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: Загороднов Е.А.

Проверил:

Р.В. Пимонов

Москва 2023

Содержание

Введение

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

Результаты оценки безопасности системы представлены в файле “Загороднов_ЕА_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.

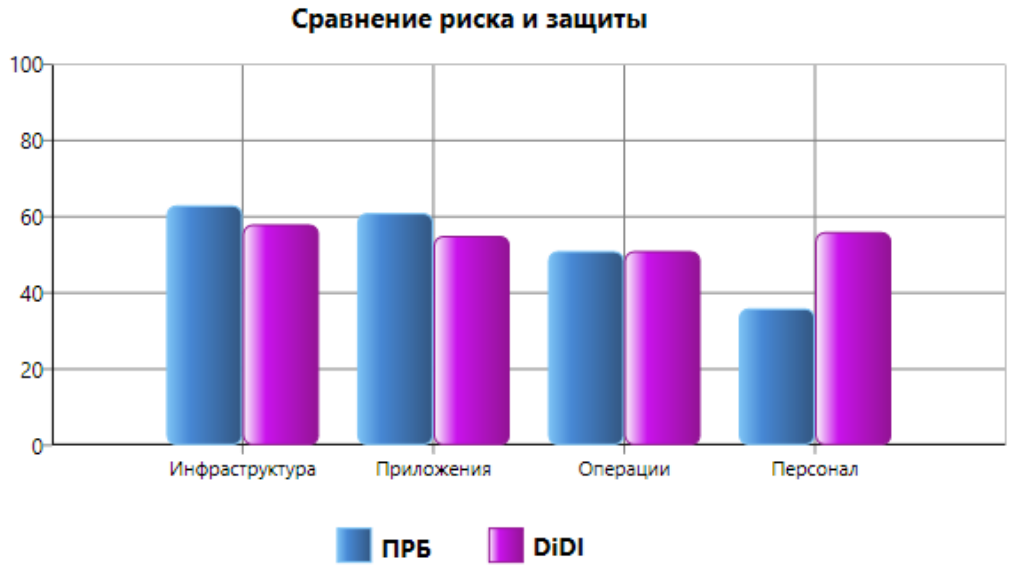


Рисунок 1 – График, отражающая разность показателей эшелонированный защиты, упорядоченных по областям анализа

Профиль риска для бизнеса (ПРБ) - величина измерения риска, которому подвергается организация, в зависимости от бизнес-среды и отрасли, в условиях которых она конкурирует.

Показатель ПРБ находится в диапазоне от 0 до 100, где более высокая оценка подразумевает более высокий показатель потенциального риска для бизнеса в данной специфической области анализа (AoA).

AoAs – это области анализа, которые являются инфраструктуры, приложений, операции, и люди.

Важно отметить, что нулевое значение в данном случае невозможно, так как деловая деятельность сама по себе подразумевает наличие какого-то уровня риска. Кроме того, важно понимать, что существуют определенные аспекты ведения бизнеса, для которых отсутствует прямая стратегия снижения риска.

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

Индекс DiDI также находится в диапазоне от 0 до 100. Высокий показатель свидетельствует о среде, в которой было принято множество мер для развертывания стратегий эшелонированной защиты (DiD) в конкретной области (AoA). Показатель DiDI не отражает общей эффективности безопасности или же ресурсы, затраченные на безопасность. Это, скорее, отражение общей стратегии, использованной для защиты среды.

Существует две категории ПРБ и DiDI, где лучшим вариантом является иметь одинаковый рейтинг данных показателей. Если есть дисбаланс между разными категориями – это значит, что у организации необходимо провести перегруппировку инвестиций в ИТ.

В нашем случае в сравнении с DIDI, наши показатели ПРБ оказались почти во всех категориях выше(кроме персонал). Хотя различия небольшие, они все же отмечаются. Это свидетельствует о том, что вопросы

эффективности и результативности в области информационных технологий в банке требуют внимания.

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 банковских операций и обеспечить более устойчивую работу информационных систем. Это также подчеркивает важность постоянного мониторинга и обновления инвестиционных стратегий в области IT для поддержания конкурентоспособности и современности банковского бизнеса.

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 ПАО “ЗенитБанк” показаны на рисунке 2 и 3.

Инфраструктура	🟡
Защита по периметру	🔴
Правила и фильтры межсетевого экрана	🟡
Антивирус	🟡
Антивирус - Настольные компьютеры	🟢
Антивирус - Серверы	🔴
Удаленный доступ	🟡
Сегментация	🔴
Система определения вторжения (IDS)	🔴
Беспроводная связь	🟡
Проверка подлинности	🟢
Административные пользователи	🟢
Внутренние пользователи	🟢
Пользователи с удаленным доступом	🔴
Политики паролей	🟢
Политики паролей - Учетная запись администратора	🟢
Политики паролей - Учетная запись пользователя	🟢
Политики паролей - Учетная запись для удаленного доступа	🟢
Неактивные учетные записи	🟢
Управление и контроль	🟡
Нарушения безопасности: реагирование и создание отчетов	🟢
Защищенная сборка	🔴
Физическая безопасность	🟡
Приложения	🟡

Операции	🔴
Среда	🟢
Узел управления	🟢
Узел управления - Серверы	🟢
Узел управления - Сетевые устройства	🟢
Политика безопасности	🟡
Классификация данных	🟡
Утилизация данных	🔴
Протоколы и службы	🟢
Правильное использование	🟢
Управление учетными записями	🔴
Управление	🟢
Политика безопасности	🟢
Управление средствами исправления и обновления	🔴
Документация о сети	🔴
Поток данных приложений	🟢
Управление средствами исправления	🔴
Управление изменениями и конфигурация	🟢
Архивация и восстановление	🔴
Файлы журнала	🟢
Планирование аварийного восстановления и возобновления деятельности предприятия	🔴
Архивация	🟢
Резервные носители	🔴
Архивация и восстановление	🔴

Рисунок 2 – Результаты аудита система ПАО “ЗенитБанк”

Приложения	
Развертывание и использование	
Балансировка нагрузки	
Кластеризация	
Восстановление приложений и данных	
Независимый сторонний поставщик программного обеспечения	
Внутренняя разработка	
Уязвимые места в системе	
Схема приложения	
Проверка подлинности	
Политики паролей	
Авторизация и управление доступом	
Ведение журнала	
Подтверждение ввода	
Методологии разработки систем безопасности программного обеспечения	
Хранение данных и связь	
Шифрование	
Шифрование - Алгоритм	

Архивация и восстановление	
Персонал	
Требования и оценки	
Требования по безопасности	
Оценки безопасности	
Политика и процедуры	
Проверка в фоновом режиме	
Политика отдела кадров	
Сторонние взаимосвязи	
Обучение и осведомленность	
Осведомленность о безопасности	
Обучение в области безопасности	

Рисунок 3 – Результаты аудита система ПАО “ЗенитБанк”

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 безопасности. В данном пункте распределены угрозы по различным приоритетам их усовершенствования. Инициативы по обеспечению безопасности показаны на рисунке 4.

Высокий приоритет	Средний приоритет	Низкий приоритет
• Защищенная сборка • Сегментация • Пользователи с удаленным доступом • Независимый сторонний поставщик программного обеспечения • Уязвимые места в системе	• Осведомленность о безопасности • Физическая безопасность • Шифрование • Беспроводная связь • Оценки безопасности	• Узел управления - Серверы • Узел управления - Сетевые устройства • Правильное использование • Архивация • Антивирус - Настольные компьютеры

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.

Распишем некоторые рекомендации.

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

В частности, в ПАО Банк ЗенитБанк выполнить проверку этого открытого элемента с участием ИТ-персонала или специалиста по безопасности, на всех компьютерах среды организации необходимо установить антивирусное программное обеспечение и также рассмотреть необходимость развертывания антивирусного решения сначала на критических файловых серверах, а затем на почтовых серверах, серверах баз данных и веб-серверах.

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.

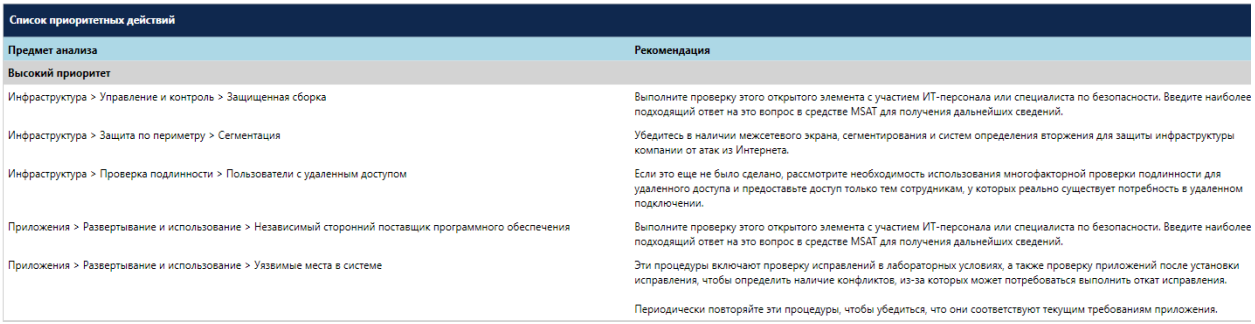
Также в нашей организации для офисных приложений используются специально разработанные макросы. Рекомендуется, что из-за использования собственных макросов, настройки безопасности пакета Office необходимо понизить, в результате чего офисные приложения могут быть подвержены заражению документами злоумышленников.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

В **разделе операции** также есть рекомендации для нашей компании. А именно:

- В анкете было указано, что оценки безопасности для вашей организации выполняются внутренним персоналом. Рекомендация MSAT заключается в том, что нужно продолжать практику частых проверок безопасности внутренним персоналом, но в дополнение к этому привлекайте заслуживающую доверия стороннюю организацию.
- В анкете было указано, что обучение, связанное с осведомленностью, не охватывает средства контроля и политики безопасности вашей организации. Рекомендация MSAT заключается в том, что обучение по вопросам безопасности должно затрагивать все аспекты, включая средства контроля и политики безопасности, сообщение о

подозрительных действиях, конфиденциальность, безопасность электронной почты, безопасность Интернета и компьютера.

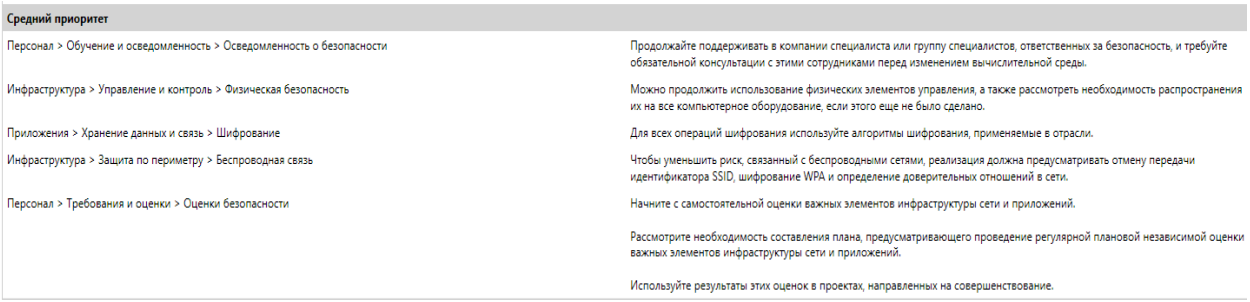
В конце полного отчета присутствует раздел **список приоритетных действий**. В данном разделе описаны конкретные разделы и рекомендации по улучшению данных разделов. Список действий с высоким приоритетом показаны на рисунке 5.



Список приоритетных действий	
Предмет анализа	**Рекомендация**
Высокий приоритет	
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.
Инфраструктура > Защита по периметру > Сегментация	Убедитесь в наличии межсетевого экрана, сегментирования и систем определения вторжения для защиты инфраструктуры компании от атак из Интернета.
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.
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.
Приложения > Развертывание и использование > Уязвимые места в системе	Эти процедуры включают проверку исправлений в лабораторных условиях, а также проверку приложений после установки исправления, чтобы определить наличие конфликтов, из-за которых может потребоваться выполнить откат исправления. Периодически повторяйте эти процедуры, чтобы убедиться, что они соответствуют текущим требованиям приложения.

Рисунок 5 – Список действий с высоким приоритетом

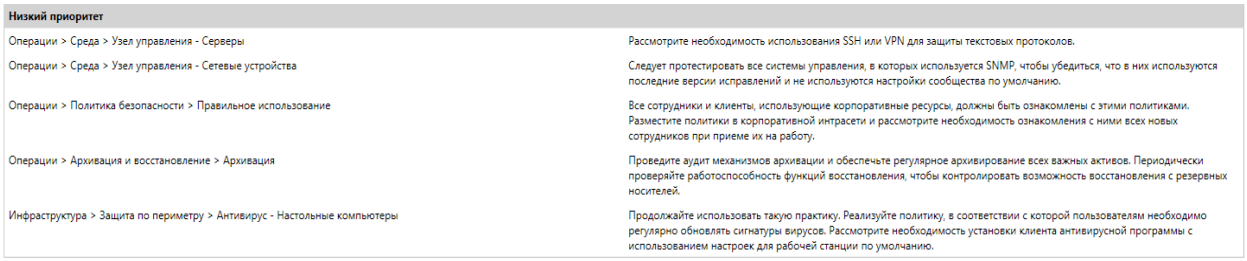
Список действий с средним приоритетом показаны на рисунке 6.



Средний приоритет	
Персонал > Обучение и осведомленность > Осведомленность о безопасности	Продолжайте поддерживать в компании специалиста или группу специалистов, ответственных за безопасность, и требуйте обязательной консультации с этими сотрудниками перед изменением вычислительной среды.
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.

Рисунок 6 – Список действий со средним приоритетом

Список действий с низким приоритетом показаны на рисунке 7.



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 - Настольные компьютеры	Продолжайте использовать такую практику. Реализуйте политику, в соответствии с которой пользователям необходимо регулярно обновлять сигнатуры вирусов. Рассмотрите необходимость установки клиента антивирусной программы с использованием настроек для рабочей станции по умолчанию.

Рисунок 7 – Список действий с низким приоритетом

План улучшения

1) Следует обратить внимание на настройку удаленного доступа. Это критически важный аспект, учитывая современные тенденции в использовании удаленных рабочих мест. Эффективная настройка этой функции поможет предотвратить возможные угрозы безопасности.

2) Установить систему мониторинга и обнаружения инцидентов для раннего выявления потенциальных угроз. Постоянный мониторинг активности в сети поможет своевременно обнаруживать аномалии, подозрительные действия и атаки. Это позволит оперативно реагировать на инциденты и минимизировать возможные ущербы.

3) Реализовать систему многофакторной аутентификации для всех уровней доступа в организации. Это дополнительный слой безопасности, который требует подтверждения личности не только по паролю, но и с использованием других уникальных параметров, таких как биометрические данные или одноразовые коды. Это повысит уровень защиты от несанкционированного доступа.

4) Внедрить систему регулярного обновления и обучения персонала по вопросам безопасности информации. Это включает в себя не только обучение сотрудников базовым принципам безопасности, но и предоставление информации о последних трендах в области кибербезопасности. Обученный персонал является важным звеном в общей стратегии безопасности, и регулярные обновления помогут им оставаться впереди потенциальных угроз.

5) Провести регулярные аудиты безопасности для оценки уровня защиты и выявления новых потенциальных угроз. Аудиты помогут идентифицировать слабые места в системе безопасности, а также оценить эффективность внедренных мер и внести соответствующие коррективы в план улучшений.

6) Пересмотреть защитные решения для как персональных компьютеров, так и серверов. Укрепление средств защиты является важным этапом для обеспечения целостности и безопасности информационной среды 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.

Для более актуального анализа рекомендуется использовать более современные версии аналогичного программного обеспечения. Такие обновленные версии обычно включают в себя последние методологии и инструменты, что позволяет более точно и в полном объеме оценить состояние безопасности организации. Переход к современным решениям также способствует поддержке последних стандартов безопасности и обеспечивает более надежный анализ с точки зрения актуальных угроз и рисков.

Кроме того, обновленные версии программ могут предоставлять более усовершенствованные функции, такие как интеграция с облачными сервисами, расширенные возможности мониторинга и более точные механизмы анализа данных. Использование таких современных решений также обеспечивает лучшую совместимость с последними технологическими тенденциями и стандартами 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.