F6

Sphere

Обзор подписки

Подписка на услуги ИБ от ведущих экспертов компании F6

Неудобства классического подхода к приобретению услуг

Непредсказуемость на этапе бюджетирования

Компаниям сложно заранее понять, какие услуги ИБ понадобятся в ближайшие 1–3 года. Ещё сложнее — точно оценить их стоимость на фоне сложно прогнозируемого рынка

Невозможность перераспределения приоритетов

Утверждённый бюджет не учитывает срочные задачи в ИБ. В итоге — либо сложное перераспределение средств, либо отказ от нужных решений. Оба варианта снижают операционную гибкость бизнеса

Бюрократия

Чтобы получить нужную услугу, необходимо проходить длинный путь: пресейл-этапы, юридические согласования. Всё это занимает время и тормозит запуск работ

Проблемы в процессе коммуникации

Из-за большого числа разных подрядчиков, а иногда и при взаимодействии с одним поставщиком, приходится заново погружать новых людей в контекст и повторно объяснять одни и те же задачи

«Мы давно работаем в сфере ИБ и видим, сколько организационных сложностей возникает при реализации разовых проектов. Поэтому мы создали подписку Sphere — формат с быстрым доступом к нашей экспертизе, приоритетной поддержкой и фокусом на актуальных задачах защиты цифровых активов».

Александр Соколов
Директор сервисного блока компании F6

Преимущества формата Sphere

Sphere — это формат подписки на услуги ИБ по пакету часов

OPEX → CAPEX

Модель позволяет перевести затраты на ИБ из операционных в капитальные. При этом нет необходимости каждый раз проходить сложный бюрократический цикл

Используйте по необходимости

Часы по подписке можно расходовать на услуги, которые нужны вашей компании именно в тот момент, когда возникает потребность

Быстро и удобно

Все договорные процессы уже пройдены, поэтому запуск работ занимает минимум времени. Фокус — на результате, а не на согласованиях

Спокойное планирование

Вы заранее согласовываете с нашей командой план работ на год, но при необходимости можете менять приоритеты, состав и очередность услуг

Постоянная команда

С вами работают персональный менеджер и закреплённые специалисты. Они знают специфику вашей компании, поэтому коммуникация проще, а задачи решаются быстрее

Консультационная поддержка

В рамках пакета вы получаете не только услуги, но и экспертные консультации по вопросам ИБ

Направления услуг, входящих в подписку

Аудит и консалтинг

Технический аудит и оценка соответствия

Реагирование и криминалистика

Реагирование на инциденты, поиск следов компрометации

Расследования киберпреступлений

Поиск злоумышленников и помощь в решении сложных ситуаций

Центр обучения

Курсы и практические занятия по направлениям ИБ

Полный перечень услуг

Ниже приведен список услуг, входящих в подписку. По взаимному согласованию вы можете обратиться за услугами, не входящими в стандартный перечень, например, **Purple Teaming**, **Red Teaming** и др.

Аудит и консалтинг

Услуга	Описание	Подробнее
Внешнее тестирование на проникновение	Обнаружение недостатков и уязвимостей доступной из интернета сетевой инфраструктуры компании в двух форматах. «Тестирование на проникновение» на практике покажет наиболее критичные проблемы безопасности и вероятные векторы атаки. «Анализ защищённости» позволит провести инвентаризацию уязвимостей различного уровня риска на наиболее важных опубликованных ресурсах.	
Внутреннее тестирование на проникновение	Поиск недостатков и уязвимостей во внутренней корпоративной сети в двух форматах. «Тестирование на проникновение» показывает возможности внутреннего атакующего по компрометации информационных систем, эскалации привилегий в локальной сети и получению доступа к чувствительной информации. «Анализ защищённости» предназначен для поиска всевозможных уязвимостей на ограниченном количестве критичных активов.	
Социотехническое тестирование	Практическое тестирование осведомлённости сотрудников путем имитации рассылки фишинговых писем. Поможет оценить возможные риски реализации атак с участием вашего персонала.	
Тестирование беспроводных сетей	Оценка уровня защищённости точек доступа Wi-Fi (рассматриваются диапазоны 2,4 и 5 ГГц). Анализ потенциально «слабых мест» в инфраструктуре беспроводных сетей, а также исследование возможностей дальнейшего развития атаки на локальную сеть.	
Тестирование веб-приложений	Поиск возможных известных уязвимостей веб-приложений. Своевременное устранение подобных проблем позволит избежать утечки чувствительной информации, обрабатываемой приложениями, а также массы иных связанных с ними рисков.	
Тестирование мобильных приложений	Обнаружение недостатков безопасности мобильных приложений. Выявляются уязвимости, способные повлечь нелегитимный доступ к обрабатываемой и хранимой приложениями информации, а также полный или частичный контроль над ними.	

Услуга	Описание	Подробнее
Тестирование смарт-контрактов	Выявление и попытки эксплуатации уязвимостей, которые потенциально приводят к хищению средств, нарушению логики работы контракта и прочим воздействиям, оказывающим негативное влияние на ваш бизнес.	
Проверка устранения выявленных в результате оказания услуги недостатков	Может быть реализована после устранения вами недостатков, обнаруженных в ходе проведённого нами технического аудита. Распространяется на внешнее и внутреннее тестирование, анализ приложений и смарт-контрактов.	
Аудит по 152-ФЗ «О персональных данных» и подзаконным НПА	Выявление недостатков в процессах обработки и защиты персональных данных с позиции законодательных требований. Поможет определить потенциальные угрозы для информационных систем персональных данных с учетом актуальных нарушителей и сценариев атак, а также обновить организационно-распорядительную документацию.	
Услуги в рамках законодательства в области КИИ	Помогут сформировать перечень объектов КИИ, провести их категорирование, выявить актуальные угрозы, привести в соответствие требованиям законодательства принимаемые меры защиты информации, разработать или доработать документацию.	
Оценка соответствия требованиям Банка России	Аудит по требованиям ГОСТ Р 57580.1-2017 и актуальных положений Центрального Банка, регламентирующих защиту информации.	
Оценка соответствия лучшим практикам по ИБ	Комплексная оценка системы обеспечения ИБ в соответствии с международными стандартами и лучшими практиками. Вариативность предоставляемой услуги позволяет сформировать набор задач, решаемых в рамках аудита, под цели и потребности вашей организации.	
Аудит по ФЗ-98 «О коммерческой тайне»	Выявление недостатков текущей системы защиты для введения юридически значимого режима коммерческой тайны. Услуга поможет легитимизировать потенциальное судебное взаимодействие с субъектами, допустившими утечку конфиденциальной информации, и тем самым снизить её риски.	
Консультирование	Развернутые ответы на различные вопросы, связанные с лучшими практиками и законодательными требованиями в области ИБ.	

Работа с инцидентами и компьютерная криминалистика

Услуга	Описание	Подробнее
Реагирование на инцидент	Полный цикл реагирования от специалистов с уникальной экспертизой для компании любой отрасли: выявление угроз, ликвидация, разработка практических рекомендаций.	
Выявление следов компрометации	Комплексная проверка всей ИТ-инфраструктуры для обнаружения признаков несанкционированного доступа, нелегитимной активности и скрытых угроз, которые могут длительное время оставаться незамеченными. При обнаружении угроз позволяет своевременно локализовать их и, если возможно, установить причины возникновения.	
Цифровая криминалистика	Криминалистический анализ любых электронных устройств, восстановление удалённых и скрытых данных, анализ вредоносного ПО. Выявление обстоятельств произошедшего инцидента и формирование доказательственной базы в виде отчётов и заключений, оформленных в соответствии с законодательными требованиями.	
Исследование инцидентов ИБ	Услуга поможет выяснить, кто стоит за атакой, и привлечь виновных к ответственности. Оказывается поддержка в расследовании любых киберпреступлений: хищение данных, атаки с использованием ВПО, финансовые преступления, репутационный ущерб, нарушение интеллектуальных прав. В ходе услуги устанавливается подробный профиль злоумышленника и оформляется независимая экспертиза для передачи её в правоохранительные органы. Также возможно консультирование по взаимодействию с регуляторами, судебными инстанциями и другими государственными структурами.	

Обучение

Курс	Описание
Анализ данных киберразведки	Изучение методов сбора информации о киберугрозах и обогащения процессов кибербезопасности данными Threat Intelligence для эффективного мониторинга угроз и реагирования на инциденты.
Сетевая криминалистика	Курс по исследованию сетевого трафика в рамках реагирования на инциденты. Участники научатся анализировать сетевые доказательства, собирать и обрабатывать данные о кибератаках для улучшения процесса расследования инцидентов.
Исследование киберпреступлений	Курс учит требованиям законодательства (152-ФЗ) и правилам обработки ПДн. Позволяет корректно исполнять обязанности оператора ПДн и минимизировать правовые риски. Направлен на специалистов, которые в своей работе непосредственно взаимодействуют с ПДн.
Реагирование на инциденты ИБ	Курс по эффективному реагированию на выявленные инциденты и ликвидации их последствий. Анализ атак, изучение современных техник и инструментов сбора артефактов, выстраивание процесса реагирования.
Интенсив по защите ПДн	Тренинг направлен на повышение компетенций сотрудников в области обработки и защиты ПДн различных категорий субъектов. Программа поможет выстроить внутренние процессы обработки ПДн в соответствии с требованиями нормативных документов.
Видеокурс «Анализ вредоносного ПО»	Изучение функциональности вредоносных программ для раскрытия применяемых злоумышленниками тактик, техник и процедур. Изучение основ анализа вредоносного кода, работа с ассемблером, песочницами и дизассемблером IDA Pro. Практические задания, которые разработали специалисты F6 на основе реальных кейсов.
Аналитик SOC	Курс посвящен эффективному мониторингу событий ИБ, быстрому выявлению угроз и тому, как отличать реальные инциденты от ложных сработок. Практические методы криминалистики операционных систем и сетей, разработка правил детектирования и Threat Hunting с использованием инструмента XDR. Анализ атак с разложением этапов на MITRE/CKC для формирования стратегии по недопущению возникновения критичных инцидентов. Практика работы с инструментами XDR, GRAPH TI, ASM.
Компьютерная криминалистика и реагирование на инциденты в ОС Windows	Курс учит методикам охоты за угрозами (Threat Hunting): проверке гипотез и анализу телеметрии. Позволяет выявлять скрытые и продвинутые атаки (APT) до нанесения ущерба. Направлен на развитие навыков проактивного поиска злоумышленников в инфраструктуре.
Компьютерная криминалистика и реагирование на инциденты в ОС Linux	Двухдневный интенсив по реагированию на инциденты в Linux-системах. Освоение ключевых элементов Linux DFIR: сбора данных, анализа оперативной памяти и хостовой криминалистики — с практическими кейсами и отработкой навыков.
Исследование атак шифровальщиков	Трехдневный интенсив по киберразведке, расследованию атак и анализу шифровальщиков: разбор тактик злоумышленников, изучение хостовой криминалистики и методов атрибуции атакующих на реальных кейсах.
Разведка: основной этап в пентесте	Наши практикующие специалисты расскажут о том, как собирать и анализировать информацию об опубликованных системах и сервисах компании с помощью современных техник разведки.

Курс	Описание
ASM в действии: автоматизированная защита внешних сервисов	Курс о способах выявления уязвимостей в публично доступных сервисах, тактиках атакующих, современных инструментах мониторинга и эффективных методах защиты.
Безопасность в киберпространстве	Изучение мотивов и методов киберпреступников, правил защиты корпоративных и личных устройств от утечки информации и компрометации учетных данных. Даём инструкции для настроек конфиденциальности в соцсетях и мессенджерах, а также описание актуальных схем кибератак.
Проактивный поиск киберугроз	Курс о том, как выдвигать успешные гипотезы, применять матрицу MITRE ATT&CK®, использовать возможности компьютерной криминалистики в рамках проактивного поиска угроз и реализовывать Threat Hunting в масштабах организации.

Запись в наборную группу обучения — запрос места не менее чем за **3 недели** до старта курса

Организация обучения для корпоративной группы по готовым курсам — не менее чем за **6 недель**

Организация обучения для корпоративной группы и разработка темы под запрос — не менее чем за **12 недель**

Тарифные планы подписки

Наименование	1 год	2 года	3 года	SLA на реакцию*
White	500 часов			3 рабочих дня
Purple	1000 часов	1000 часов		2 рабочих дня
Black	1500 часов	1500 часов	1500 часов	1 рабочий день

*SLA в случае потребности реагирования на инцидент — до 2-х часов

Скидка 5%

На приобретение **двух** сертификатов одного номинала по 1000 часов

Скидка 10%

На приобретение **трёх** сертификатов одного номинала по 1000 часов

Пример использования часов

Ниже приведены примеры услуг, которые могут входить в стандартный объём работ в рамках доступных часов. Состав пакета можно адаптировать под ваши задачи

500 часов

- Внешнее тестирование на проникновение
- Оценка соответствия требованиям законодательства Российской Федерации о персональных данных (152-ФЗ, ПП N 1119, 21 Приказ ФСТЭК), без модели угроз и без разработки ОРД
- Выявление следов компрометации, суммарно до **1000** анализируемых хостов
- Реагирование на инцидент
- Обучение кибербезопасности от экспертов F6, до **2 программ** обучения

1000 часов

- Внешнее тестирование на проникновение
- Внутреннее тестирование на проникновение
- Оценка защищённости Wi-Fi до **5 точек** доступа (**1 площадка** в г. Москва) или оценка осведомленности сотрудников посредством фишинговых рассылок
- Анализ защищённости веб-приложения, кроме Интернет-банкинга
- Оценка соответствия требованиям законодательства Российской Федерации о персональных данных (152-ФЗ, ПП N 1119, 21 Приказ ФСТЭК), разработка модели угроз по методологии ФСТЭК, а также разработка комплекта ОРД
- Выявление следов компрометации (анализ **5000 хостов**) или выявление следов компрометации (анализ **1000 хостов**) и оценка готовности к реагированию на инциденты ИБ
- Реагирование на инцидент с расширенными консультациями
- Обучение кибербезопасности от экспертов F6, до **4 программ** обучения

1500 часов

- Внешнее тестирование на проникновение
- Внутреннее тестирование на проникновение
- Оценка защищённости Wi-Fi до **5 точек** доступа (**1 площадка** в г. Москва)
- Оценка осведомлённости сотрудников посредством фишинговых рассылок
- Анализ защищённости веб-приложения, включая Интернет-банкинг
- Анализ защищенности **1 мобильного приложения** на **2 платформах**
- Оценка соответствия требованиям законодательства Российской Федерации о персональных данных (152-ФЗ, ПП N 1119, 21 Приказ ФСТЭК), разработка модели угроз по методологии ФСТЭК, а также разработка комплекта ОРД
- Оценка соответствия вашей компании международным стандартам и лучшим практикам в области ИБ
- Выявление следов компрометации (анализ **5000 хостов**) или выявление следов компрометации (анализ **3000 хостов**) и оценка готовности к реагированию на инциденты ИБ
- Реагирование на инцидент с расширенными консультациями
- Обучение кибербезопасности от экспертов F6, до **5 программ** обучения

Прозрачная коммуникация

После подключения **Sphere** персональный менеджер помогает сформировать план работ на год. При необходимости его можно скорректировать в любой момент — изменить приоритеты или выбрать другие услуги

Мы заинтересованы в том, чтобы вы использовали весь объём часов в течение срока действия пакета.

После получения запроса специалист связывается с вами в рамках SLA*: уточняет детали или направляет предложение с составом работ, сроками, объёмом часов и ближайшей датой старта. После подтверждения часы резервируются до завершения и приёмки работ.

* SLA на заявку от 1 до 3 дней в зависимости от тарифа, SLA на услуги в соответствии с таблицей в разделе Полный перечень услуг

Результаты оказания услуг

По итогам всех услуг, за исключением курсов, предоставляем отчёт с понятными выводами для бизнеса и практическими рекомендациями для ИБ-специалистов

Отчёт включает два уровня представления информации:

Для менеджмента

Ключевые выводы, риски и рекомендации, изложенные в бизнес-терминах.
Это позволяет руководству оперативно принимать управленческие решения

Для технических специалистов

Детализированные результаты: технические находки, описание уязвимостей, артефакты расследования, рекомендации по устранению. Эти данные служат основой для конкретных технических действий

Такой формат обеспечивает прозрачность результатов. Это позволяет руководству принимать стратегические решения, а ИТ- и ИБ-командам — оперативно устранять проблемы и укреплять защиту.

Ключевые преимущества F6

Более 20 лет наши услуги помогают организациям справляться с инцидентами, проверять защищённость, получать профильные компетенции и противостоять злоумышленникам

1.

Уникальная экспертиза и лидерство в расследованиях

Первая в России лаборатория, специализирующаяся на расследовании инцидентов ИБ. За плечами сотни успешных исследований киберпреступлений и более 70 000 часов реагирования. Мы используем собственные методики и инструменты для выявления следов компрометации и поиска злоумышленников

2.

Полный спектр услуг в сфере кибербезопасности

Закрываем полный цикл задач: от мониторинга и реагирования до моделирования угроз и проверки защищённости. В портфеле — пентесты, Red и Purple Teaming, аудит на соответствие требованиям регуляторов, обучение сотрудников и другие направления

3.

Практический подход с акцентом на пользу клиентам

Работаем не «для отчёта», а на результат. Каждый проект повышает реальный уровень защищённости клиента — поэтому нам доверяют сложные и критичные задачи

4.

Высокие стандарты качества и надежность

Строгие процессы и глубокая техническая экспертиза команды позволяют внедрять устойчивую систему кибербезопасности, а не точечные меры защиты

Кому будет полезна подписка

Организациям без собственной ИБ-команды или с необходимостью усиления экспертизы

Компаниям с регулярными потребностями в услугах ИБ

F6

Технологии для борьбы с киберугрозами

+7 495 984-33-64
info@f6.ru