



МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования

«МИРЭА – Российский технологический университет»
РТУ МИРЭА

Институт комплексной безопасности и специального приборостроения
КБ-4 «Интеллектуальные системы информационной безопасности»

Отчёт
по практической работе
по дисциплине «Управление информационной
безопасностью»
на тему: «Проведение аудита системы менеджмента
информационной безопасности»

Выполнил студент:
Группы: ББМО-02-22
Исаев А.М.

Проверил: Пимонов Р.В.

Москва 2022

Введение

В качестве основной цели выполнения практики является проведение аудита и оценка системы безопасности ГК «ИННОХЕТ»

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.

Уровень безопасности - это величина измерения способностей организации к эффективному использованию инструментов, доступных для создания стабильного уровня безопасности по многим дисциплинам.

В качестве обзора областей анализа можно сделать вывод что уровень безопасности соответствует передовым методикам.

Области анализа	Сравнение риска и защиты	уровень безопасности
Персонал	●	●
Операции	●	●
Приложения	●	●
Инфраструктура	●	●

Рисунок 1 – сравнительная таблица уровней безопасности и сравнения риска и защиты

Профиль риска для бизнеса и индекс эшелонированной защиты Сводный отчет



Рисунок 2 – диаграмма сравнения ПРБ и DiDI «ГК ИННОХЕТ»

В нашем случае присутствует дисбаланс показателей ПРБ и DiDL в колонках «инфраструктура», «операции» и «персонал», существует необходимость добиться баланса

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 ее обслуживание. Действительная безопасность инфраструктуры обеспечит значительные улучшения в областях сетевой защиты, реагирования на происшествия, сетевой доступности и анализа отказов. Создав надежную и понятную инфраструктуру 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.

Ниже представлена сравнительная таблица, применимая для «ГК Иннохет»

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	●

Рисунок 3 – Сравнительная оценка «Инфраструктура» для «ГК Иннохет»

В качестве приоритетных действий необходимо:

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	Необходимо реализовать политику, в рамках которой необходимо проводить периодические проверки настроек по умолчанию для межсетевого экрана, чтобы стали возможны изменения в используемых приложениях или службах.
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.
Инфраструктура> Проверка подлинности> Административные пользователи	Рассмотрите необходимость внедрения дополнительного фактора проверки подлинности, тем самым значительно снижается риск несанкционированного доступа
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.

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 приступить 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

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	●

Рисунок 4 – Сравнительная оценка «Приложения» для «ГК Иннохет»

В качестве приоритетных действий необходимо:

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.
Приложения> Развертывание и использование> Восстановление приложений и данных	Все важные бизнес-приложения следует периодически проверять на безопасность, регулярно архивировать и полностью документировать. Кроме этого, необходимо предусмотреть непредвиденные расходы, если эти меры не помогут.
Приложения> Схема приложения> Методологии разработки систем безопасности программного обеспечения	Продолжайте использовать методологии разработки систем безопасности программного обеспечения.
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.

Операции

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:

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 5 – Сравнительная оценка «Операции» для «ГК Иннохет»

В качестве приоритетных действий необходимо:

Операции> Архивация и восстановление> Планирование аварийного восстановления и возобновления деятельности предприятия	Продолжайте поддерживать и тестировать планы аварийного восстановления и возобновления деятельности предприятия.
Операции> Среда> Узел управления -Серверы	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> Среда> Узел управления -Сетевые устройства	Все важные бизнес-приложения следует периодически проверять на безопасность, регулярно архивировать и полностью документировать. Кроме этого, необходимо предусмотреть непредвиденные расходы, если эти меры не помогут.
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.

Персонал

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:

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 6 – Сравнительная оценка «Персонал» для «ГК
Иннохет»

В качестве приоритетных действий необходимо:

Персонал> Политика и процедуры> Сторонние взаимосвязи	Системы должны настраиваться внутренним персоналом в соответствии с проверенным образом.
-------------------------------------------------------	------------------------------------------------------------------------------------------