|  |
| --- |
|  |
| 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»

Группа:

ББМО-02-22

Выполнила:

Бардасова И.А.

Проверил:

Пимонов Р.В.

Москва, 2023

Содержание

[ВВЕДЕНИЕ 3](#_Toc152425035)

[Анализ полученных результатов 4](#_Toc152425036)

[План улучшения 12](#_Toc152425037)

[ЗАКЛЮЧЕНИЕ 14](#_Toc152425038)

# ВВЕДЕНИЕ

MSAT — это обновленная версия средства Microsoft Security Risk Self-Assessment Tool (MSRSAT), выпущенного в 2004 году, и средства Microsoft Security Assessment Tool 2.0, выпущенного в 2006 году. Данное 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 ООО «Стройстрит» на примере применения программного средства «Microsoft Security Assessment Tool (MSAT)».

Результат оценки безопасности системы будет находиться в файле «Бардасова\_ИА\_ББМО-02-22\_прз1\_12.xps».

# Анализ полученных результатов

В самом начале можем увидеть сводный отчет. На этой странице представлен в графическом виде профиль риска для бизнеса и индекс эшелонированной защиты. Диаграмма, отражающая разность показателей эшелонированный защиты, упорядоченных по областям анализа показана на рисунке 1.

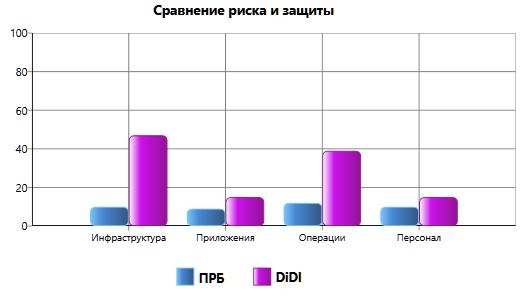


Рисунок 1 – Разность показателей эшелонированный защиты, упорядоченных по областям анализа

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.

В нашем случае в сравнении с DIDI, наши показатели ПРБ оказались во всех категориях ниже.

Из полученных результатов можно сделать вывод о необходимости пересмотра стратегии инвестирования в IT-ресурсы банка. 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 ООО «Стройстрит». 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 ООО «Стройстрит» показаны на рисунке 3.



Рисунок 3 – Результаты аудита система ООО «Стройстрит»

Очевидно, что у нас в организации существуют недостатки в: инфраструктуре, в частности - защите по периметру; операциях, в частности - политике безопасности и управлении средствами обновления; приложениях; персонале. Следует обратить внимание на выявленные проблемы и принять меры в тех областях, где безопасность требует усиления (особенно красные точки). Данная оценка подчеркивает важность проведения дополнительных мероприятий и внедрения улучшений в каждой области.

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.

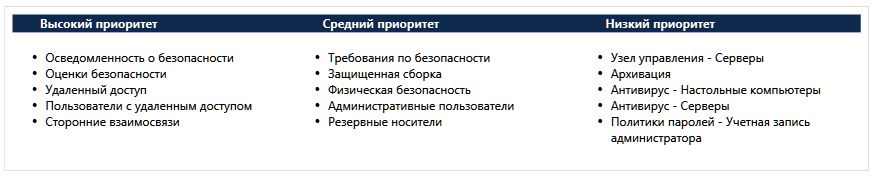


Рисунок 4 – Инициативы по обеспечению безопасности

Необходимо обратить внимание на обнаруженные проблемы и принять соответствующие меры в областях, где требуется усиление безопасности.

В первую очередь стоит обратить внимание на высокий приоритет. Данную категорию нужно устранять и усовершенствовать в первую очередь.

Следующий раздел в отчёте, это оценочный анализ. В нём описаны четыре части, посвященные основным областям анализа — инфраструктура, приложения, операции и персонал. В каждой части описаны рекомендации для каждой подкатегории.

Уделим внимание некоторым рекомендациям.

В каждом разделе, как и говорилось ранее, были обнаружены уязвимости. Рассмотрим их.

Рекомендуется уделить внимание правилам и фильтрам межсетевого экрана. Регулярно проверять их правильную работу и совершенствовать.

На всех компьютерах среды организации необходимо установить антивирусное программное обеспечение. Реализовать политику, в соответствии с которой пользователям необходимо регулярно обновлять сигнатуры вирусов. 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.

Необходимо будет развернуть сеть VPN, чтобы обеспечить подключение пользователей с удаленным доступом на основе технологий IP-безопасности (IPSec), SSL (Secure Sockets Layer) и SSH (Secure Shell).

В каждом сегменте внешней сети должна быть разрешена передача трафика только определенного приложения на определенные узлы и порты, которые используются для предоставления услуг клиентам. Необходимо ограничить доступ к сетевым службам на входе и выходе, а также ограничить доступ между разными сетевыми сегментами.

Чтобы снизить риск взлома пароля в административных учетных записях, следует выполнить следующие рекомендации:

+ добавить истечение срока действия пароля

+ блокировать учетную запись после 7 - 10 попыток неправильного ввода пароля

+ вести журнал системы

Следует рассмотреть необходимость внедрения дополнительного фактора проверки подлинности, который позволит существенно снизить риск несанкционированного доступа с использованием учетной записи пользователя.

Необходимо реализовать политику паролей для учетных записей удаленного доступа на основе передовых методик.

Нужно будет регулярно просматривать узлы поставщиков и систем безопасности для ознакомления с предупреждениями о недавних атаках и появлении новых вирусов. Регулярно выполнять аудит удаленных пользователей, чтобы проверить, выполняют ли они обновление своих систем.

Следует требовать от удаленных пользователей регулярного обновления их систем.

Необходимо разработать и внедрить процедуры создания отчетов и реагирования на нарушения безопасности, а также на все проблемы, связанные с безопасностью.

Сетевое оборудование следует установить запираемой комнате или в шкафу. Нужно перенести сетевого оборудования в более безопасное место, это обеспечит дополнительную защиту от несанкционированного использования.

Серверы следует установить запираемой комнате или в шкафу.

Важные документы следует хранить в запираемых шкафах, чтобы предотвратить кражу и разглашение конфиденциальной информации.

Немедленно нужно начать работу с отделом кадров по разработке официальной политики увольнения сотрудников.

Должны быть разработаны отдельные политики в отношении увольнения как по обычным причинам, так и при наличии конфликтов.

Наиболее важным компонентом этой политики является гарантированное прекращение действия физического доступа и привилегий специалиста отдела ИТ для данного сотрудника

В конце полного отчета присутствует раздел список приоритетных действий.

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



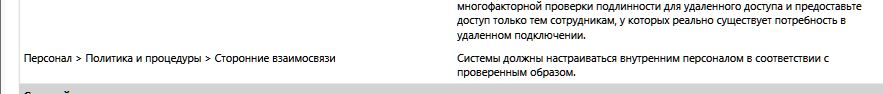


Рисунок 5 – Список приоритетных действий

Список действий с средним приоритетом показаны на рисунке 6.

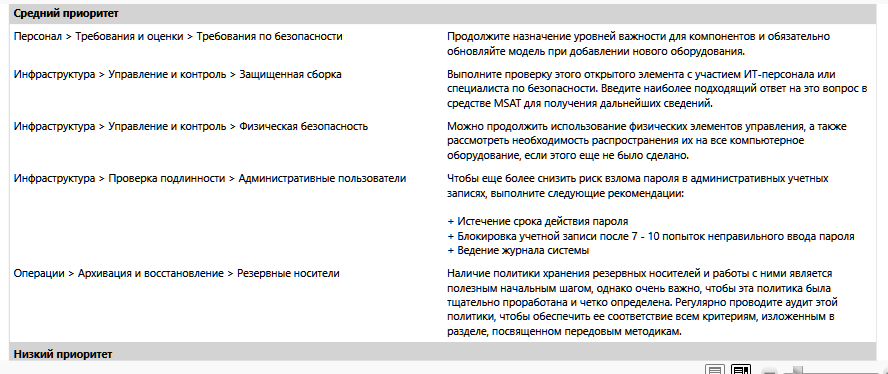


Рисунок 6 – Список действий со средним приоритетом

Список действий с низким приоритетом показаны на рисунке 7.

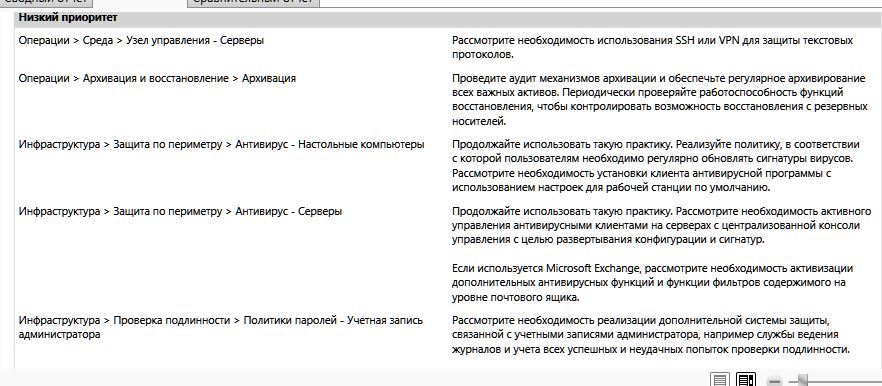


Рисунок 7 – Список действий с низким приоритетом

# План улучшения

1. Развернуть сеть VPN, чтобы обеспечить подключение пользователей с удаленным доступом на основе технологий IP-безопасности (IPSec), SSL (Secure Sockets Layer) и SSH (Secure Shell).

2. Системы должны настраиваться внутренним персоналом в соответствии с проверенным образом.

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

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

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. Чтобы еще более снизить риск взлома пароля в административных учетных записях, необходимо выполнить следующие действия:

+ Добавить истечение срока действия пароля;

+ Блокировать учетную запись после 7 - 10 попыток неправильного ввода пароля;

+ Вести журнал системы.

8. Проводить аудит механизмов архивации и обеспечивать регулярное архивирование всех важных активов. Периодически проверять работоспособность функций восстановления, чтобы контролировать возможность восстановления с резервных носителей.

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

# 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 ООО «Стройстрит».