Изображение выглядит как корона

Автоматически созданное описание

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«МИРЭА – Российский технологический университет»**

**РТУ МИРЭА**

ИКБ направление «Киберразведка и противодействие угрозам с применением технологий искусственного интеллекта» 10.04.01

Кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

**Проведение аудита системы менеджмента информационной безопасности**

по дисциплине

«Управление информационной безопасностью»

Группа:

ББМО-02-22

Выполнил:

Шитов А.В.

Проверил:

Пимонов Р.В.

Москва 2023

**Задание:**

Провести аудит и оценку системы безопасности организации на примере применения программного средства «Microsoft Security Assessment Tool (MSAT)».

1 Установка и настройка MSAT

Загрузим MSAT используя ссылку из задания:

https://1drv.ms/u/s!AlN4iiJAxsjbgVFPORW-RKNC5A7q?e=Qx5vv1

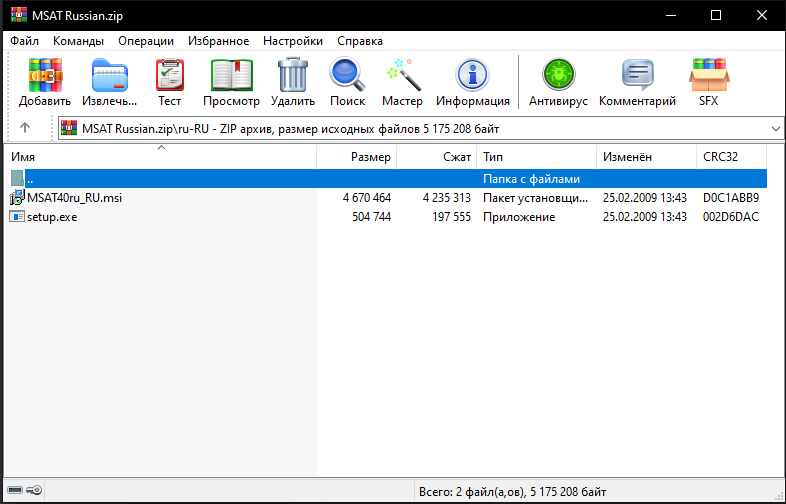


Рисунок 1.1 – Архив с программой

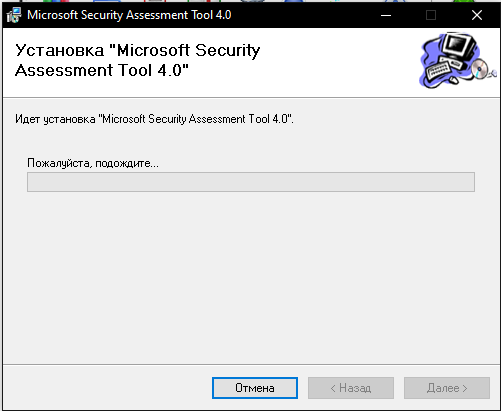


Рисунок 1.2 – Установщик MSAT

Программа не работает с Windows 10, поэтому была создана виртуальная машина с Windows 7 (средство виртуализации VMWare: Workstation Pro 17). Устанавливаем MSAT, после чего создаём профиль и переходим к оценке.

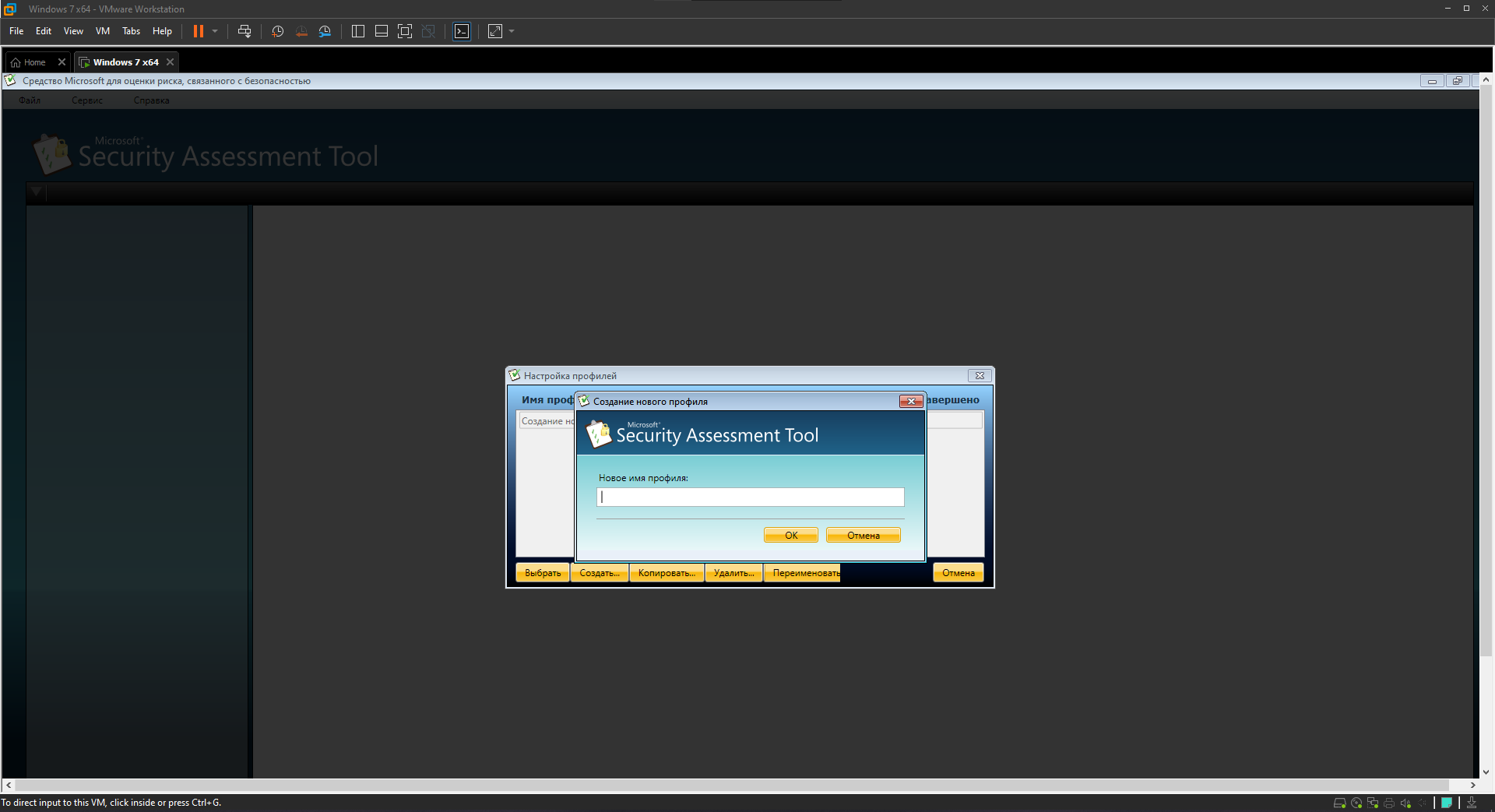


Рисунок 1.3 – Запуск MSAT

2 Запуск оценки и анализ результатов

Проанализируем полученные результаты оценки, выявив основные уязвимости и риски безопасности для организации ГК Астра

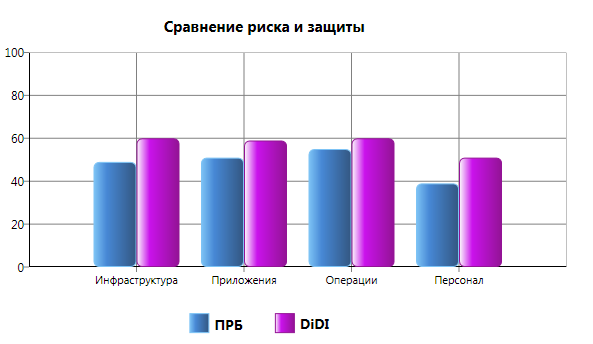


Рисунок 2.1 – Сравнение риска и защиты

Профиль риска для бизнеса (ПРБ) создается рассчитывается на основе серии предварительных вопросов о бизнес-модели компании, измеряя риск для бизнеса. Индекс эшелонированной защиты (DiDI) используется для измерения уровней защиты. Затем ПРБ и DiDI сравниваются для измерения распределения риска по всем аспектам анализа, включая инфраструктуру, приложения, операции и персонал. Далее формируются рейтинги

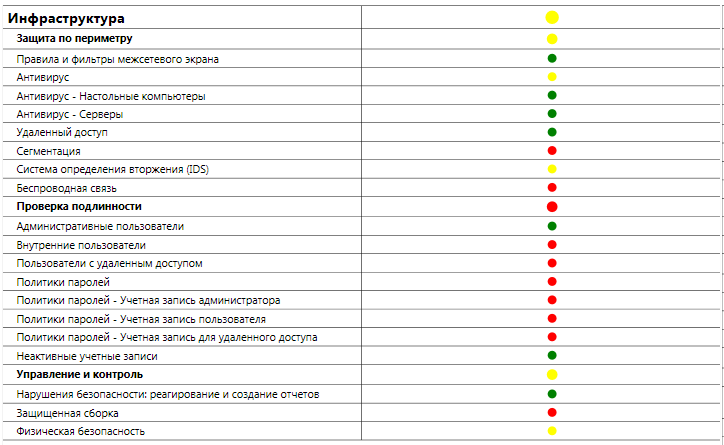


Рисунок 2.2 – Рейтинги категории «Инфраструктура»



Рисунок 2.3 – Рейтинг категории «Приложения»



Рисунок 2.4 – Рейтинг категории «Операции»

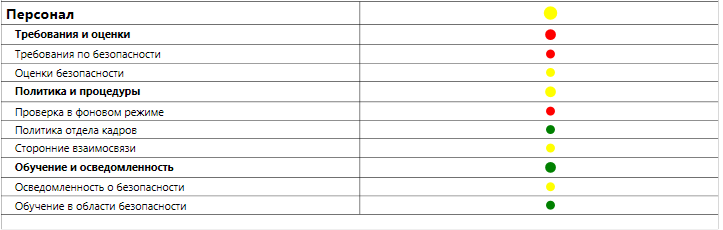


Рисунок 2.5 – Рейтинг категории «Персонал»

Исходя из тестирования были присвоены рейтинги и выявлены наиболее уязвимые сферы безопасности. Красным цветом обозначаются неудовлетворительные результаты, желтым цветом сферы, которые требуют улучшения, зеленым цветом сферы, соответствующие передовым методикам.

По результатам, полученным в ходе опроса, было выявлено, что защита выбранной организации среднего качества. Далее уязвимые сферы были распределены по приоритету.

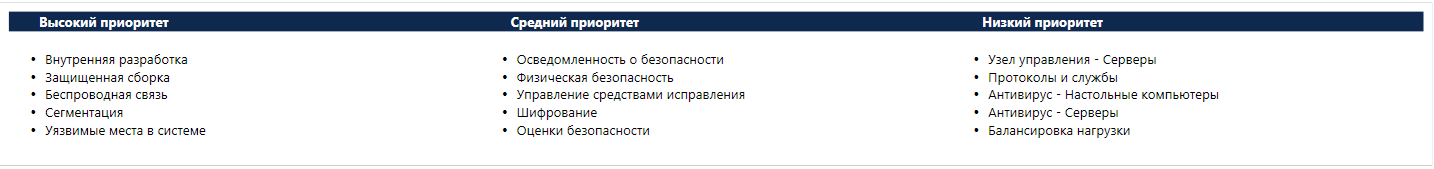


Рисунок 2.6 – Приоритет уязвимых сфер безопасности

В данном случае самыми уязвимыми сферами являются внутренняя разработка, защищенная сборка, беспроводная связь, сегментация и уязвимые места в системе

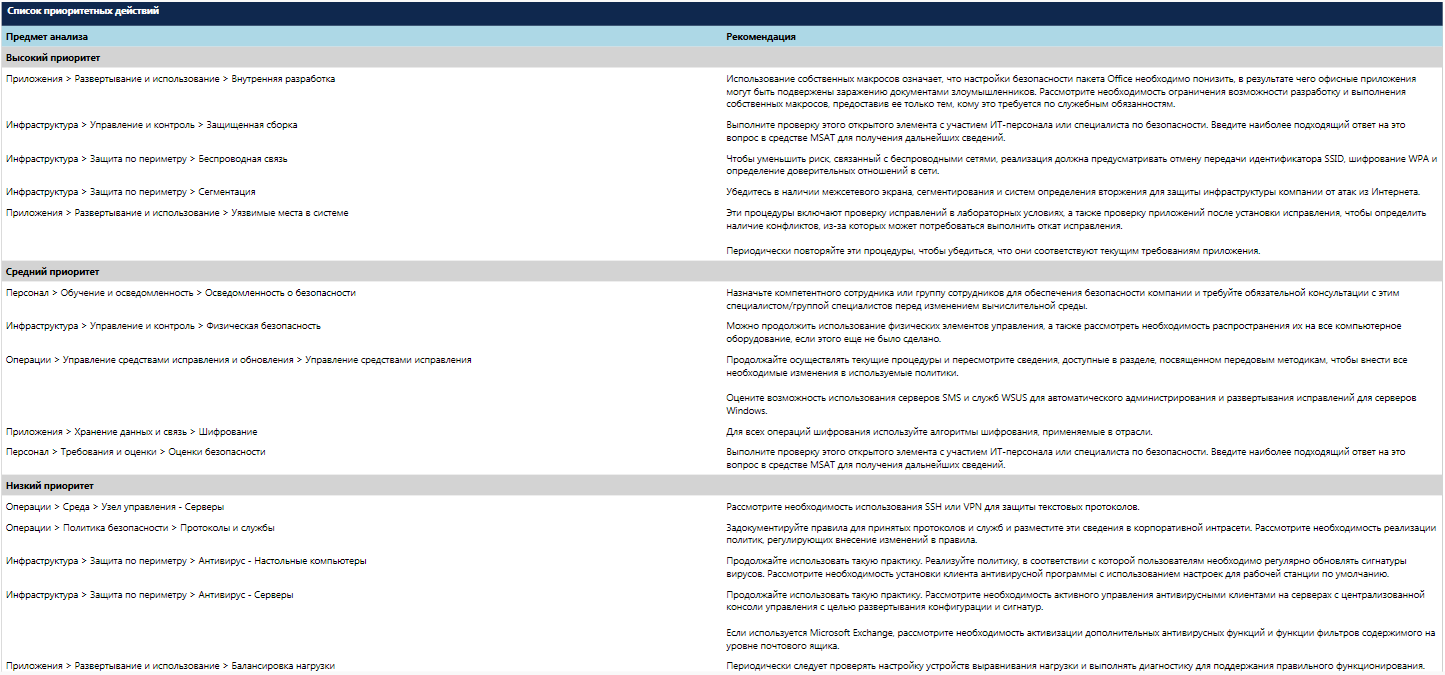


Рисунок 2.7 – Список приоритетных действий

Исходя из приоритетных действий предлагается следующий план улучшений:

1. Защищенная сборка образов приложений
2. Минимизирование использования беспроводных сетей
3. Внедрение межсетевого экрана, сегментирования и систем определения вторжения для защиты инфраструктуры компании.
4. Назначить компетентного сотрудника или группу сотрудников для обеспечения безопасности компании
5. Пересмотреть текущие политики управления доступом
6. Актуализация алгоритмов шифрования
7. Задокументировать правила для принятых протоколов и служб и разместить эти сведения в корпоративной интрасети.