Департамент интеграции систем ИБ

Solid Solutions

О нас

6 лет на рынке информационной безопасности	Захватываем международный рынок	Работаем во всех регионах РФ, в том числе и на новых территориях	30 человек в команде (как молодые специалисты, так и люди с опытом 20 и более лет)
Оперативно реагируем на обращения	Быстрый и прозрачный расчет коммерческих предложений	Открыты к сотрудничеству	

Для осуществления деятельности получены лицензии

ФСТЭК России
№ Л024-00107-77/03208276

на деятельность в области технической защиты информации

ФСТЭК России
№ Л050-00107-77/03552577

на деятельность по разработке и производству средств защиты конфиденциальной информации

ФСБ России
№ 18341

на деятельность в области шифровальных (криптографических) средств

Услуги

Полный цикл обеспечения ИБ :

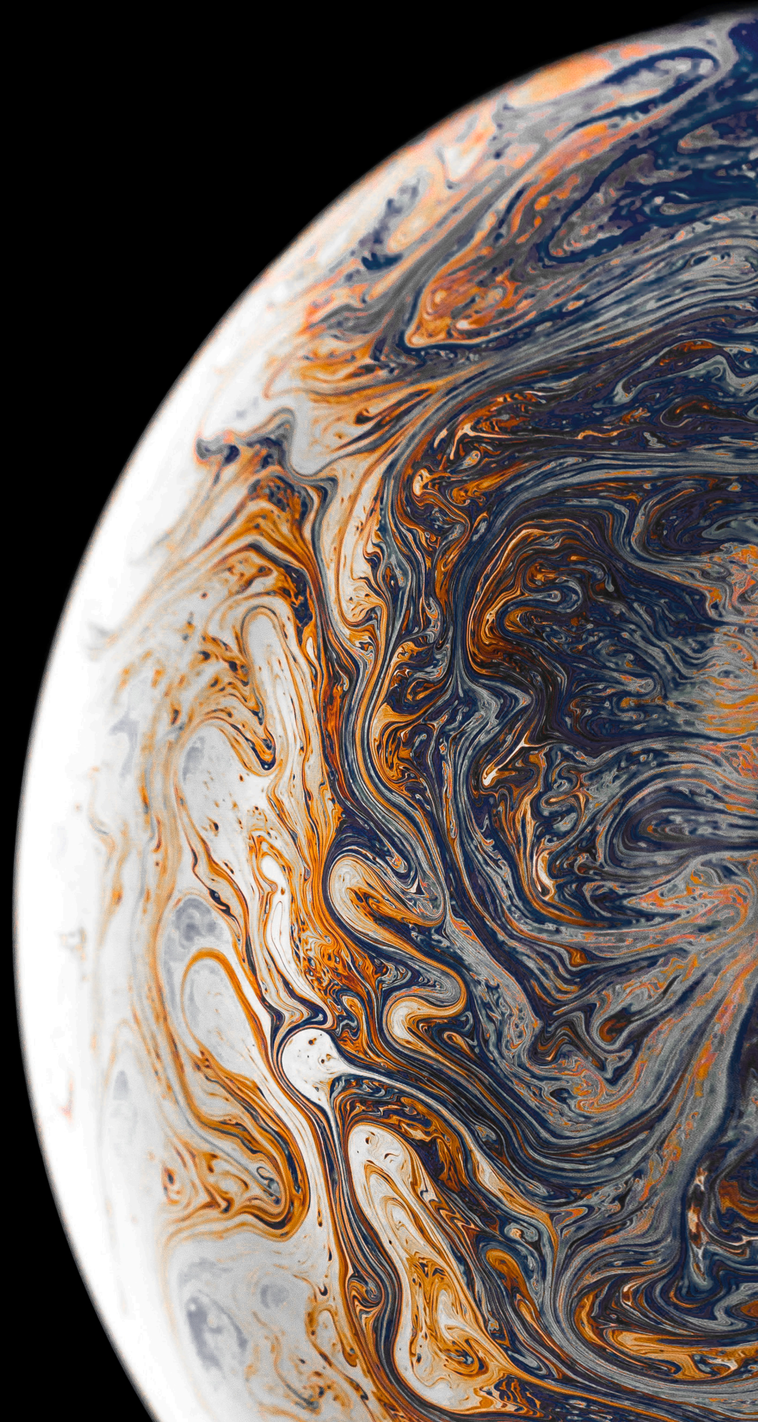
01 Комплекс услуг по аудиту и анализу защищенности

02 Подбор решений ИБ, проведение пилотных тестирований

03 Внедрение, сопровождение и поддержка СЗИ

Комплекс услуг по аудиту и анализу защищенности

01



Комплекс услуг по аудиту и анализу защищенности

- **Работаем от малых и средних организаций до крупных государственных заказчиков**
- **Проводим подробный аудит, анализируем риски, готовим модели угроз под разные сценарии**

Оказываем услуги по следующим направлениям:

1. Обследование ИБ-состояния
2. Аудит и оценка соответствия
3. Тестирование на проникновение (Pentest)
4. Анализ защищенности (Vulnerability Assessment)
5. Оценка защищенности от целевых атак (Red Teaming)
6. Анализ архитектурной безопасности

1.1 Обследование ИБ-состояния

- Сбор информации об IT-инфраструктуре, бизнес-процессах и текущих мерах защиты
- Анкетирование и интервьюирование ответственных сотрудников
- Анализ существующей документации, политик и инструкций
- Идентификация критических активов и цепочек обработки данных
- Оценка зрелости процессов информационной безопасности и уровня осведомлённости персонала
- Формирование предварительных выводов и зон риска для последующего аудита или тестирования

1.2 Аудит и оценка соответствия

Проводим оценку готовности и соответствия требованиям законодательства РФ, международных стандартов и отраслевых регуляторов, включая:

АСУ ТП и промышленные сети

- Аудит безопасности автоматизированных систем управления
- Анализ сегментации, изоляции, и взаимодействия технологической и офисной ИТ-инфраструктуры
- Оценка уязвимостей SCADA, PLC, HMI и других компонентов АСУ ТП
- Проверка соответствия методическим документам ФСТЭК

Общие работы

- Инвентаризация ИТ-активов и обработок информации
- Анализ локальных нормативных актов, политик, регламентов и архитектуры ИБ
- Gap-анализ текущего состояния по выбранному стандарту/регулятору
- Подготовка дорожной карты устранения несоответствий
- Методическое сопровождение при внедрении и сертификации

КИИ (ФЗ-187)

- Категорирование объектов КИИ
- Подготовка перечня значимых объектов (ЗО КИИ)
- Проверка выполнения требований:
  - Федеральный закон № 187-ФЗ,
  - Приказы ФСТЭК № 235, № 239, № 239д,
  - Методические материалы ФСТЭК
- Оценка устойчивости, резервирования и защищенности объектов

Персональные данные (ФЗ-152)

- Проверка соответствия:
  - Федеральный закон № 152-ФЗ, Постановления № 1119, № 687, Приказ ФСТЭК № 21, Приказ ФСБ №378, Методика определения уровня защищенности (ФСТЭК), Методические рекомендации Роскомнадзора
- Проверка правомерности обработки, прав субъектов, согласий, трансграничной передачи
- Оценка защищенности ИСПДн, в том числе в форме аттестационных испытаний

1.2 Аудит и оценка соответствия

Проводим оценку готовности и соответствия требованиям законодательства РФ, международных стандартов и отраслевых регуляторов, включая:

ЦБ РФ / Банк России (ГОСТ Р 57580, СТО БР ИББС)

- Аудит проводится по 757-П, 683-П, ГОСТ Р 57580.1-2017
- Проверка процессов управления ИБ в финансовых организациях
- Оценка рисков, зрелости процессов, контроля доступа, реагирования на инциденты
- Подготовка к проверкам и сертификациям, формирование рекомендаций

ISO 27001, ISO 22301, PCI DSS и другие

- Подготовка к международной сертификации:
  - ISO/IEC 27001 — система управления ИБ,
  - ISO/IEC 22301 — непрерывность бизнеса,
  - PCI DSS — защита данных платёжных карт
- Проведение предаудитов и внутренних проверок
- Сопровождение проекта внедрения СУИБ или других стандартов

Государственные информационные системы

- Аудит ГИС на соответствие:
  - Постановлениям № 1236, № 719, № 1746,
  - Методическим рекомендациям ФСТЭК,
  - Приказам № 17, № 21 (ФСТЭК)
- Формирование модели угроз, проектной и эксплуатационной документации
- Подготовка пакета документов для аттестации
- Консультации и сопровождение при прохождении проверок надзорных органов
- Проведение аттестационных испытаний

Коммерческая тайна

- Аудит соблюдения режима КТ:
  - Проверка правового оформления, меток конфиденциальности, договорных обязательств, контроля доступа
  - Оценка рисков утечек при удаленной работе, использовании облачных сервисов и при передаче третьим лицам
- Разработка и корректировка локальных актов (Положение о КТ, политика доступа, регистрационные журналы)
- Сопровождение внедрения системы защиты КТ в организации

1.3 Тестирование на проникновение

Поиск уязвимостей в веб-приложениях, внешнем и внутреннем периметре

Оценка защищенности инфраструктуры через моделирование атак злоумышленников

Проведение социальной инженерии (фишинг, поддельные устройства, физический доступ)

Аудит конфигураций СЗИ, серверов, СУБД, облаков

Подготовка отчета с рекомендациями и возможным вектором развития атаки

1.4 Анализ защищенности

Автоматическое и ручное сканирование на наличие уязвимостей

Классификация и верификация критических недостатков

Приоритезация уязвимостей с учетом бизнес-контекста

Выдача отчета с перечнем мер по устранению и снижению рисков

1.5 Оценка защищенности от целевых атак

Имитация действий реальных злоумышленников

Применение подходов Recon, Initial Access, Privilege Escalation, Lateral Movement

Проверка устойчивости организации и реакции ИБ-команды (SOC, SIEM)

Подготовка отчета, включающего цепочки атак и зоны риска

Разработка рекомендаций по усилению защитных рубежей

1.6 Анализ архитектурной безопасности

Оценка сегментации сети, уровня изоляции, применения принципа наименьших привилегий

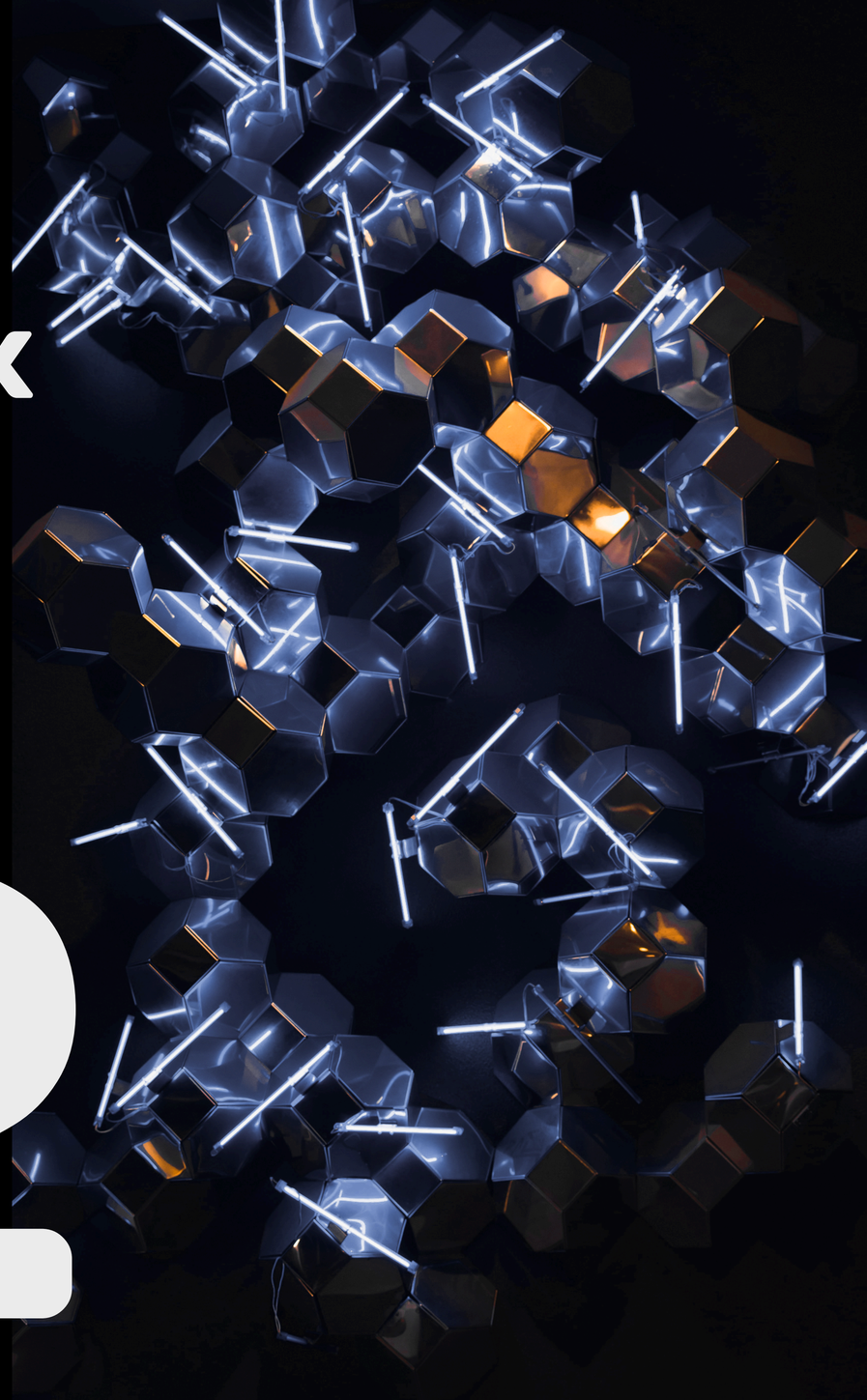
Анализ механизмов защиты от DDoS, APT, утечек данных

Проверка стратегий резервного копирования, отказоустойчивости и восстановления

Рекомендации по повышению архитектурной устойчивости и управляемости безопасности

Подбор решений ИБ, проведение пилотных тестирований

02



Подбор решений ИБ, проведение пилотных тестирований

- Разработка ПМИ, позволяющая провести тестирование по всем необходимым требованиям заказчика. Подготовка критериев успешности испытаний
- Подготовка тестовых стендов в офисе компании. Настройка оборудования в соответствии с инфраструктурой заказчика. Подготовка нагрузочных профилей для имитации реального трафика заказчика
- Подготовка тестового контура в инфраструктуре заказчика. Настройка оборудования в пилотной среде. Обеспечение минимального влияния на продуктивный контур во время тестирования
- Проведение испытаний СЗИ для подтверждения пригодности решения к эксплуатации в инфраструктуре заказчика

Внедрение, сопровождение и поддержка СЗИ

03

Внедрение, сопровождение и поддержка СЗИ

Обеспечение базового уровня защищённости информационной инфраструктуры, приведение технических средств и программного обеспечения в соответствии с нормативными требованиями и лучшими практиками в области информационной безопасности

Внедрение

Тонкая настройка

Сопровождение

Техническая поддержка

3.1 Внедрение СЗИ

Монтаж оборудования	Установка ПО
• Физическая установка и подключение компонентов СЗИ: межсетевых экранов, криптошлюзов, сенсоров DLP/IDS/IPS, серверов управления, систем контроля трафика и др. программно-аппаратных средств защиты информации • Организация стоечного размещения, подключение к сетям передачи данных, системам электропитания и резервного питания (ИБП) • Прокладка, маркировка и тестирование сетевых соединений (в том числе создание выделенных сегментов для управления и передачи трафика)	• Инсталляция базовых компонентов СЗИ (средства защиты от несанкционированного доступа, средства анализа защищенности, межсетевые экраны, системы предотвращения вторжений, криптосредства, антивирусы, DLP, средства контроля целостности и др.) • Установка управляющих модулей и агентов на серверы, рабочие станции, сетевые устройства • Первичная настройка и активация лицензий, настройка доступа к источникам обновлений и центрам сертификации (если требуется)

3.1 Внедрение СЗИ

Базовая настройка

- Настройка минимально необходимого уровня защиты:
  - Базовые политики фильтрации трафика;
  - Установка правил межсетевого экрана;
  - Настройка журналирования событий безопасности;
  - Интеграция с Active Directory/LDAP;
  - Ограничение прав доступа, распределение ролей;
  - Настройка безопасной аутентификации
- Подготовка шаблонов конфигураций для типовых рабочих мест и серверов
- Подключение к системам централизованного мониторинга

Проверка функционирования

- Комплексное тестирование работоспособности компонентов
- Контроль механизмов регистрации и хранения событий:
  - Проверка логирования системных и пользовательских действий;
  - Передача логов в централизованное хранилище
- Проверка базовых механизмов защиты:
  - Разграничение прав;
  - Контроль целостности конфигураций;
  - Реакция на попытки обхода политики;
  - Обновление сигнатур
- Проверка штатной работы всех служб и отключения неиспользуемых функций

3.2 Тонкая настройка СЗИ

Повышение эффективности
и адаптация СЗИ под особенности инфраструктуры с учётом рисков, моделей угроз и организационной структуры.

Оптимизация политик безопасности

- Настройка правил фильтрации, DPI, IDS/IPS в соответствии с ролью пользователя, сегментом сети и критичностью ресурсов;
- Уточнение правил доступа к защищаемым ресурсам

Интеграция с ИТ-инфраструктурой

- Связь с SIEM, CMDB, сервис-деском, средствами учёта оборудования и пользователей;
- Интеграция с почтовыми, файловыми, базами данных и приложениями для более точного анализа событий

Настройка уведомлений и сценариев реагирования

- Конфигурация автоматических реакций на инциденты: блокировки, алерты, изоляция узлов;
- Настройка правил корреляции событий

3.2 Тонкая настройка СЗИ

Повышение эффективности
и адаптация СЗИ под особенности инфраструктуры с учётом рисков, моделей угроз и организационной структуры.

Проверка и отладка эффективности настроек

- Анализ ложных срабатываний;
- Проведение тестовых атак и имитаций нарушений;
- Подстройка чувствительности систем и правил анализа

Создание пользовательских сигнатур, фильтров, шаблонов отчётности

3.3 Сопровождение СЗИ

Поддержание актуальности, эффективности и надёжности систем защиты информации в условиях изменения угроз и инфраструктуры

Мониторинг состояния СЗИ

- Проверка работоспособности сервисов;
- Контроль за своевременным обновлением баз, политик, сигнатур

Обновления и сопровождение

- Установка патчей безопасности;
- Обновление версий программного обеспечения;
- Резервное копирование конфигураций

Поддержка по SLA

- Обработка инцидентов и обращений;
- Выездные и удалённые работы;
- Ведение базы знаний и отчётность

3.3 Сопровождение СЗИ

Поддержание актуальности, эффективности и надёжности систем защиты информации в условиях изменения угроз и инфраструктуры

Периодический аудит конфигураций и эффективности СЗИ

- Проверка актуальности политик;
- Выявление узких мест и «дыр» в защите;
- Подготовка рекомендаций по улучшению

Подготовка и сопровождение проверок и аудитов

- Формирование отчётности;
- Консультации для служб ИБ и ИТ заказчика;
- Поддержка при взаимодействии с регуляторами

Обучение и консультации

- Организация обучения в учебных центрах;
- Проведение инструктажей, тренингов;
- Консультирование ИБ и ИТ-специалистов, пользователей

Внедряемые решения

Solid Solutions

- МираМобайл

Infotecs

- VipNet HW4
- VipNet HW5

- UserGate
- S-terra
- Ideco
- Kaspersky

Код Безопасности

- Континент 4
- Континент 3
- Континент WEB (WAF+ TLS)
- Континент АП/ZTN
- vGate
- SecretNet
- Orchestrator

Positive Technologies

- MaxPatrol
- SandBox
- NAD
- XDR
- и другие

- Dr.Web
- НПО «Эшелон»
- InfoWatch

3.4 Услуга Diamond Support

Оказание услуги технической поддержки на уровне, выше VIP ТП вендоров

- **Дежурная группа** инженеров для мгновенного выезда к заказчику в случае аварии на оборудовании. Время реагирования по Москве до 1 часа, по МО до 3
- **Отсутствие линий ТП.** Все инциденты будут сразу попадать компетентным специалистам
- **Регулярный анализ** архитектуры системы заказчика и подготовка предложений по модернизации и оптимизации системы
- Проведение **регулярных технически-маркетинговых презентаций** внедряемых решений
- **Строгий SLA** по ответам заказчику в различных средства связи (мессенджеры и почта). Возможность организации выделенного мессенджера для взаимодействия с заказчиком
- **Выделенная линия** удаленного управления (по согласованию). Для того, чтобы кратно уменьшить время решения проблемы, можно организовать выделенный канал управления оборудованием и ПК заказчика

3.4 Услуга Diamond Support

Оказание услуги технической поддержки на уровне, выше VIP ТП вендоров

- **Персональный dashboard [в планах]**, содержащий информацию по статусу, количеству и по статистике инцидентов. Также возможно предоставлении статистики (среднее время решения инцидентов в зависимости от сложности и критичности). Также на отдельную вкладку дашборда можно будет выводить информацию по текущим активным проектам компании

- **Прозрачный и простой мониторинг** (по согласованию). Заказчику устанавливается сервер с простым набором компонентов, не собирающий никакой информации, кроме диагностической. Сервер находится на территории заказчика, а специалисты ТП уже получают доступ к графикам, а не наоборот