документ, который изучается аудиторами во время сертификации.




В составе системы есть специальный модуль управления документами, который позволяет хранить все документы, имеющие отношение к функционированию СУИБ в центральной базе данных, публиковать и управлять доступом к этим документам для различных рабочих групп через веб-интерфейс. При помощи этого инструмента выполняются такие необходимые задачи, как согласование и утверждение документов, а также контроль версий.


Callio Secura 17799 служит примером системы, которая объединяет функции управления рисками с функциями поддержки других процессов жизненного цикла СУИБ, таких как управление документами, контроль соответствия требованиям стандарта ISO 17799 и предсертификационный аудит СУИБ.