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

Институт кибербезопасности и цифровых технологий

Практическая работа № 1.12

по дисциплине

«Управление информационной безопасностью»

Группа:

ББМО-02-23

Выполнил:

Дурягин М.Р.

Москва, 2024

Содержание

[ВВЕДЕНИЕ 3](#_Toc152425035)

[Анализ полученных результатов 4](#_Toc152425036)

[План улучшения 12](#_Toc152425037)

[ЗАКЛЮЧЕНИЕ 14](#_Toc152425038)

# 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.

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

# Анализ полученных результатов

Оценка предназначена для выявления риска для бизнеса организации и определения мер безопасности, предпринимаемых для снижения риска. Сосредоточение внимания на общих проблемах этого сегмента рынка позволило разработать вопросы для обеспечения высококачественной оценки рисков, которые представляют для ведения бизнеса используемые технологии, процессы и персонал.

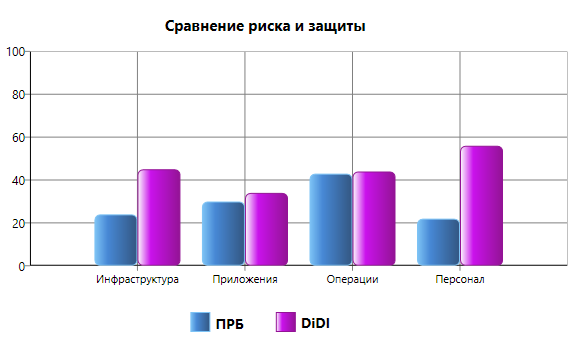
Профиль риска для бизнеса (ПРБ) создается средством на основе серии предварительных вопросов о бизнес-модели компании, и тем самым измеряется риск для бизнеса, с которым компания сталкивается в данной отрасли и в условиях выбранной бизнес-модели. Вторая группа вопросов предлагается с целью составления списка мер безопасности, которые со временем должны быть предприняты компанией. В целом, эти меры безопасности формируют уровни защиты, обеспечивающие более серьезную защиту от угроз безопасности и конкретных уязвимых мест в системе. Каждый уровень способствует укреплению комбинированной стратегии эшелонированной защиты. В сумме это рассматривается как индекс эшелонированной защиты (DiDI). Затем ПРБ и DiDI сравниваются для измерения распределения риска по всем областям анализа — инфраструктуре, приложениям, операциям, персоналу.

Рисунок 1 – Разность показателей эшелонированный защиты, упорядоченных по областям анализа

Из полученных результатов можно сделать вывод о необходимости пересмотра стратегии инвестирования в IT-ресурсы . Видимые различия в показателях говорят о потребности в более балансированном распределении ресурсов, чтобы повысить эффективность и обеспечить более устойчивую работу информационных систем.

Дисбаланс внутри одной категории или между разными категориями — в любом направлении — может означать необходимость перегруппировки инвестиций в ИТ.

Теперь посмотрим на отчёт ситуационного анализа. В этом разделе в графическом виде представлены концепции для АО «РОСЭНЕРГОАТОМ»

Результаты представлены на рисунке 2.



Рисунок 2 – Результаты оценки безопасности

Ниже увидим результаты аудита нашей системы, где зеленый знак означает, что позиция соответствует передовым методикам, желтый знак – необходимость доработки, а красный знак – неудовлетворительно. Результаты проверки системы АО «РОСЭНЕРГОАТОМ» показаны на рисунке 3.





Рисунок 3 – Результаты аудита система АО «РОСЭНЕРГОАТОМ»

Очевидно, что у нас в организации существуют недостатки, например:

* Инфраструктура
* Защита по периметру
* Антивирус - Настольные компьютеры
* Пользователи с удаленным доступом
* Операции
* Управление средствами исправления и обновления
* Архивация и восстановление
* Приложения
* Политика и процедуры

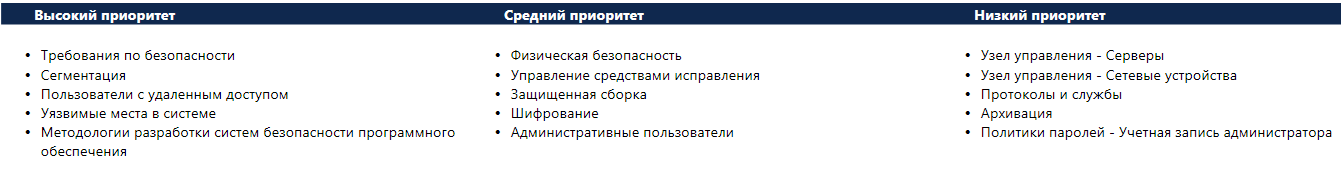
Далее следуем по итоговому отчету и видим пункт инициативы по обеспечению безопаcности. В данном пункте распределены угрозы по различным приоритетам их усовершенствования. Инициативы по обеспечению безопасности показаны на рисунке 4.

Рисунок 4 – Инициативы по обеспечению безопасности

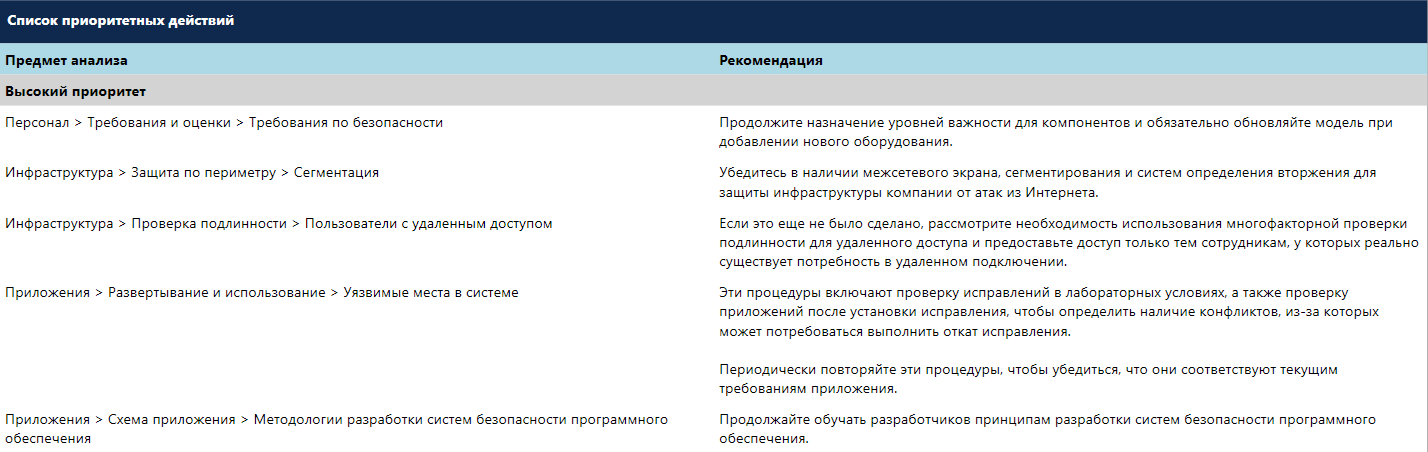
В данном разделе описаны конкретные разделы и рекомендации по улучшению данных разделов. Список действий с высоким приоритетом показаны на рисунке 5.

Рисунок 5 – Список приоритетных действий

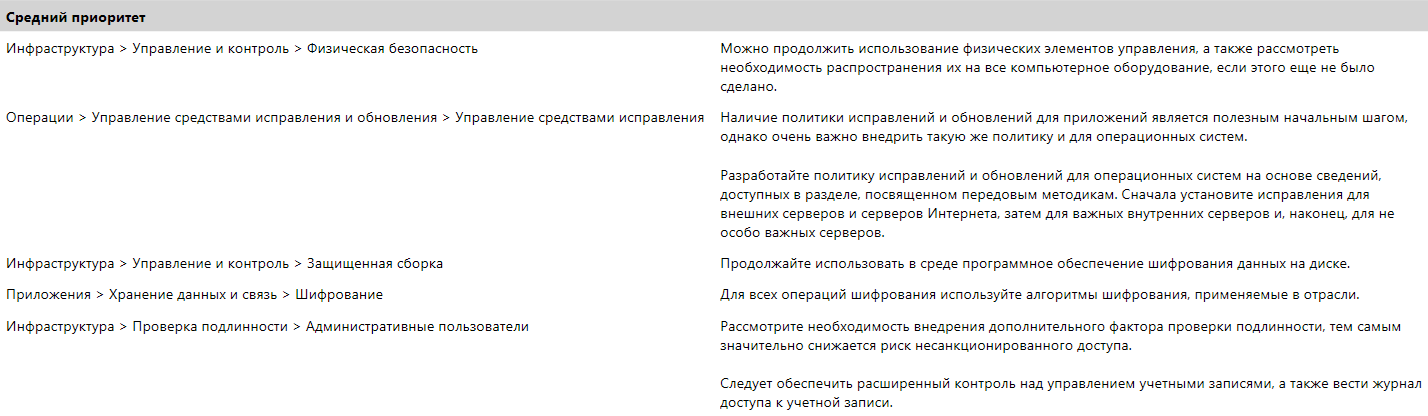
Список действий с средним приоритетом показаны на рисунке 6.

Рисунок 6 – Список действий со средним приоритетом

Список действий с низким приоритетом показаны на рисунке 7.

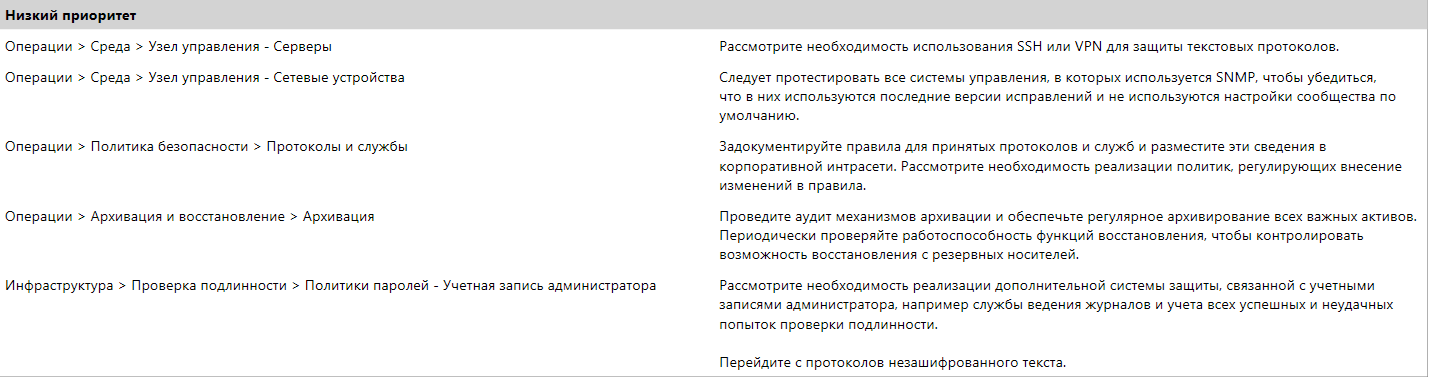


Рисунок 7 – Список действий с низким приоритетом

# 

# План улучшения

1. Прежде всего, требовать введения различных учетных записей для административных/управленческих процессов, и убедитесь, что учетные данные для группы администраторов меняются часто..
2. Затем целесообразно обратить внимание на необходимость внедрения дополнительного фактора проверки подлинности, который позволит существенно снизить риск несанкционированного доступа с использованием учетной записи пользователя.
3. В условиях широкого распространения социальной инженерии в настоящее время, особое внимание следует уделить обучению персонала. Уязвимость организации часто связана с действиями сотрудников, поэтому обучение основам безопасности и распознаванию потенциальных атак становится неотъемлемой частью нашего плана.
4. рассмотрите необходимость использования многофакторной проверки подлинности для удаленного доступа и предоставьте доступ только тем сотрудникам, у которых реально существует потребность в удаленном подключении.
5. Регулярно просматривайте узлы поставщиков и систем безопасности для ознакомления с предупреждениями о недавних атаках и появлении новых вирусов. Регулярно выполняйте аудит удаленных пользователей, чтобы проверить, выполняют ли они обновление своих систем.

# ЗАКЛЮЧЕНИЕ

Подводя итоги, можно сказать, что данная оценка предназначена для выявления риска для бизнеса организации и определения мер безопасности, предпринимаемых для снижения риска. MSAT является эффективным инструментом для анализа состояния безопасности в организации и предоставления рекомендаций по её улучшению. Однако, стоит учесть, что данный продукт разработан достаточно давно и может не в полной мере учитывать современные требования и угрозы в области информационной безопасности.

Были выявлены с помощью MSAT уязвимости и описаны рекомендации по усовершенствованию системы безопасности организации АО «РОСЭНЕРГОАТОМ».