|  |
| --- |
|  |
| МИНОБРНАУКИ РОССИИ |
| **Федеральное государственное бюджетное образовательное учреждение**  высшего образования  «МИРЭА – Российский технологический университет» |

Институт кибербезопасности и цифровых технологий

Практическая работа № 1.12

по дисциплине

«Управление информационной безопасностью»

**Выполнил:**

ББМО–01–22

Чадов В. Т.

**Проверил:**

Пимонов Р. В.

«Зачтено» «\_\_»\_\_\_\_\_\_\_\_\_2023 г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Москва 2023

Содержание

**Анализ результатов, приведённых с помощью «Microsoft Security Assessment Tool (MSAT)»** 3

Введение 3

Анализ отчета MSAT 3

План улучшений 7

**Анализ результатов, приведённых с помощью «Microsoft Security Assessment Tool (MSAT)»**

Введение

Средство Microsoft для оценки риска, связанного с безопасностью, предназначено для оказания помощи в определении и устранении угроз безопасности в существующей вычислительной среде. В данном средстве реализован целостный подход к оценке стратегии обеспечения безопасности с учетом персонала, процессов и технологий. Кроме полученных результатов, приводятся рекомендации по снижению риска, а также ссылки на дополнительную информацию, которая содержит другие необходимые советы. Эти ресурсы могут помочь в получении дополнительных знаний о специальных средствах и методах, позволяющих повысить безопасность среды.

Анализ отчета MSAT

После ответа на ряд вопросов о организации программа выдает отчет в нескольких форматах. Первый это сводный отчет. На нем представлен график (рисунок 1) и его обьяснение.

ПРБ является мерой, отражающей риск для бизнеса, с которым компания сталкивается в данной отрасли и в условиях выбранной бизнес-модели. DiDI - это величина измерения защитных мер по обеспечению безопасности, используемых в отношении персонала, процессов и технологий для снижения рисков, выявленных на предприятии. Уровень безопасности - это величина измерения способностей организации к эффективному использованию инструментов, доступных для создания стабильного уровня безопасности по многим дисциплинам.

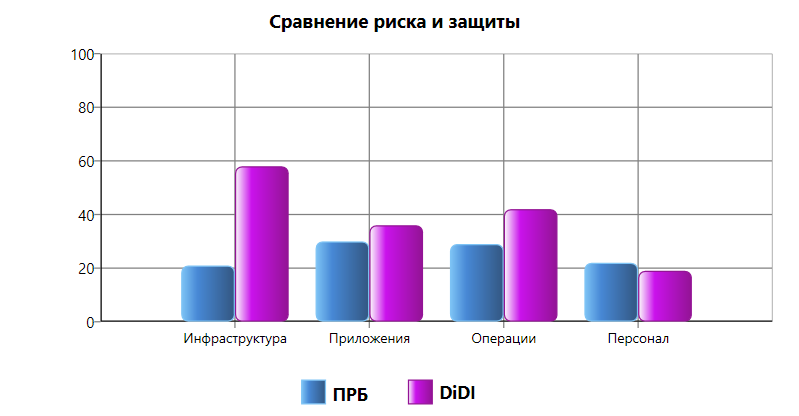


Рисунок 1 – График, отражающая разность показателей эшелонированный защиты, упорядоченных по областям анализа

На первый взгляд, может показаться, что низкий показатель ПРБ и высокий показатель DiDI - это хороший результат, но это не всегда так. Масштаб данной самооценки не предусматривает все факторы, которые следует принять во внимание. 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.

Уровень безопасности включает элементы управления (как физические, так и технические), техническую интуицию ИТ-ресурсов, политику, процесс и стабильные методики. Уровень безопасности можно измерить только способностью организации к эффективному использованию инструментов, доступных для создания стабильного уровня безопасности по многим дисциплинам. Для определения областей, на которые должны быть нацелены программы безопасности организации, необходимо установить и применить базис уровня безопасности. Не все организации могут достичь оптимизированного уровня, однако все они должны оценить, на каком уровне они находятся и на каком должны находиться, учитывая существующий риск для бизнеса. Например, компании, осуществляющей деятельность в среде с низким риском, усовершенствования, находящиеся выше верхнего предела уровня "Базис" или ниже нижнего предела уровня "Стандарт", могут никогда не потребоваться. Компании же, осуществляющей деятельность в среде с высоким риском, возможно, потребуется выйти на уровень "Оптимизация". Показатели профиля риска для бизнеса помогают оценить уровень риска.

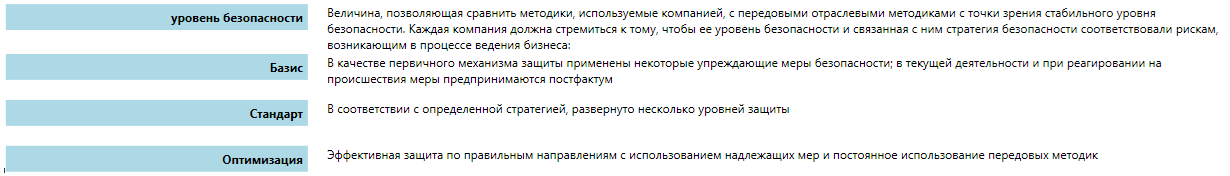


Рисунок 2 – Уровни безопасности

Второй это полный отчет. Он содержит результаты аудита нашей системы (рисунки 3-5), где зеленый знак означает, что позиция соответствует передовым методикам, желтый знак – требует усовершенствования, а красный знак – неудовлетворительно.



Рисунок 3 – Ситуационный анализ





Рисунок 4 – Результаты аудита системы

Также анализ содержит инициативы по обеспечению безопасности. В этом разделе отчета содержатся подробные результаты для каждой категории, а также описываются передовые методики, даются рекомендации и ссылки на дополнительную информацию.

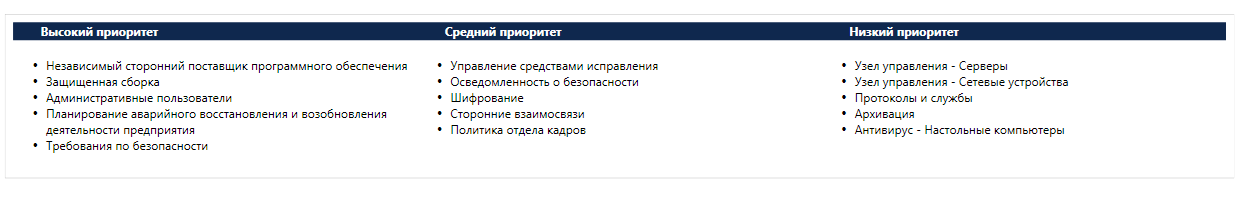
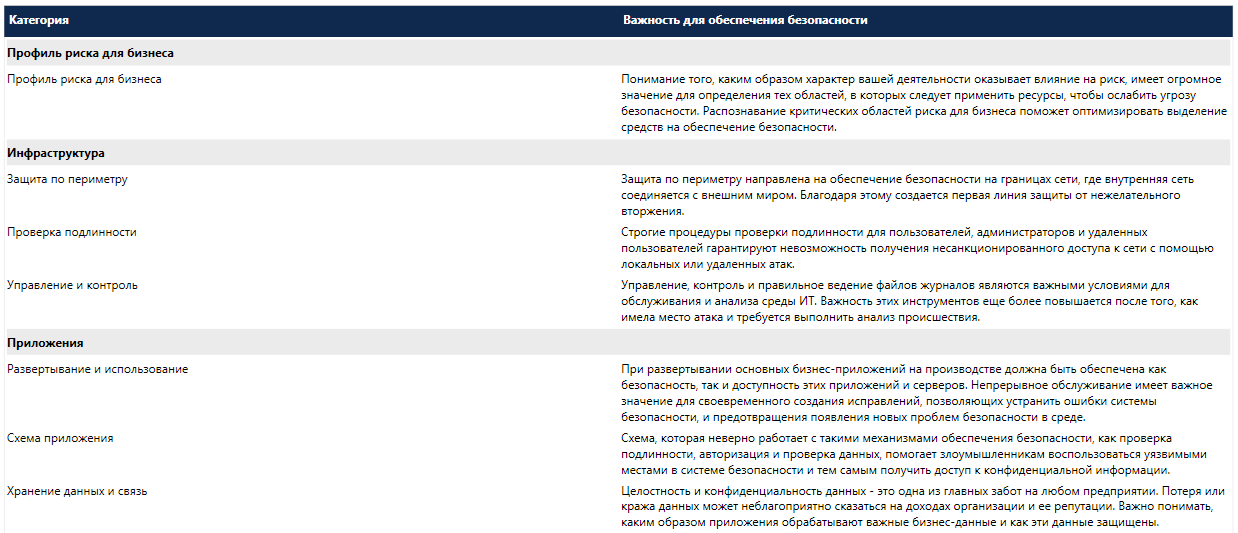


Рисунок 5 – Инициативы по обеспечению безопасности



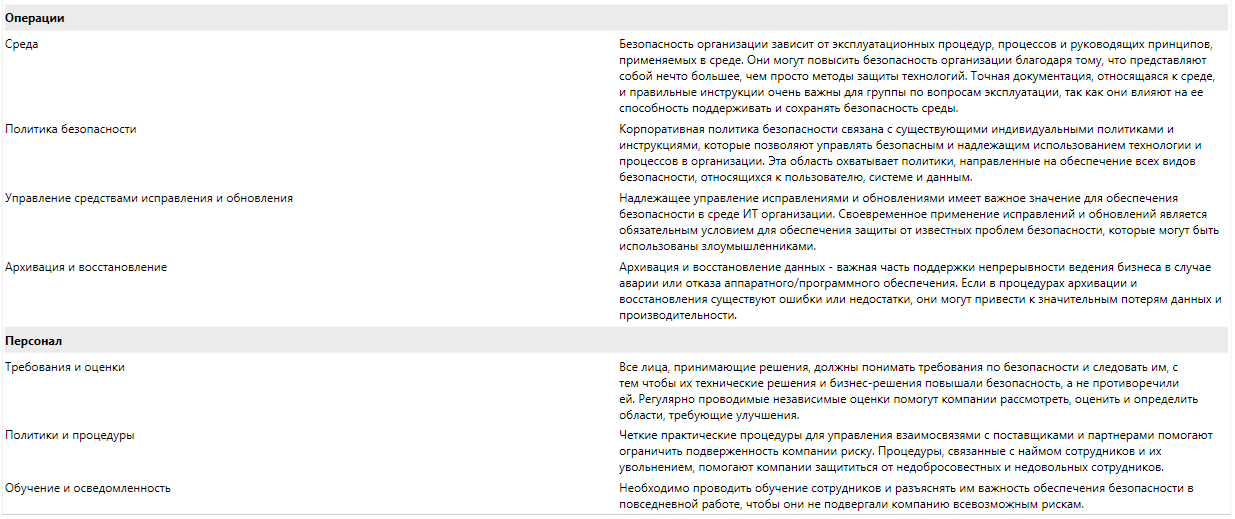
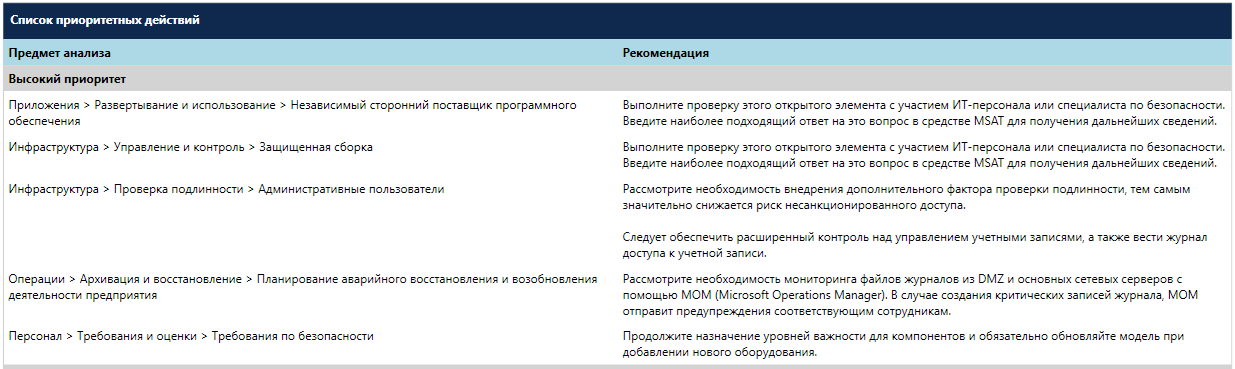


Рисунок 6 – Подробная оценка

План улучшений

Обратим внимание на финальный раздел отчета – список приоритетных действий. Он является в достаточной степени полной инструкцией для улучшения безопасности организации. Для последующего улучшения или в случае изменения организации можно создать следующий отчет с изменённым набором рекомендации и другими приоритетами.

В случае организации ООО “Цифровая независимость” следует дополнительно обратить внимание на категорию персонал, ее рейтинг DiDI ниже, чем рейтинг ПРБ. Это говорит о недостаточных мерах защиты.



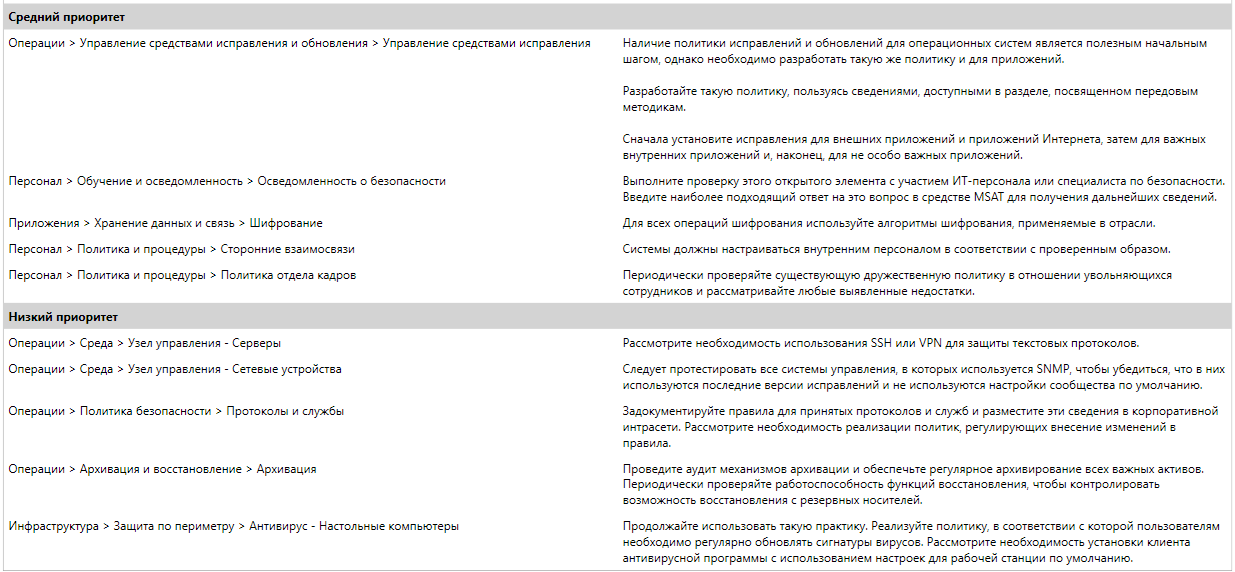


Рисунок 7 – Список приоритетных действий