|  |
| --- |
|  |
| 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

по дисциплине: «Управление информационной безопасностью»

на тему: «Проведение аудита системы менеджмента информационной безопасности»

**Выполнил**:

Студент группы ББМО-02-22

Кузьмин Владимир Дмитриевич

**Проверил**:

Пимонов Роман Владимирович

Москва 2023

СОДЕРЖАНИЕ

[ВВЕДЕНИЕ 3](#_Toc152100862)

[АНАЛИЗ РЕЗУЛЬТАТОВ 4](#_Toc152100863)

[ПЛАН УЛУЧШЕНИЯ 12](#_Toc152100864)

[ЗАКЛЮЧЕНИЕ 13](#_Toc152100865)

# ВВЕДЕНИЕ

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

Результаты оценки безопасности системы представлены в файле «Кузьмин\_В.Д.\_ББМО-02-22\_прз1.12.xps». Перейдём к анализу полученных результатов.

# АНАЛИЗ РЕЗУЛЬТАТОВ

Анализ результатов, приведённых с помощью ПО «Microsoft Security Assessment Tool (MSAT)». Отчет начинается с ситуационного анализа. В этом разделе в графическом виде представлены концепции для ПАО «Роснефть». Результаты оценки безопасности представлены на рисунке 1.

## 

## Рисунок 1 – Результаты оценки безопасности

После того, как был запрошен отчет в программе MSAT, отображается страница сводного отчета. На этой странице представлен профиль риска для бизнеса и индекс эшелонированной защиты с графическим представлением. Чрезвычайно информативным является график, который отражает разность показателей эшелонированной защиты, упорядоченных по различным областям анализа. Этот график можно увидеть на рисунке 2, который также представляет большой интерес для анализа.

## Рисунок 2 – График, отражающая разность показателей эшелонированный защиты, упорядоченных по областям анализа

где:

* BRP 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.

Затем следует перейти на вкладку с полным отчётом и изучить результаты проверки нашей системы. Зелёный значок свидетельствует о соответствии стандартам, жёлтый – о необходимости доработки, а красный сигнализирует о неудовлетворительном состоянии. Результаты проверки системы ПАО «Роснефть» показаны на рисунках 3 и 4.

## 

## Рисунок 3 – Результаты аудита система ПАО «Роснефть»

## 

## Рисунок 4 – Результаты аудита система ПАО «Роснефть»

Сразу заметно, что в нашей организации есть некоторые недоработки в сфере обучения и информированности сотрудников, а также в приложениях и защите по периметру. Но раздел «операции» и «проверка подлинности» не вызывают нареканий, что, безусловно, радует. Важно обратить внимание на обнаруженные проблемы и принять соответствующие меры в областях, где требуется усиление безопасности. Эта оценка указывает на необходимость проведения дополнительных мероприятий и внедрения усовершенствований в сфере защиты приложений и операций. Она также подчеркивает значимость постоянного мониторинга и анализа для гарантии высокого уровня безопасности и обеспечения надежной защиты информационных ресурсов организации. Для повышения уровня безопасности организации необходимо уделить внимание обучению и осведомленности сотрудников, а также улучшению качества приложений и системы защиты по периметру. Кроме того, следует проводить регулярный мониторинг и анализ всех операций, связанных с защитой информации, чтобы своевременно выявлять и устранять возможные угрозы.

Далее следуем по итоговому отчету и видим пункт инициативы по обеспечению безопасности. В данном пункте распределены угрозы по различным приоритетам их усовершенствования. Инициативы по обеспечению безопасности показаны на рисунке 5.

## 

## Рисунок 5 – Инициативы по обеспечению безопасности

Самое важное, на что стоит обратить внимание – это высокий приоритет указанных категорий. Их необходимо устранять и улучшать в первую очередь.

После раздела инициативы по обеспечению безопасности идет раздел области анализа. В данном разделе перечислены области, использованные для обеспечения высокого качества анализа при оценке угроз безопасности, и описана значимость каждой области для безопасности. Таблица данного разделе с категориями и их важностью для обеспечения безопасности представлены на рисунках 6 и 7.

## 

## Рисунок 6 – Области анализа

## 

## Рисунок 7 – Области анализа

Далее, продолжая изучать полный отчёт, мы сталкиваемся со следующим разделом – оценочным анализом. В рамках данного анализа рассмотрены четыре основных области – инфраструктура, приложения, операции и персонал. По каждому из этих разделов представлены рекомендации.

В конце полного отчёта находится раздел со списком приоритетных действий. Здесь перечислены конкретные разделы и рекомендации по их улучшению. Список действий с различными приоритетами представлены на таблице 1.

Таблица 1 – Список приоритетных действий

|  |  |  |
| --- | --- | --- |
| **Список приоритетных действий** | | |
| ***Предмет анализа*** | | ***Рекомендация*** |
| **Высокий приоритет** | | |
| Инфраструктура > Проверка подлинности > Пользователи с удаленным доступом | Если это еще не было сделано, рассмотрите необходимость использования многофакторной проверки подлинности для удаленного доступа и предоставьте доступ только тем сотрудникам, у которых реально существует потребность в удаленном подключении. | |
| Инфраструктура > Управление и контроль > Защищенная сборка | Выполните проверку этого открытого элемента с участием ИТ-персонала или специалиста по безопасности. Введите наиболее подходящий ответ на это вопрос в средстве MSAT для получения дальнейших сведений. | |
| Операции > Архивация и восстановление > Планирование аварийного восстановления и возобновления деятельности предприятия | Продолжайте поддерживать и тестировать планы аварийного восстановления и возобновления деятельности предприятия. | |
| Инфраструктура > Защита по периметру > Сегментация | Убедитесь в наличии межсетевого экрана, сегментирования и систем определения вторжения для защиты инфраструктуры компании от атак из Интернета. | |
| Приложения > Развертывание и использование > Независимый сторонний поставщик программного обеспечения | Выполните проверку этого открытого элемента с участием ИТ-персонала или специалиста по безопасности. Введите наиболее подходящий ответ на это вопрос в средстве MSAT для получения дальнейших сведений. | |
| **Средний приоритет** | | |
| Инфраструктура > Управление и контроль > Физическая безопасность | Можно продолжить использование физических элементов управления, а также рассмотреть необходимость распространения их на все компьютерное оборудование, если этого еще не было сделано. | |
| Приложения > Хранение данных и связь > Шифрование | Для всех операций шифрования используйте алгоритмы шифрования, применяемые в отрасли. | |
| Инфраструктура > Защита по периметру > Беспроводная связь | Чтобы уменьшить риск, связанный с беспроводными сетями, реализация должна предусматривать отмену передачи идентификатора SSID, шифрование WPA и определение доверительных отношений в сети. | |
| Персонал > Требования и оценки > Оценки безопасности | Начните с самостоятельной оценки важных элементов инфраструктуры сети и приложений. Рассмотрите необходимость составления плана, предусматривающего проведение регулярной плановой независимой оценки важных элементов инфраструктуры сети и приложений.  Используйте результаты этих оценок в проектах, направленных на совершенствование. | |
| Операции > Управление средствами исправления и обновления > Управление изменениями и конфигурация | По-прежнему используйте процесс официального управления изменениями и конфигурацией для проверки и документирования всех обновлений перед развертыванием. | |
| **Низкий приоритет** | | |
| Операции > Среда > Узел управления - Серверы | Рассмотрите необходимость использования SSH или VPN для защиты текстовых протоколов. | |
| Операции > Среда > Узел управления - Сетевые устройства | Следует протестировать все системы управления, в которых используется SNMP, чтобы убедиться, что в них используются последние версии исправлений и не используются настройки сообщества по умолчанию. | |
| Операции > Политика безопасности > Правильное использование | Все сотрудники и клиенты, использующие корпоративные ресурсы, должны быть ознакомлены с этими политиками. Разместите политики в корпоративной интрасети и рассмотрите необходимость ознакомления с ними всех новых сотрудников при приеме их на работу. | |
| Операции > Архивация и восстановление > Архивация | Проведите аудит механизмов архивации и обеспечьте регулярное архивирование всех важных активов. Периодически проверяйте работоспособность функций восстановления, чтобы контролировать возможность восстановления с резервных носителей. | |
| Инфраструктура > Защита по периметру > Антивирус - Серверы | Продолжайте использовать такую практику. Рассмотрите необходимость активного управления антивирусными клиентами на серверах с централизованной консоли управления с целью развертывания конфигурации и сигнатур. Если используется Microsoft Exchange, рассмотрите необходимость активизации дополнительных антивирусных функций и функции фильтров содержимого на уровне почтового ящика. | |

# ПЛАН УЛУЧШЕНИЯ

1. Улучшение систем контроля доступа, включая установку видеонаблюдения и биометрических систем аутентификации.

2. Внедрение современных средств защиты информации, таких как межсетевые экраны, антивирусное программное обеспечение и системы обнаружения вторжений.

3. Проведение регулярных обучающих семинаров для сотрудников с целью повышения их осведомленности о правилах работы с конфиденциальной информацией и мерах по ее защите.

4. Разработка и внедрение четких политик и процедур, которые будут регулировать работу с персональными данными и обеспечивать их защиту.

5. Проведение регулярного мониторинга и аудита информационной системы на предмет уязвимостей и возможных угроз.

6. Внедрение систем обнаружения и предотвращения утечек данных (DLP), которые помогут предотвратить несанкционированный доступ к конфиденциальной информации.

7. Внедрение системы управления мобильными устройствами (MDM) для контроля над доступом к корпоративным ресурсам с мобильных устройств.

8. Использование надежных облачных провайдеров и обеспечение строгой аутентификации и авторизации пользователей при доступе к данным в облаке.

9. Создание системы резервного копирования данных и регулярного тестирования процедур восстановления информации в случае возникновения инцидентов.

10. Регулярное обновление и совершенствование мер защиты с учетом новых угроз и технологий, а также проведение регулярных оценок эффективности существующих мер защиты.

# ЗАКЛЮЧЕНИЕ

На основании проведённой работы, можно прийти к выводу, что MSAT является эффективным инструментом для анализа состояния безопасности в организации и предоставления рекомендаций по её улучшению. Однако, стоит учесть, что данный продукт был разработан достаточно давно и может не в полной мере учитывать современные требования и угрозы в области информационной безопасности.

В связи с этим, для более актуального и современного анализа рекомендуется использование более новых версий аналогичного программного обеспечения, которые включают в себя актуальные методологии и инструменты для оценки состояния безопасности. Переход на такие решения способствует соответствию последним стандартам безопасности и предоставляет более надёжный анализ в контексте актуальных угроз и рисков, а также предоставляет усовершенствованные функции и лучшую совместимость с современными технологиями.

Такой переход к современным решениям является инвестицией в долгосрочное обеспечение безопасности, позволяя эффективно адаптироваться к меняющейся среде киберугроз и снижать риски в соответствии с новыми вызовами и требованиями в области информационной безопасности.