ЛАБОРАТОРНАЯ РАБОТА

Анализ защищенности инфраструктуры с помощью Microsoft Security Assessment Tool

Цель работы

Познакомимся с разработанной Microsoft программой для самостоятельной оценки рисков, связанных с безопасностью – Microsoft Security Assessment Tool (MSAT).

Теоретические сведения

Как отмечают разработчики, приложение предназначается для организаций с числом сотрудников менее 1000 человек, чтобы содействовать лучшему пониманию потенциальных проблем в сфере безопасности.

Кроме измерения соотношения угрозы безопасности и методов защиты, средство также измеряет уровень безопасности организации. Уровень безопасности подразумевает развитие высокоэффективных и стабильных методик обеспечения безопасности. При низком значении используется ограниченное число методов защиты, а для действий характерно быстрое реагирование. При высоком значении практикуются устоявшиеся и проверенные процессы, которые позволяют компании предпринимать упреждающие меры и при необходимости реагировать еще эффективнее и согласованнее.

В ходе работы, пользователь, выполняющий роль аналитика, ответственного за вопросы безопасности, отвечает на две группы вопросов.

Первая из них посвящена бизнес-модели компании, и призвана оценить риск для бизнеса, с которым компания сталкивается в данной отрасли и в условиях выбранной бизнес-модели. Создается так называемый профиль риска для бизнеса (ПРБ).

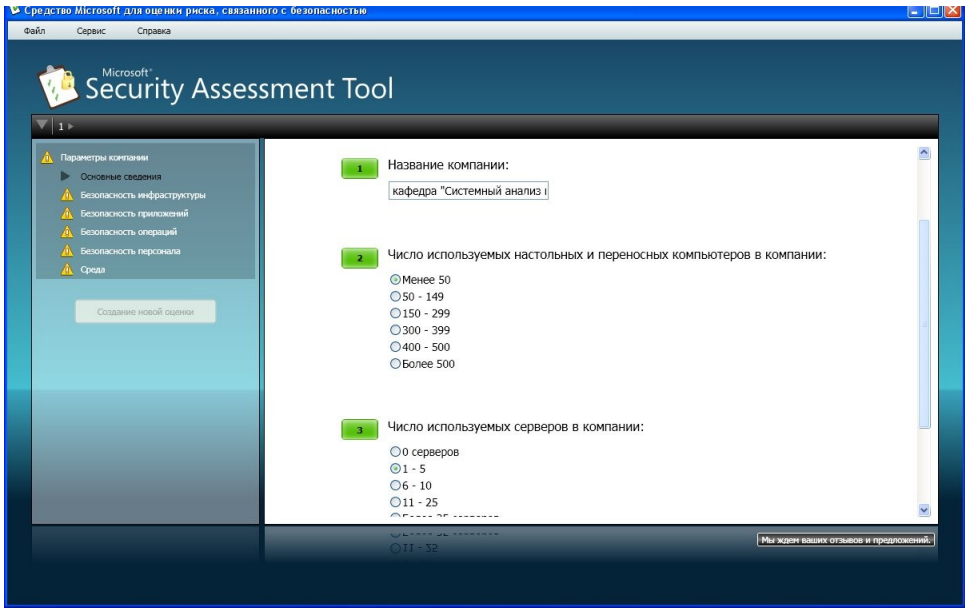

Рисунок 1 – Первая группа вопросов «Информация о компании»

Вопросы этого этапа разбиты на 6 групп. Первая (рисунок 1) касается общих сведений о компании – название, число компьютеров, серверов и т.д. Вторая группа вопросов озаглавлена «Безопасность инфраструктуры». Примеры вопросов – «использует ли компания подключение к Интернет», «размещаются ли службы, используемые как внешними, так и внутренними клиентами, в одном и том же сегменте» и т.д. Остальные группы – «Безопасность приложений», «Безопасность операций», «Безопасность персонала», «Среда».

Надо отметить, что при локализации не все вопросы первого этапа были качественно переведены с английского. Однако во всех случаях можно из контекста понять.

Когда проведен первый этап оценки, полученная информация обрабатывается (для этого требуется подключение к Интернет), после чего начинается второй этап анализа. Для технических специалистов он будет более интересен, т.к. касается используемых в компании политик, средств и механизмов защиты (рисунок 2).

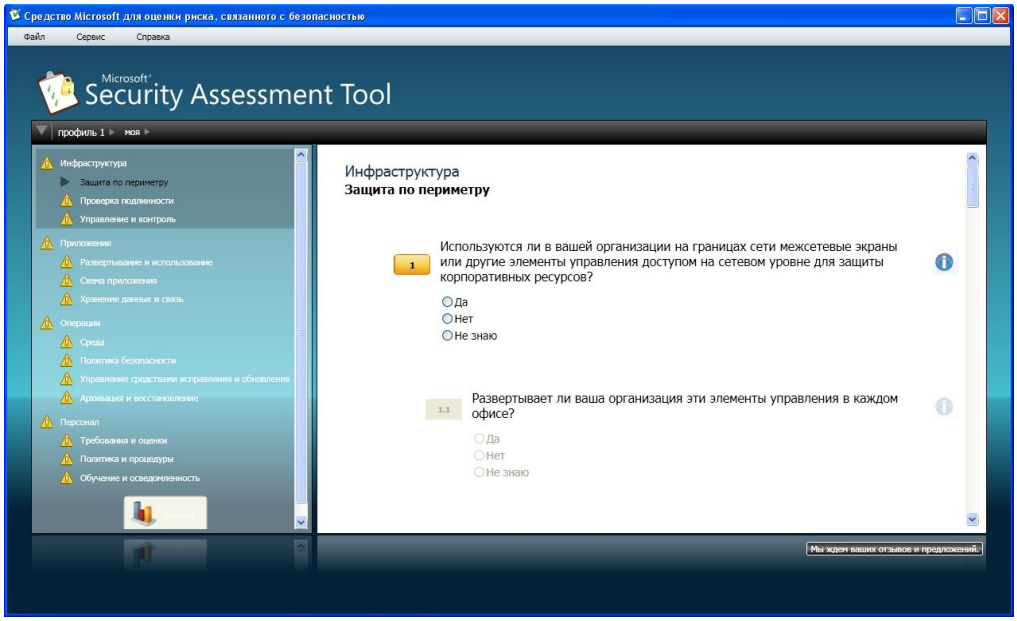

Рисунок 2 – Анализ используемых механизмов защиты

Вопросы организованы в соответствии с концепцией многоуровневой (эшелонированной) защиты. Сначала рассматривается защита инфраструктуры (защита периметра, аутентификация…), затем вопросы защиты на уровне приложений, далее проводится анализ безопасности операций (определена ли политика безопасности, политика резервного копирования и т.д.), последняя группа вопросов касается работы с персоналом (обучение, проверка при приеме на работу и т.д.).

Во многом тематика вопросов соответствует разделам стандартов ISO 17799 и 27001, рассмотренных в теоретической части курса.

После ответа на все вопросы программа вновь обращается к удаленному серверу и генерирует отчеты. Наибольший интерес для технических специалистов представляет «Полный отчет». В частности, он содержит

предлагаемый список приоритетных действий. Фрагмент списка представлен в таблице 1

Таблица 1 – Список предлагаемых действий

Предмет анализа	***Рекомендация***
Высокий приоритет	
Операции > Управление средствами исправления и обновления > Управление средствами исправления	Наличие политики исправлений и обновлений для операционных систем является полезным начальным шагом, однако необходимо разработать такую же политику и для приложений. Разработайте такую политику, пользуясь сведениями, доступными в разделе, посвященном передовым методикам. Сначала установите исправления для внешних приложений и приложений Интернета, затем для важных внутренних приложений и, наконец, для не особо важных приложений.

Порядок выполнения работы

Подробно опишите реально существующее или вымышленное малое предприятие: сферу деятельности, состав и структуру информационной системы, особенности организации процесса защиты информации, применяемые методы и средства.

С помощью программы MSAT проведите оценку рисков для предприятия.

Требования к отчету

Отчет по лабораторной работе должен содержать:

- титульный лист;
- полный отчет, сгенерированный программой;
- выводы по работе.