

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»

**Практическая работа №5**

по дисциплине: «Управление информационной безопасностью»   
На тему:

«Проведение аудита системы менеджмента информационной безопасности»

Группа:

ББМО-01-22

Выполнил:

Гребенник Г.С

Проверил:

Пимонов Р.В.

Москва, 2023

**СОДЕРЖАНИЕ**

[**Введение** 3](#_Toc156937398)

[**Создание нового профиля для оценки** 4](#_Toc156937399)

[**Инфраструктура** 7](#_Toc156937400)

[**Приложения** 7](#_Toc156937401)

[**Операции** 7](#_Toc156937402)

[**Персонал** 7](#_Toc156937403)

# **Введение**

MSAT —. средство использует целостный подход к оценке системы безопасности, анализируя влияние человеческого фактора, процессов и технологий. Полученные результаты предоставляются пользователям вместе с подробным руководством, рекомендациями по снижению угроз и ссылками на отраслевые руководства, содержащие дополнительные сведения. Эти ресурсы могут помочь организациям получить информацию о средствах и методах, способных повысить безопасность ИТ-среды организации.

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

Задачи:

– Установить и настроить MSAT

– Провести оценку при помощи MSAT

– Провести анализ результатов оценки: проанализируйте полученные результаты оценки, выявив основные уязвимости и риски безопасности.

2. Определите какие аспекты безопасности требуют немедленного внимания.

– Предложить план улучшений со стороны различных аспектов оценки MSAT.

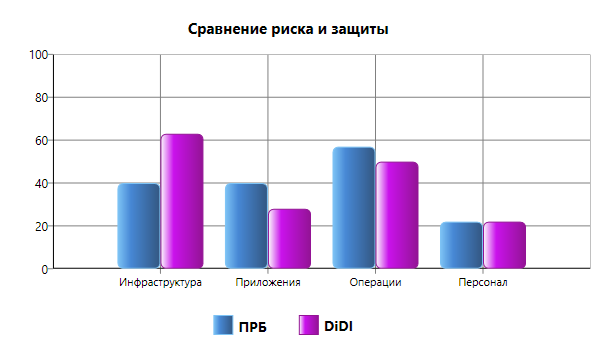
Ход работы:

# **Создание нового профиля для оценки**

После создания профиля оценки, необходимо определить базовую составляющую инфраструктуры АО «Россети» ИБ. Далее программа, в форме опроса, собирает данные о «важности» составляющих бизнеса в качестве риск-ориентированного подхода. После чего будут собраны данные для оценки защищенности составляющих по направлениям инфраструктуры, приложений, операций и персонала.

В качестве ответов на вопросы по защищенности направлений брались ответы после внедрения комплекса мер защиты в соответствии с практиками 1-4. Внедрялись меры по устранению угроз из модели угроз, а также меры по снижению рисков.

В итоге мы получим профиль риска для бизнеса и индекс эшелонированной защиты. Сводка будет отображена в виде диаграммы, с сравнением рисков и защиты направлений.



- Профиль риска для бизнеса (ПРБ) — является мерой, отражающей риск для бизнеса, с которым компания сталкивается в данной отрасли и в условиях выбранной бизнес-модели.

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

Вообще, для одной и той же категории лучше всего иметь и рейтинг DiDI, и рейтинг ПРБ. Дисбаланс внутри одной категории или между разными категориями — в любом направлении — может означать необходимость перегруппировки инвестиций в ИТ.

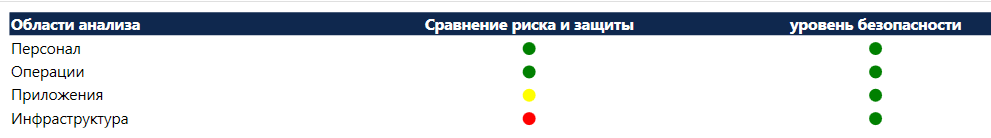
Инфраструктура — данная сфера в организации является самой безопасной и проработанной сферой, на которую компания выделяла средства для организации ее защищенности, при этом судя по анализу и сравнению рисков с защитой, были выполнены излишние действия.

Приложения — данная сфера в нашей компании не является ключевой и занимающей важную нишу, в следствие этого мы можем наблюдать перевес рисков в отношении принятых мер защиты. Что должно быть исправлено.

Операции — данная категория так же является не самой важной и можно сказать даже отстающей сферой.

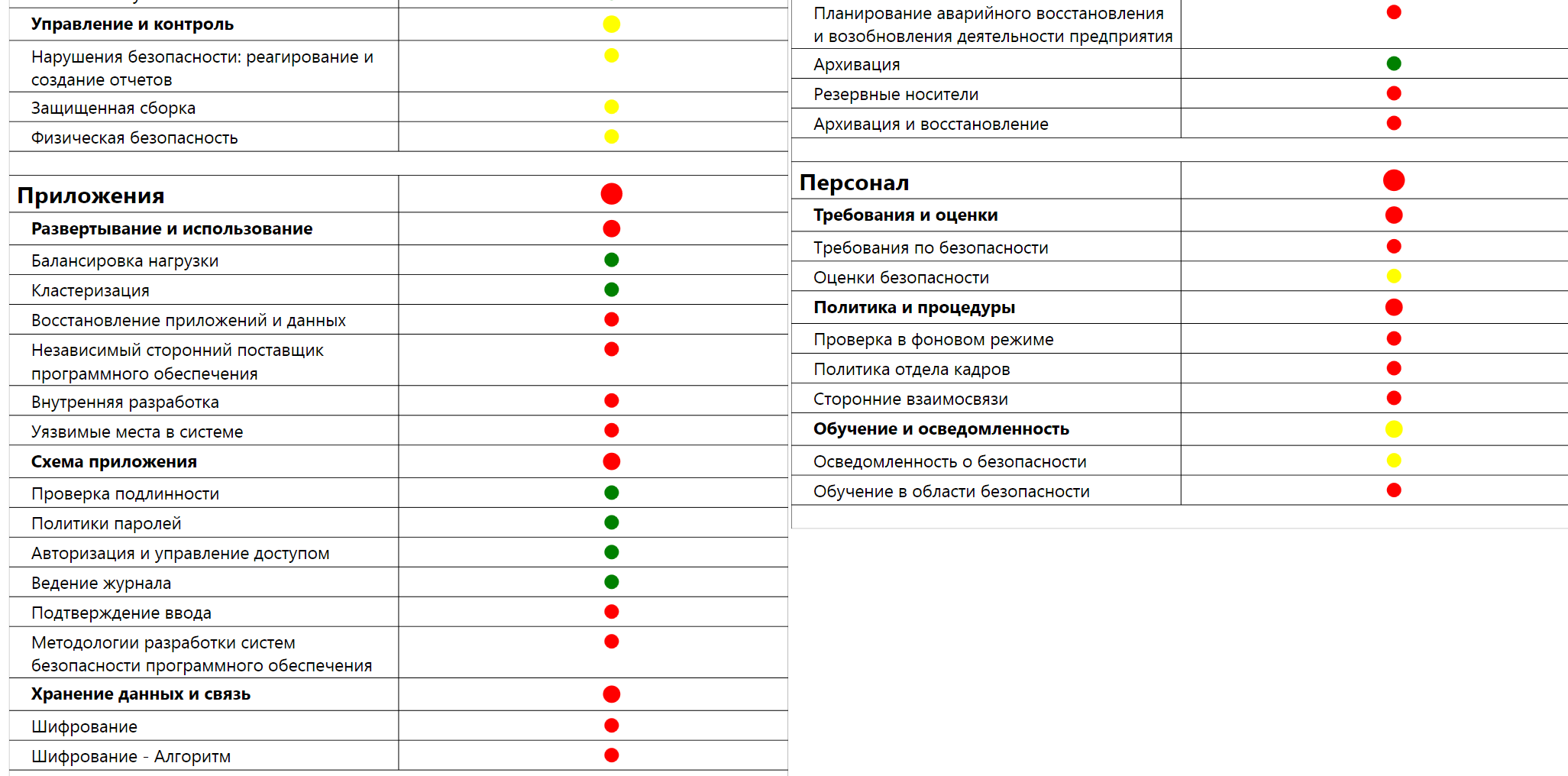
Персонал — данная сфера в компании является идеальным вариантом, в котором были проведены все необходимые меры по организации защиты информации. Но в ней так же присутствуют минусы о которых будет сказано далее.

На данном графике представлены отчеты ситуационного анализа для нашей организации:



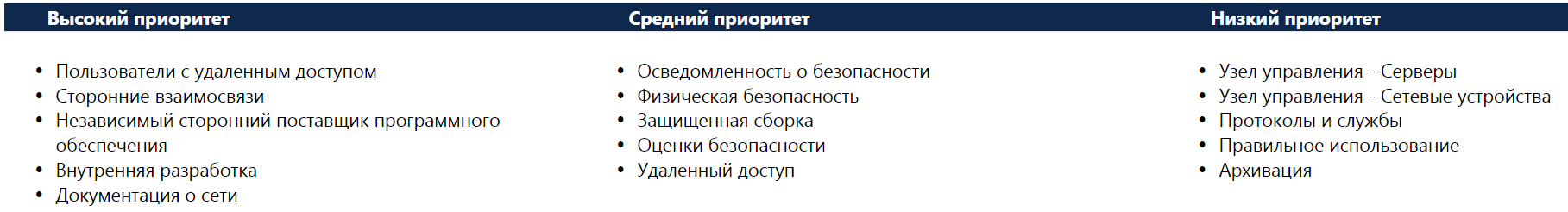
Далее в отчете предоавленном программой мы можем обнаружить аудит нашей систем:





По итогам проведенного аудита явной и первостепенной проблемой, которая требует решения в компании является хранение и шифрование информации, далее так же из насущных тем присутствует малая осведомлённость персонала.

Двигаясь далее по отчету натыкаемся на раздел с инициативами по обеспечению безопасностию:



Категорически необходимо будет выполнение всех задач и проблем с высоким приоритетом.

## **Инфраструктура**

Проводя анализ данной сферы можно выделить области:

* Защита даленного доступа,
* Постановка антивирусных мер защиты на серверную инфраструктуру,
* Организация защиты беспроводной связи (но данный пункт отходит в следствии неиспользования беспроводной связи в организации).

## **Приложения**

Данный пункт аудита является самым слабым в реализации мер защиты информации, так для исправления данной ситуации следует применять такие меры защиты как:

* Безопасность хранения и реплицирования данных приложений;
* Разработку собственных средств и мер ПО(данный пункт не является нужным в следствии огромной затратности и ненужности с неэффективностью данной меры в рамках нашей организации);
* Важным является меры защиты приложений, как вариант решения данной проблемы возможность организации отдела сферы ИБ для приложений;
* Повышение более сильных и новых алгоритмов шифрования.

## **Операции**

В данном пункте можно выделить следующие меры безопасности:

* Регламентированная утилизация данных;
* Регламент регулирования центром обновлений;
* Документация сетевой инфраструктуры компании каждый год, в ситуациях без критических изменений;
* Продумывание выделения доп. средств для аварийного резервирования.

## **Персонал**

В данном направлении следует отметить следующие меры защиты:

* Обновление политик безопасности для персонала за АРМ;
* Проведение раз в полгода обучения персонала внутреннему регламенту и общим понятиям, и мерам иб;
* Согласованность передачи информации и ее актуальность с отделом кадров;
* Проведение аудитов безопасности в незапланированное время.

Подводя итог, повышенное внимание к вышеописанным пунктам помогут нашей организации повысить показатели каждой из сферы безопасности. Инструмент MSAP показал высокую эффективность и помог нам вычленить проблемные участки в нашей компании, но стоит отметить и то, что не все предложения данного инструмента актуальны для АО «Россети», так как некоторые из мер предложенные инструментом не являются нужными в следствии отсутствия, либо же незначительного улучшения степени защищенности нашей организации. Так же некоторые невыполнимы в плане финансовых затрат на реализацию.

Основной задел для проведения работ по увеличению мер защиты:

