

Оценка системы безопасности ИТ-инфраструктуры
с помощью Microsoft Security Assessment Tool

2024

Макаров Михаил Максимович

ББМО-02-23

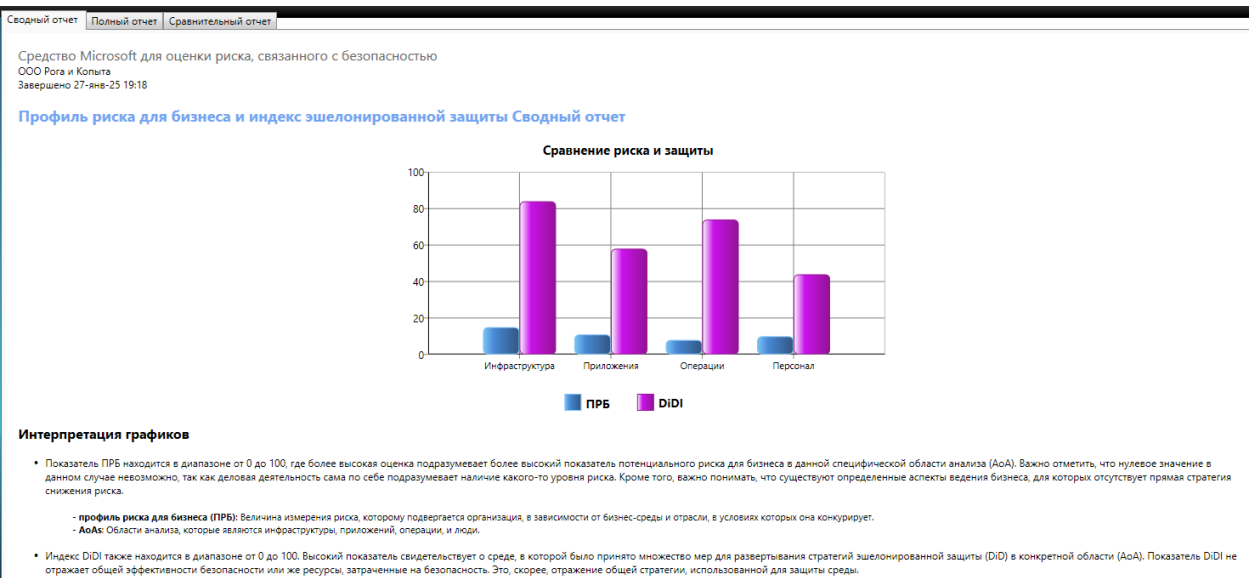
Содержание

Содержание	2
Основные функции MSAT:	3
Результаты.....	3
Высокий приоритет:.....	4
Средний приоритет:	5
Низкий приоритет:	6
Общие рекомендации по совершенствованию СМИБ.....	7
Выводы	7

Основные функции MSAT:

- Оценка рисков: помогает определить текущий уровень безопасности и выявить потенциальные угрозы.
- Рекомендации: предоставляет конкретные рекомендации по улучшению безопасности на основе результатов оценки.
- Сравнение с отраслевыми стандартами: позволяет сравнить результаты с данными других компаний в той же отрасли или с аналогичными размерами.
- Конфиденциальность данных: гарантирует анонимность передаваемых данных — результаты передаются на защищенный веб-сервер MSAT без сбора личных сведений об отправителях.

Результаты



Сводный отчет

Полный отчет

Сравнительный отчет

Результаты

Исходя из ваших ответов на вопросы, связанные с оценкой рисков, вашим защитным мерам присвоены следующие рейтинги. В разделах [Подробная оценка](#) и [Список рекомендуемых действий](#) настоящего отчета содержится более подробные сведения о результатах, передовых методиках и рекомендациях.

Подписи:

● Соответствует передовым методикам

● Требуется усовершенствования

● Неудовлетворительно

Инфраструктура	●	Операции	●
Защита по периметру	●	Среда	●
Правила и фильтры межсетевого экрана	●	Узел управления	●
Антивирус	●	Узел управления - Серверы	●
Антивирус - Настольные компьютеры	●	Узел управления - Сетевые устройства	●
Антивирус - Серверы	●	Политика безопасности	●
Удаленный доступ	●	Классификация данных	●
Сегментация	●	Утилизация данных	●
Система определения вторжения (IDS)	●	Протоколы и службы	●
Беспроводная связь	●	Правильное использование	●
Проверка подлинности	●	Управление учетными записями	●
Административные пользователи	●	Управление	●
Внутренние пользователи	●	Политика безопасности	●
Пользователи с удаленным доступом	●	Управление средствами исправления и обновления	●
Политики паролей	●	Документация о сети	●
Политики паролей - Учетная запись администратора	●	Поток данных приложений	●
Политики паролей - Учетная запись пользователя	●	Управление средствами исправления	●
Политики паролей - Учетная запись для удаленного доступа	●	Управление изменениями и конфигурация	●
Неактивные учетные записи	●	Архивация и восстановление	●
Управление и контроль	●	Файлы журнала	●
Нарушения безопасности: реагирование и создание отчетов	●	Планирование аварийного восстановления и возобновления деятельности предприятия	●
Защищенная сборка	●	Архивация	●
Физическая безопасность	●	Резервные носители	●

рекомендации охватывают различные аспекты информационной безопасности, включая персонал, приложения, инфраструктуру и операции.

Высокий приоритет:

1. Персонал > Обучение и осведомленность > Осведомленность о безопасности:

- **Пояснение:** Важно поддерживать специалиста или группу специалистов по безопасности, чтобы они консультировали сотрудников перед изменениями в вычислительной среде. Это помогает предотвратить ошибки и повысить общий уровень безопасности.
- **Направление совершенствования:** Регулярное обучение и повышение осведомленности сотрудников о новых угрозах и методах защиты.

2. Приложения > Хранение данных и связь > Шифрование - Алгоритм:

- **Пояснение:** Рекомендуется обновить шифрование с 3DES на более современный AES для повышения безопасности данных и усложнения задачи их взлома.
- **Направление совершенствования:** Внедрение AES для защиты данных и регулярный аудит используемых алгоритмов шифрования.

3. Персонал > Политика и процедуры > Сторонние взаимосвязи:

- **Пояснение:** Системы должны настраиваться и обслуживаться внутренним персоналом в соответствии с проверенными

методами, чтобы избежать рисков, связанных с привлечением сторонних специалистов.

- **Направление совершенствования:** Разработка и внедрение строгих процедур для управления сторонними взаимосвязями и их настройкой.

4. Приложения > Развертывание и использование > Внутренняя разработка:

- **Пояснение:** Использование собственных макросов в офисных приложениях может снизить их безопасность. Рекомендуется ограничить возможность разработки и выполнения макросов только необходимыми сотрудниками.
- **Направление совершенствования:** Ограничение использования макросов и повышение безопасности офисных приложений.

5. Операции > Архивация и восстановление > Планирование аварийного восстановления и возобновления деятельности предприятия:

- **Пояснение:** Планы аварийного восстановления должны поддерживаться и тестироваться регулярно для обеспечения их готовности и эффективности.
- **Направление совершенствования:** Регулярное тестирование и обновление планов аварийного восстановления.

Средний приоритет:

1. Инфраструктура > Защита по периметру > Сегментация:

- **Пояснение:** Необходимо обеспечить наличие межсетевого экрана, сегментирования и систем определения вторжения для защиты инфраструктуры от интернет-атак.
- **Направление совершенствования:** Внедрение и поддержка систем сегментации и защиты периметра.

2. Инфраструктура > Проверка подлинности > Административные пользователи:

- **Пояснение:** Рекомендуется внедрить дополнительный фактор проверки подлинности для снижения риска несанкционированного доступа.
- **Направление совершенствования:** Внедрение многофакторной аутентификации для административных пользователей.

3. Операции > Архивация и восстановление > Резервные носители:

- **Пояснение:** Политика хранения резервных носителей должна быть тщательно проработана и регулярно аудироваться.
- **Направление совершенствования:** Регулярный аудит и обновление политики хранения резервных копий.

4. Приложения > Схема приложения > Методологии разработки систем безопасности программного обеспечения:

- **Пояснение:** Важно продолжать использовать методологии разработки безопасных систем программного обеспечения.
- **Направление совершенствования:** Постоянное обновление и адаптация методологий разработки для соответствия современным требованиям безопасности.

5. Персонал > Требования и оценки > Оценки безопасности:

- **Пояснение:** Рекомендуется начать с самостоятельной оценки важных элементов инфраструктуры и приложений, а также планировать регулярные независимые оценки.
- **Направление совершенствования:** Проведение регулярных независимых оценок безопасности и использование их результатов для улучшения системы.

Низкий приоритет:

1. Операции > Среда > Узел управления - Серверы:

- **Пояснение:** Рассмотрите использование SSH или VPN для защиты текстовых протоколов.
- **Направление совершенствования:** Внедрение SSH или VPN для повышения безопасности серверов.

2. Операции > Среда > Узел управления - Сетевые устройства:

- **Пояснение:** Тестирование систем управления с SNMP на наличие последних версий исправлений и отсутствие настроек по умолчанию.
- **Направление совершенствования:** Регулярное обновление и проверка настроек сетевых устройств.

3. Операции > Политика безопасности > Правильное использование:

- **Пояснение:** Все сотрудники и клиенты должны быть ознакомлены с политиками безопасности, которые размещены в корпоративной интрасети.
- **Направление совершенствования:** Ознакомление новых сотрудников с политиками безопасности и их регулярное обновление.

4. Операции > Архивация и восстановление > Архивация:

- **Пояснение:** Аудит механизмов архивации и обеспечение регулярного архивирования важных активов.
- **Направление совершенствования:** Регулярное архивирование и проверка функций восстановления.

5. Инфраструктура > Защита по периметру > Антивирус - Настольные компьютеры:

- **Пояснение:** Продолжайте использовать антивирусные программы и политику регулярного обновления сигнатур вирусов.
- **Направление совершенствования:** Установка антивирусных программ с настройками для рабочих станций по умолчанию и регулярное обновление сигнатур.

Общие рекомендации по совершенствованию СМИБ

- **Регулярный аудит и оценка:** проводить регулярные аудиты и оценки безопасности, чтобы выявлять слабые места и улучшать систему.
- **Обучение сотрудников:** проверять, что все сотрудники понимают политики безопасности и свои обязанности.
- **Внедрение современных технологий:** использовать современные технологии, такие как MFA, шифрование и системы обнаружения вторжений.
- **Документирование и тестирование:** документировать все процессы и регулярно тестируйте их на эффективность.

Выводы

Для улучшения Системы менеджмента информационной безопасности (СМИБ) ООО «Техно-Телеком» необходимо сосредоточиться на нескольких ключевых направлениях. Важно внедрить регулярные тренинги и тестирования по информационной безопасности для повышения осведомленности сотрудников, используя интерактивные методы обучения. Следует установить систему управления правами доступа (IAM) и

многофакторную аутентификацию (MFA) для контроля доступа, а также регулярно проводить аудит прав доступа.

Необходимо обеспечить защиту от современных угроз с помощью решений типа NGAV и IPS, обновлять антивирусные базы и проводить тестирование на проникновение. Регулярное тестирование процессов восстановления данных и внедрение облачных решений для резервного копирования помогут в защите данных. Важно разработать план аварийного восстановления (DRP).

Для мониторинга и реагирования на инциденты следует внедрить систему SIEM и процедуры автоматического реагирования, а также проводить регулярные учения. Защита периметра сети включает внедрение защиты от DDoS-атак и технологии сегментации сети, а также регулярный аудит конфигурации межсетевых экранов.

Регулярный пересмотр и актуализация политик и процедур, внедрение системы управления политиками и проведение аудитов на соответствие стандартам обеспечат соответствие современным требованиям. Управление уязвимостями включает внедрение системы управления уязвимостями и процесс управления исправлениями, а также регулярное сканирование на уязвимости.

Для защиты мобильных устройств и удаленных рабочих мест следует внедрить политику BYOD, использовать решения MDM и VPN, а также обучать сотрудников безопасному использованию мобильных устройств. Регулярная оценка рисков с использованием методологий OCTAVE и NIST, а также внедрение системы мониторинга рисков помогут минимизировать возможные угрозы и обеспечить высокий уровень информационной безопасности.