AKTIV.
CONSULTING

Профильные специалисты по информационной безопасности и бизнес-процессам

Оглавление

Консалтинг — инструмент эффективного управления изменениям

Консалтинг позволяет повысить результативность бизнеса за счет:

- Привлечения необходимых компетенций для реализации проекта и разгрузки внутренних специалистов
- Использования лучших мировых и российских практик
- Обеспечения внешней независимой оценки бизнес-процессов организации

Консалтинг в сфере ИБ позволяет:

- Трансформировать информационную безопасность в полноценную бизнес-функцию
- Найти точки развития для направления ИБ, позволяющие эффективно реализовать бизнес-стратегию организации
- Выстроить диалог между ИБ-подразделением и бизнесом
- Разработать понятные бизнесу метрики оценки эффективности функции ИБ

Формируем диалог между службой ИБ и менеджментом

Руководителям службы ИБ	Руководителям бизнеса
Управление функцией ИБ: • Разработка стратегии развития ИБ • Внедрение и отладка процессов ИБ • Аутсорсинг руководства проектами ИБ	Трансформация ИБ в бизнес-функцию: • Разработка блока ИБ в стратегии организации • Оценка эффективности функции ИБ • Внедрение системы KPI для функции ИБ • Оценка операционных и киберрисков • Оценка безопасности бизнес-процессов • Бизнес-аналитика по вопросам ИБ • Консультации для бизнеса по вопросам ИБ
Обеспечение ИБ: • Технические консультации по ИБ и аутсорсинг компетенций • Анализ защищенности и проведение пентестов • Разработка политик и регламентов по ИБ	
Соответствие требованиям ИБ: • Разработка дорожной карты по ИБ-комплаенсу • Оценка соответствия требованиям ИБ • Внедрение требований по ИБ	

Консалтинговые услуги по ИБ

ИБ-комплаенс	• Оценка соответствия требованиям ИБ-стандартов и разработка дорожной карты внедрения • Разработка и внедрение требований по ИБ к экспортируемым цифровым продуктам
Управление функцией ИБ	• Постановка функции и процессов ИБ в соответствии с комплаенс- и бизнес-целями организации • Разработка стратегии и программ развития функции ИБ в средней и долгосрочной перспективах
Защита ИС и инфраструктуры	• Проведение анализа защищенности и тестов на проникновение • Разработка требований по ИБ к автоматизированным системам управления предприятия (АСУП)
Киберриски	• Проектирование и постановка процессов управления киберрисками • Создание адаптированной методологии по оценке киберрисков, включая математическую модель
Безопасная разработка ПО	• Проектирование и внедрение процесса безопасной разработки программного обеспечения • Проведение статического и динамического анализа уязвимостей ПО
Конфиденциальная информация	• Постановка процессов по защите конфиденциальной информации, включая коммерческую тайну • Внедрение процессов защиты персональных данных в соответствии с требованиями регуляторики

Для финансовых организаций

Консультанты AKTIV.CONSULTING оказывают комплексные услуги по информационной безопасности для финансовых организаций, среди которых:

01

Приведение к соответствию требованиям регуляторов (в том числе: 683-П, 747-П, 719-П, 757-П, ГОСТ Р 57580, 152-ФЗ)

Мы предлагаем комплексный подход, позволяющий существенно сэкономить финансовые и временные ресурсы за счет кросс-регуляторного внедрения требований различных нормативных документов, законодательных актов и стандартов.

02

Внедрение процессов управления операционными и киберрисками (в соответствии с 716-П, 779-П, 787-П)

Наша экспертиза и компетенции в области оценки операционных и киберрисков позволяют сформировать продуктивную систему внутреннего контроля и управления рисками, отвечающую целям вашей компании.

03

Обеспечение безопасности финансовых информационных систем:

- проведение регулярного анализа защищенности и тестов на проникновение,
- разработка требований по ИБ для автоматизированных финансовых систем (АБС, ДБО, ЛК и т.п.),
- внедрение процесса безопасной разработки прикладного ПО,
- оценка соответствия программного обеспечения по требованиям ОУД4.

Знание специфики финансовой сферы и реальный опыт позволяют комплексно подходить к вопросу обеспечения ИБ и подбирать оптимальный набор инструментов для всесторонней проверки безопасности информационных систем.

Пример проекта для финансовых организаций

Некредитная финансовая организация из ТОП-3

Внедрение требований ГОСТ Р 57580 и 757-П

Срок реализации 9 месяцев

1 этап Обоснование

- определение целей и задач проекта
- разработка обоснования

→ принятие решения о реализации проекта

10 рабочих дней

2 этап Аудит

- оценка соответствия требованиям
- GAP-анализ
- разработка рекомендаций

→ рекомендации по реализации требований

60 рабочих дней

3 этап Дорожная карта

- приоритезация организационных и технических мер
- разработка плана перехода

→ утвержденная дорожная карта

15 рабочих дней

4 этап Внедрение

- разработка ОРД и внедрение процессов
- сопровождение внедрения технических мер

→ соответствие регуляторным требованиям

90 рабочих дней

5 этап Регулярный пентест

- проведение внешних и внутренних тестов на проникновение

→ отчет с рекомендациями по устранению уязвимостей

20 рабочих дней

Результат: подтверждение третьему уровню соответствия ГОСТ Р 57580.1-2017

Bonus: рекомендации по достижению четвертого уровня соответствия и сопровождение проверок ЦБ

Для защиты АСУ ТП и объектов КИИ

Консультанты AKTIV.CONSULTING оказывают комплексные услуги по обеспечению защиты АСУ ТП и ЗО КИИ, среди которых:

01

Приведение к соответствию требованиям регуляторов (Приказы №367, №368, №31, №235, Указы №250, №166 и 187-ФЗ)

Наши консультанты на основе своего практического опыта по реализации требований регуляторов в АСУ ТП и ЗО КИИ разработали методологию, объединяющую требования регуляторов, что позволяет комплексно подойти к вопросу обеспечения информационной безопасности и создать реально работающую систему защиты информации.

02

Внедрение процесса безопасной разработки ПО (Приказ ФСТЭК РФ №239)

Практический опыт внедрения процесса БРПО в ЗО КИИ позволяет нам подходить к реализации проектов, учитывая требования регулятора, бизнес-цели организации, существующие процессы, а также ее технические, временные и другие ресурсные ограничения.

03

Защита автоматизированных систем управления технологическими процессами (АСУ ТП):

- проведение анализа защищенности и тестов на проникновение,
- разработка требований по ИБ для АСУ ТП на этапе проектирования,
- обеспечение защиты АСУ ТП, в том числе в соответствии с национальными и международными стандартами.

Мы практикуем бережный подход, направленный не только на достижение целевого результата, но и на сохранение сложившейся внутри предприятия практики производства. Опыт реализации проектов по защите АСУ ТП позволяет нам предлагать те способы, которые будут максимально эффективны для ИТ-инфраструктуры вашего предприятия.

Пример проекта по защите АСУ ТП

Сталелитейное предприятие

Обеспечение безопасности в соответствии с требованиями Приказа №31 ФСТЭК РФ

Срок реализации 4 месяца

1 этап
Обоснование

- определение целей и задач проекта
- разработка обоснования

→ принятие решения о реализации проекта

10 рабочих дней

2 этап
Аудит

- GAP-анализ
- классификация АСУ ТП
- модель угроз
- требования к системе защиты

→ требования к системе обеспечения ИБ в АСУ ТП

30 рабочих дней

3 этап
Разработка

- проектирование системы защиты
- выявление уязвимостей
- разработка политики ИБ

→ организационные и технические мероприятия

40 рабочих дней

4 этап
Внедрение

- проектная документация
- разделы ИБ в эксплуатационной документации
- осведомленность персонала

→ внедрение мероприятий ИБ в требуемом объеме

30 рабочих дней

5 этап
Контроль

- проверка полноты и достаточности внедренных мероприятий

→ положительное заключение

10 рабочих дней

Результат: внедренная система информационной безопасности АСУ ТП в соответствии с требованиями Приказа №31 ФСТЭК РФ

Для разработчиков прикладного ПО и СЗИ

01

Проектирование и внедрение процесса безопасной разработки ПО (БРПО)

Наши специалисты спроектируют процесс безопасной разработки и подготовят проект по его внедрению, включая разработку ТЭО и дорожной карты. Консультанты также помогут обеспечить реализацию организационных и технических мер, проведут контрольные мероприятия для проверки соответствия целевому состоянию.

02

Проведение независимой оценки процессов разработки ПО

Внешняя независимая оценка процессов создания ПО позволит найти точки оптимизации за счет внедрения передовых практик и технологий безопасной разработки, а также позволит выстроить сквозные процессы и качественный диалог между бизнесом, разработчиками, ИТ- и ИБ-подразделениями.

03

Разработка требований по ИБ к информационным системам

Наши специалисты разработают техническое задание по ИБ к создаваемым информационным системам, ориентируясь на сценарии их использования, актуальную модель угроз и требования регуляторов.

04

Проведение анализа уязвимостей и тестов на проникновение

Наш практический опыт использования технических средств позволит подобрать оптимальные способы проверки кода и проведения пентестов, регулярность и своевременность которых обеспечит значительное снижение рисков информационной безопасности и операционных рисков в целом.

05

Приведение к соответствию требованиям регуляторов по БРПО

Собственная уникальная методология позволит сконфигурировать проект по внедрению БРПО, а также целевое состояние процесса безопасной разработки с учетом регуляторных требований, международных и отраслевых стандартов. При этом учитываются не только цели комплаенса, но и бизнес-потребности организации.

Пример проекта по внедрению БРПО

Разработчик АИС для субъектов КИИ

Выполнение требований Приказа ФСТЭК РФ №239

Срок реализации 4 месяца

1 этап Обоснование

- определение целей и задач проекта
- разработка обоснования

→ принятие решения о реализации проекта

10 рабочих дней

2 этап Аудит

- обследование процессов разработки
- формирование целевого состояния БРПО
- GAP-анализ

→ рекомендации по внедряемым процессам

20 рабочих дней

3 этап Дорожная карта

- приоритезация организационных и технических мер
- разработка плана перехода

→ утвержденная дорожная карта

15 рабочих дней

4 этап Внедрение

- организационные меры (ОРД, ЛНА, обучение)
- технические меры (SAST, DAST, Fuzzing)

→ функционирующие процессы БРПО

30 рабочих дней

5 этап Контроль

- проверка полноты и достаточности внедренных мероприятий

→ свидетельства функционирования процессов БРПО

5 рабочих дней

Результат: Подтверждение соответствия требованиям Приказа ФСТЭК РФ №239, относящихся к использованию прикладного ПО на объектах ЗО КИИ.

Почему выбирают AKTIV.CONSULTING?

Сокращаем время и затраты на внедрение информационной безопасности как полноценной бизнес-функции за счет уникальной методологии и компетенций.

Гарантируем быстрый и прозрачный расчет стоимости. Предлагаем услуги, оптимально сочетающие цену и качество, а также соизмеримые по стоимости с получаемыми выгодами.

Практикуем гибкий подход. Учитываем реальные потребности клиентов, зрелость ваших бизнес-процессов, имеющиеся бюджетные, временные и ресурсные ограничения.

Обладаем многолетним опытом работы в области ИБ. Опираемся на лучшие мировые и отраслевые практики. Эксперты AKTIV.CONSULTING принимают участие в рабочих группах и комитетах по стандартизации.

Приносим измеримый плановый бизнес-результат. Для оценки результатов проекта используем метрики, понятные бизнесу.

Дегустационная консультация

Мы разделяем мнение, что самый ценный ресурс любого специалиста — это время, поэтому приглашаем вас на полноценную бесплатную консультацию по заранее обозначенным вами вопросам.

По итогам консультации вы получите:

- Сформулированные или уточненные задачи ИБ-подразделения с оценкой необходимых ресурсов для их реализации.
- Верхнеуровневый перечень возможных действий, включая организационные и технические меры, для реализации поставленных задач.

Формат проведения предполагает личное общение в онлайн или офлайн формате на протяжении 2–3 часов.

Для достижения максимальной эффективности мы вместе предварительно сформулируем тему и ожидаемый результат, определим необходимый состав участников с обеих сторон.

Для заказа дегустационной консультации необходимо связаться с Олегом Симаковым, руководителем направления по работе с клиентами ACTIV.CONSULTING
simakov@aktiv.consulting

Наша команда

Анастасия Харыбина

Руководитель AKTIV.CONSULTING
Председатель Ассоциации АБИСС

Олег Симаков

Руководитель направления
по работе с клиентами

Александр Моисеев

Ведущий консультант по
информационной безопасности

Анастасия Николаева

Ведущий консультант по
информационной безопасности

AKTIV.CONSULTING — бизнес-направление компании «Актив», специализирующееся на оказании услуг консалтинга и аудита в области информационной безопасности. Компания «Актив» является на 100% российской организацией, имеет все необходимые лицензии ФСТЭК РФ и ФСБ РФ.

Команда AKTIV.CONSUALTING — консультанты и аудиторы по информационной безопасности, обладающие профессиональной экспертизой в вопросах построения систем защиты информации, проведения аудита безопасности и анализа соответствия стандартам.

www.aktiv.consulting
info@aktiv.consulting
+7 495 925-77-90