|  |  |  |
| --- | --- | --- |
|  |  |  |
| МИНОБРНАУКИ РОССИИ | | |
| Федеральное государственное бюджетное образовательное учреждение  высшего образования  **«МИРЭА – Российский технологический университет»**  **РТУ МИРЭА** | | |
| Институт кибербезопасности и цифровых технологий  Кафедра КБ-4 «Интеллектуальные системы информационной безопасности» | | |

**Отчёт по практической работе № 1**

**по дисциплине «Управление информационной безопасностью»**

**Тема:** «**Система управления информационной безопасностью**»

Выполнил

Студент 2 курса

Группы ББМО-01-23

Белов Владимир Станиславович

Шифр 23Б1716

Москва 2024

**Задание.**

1. Установка и настройка MSAT
2. Запуск оценки
3. Анализ результатов
4. Разработка плана улучшений

Отчёт по практической работе

MSAT — это бесплатное средство, разработанное чтобы помочь организациям оценить уязвимости в ИТ-средах, предоставить список расставленных по приоритетам проблем и список рекомендаций по минимизации этих угроз. MSAT разработан, чтобы помочь в определении и устранении угроз безопасности в ИТ-среде. Это средство применяет целостный подход к измерению уровня безопасности и охватывает такие темы, как персонал, процессы и технологии.

Чтобы установить приложение Microsoft Security Assessment Tool на

вашу локальную рабочую станцию ​​или ноутбук потребуется права администратора. После того, как вы примете соглашение, вам будет предоставлена возможность ввести промокод в текстовое поле. Для установки или проведения оценки безопасности с использованием MSAT промокод не требуется.

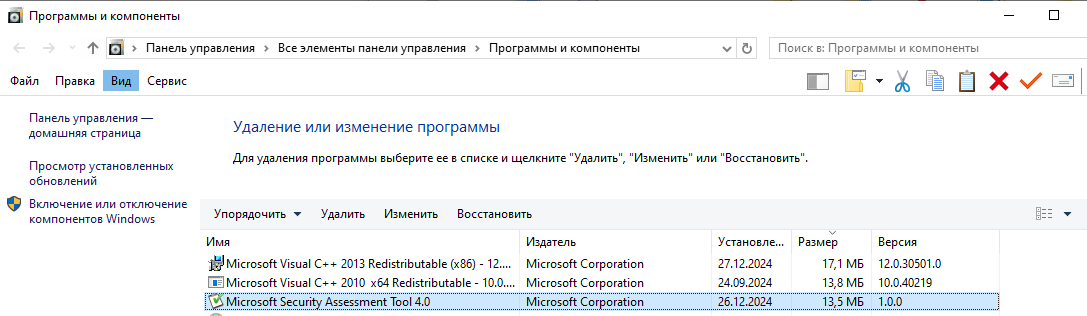


Рисунок 1. Установленный MSAT 4.0 на ПК студента

После установки и настройки профиля партнера вы можете создать новый профиль клиента, выбрав «Создать» на левой навигационной панели в

MSAT.

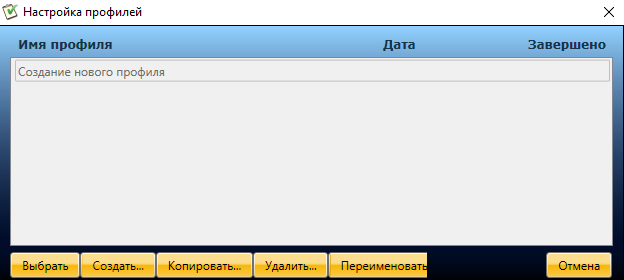


Рисунок 2. Настройка профилей

Введем уникальное имя клиента на экране «Создать» и нажмите OK.

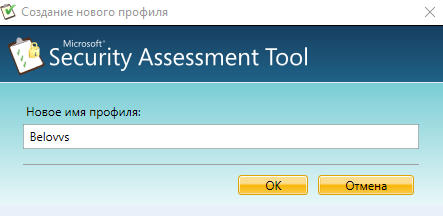


Рисунок 3. Создание профиля

Заполните профиль бизнес-рисков (Рисунок 4). Обычно для заполнения этого раздела может потребоваться ввод данных от лица, принимающего бизнес-решения, руководителя высшего звена или технического лица, принимающего решения. Обратите внимание, что в первом вопросе имя клиента должно совпадать с именем, которое вы ввели при создании профиля.

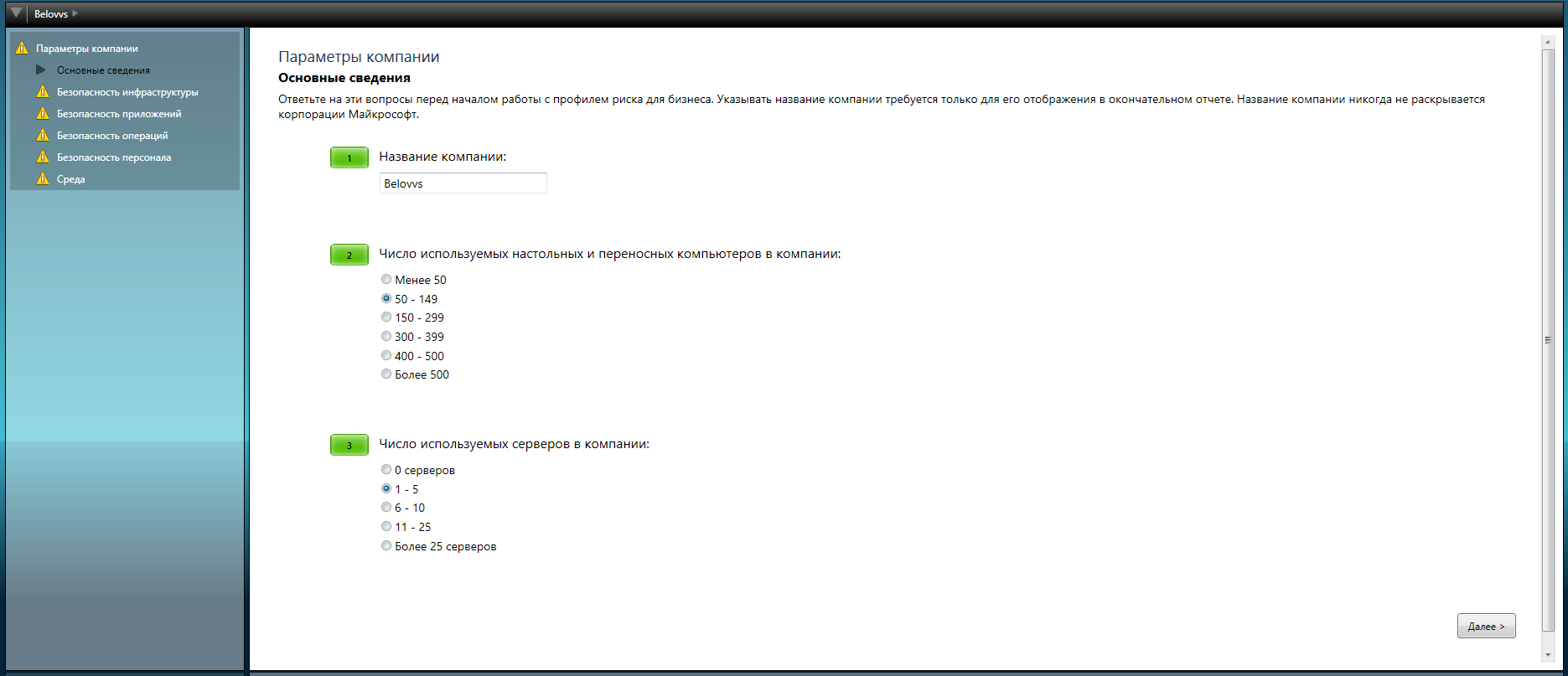


Рисунок 4. Настройка профиля

После ответа на вопросы профиля бизнес-рисков создадим профиль оценки.

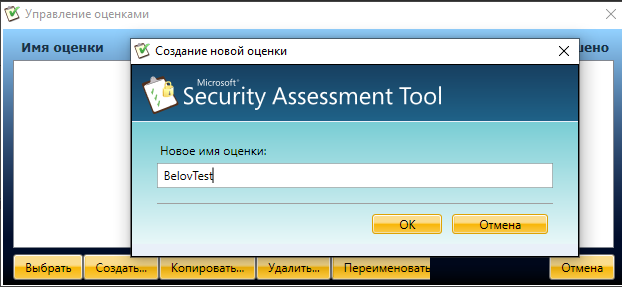


Рисунок 5. Создание профиля оценки

После необходимо ответить на вопросы для составления отчёта.

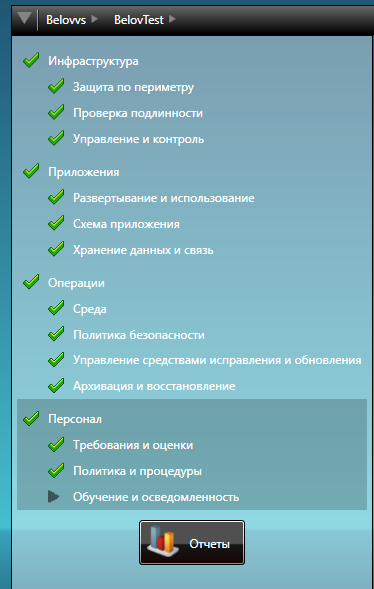


Рисунок 6. Ответы на вопросы

После ответа на ряд вопросов о организации программа выдает отчет в нескольких форматах. Первый это сводный отчет. На нем представлен график и его обьяснение.

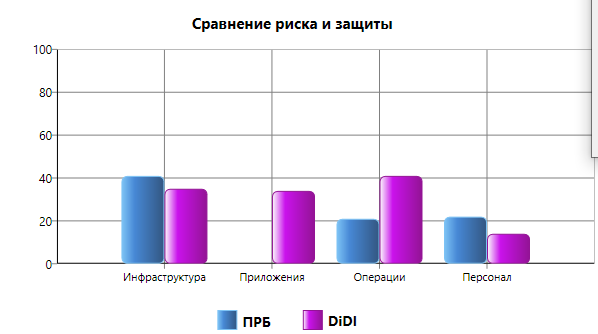


Рисунок 7. График «Сравнение риска и защиты»

**Профиль риска для бизнеса (ПРБ)**: Величина измерения риска, которому подвергается организация, в зависимости от бизнес-среды и отрасли, в условиях которых она конкурирует.

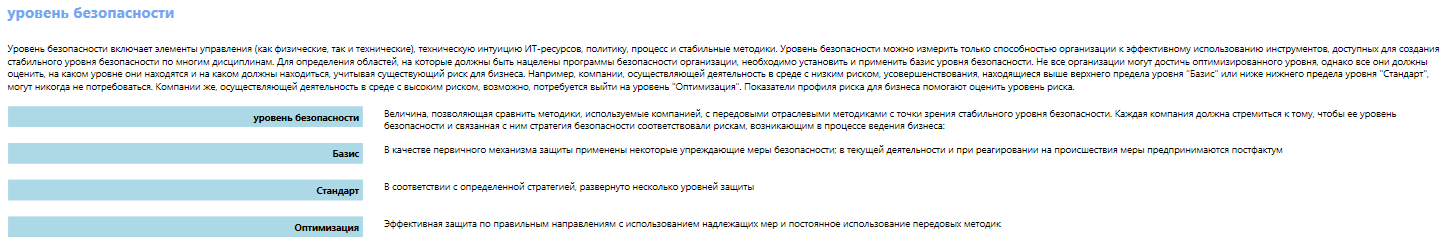
**AoA**: Области анализа, которые являются инфраструктуры, приложений, операции, и люди.

**Индекс эшелонированной защиты (DiDI)**: Величина измерения защитных мер по обеспечению безопасности, используемых в отношении персонала, процессов и технологий для снижения рисков, выявленных на предприятии.

На первый взгляд, может показаться, что низкий показатель ПРБ и высокий показатель DiDI — это хороший результат, но это не всегда так. При значительной диспропорции между показателями ПРБ и DiDI в конкретной области анализа рекомендуется изучить ее (AoA) как можно глубже. При анализе результатов важно учитывать индивидуальные показатели, как для ПРБ, так и DiDI, по отношению друг к другу. Стабильная среда, вероятно, будет представлена сравнительно одинаковыми показателями во всех областях. Разница между показателями DiDI — это явный признак того, что общая стратегия безопасности базируется на одной методике снижения риска. Если стратегия обеспечения безопасности не уравновешивает аспекты, связанные с персоналом, процессами и технологиями, то для среды существует вероятность повышенной уязвимости для злонамеренных атак.

Открыв вкладку полного отчёта, можем найти следующее замечания:





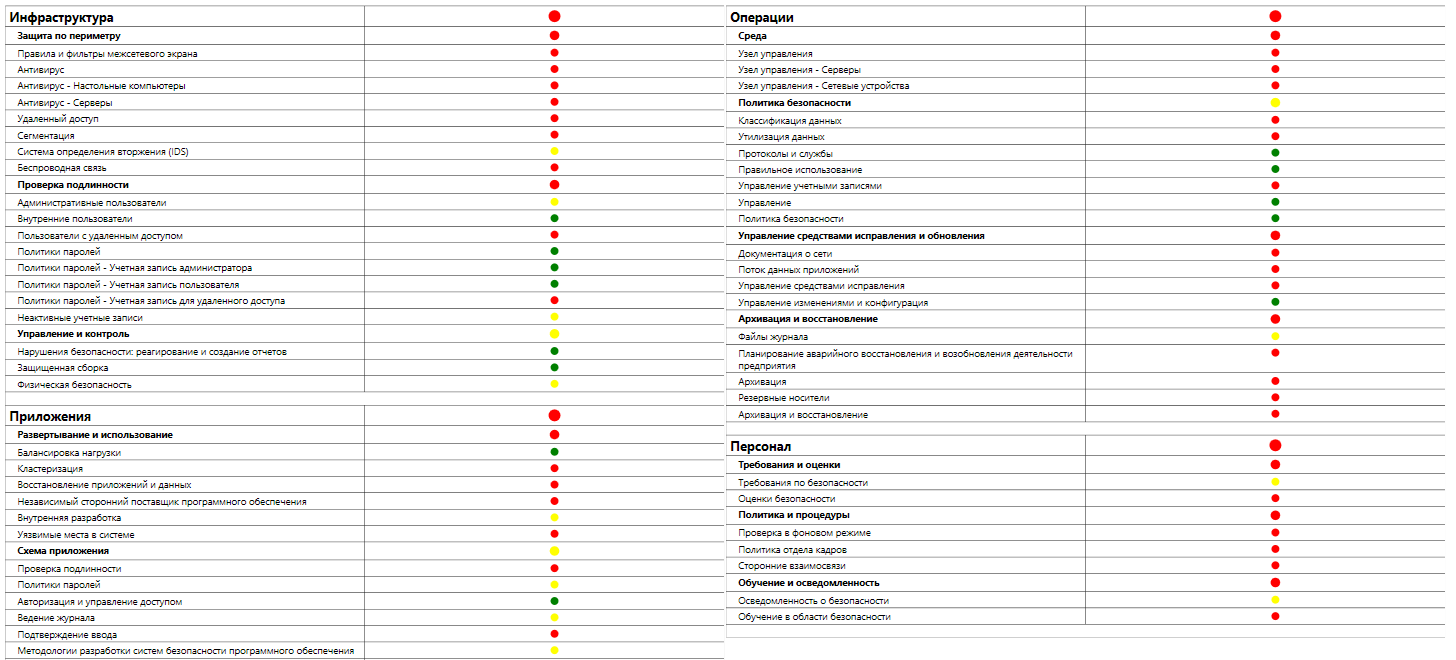


Рисунок 8-10. Таблицы результатов анализа уровня защищенности

Вывод: данное средство не рассчитано на измерение эффективности используемых мер безопасности. Таким образом, настоящий отчет следует использовать как предварительное руководство, позволяющее сосредоточить внимание на определенных областях, требующих более пристального изучения. Он не должен заменять оценки в специфических областях, предлагаемые компетентными сторонними группами оценки.

План действий на основе результатов следующий:

* Устаревшие или недействительные приложения стоит обновить до передовых норм
* Следует дополнительно обратить внимание на категорию персонал и выровнить диспропорции между показателями ПРБ и DiDI