МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА – Российский технологический университет»
РТУ МИРЭА

ИКБ направление «Кибербразведка и противодействие угрозам с применением технологий искусственного интеллекта» 10.04.01

Кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

Проведение аудита системы информационной безопасности

по дисциплине

«Управление информационной безопасностью»

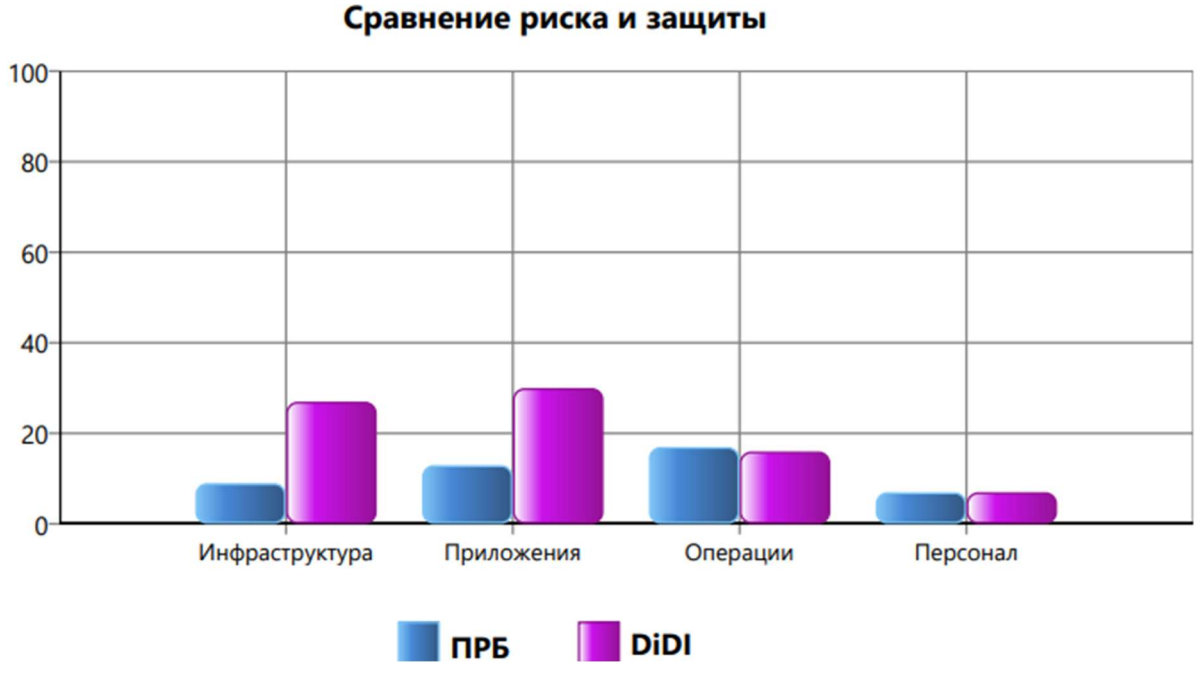
Группа:
ББМО-02-22
Выполнил:
Щелкушкин Е.Р.

Проверил:
Пимонов Р.В.

Москва 2023

Оценка предназначена для выявления риска для бизнеса организации и определения мер безопасности, предпринимаемых для снижения риска. Сосредоточение внимания на общих проблемах этого сегмента рынка позволило разработать вопросы для обеспечения высококачественной оценки рисков, которые представляют для ведения бизнеса используемые технологии, процессы и персонал.

Профиль риска для бизнеса (ПРБ) создается средством на основе серии предварительных вопросов о бизнес-модели компании, и тем самым измеряется риск для бизнеса, с которым компания сталкивается в данной отрасли и в условиях выбранной бизнес-модели. Вторая группа вопросов предлагается с целью составления списка мер безопасности, которые со временем должны быть предприняты компанией. В целом, эти меры безопасности формируют уровни защиты, обеспечивающие более серьезную защиту от угроз безопасности и конкретных уязвимых мест в системе. Каждый уровень способствует укреплению комбинированной стратегии эшелонированной защиты. В сумме это рассматривается как индекс эшелонированной защиты (DiDI). Затем ПРБ и DiDI сравниваются для измерения распределения риска по всем областям анализа — инфраструктуре, приложениям, операциям, персоналу.



Посмотрим присвоенные защитным мерам моей компании рейтинги.

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

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

реагирование и создание отчетов

Защищенная сборка

Физическая безопасность

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

Резервные носители

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

В следующих областях существует недостаток передовых методик, и для повышения безопасности среды они требуют усовершенствования.

Высокий приоритет	Средний приоритет	Низкий приоритет
• Удаленный доступ • Шифрование • Оценки безопасности • Сегментация • Защищенная сборка	• Политики паролей • Обучение в области безопасности • Правила и фильтры межсетевого экрана • Антивирус • Утилизация данных	• Классификация данных • Протоколы и службы • Проверка подлинности • Файлы журнала

Также представлены рекомендации.

Список приоритетных действий	
Предмет анализа	**Рекомендация**
Высокий приоритет	
Инфраструктура > Защита по периметру > Удаленный доступ	Разверните сеть VPN, чтобы обеспечить подключение пользователей с удаленным доступом на основе технологий IP-безопасности (IPSec), SSL (Secure Sockets Layer) и SSH (Secure Shell). Разверните подключение между узлами на основе технологии IPSec. Настройте списки доступа к сети и списки доступа пользователей для ограничения доступа к необходимым корпоративным ресурсам.
Персонал > Требования и оценки > Оценки безопасности	Независимые оценки очень полезны для любой организации.

	Обязательно организуйте проведение регулярных независимых оценок. В случае значительного изменения схемы и конфигурации существующей среды запланируйте и при первой возможности проведите оценку системы безопасности.
Инфраструктура > Защита по периметру > Сегментация	Убедитесь в наличии межсетевого экрана, сегментирования и систем определения вторжения для защиты инфраструктуры компании от атак из Интернета.
Инфраструктура > Управление и контроль > Защищенная сборка	Рассмотрите необходимость отказа от использования программного обеспечения удаленного контроля/управления для минимизации риска нарушения безопасности систем.
Средний приоритет	
Приложения > Схема приложения > Политики паролей	Рассмотрите необходимость распространения политики ограничения срока действия паролей на все внешние приложения и основные внутренние приложения.
Персонал > Обучение и осведомленность > Обучение в области безопасности	Ролевое и непрерывное обучение - это неотъемлемый элемент, обеспечивающий понимание всеми служащими того, что от них требуется и как они должны выполнять эти требования. Продолжайте обучение сотрудников на всех уровнях в организации и по всем аспектам безопасности в зависимости от требований к должности.
Инфраструктура > Защита по периметру > Правила и фильтры межсетевого экрана	Продолжайте развертывать межсетевые экраны или другие элементы управления доступом на сетевом уровне в каждом офисе и регулярно проверяйте их правильную работу.
Операции > Политика безопасности > Утилизация данных	Продолжайте реализовывать процедуры удаления данных
Низкий приоритет	
Операции > Политика безопасности > Классификация данных	Для всех операций шифрования используйте алгоритмы шифрования, применяемые в отрасли.
Операции > Политика безопасности > Протоколы и службы	Проведите аудит документации, выясните, какие протоколы и службы разрешены, и убедитесь, что документация соответствует настроенным спискам управления доступом и правилам межсетевого экрана на соответствующих устройствах. Опубликуйте эти сведения в корпоративной интрасети и реализуйте политики, регулирующие внесение изменений в правила.
Приложения > Схема приложения > Проверка подлинности	Чтобы еще более снизить риск взлома пароля во внешних приложениях, выполните следующие рекомендации: + Истечение срока действия пароля + Блокировка учетной записи после хотя бы 10 попыток неправильного ввода пароля + Ведение журнала системы
Операции > Архивация и восстановление > Файлы журнала	Продолжайте ведение журнала на централизованном сервере журналов.

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). Важно отметить, что нулевое значение в данном случае невозможно, так как деловая деятельность сама по себе подразумевает наличие какогото уровня риска. Кроме того, важно

понимать, что существуют определенные аспекты ведения бизнеса, для которых отсутствует прямая стратегия снижения риска.

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.

На первый взгляд, может показаться, что низкий показатель ПРБ и высокий показатель DiDI - это хороший результат, но это не всегда так. Масштаб данной самооценки не предусматривает все факторы, которые следует принять во внимание. При значительной диспропорции между показателями ПРБ и DiDI в конкретной области анализа рекомендуется изучить ее (AoA) как можно глубже. При анализе результатов важно учитывать индивидуальные показатели, как для ПРБ, так и DiDI, по отношению друг к другу. Стабильная среда, вероятно, будет представлена сравнительно одинаковыми показателями во всех областях. Разница между показателями DiDI - это явный признак того, что общая стратегия безопасности базируется на одной методике снижения риска. Если стратегия обеспечения безопасности не уравновешивает аспекты, связанные с персоналом, процессами и технологиями, то для среды существует вероятность повышенной уязвимости для злонамеренных атак.