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

Институт кибербезопасности и цифровых технологий

КБ-4 «Интеллектуальные системы информационной безопасности»

**Отчет** по практической работе №5 на тему: Проведение аудита системы менеджмента информационной безопасности

**по дисциплине:** «Управление информационной безопасностью»

**Выполнил:**

Студент группы ББМО-01-22

ФИО: Карев Д.П.

**Проверил:**

Р.В. Пимонов

**Москва 2023**

Содержание

[Введение 3](#_Toc151996376)

[Анализ результатов, приведённые с помощью программного средства «Microsoft Security Assessment Tool (MSAT)» 3](#_Toc151996377)

[План улучшения 9](#_Toc151996378)

[Вывод 10](#_Toc151996379)

# Введение

Целью данной практической работы является проведение аудита и оценка системы безопасности организации ФГБУ «НПП Гамма» на примере применения программного средства «Microsoft Security Assessment Tool (MSAT)».

Результаты оценки безопасности системы представлены в файле “Карев\_ДП\_ББМО-01-22\_прз1.12.xps”. Перейдём к анализу полученных результатов.

# Анализ результатов, приведённые с помощью программного средства «Microsoft Security Assessment Tool (MSAT)»

После такого, как запросили отчет в программе MSAT показывается страница сводный отчет. На это странице показан профиль риска для бизнеса и индекс эшелонированной защиты с графиком. Диаграмма, отражающая разность показателей эшелонированный защиты, упорядоченных по областям анализа показана на рисунке 1.

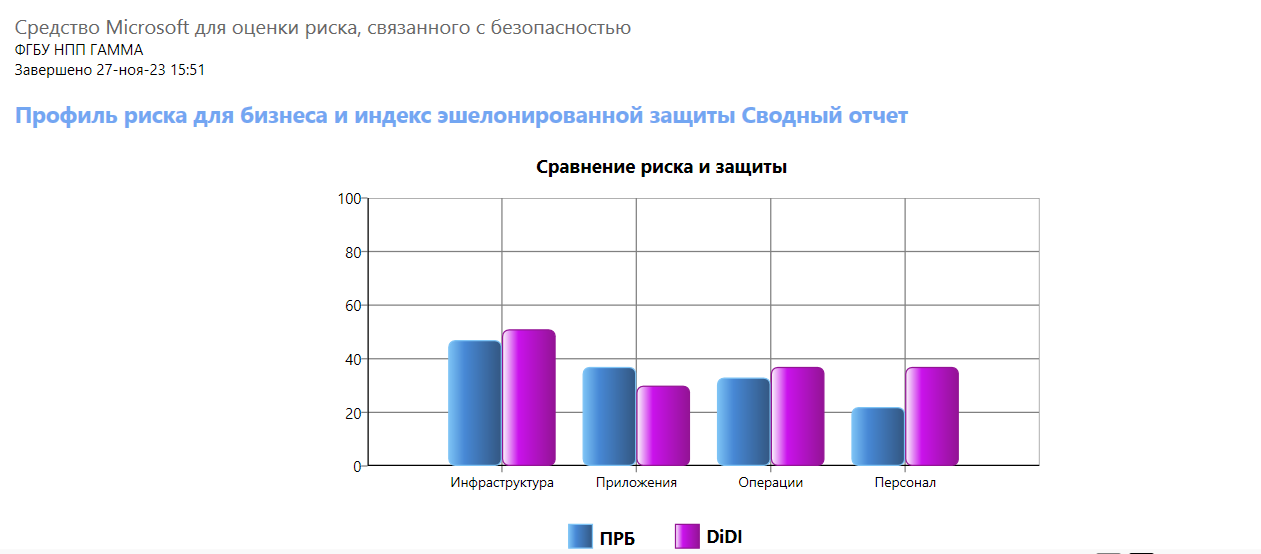


Рисунок 1 – График, отражающая разность показателей эшелонированный защиты, упорядоченных по областям анализа

В этом разделе, исходя из представленных вами ответов, в графическом виде представлены концепции, описанные выше, для вашей организации**.**

**•** 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**.**

После перейдем во вкладку полный отчет и увидим результаты аудита нашей системы, где зеленый знак означает, что позиция соответствует передовым методикам, желтый знак – требует усовершенствования, а красный знак – неудовлетворительно. Результаты аудита система ФГБУ «НПП ГАММА» показаны на рисунке 2 и 3.

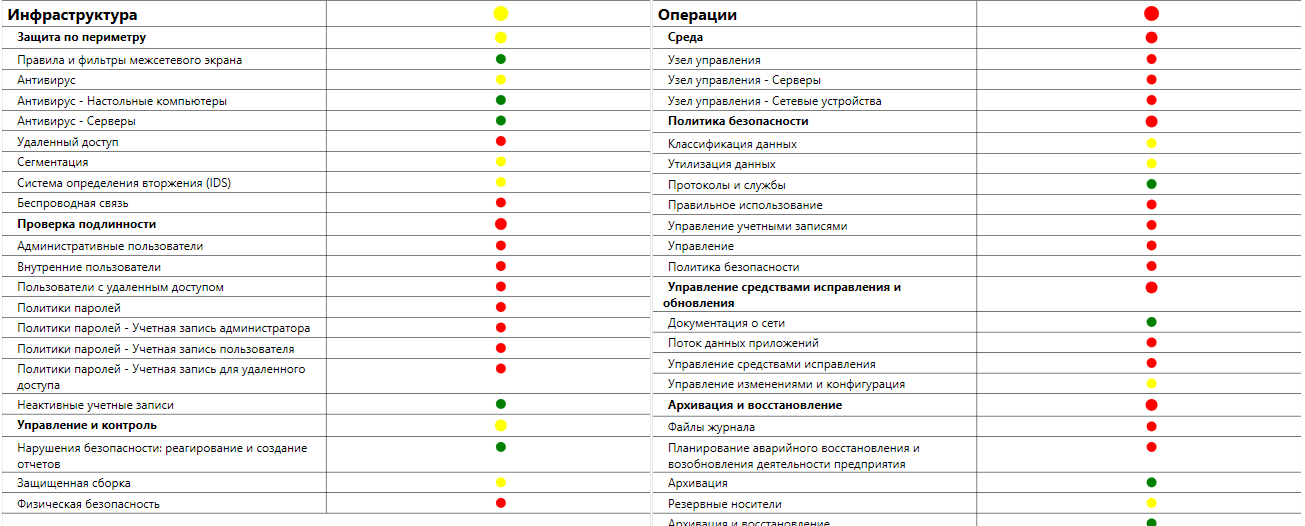


Рисунок 2 – Результаты аудита системы

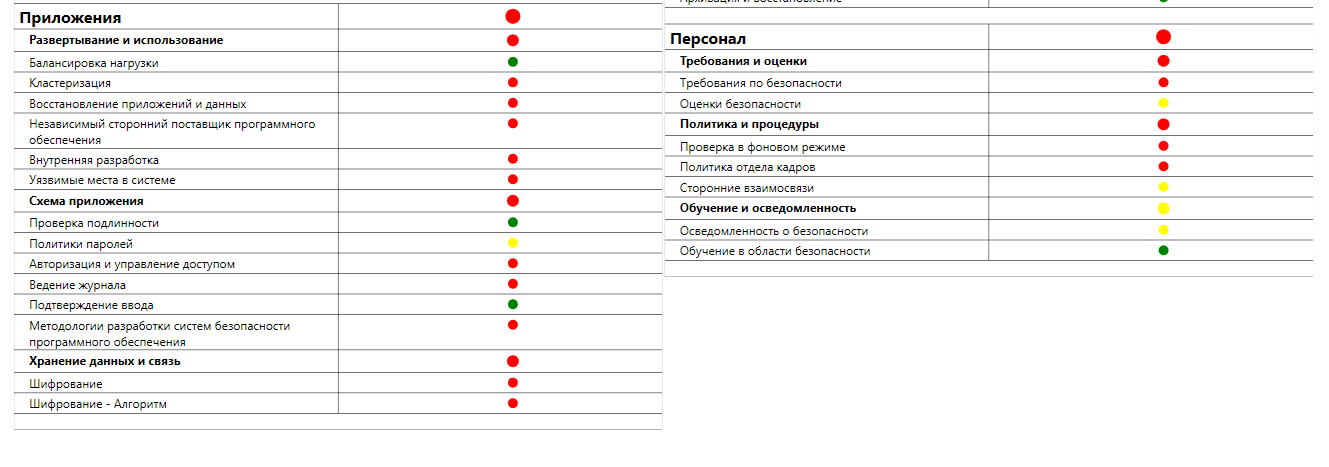


Рисунок 3 – Результаты аудита системы

Очевидно, что у нас в организации существуют недостатки в области защиты приложений и операций. В то же время, стоит отметить, что инфраструктура и персонал в целом подготовлены довольно хорошо к вопросам безопасности.

Необходимо обратить внимание на выявленные проблемы и принять меры в тех областях, где безопасность требует усиления. Данная оценка подчеркивает важность проведения дополнительных мероприятий и внедрения улучшений в сфере защиты приложений и операций. Это также подчеркивает значимость постоянного мониторинга и анализа для обеспечения высокого уровня безопасности в целом, обеспечивая надежную защиту информационных ресурсов организации.

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.

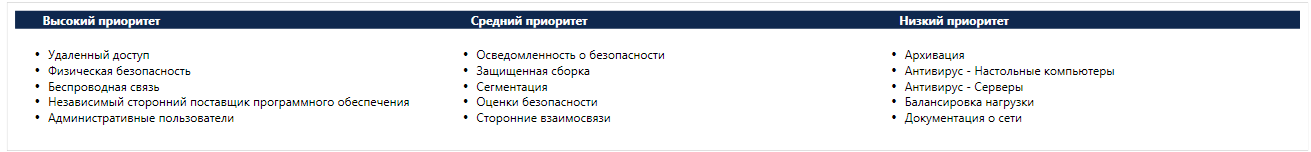


Рисунок 4 – Инициативы по обеспечению безопасности

Самое главное из этого стоит обратить внимание на высокий приоритет. Данные категории нужно устранять и усовершенствовать в первую очередь.

Дальше, идя по полному отчету, следующий раздел его — это оценочный анализ**.** В данном анализе описаны четыре части, посвященные основным областям анализа — инфраструктуре, приложениям, операциям и персоналу. По каждой областей описаны рекомендации по каждой разделу.

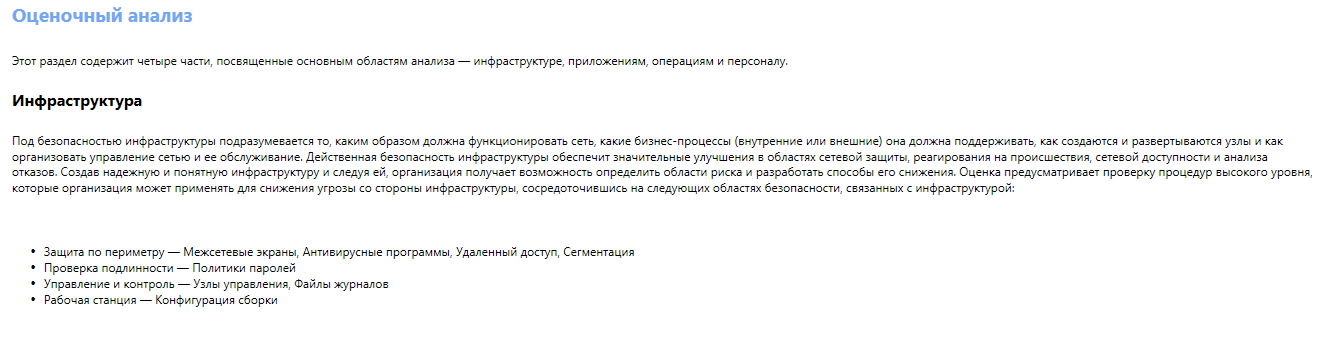


Рисунок 5 – Оценочный анализ инфраструктуры.

* В разделе инфраструктуры данной организации обнаружены уязвимости. Рекомендуется уделить внимание правилам и фильтрам межсетевого экрана, поскольку применяемые технологии в данной организации оказались недостаточно эффективными.

Установка антивирусов на соответствующие участки инфраструктуры является неотложной задачей, учитывая активное использование почты сотрудниками как основного средства обмена информацией. Кроме того, учитывая, что критически важная информация обрабатывается на серверах, обеспечение надежной защиты от внутренних и внешних угроз становится приоритетной задачей.

Также в отчете беспроводные сети используются в организации, ими пользуются, как сотрудники, так и клиенты Банка. В отчете также описаны

рекомендации по защите сети. Например, чтобы предотвратить использование точки доступа и вашей беспроводной сети, следует немедленно изменить идентификатор SSID, указав значение, которое трудно сопоставимо с вашей компанией и несмотря на то, что шифрование WEP все же лучше, чем полное его отсутствие, лучше использовать шифрование WPA, которое является более надежным.

* В разделе с приложениями также описаны некоторые рекомендации для нашей компании. В нашей компании, как и было указано раннее, сторонние поставщики разработали одно или несколько основных приложений.

Из этого рекомендуется убедиться в том, что сторонняя организация, которая разработала основное программное обеспечение, будет продолжать его поддержку, своевременно обеспечивать доставку обновлений и сможет предоставить исходный текст приложения в случае невозможности его дальнейшей поддержки.

Также в нашей организации для офисных приложений используются специально разработанные макросы. Рекомендуется, что из-за использования собственных макросов, настройки безопасности пакета Office необходимо понизить, в результате чего офисные приложения могут быть подвержены заражению документами злоумышленников. Рассмотрите необходимость ограничения возможности разработку и выполнения собственных макросов, предоставив ее только тем, кому это требуется по служебным обязанностям.

В разделе операции также содержатся рекомендации для нашей компании, а именно:

* В анкете отмечено, что оценки безопасности в вашей организации проводятся внутренним персоналом. Рекомендация MSAT заключается в том, что следует сохранять практику регулярных проверок безопасности внутренним персоналом, но, дополнительно к этому, привлекать заслуживающую доверия стороннюю организацию.
* В анкете отражено, что обучение, связанное с осведомленностью, не охватывает средства контроля и политику безопасности вашей организации. Рекомендация MSAT подчеркивает необходимость включения в обучение по вопросам безопасности все аспекты, включая средства контроля и политики безопасности, обнаружение подозрительных действий, вопросы конфиденциальности, безопасность электронной почты, а также безопасность в Интернете и на компьютере.

В конечном отчете представлен раздел, посвященный списку приоритетных действий. В данном разделе представлены конкретные области, требующие улучшений, а также рекомендации по их усовершенствованию. Действия с высоким приоритетом наглядно представлены на соответствующем рисунке 6.

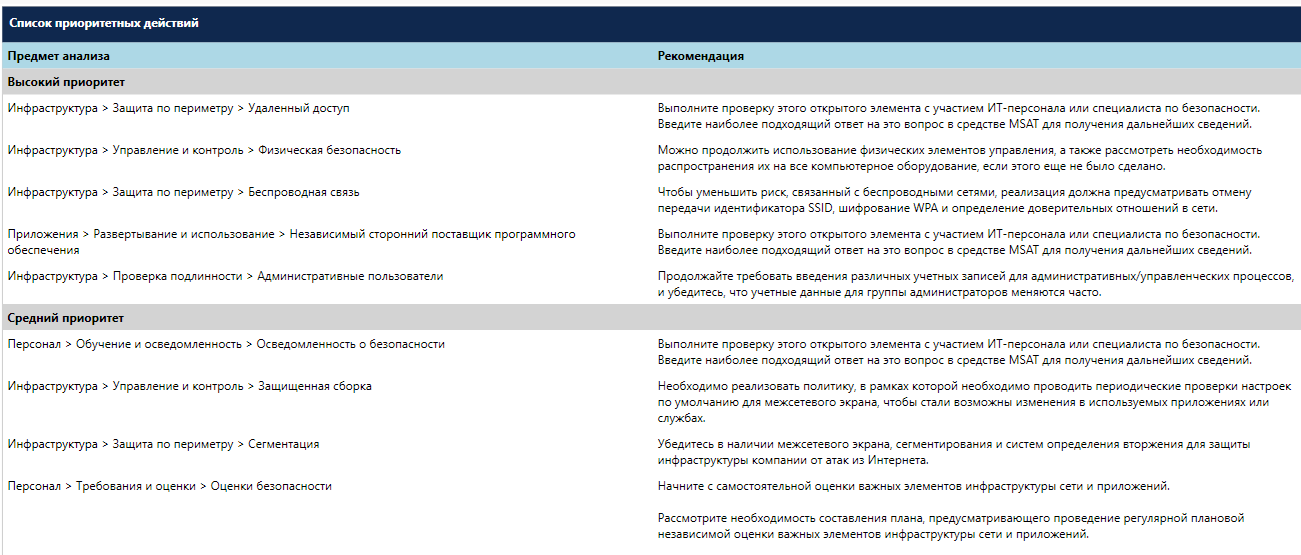


Рисунок 6 – Список действий с высоким приоритетом

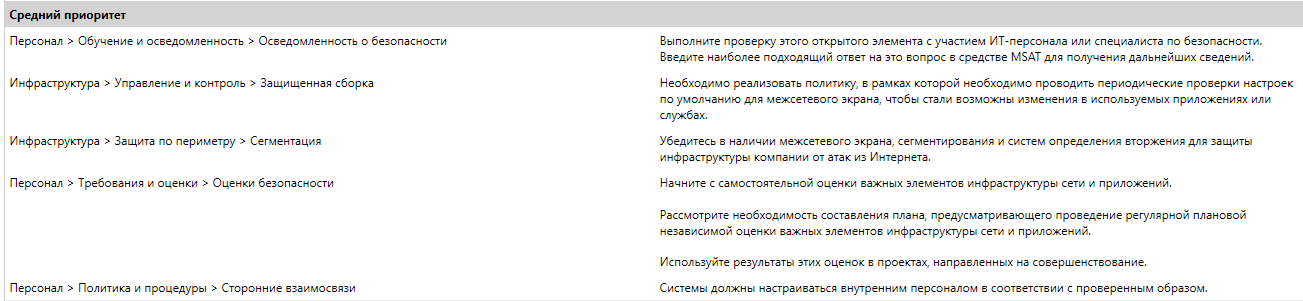


Рисунок 7 – Список действий со средним приоритетом

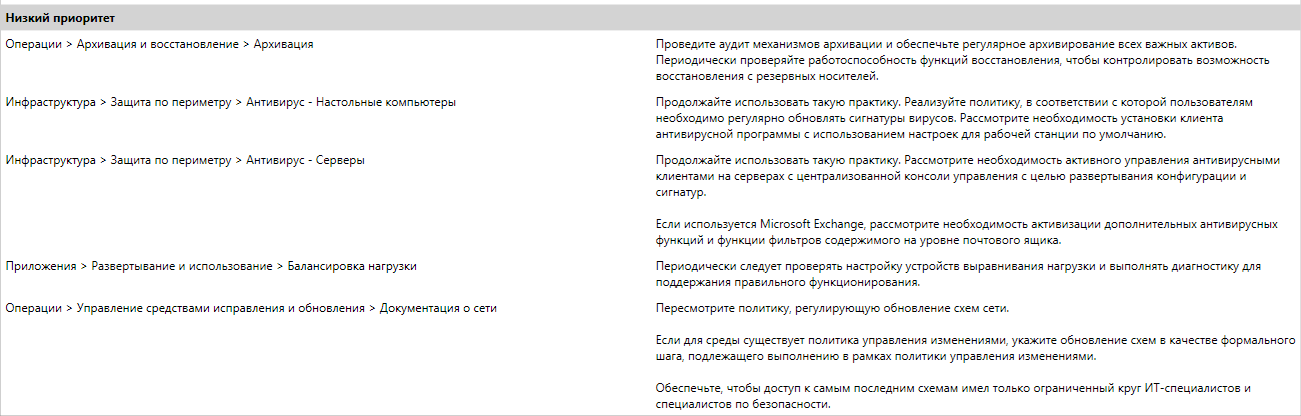


Рисунок 8 – Список действий с низким приоритетом

# 

# План улучшения

1. Прежде всего, необходимо гарантировать безопасность беспроводной сети, учитывая ранее упомянутые риски. Безопасность беспроводных сетей становится ключевым аспектом, поскольку через них может возникнуть угроза доступа к внутренней сети, даже находясь за пределами контролируемой зоны.
2. Затем целесообразно обратить внимание на настройку удаленного доступа. Этот момент приобретает критическое значение, учитывая современные тенденции использования удаленных рабочих мест. Эффективная конфигурация этой функции способствует предотвращению возможных угроз безопасности.
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. В заключение, предлагается пересмотреть защитные решения как для персональных компьютеров, так и для серверов. Укрепление мер безопасности представляет собой важный этап в обеспечении целостности и безопасности информационной среды нашей организации.

# Вывод

По итогам практической работы можно сделать вывод, что MSAT представляет собой эффективное средство для анализа собственной организации, предоставляя грамотные рекомендации. Важным моментом является то, что данная программа, несмотря на свою полезность, была разработана достаточно давно, что может влиять на ее способность полноценно учитывать современные требования и вызовы в области безопасности.

Важно отметить, что переход к более актуальным версиям программного обеспечения является инвестицией в долгосрочную безопасность организации. Это позволяет эффективно адаптироваться к изменяющейся киберугрозной среде и минимизировать риски в соответствии с современными стандартами безопасности. С учетом быстрого развития технологий и угроз, обновленные программы будут служить более надежным и актуальным инструментом для обеспечения безопасности вашей организации.

В заключение, активная защита беспроводной сети, настройка удаленного доступа, обучение персонала и пересмотр защитных решений являются важными шагами в укреплении безопасности нашей организации. Этот комплекс мер поможет предотвратить потенциальные угрозы, связанные с современными методами атак, и обеспечит надежную защиту как для внутренних, так и для удаленных рабочих сред.