

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«МИРЭА – Российский технологический университет»**

**РТУ МИРЭА**

----------------------------------------------------------------------------------------------------

Институт кибербезопасности и цифровых технологий

Кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

----------------------------------------------------------------------------------------------------

**Отчёт по практической работе № 1.12**

По дисциплине

«Управление информационной безопасностью»

Тема: «Проведение аудита системы менеджмента информационной безопасности»

Студент Кузькин Павел Александрович

Группа ББМО-01-22

Работу проверил

Пимонов Р.В.

Москва, 2023

**Введение**

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

Результаты оценки безопасности системы представлены в файле “Кузькин\_ПА\_ББМО-01-22\_прз1.12.xps”, который можно открыть с помощью MSAT. Для удобства результаты оценки безопасности системы также были сохранены в формате pdf (название файла: “Кузькин\_ПА\_ББМО-01-22\_прз1.12\_отчёт MSAT.pdf ”).

Перейдём к анализу полученных результатов.

**Анализ результатов и разработка плана улучшений**

Первым делом дадим интерпретацию диаграмме представленной на рис. 1, а также расшифруем представленные на ней записи иностранного происхождения.

**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.

В нашем случае на диаграмме присутствует дисбаланс показателей BRP и DiDI, который означает, что есть необходимость перегруппировать инвестиций в ИТ. Иными словами, необходимо стремится к балансу.

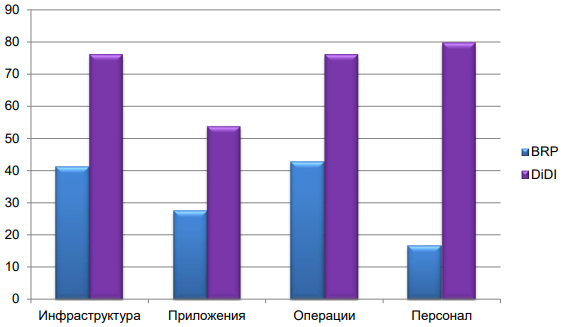


Рисунок 1 – Диаграмма, отражающая разность показателей эшелонированный защиты, упорядоченных по областям анализа

Отметим, что в данной работе проводился анализ системы безопасности организации ФГБУ «ПИЯФ» НИЦ «Курчатовский институт», следующих четырёх областей: инфраструктура, приложения, операции и персонал. Опишем поподробнее каждую из них.

1) **Инфраструктура**. Под безопасностью инфраструктуры подразумевается то, каким образом должна функционировать сеть, какие бизнес-процессы (внутренние или внешние) она должна поддерживать, как создаются и развертываются узлы и как организовать управление сетью и её обслуживание. Действенная безопасность инфраструктуры обеспечит значительные улучшения в областях сетевой защиты, реагирования на происшествия, сетевой доступности и анализа отказов. Создав надежную и понятную инфрастpуктуру и следуя ей, организация получает возможность определить области риска и разработать способы его снижения. Оценка предусматривает проверку процедур высокого уровня, которые организация может применять для снижения угрозы со стороны инфраструктуры, сосредоточившись на следующих областях безопасности, связанных с инфраструктурой:

* защита по периметру — межсетевые экраны, антивирусные программы, удаленный доступ, сегментация;
* проверка подлинности — политики паролей;
* управление и контроль — узлы управления, файлы журналов;
* рабочая станция — конфигурация сборки.

2) **Приложения**. Для полного понимания вопросов безопасности, касающихся приложений, требуются глубокие знания в области общей архитектуры приложений, а также абсолютное понимание пользовательской базы приложения. Только тогда можно приступать к определению потенциальных векторов угроз. Учитывая ограниченный масштаб данной самооценки, полный анализ архитектуры приложений и всестороннее понимание пользовательской базы невозможны. Эта оценка предназначена для обзора приложений в организации и их оценки с точки зрения безопасности и доступности. Для усовершенствования эшелонированной защиты выполняется проверка технологий, используемых в среде. Оценка предусматривает проверку процедур высокого уровня, которые организация может выполнять для снижения угрозы со стороны приложений, сосредоточившись на следующих областях безопасности, связанных с приложениями:

* развертывание и использование — механизмы повышения доступности;
* схема приложения — проверка подлинности, управление доступом, управление средствами обновления, проверка входных данных, ведение журнала и проверка;
* хранение данных и связь — шифрование, передача данных, ограничение доступа.

3) **Операции**. В этой области анализа исследуются методы, процедуры эксплуатации и рекомендации, которым следует организация, для усовершенствования эшелонированной защиты. Данная оценка предполагает проверку политик и процедур, управляющих сборками системы, сетевой документацией и использованием технологий в среде. Она также включает поддержку функций, необходимых для управления информацией и процедурами, которые используются администраторами и оперативным персоналом в данной среде. Создав понятные рабочие методики, процедуры и рекомендации и следуя им, организация может потенциально улучшить состояние эшелонированной защиты. Оценка предусматривает проверку процедур высокого уровня, которые организация может выполнять для снижения угрозы со стороны операций, сосредоточившись на следующих областях безопасности, связанных с операциями:

* среда — сборка системы, сетевая документация, поток данных приложения, архитектура приложений;
* политика безопасности — протоколы и службы, правильное использование, управление учетными записями;
* управление средствами исправления и обновления — управление исправлениями, сигнатуры вирусов;
* архивация и восстановление — архивация, хранение, проверка.

4) **Персонал**. Усилия, направленные на обеспечение безопасности, часто не включают организационные аспекты, которые важны для поддержания общей безопасности в организации. В этом разделе оценки рассматриваются внутренние процессы предприятия, определяющие корпоративную политику безопасности, процессы, связанные с персоналом, осведомленность сотрудников о безопасности и их обучение. В области анализа, связанной с персоналом, также рассматривается безопасность применительно к повседневным операциям, относящимся к назначениям и определению ролей. Оценка предусматривает проверку процедур высокого уровня, которые организация может выполнять для снижения угрозы со стороны персонала, сосредоточившись на следующих областях безопасности, связанных с персоналом:

* требования и оценки — планирование, сторонние оценки;
* политика и процедуры — кадровая политика, сторонние взаимосвязи;
* обучение и осведомленность — осведомленность о безопасности.

Результаты соответствия категорий областей анализа системы безопасности организации ФГБУ «ПИЯФ» НИЦ «Курчатовский институт» передовым методикам и рекомендациям представлены на рис. 2.

Таким образом, исходя из рис. 2, можно сделать вывод о том, какие подкатегории категорий областей анализа необходимо усовершенствовать (см. рис. 3).

Рекомендации по усовершенствованию каждой подкатегории категорий областей анализа системы безопасности организации ФГБУ «ПИЯФ» НИЦ «Курчатовский институт» представлены в файле “Кузькин\_ПА\_ББМО-01-22\_прз1.12\_отчёт MSAT.pdf ”.

Отобразим список приоритетных действий, которые необходимо совершить для того, чтобы системы безопасности организации ФГБУ «ПИЯФ» НИЦ «Курчатовский институт» соответствовала передовым методикам и рекомендациям (см. табл. 1-3).



Рисунок 2 – Сведения о соответствии подкатегорий категорий областей анализа системы безопасности организации ФГБУ «ПИЯФ» НИЦ «Курчатовский институт» передовым методикам и рекомендациям



Рисунок 3 – Приоритетность усовершенствования подкатегорий категорий областей анализа системы безопасности организации ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»

Таблица 1 – План улучшений подкатегорий категорий областей анализа системы безопасности организации ФГБУ «ПИЯФ» НИЦ «Курчатовский институт», которые имеют высокий приоритет устранения

|  |  |
| --- | --- |
| **Предмет анализа** | **Рекомендации** |
| Инфраструктура > Проверка подлинности > Пользователи с удаленным доступом | Необходимо использовать многофакторную проверку подлинности для удаленного доступа. Доступ предоставлять только тем сотрудникам, у которых существует потребность в удаленном подключении |
| Приложения > Развертывание и использование > Независимый сторонний поставщик программного обеспечения | Необходимо выполнить проверку этого открытого элемента с участием ИТ-персонала или специалиста по безопасности |
| 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. Необходимо периодически повторять эти процедуры, чтобы убедиться, что они соответствуют текущим требованиям приложения |
| Операции > Архивация и восстановление > Планирование аварийного восстановления и возобновления деятельности предприятия | Необходимо и дальше поддерживать и тестировать планы аварийного восстановления и возобновления деятельности предприятия |
| Персонал > Политика и процедуры > Сторонние взаимосвязи | Системы должны настраиваться внутренним персоналом в соответствии с проверенным образом |

Таблица 2 – План улучшений подкатегорий категорий областей анализа системы безопасности организации ФГБУ «ПИЯФ» НИЦ «Курчатовский институт», которые имеют средний приоритет устранения

|  |  |
| --- | --- |
| **Предмет анализа** | **Рекомендации** |
| Инфраструктура > Управление и контроль > Защищенная сборка | Необходимо выполнить проверку этого открытого элемента с участием ИТ-персонала или специалиста по безопасности |
| Инфраструктура > Проверка подлинности > Административные пользователи | Чтобы ещё более снизить риск взлома пароля в административных учётных записях, необходимо выполнить следующие рекомендации: 1) необходимо включить функцию истечения срока действия пароля; 2) необходимо блокировать учётную запись после 7-10 попыток неправильного ввода пароля; 3) необходимо ввести журнал системы. |
| Инфраструктура > Защита по периметру > Удаленный доступ | Необходимо выполнить проверку этого открытого элемента с участием ИТ-персонала или специалиста по безопасности |
| Приложения > Схема приложения > Методологии разработки систем безопасности программного обеспечения | Необходимо и дальше обучать разработчиков принципам разработки систем безопасности программного обеспечения |
| Инфраструктура > Защита по периметру > Система определения вторжения (IDS) | Необходимо и дальше продолжать практику развёртывания сетевой системы определения вторжения. Необходимо следить за регулярным обновлением сигнатур вирусов, а также изучать технологии предотвращения вторжения |

Таблица 3 – План улучшений подкатегорий категорий областей анализа системы безопасности организации ФГБУ «ПИЯФ» НИЦ «Курчатовский институт», которые имеют низкий приоритет устранения

|  |  |
| --- | --- |
| **Предмет анализа** | **Рекомендации** |
| Операции > Среда > Узел управления - Серверы | Необходимо использовать 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 по умолчанию |
| Операции > Политика безопасности > Правильное использование | Все сотрудники и клиенты, использующие корпоративные ресурсы, должны быть ознакомлены с этими политиками. Необходимо разместить политики в корпоративной интрасети. Кроме того, необходимо знакомить с ними всех новых сотрудников при приёме их на работу |
| Операции > Архивация и восстановление > Архивация | Необходимо провести аудит механизмов архивации и обеспечить регулярное архивирование всех важных активов. Необходимо периодически проверять работоспособность функций восстановления, чтобы контролировать возможность восстановления с резервных носителей |
| Инфраструктура > Защита по периметру > Антивирус - Настольные компьютеры | Необходимо реализовать политику, в соответствии с которой пользователям необходимо регулярно обновлять сигнатуры вирусов. Также необходимо установить клиента антивирусной программы с использованием настроек для рабочей станции по умолчанию |