Практическое занятие № 9. Security Assessment Tool

В ходе данной практической работы мы познакомимся с разработанной Microsoft программой для самостоятельной оценки рисков, связанных с безопасностью - Microsoft *Security Assessment* Tool (MSAT). Она бесплатно доступна на сайте Microsoft *по* ссылке <http://www.microsoft.com/downloads/details.aspx?displaylang=ru&FamilyID=cd057d9d-86b9-4e35-9733-7acb0b2a3ca1>.

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



[увеличить изображение](https://intuit.ru/EDI/30_10_16_3/1477779705-19779/tutorial/555/objects/4/files/05-01.jpg)
**Рис. 5.1.**Информация о компании

Вопросы этого этапа разбиты на 6 групп. Первая ([рис. 5.1](https://intuit.ru/studies/courses/531/387/lecture/8996?page=7#image.5.1)) 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. Чего стоит вопрос: "Прошла ли ваша организация через "*копирование* и замена" касающиеся любого основного компонента технологии, за последние 6 месяцев ?"! Однако во всех случаях можно из контекста понять, о чем идет речь (в приведенном примере вопрос был, относительно того, менялись ли используемые технологии обработки информации).

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 ([рис. 5.2](https://intuit.ru/studies/courses/531/387/lecture/8996?page=7#image.5.2)). Стоит сказать, что и перевод вопросов второго этапа выполнен существенно лучше.



[увеличить изображение](https://intuit.ru/EDI/30_10_16_3/1477779705-19779/tutorial/555/objects/4/files/05-02.jpg)
**Рис. 5.2.**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 [табл. 5.1](https://intuit.ru/studies/courses/531/387/lecture/8996?page=7#table.5.1)

|  |
| --- |
| Таблица 5.1. Список предлагаемых действий |
| **Список приоритетных 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. |

**Задание**

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

C помощью программы MSAT проведите оценку рисков для предприятия.