Анализ состояния информационной безопасности компании

Комплексный проект по оценке текущего уровня защищённости информационных активов: от организационных регламентов до технической инфраструктуры. По результатам работ компания получает структурированную оценку действующих мер ИБ, перечень выявленных разрывов и поэтапный план улучшений.

Снижение рисков утечки данных

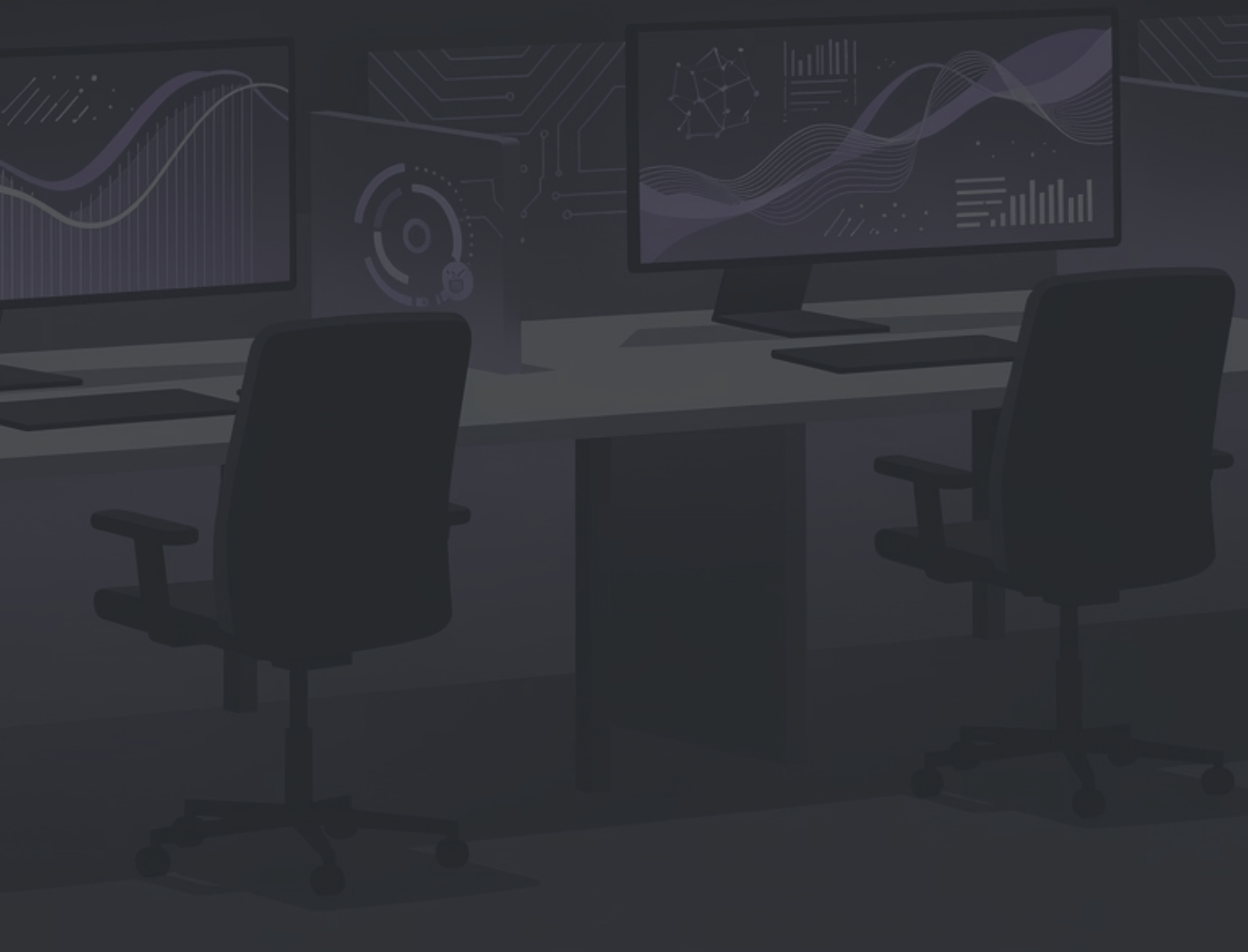
Выявление уязвимых каналов передачи информации и формирование мер контроля

Управляемость процессов ИБ

Оценка зрелости организационного контура и актуальности нормативной базы

Защищённость инфраструктуры

Обследование технических конфигураций и рекомендации по харденингу



Этапы выполнения работ

Работы выполняются в три последовательных этапа. Каждый этап завершается передачей отчётных материалов и рекомендаций по соответствующему направлению.

1	2	3
Анализ регламентов и организационных мер ИБ Оценка полноты, актуальности и согласованности политик, регламентов, инструкций и стандартов. Подготовка рекомендаций по доработке документов и чек-листа недостающих регламентов, которые нужно разработать или формализовать. **Результат:** отчёт по организационному контуру ИБ, перечень разрывов, рекомендации, чек-лист недостающих политик.	**Анализ каналов утечки информации** Оценка основных каналов утечки: удалённый доступ, электронная почта, мессенджеры. Анализ ограничений, средств контроля, пользовательских практик и сценариев несанкционированной передачи данных. **Результат:** отчёт по каналам утечек, карта рисков, рекомендации по организационным и техническим мерам защиты.	**Анализ ИТ-инфраструктуры и харденинг** Обследование инфраструктуры: управление уязвимостями, настройка защитных механизмов, управление доступом, обновления и резервное копирование. Формирование приоритизированного плана устранения недостатков. **Результат:** технический отчёт, перечень замечаний, рекомендации по харденингу и roadmap первоочередных мероприятий.

Подход к выполнению работ

Работы выполняются поэтапно с проведением интервью, анализом имеющейся документации, изучением применяемых процессов и выборочной оценкой технических настроек. Приоритет рекомендаций определяется на основе **риск-ориентированного подхода** с учётом критичности активов, вероятности эксплуатации недостатков и потенциального влияния на бизнес-процессы компании.

Формат взаимодействия

- Удалённое взаимодействие и анализ документов
- Анализ конфигурационных материалов
- Дистанционные интервью с ответственными сотрудниками
- Рабочие сессии с командой заказчика

Итоговые материалы

- Отчётные материалы по каждому из трёх этапов
- Консолидированный перечень выявленных замечаний
- Практические рекомендации по повышению уровня ИБ
- Единая дорожная карта реализации рекомендаций с разбивкой на первоочередные, среднесрочные и стратегические меры

Сроки, состав участников и стоимость работ определяются после уточнения масштаба инфраструктуры и текущего состояния процессов ИБ.

Дорожная карта реализации рекомендаций

По завершении всех этапов формируется единая дорожная карта с чёткой приоритизацией мероприятий. Меры разбиваются на три горизонта в зависимости от критичности и сложности реализации.

1

Первоочередные меры

Устранение критичных уязвимостей, закрытие наиболее опасных каналов утечки, формализация ключевых регламентов

2

Среднесрочные меры

Доработка нормативной базы, усиление технических средств контроля, выстраивание процессов управления доступом и мониторинга

3

Стратегические меры

Повышение зрелости ИБ-функции, внедрение DRP/BCP, построение системного управления техническими рисками

Владимир Бондарев

> Руководитель-практик с опытом уровня ИТ-директора.

Более 25 лет я помогаю бизнесу выстраивать ИТ и информационную безопасность как управляемую функцию: с понятной ответственностью, надежной инфраструктурой, зрелыми процессами и командами, которые работают на результат.

Я рассматриваю ИТ не как статью расходов, а как инструмент устойчивости и конкурентоспособности: быстрее, надежнее, безопаснее.

Мой принцип - не усложнять систему ради системы. Сначала понять бизнес-задачу и реальную ответственность, затем выбрать меры, которые команда сможет внедрить и поддерживать.

25+ лет в ИТ и ИБ

Опыт уровня ИТ-директора в крупных корпоративных средах.

Стратегия и практика

Управленческое видение и глубокое понимание технического контура для реалистичных планов внедрения.

Контакты

Telegram: @vbondarev
Email: contact [at] vbondarev.ru
Сайт: vbondarev.ru