КСБ-СОФТ

Информационная безопасность и импортозамещение информационных технологий

О КОМПАНИИ

КСБ-СОФТ – системный интегратор в сфере информационной безопасности и импортозамещения информационных технологий

- ✓ В 2014 году структурное подразделение компании «Кейсистемс», выполняющее комплексные проекты по защите информации регионального значения, выросло в отдельную организацию федерального уровня.
- ✓ Благодаря опытным ИБ-специалистам и талантливым разработчикам программного обеспечения, сегодня «КСБ-СОФТ» – это крупный системный интегратор в сфере информационной безопасности, выполняющий комплексные проекты: классический compliance ГИС, ИСПДн, КИИ и АСУ ТП, практические работы по анализу уязвимостей и тестированию на проникновение (PenTest), мониторингу и реагированию на инциденты ИБ (SOC), а также консалтингу по безопасной разработке (SDL) и сертификации средств защиты информации.

КОМПЛЕКСНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аудит и исследования

- ✓ Аудит предприятия с целью выявления потребностей в модернизации ИТ или ИБ инфраструктуры
- ✓ Анализ уязвимостей и тестирование на проникновение предприятия

Сервисы сопровождения и консалтинг

- ✓ Техническое сопровождение
- ✓ Мониторинг инцидентов
- ✓ Консалтинг, сопровождение проверок

Проектирование и внедрение

- ✓ Проектирование подсистем обеспечения информационной безопасности
- ✓ Внедрение средств защиты информации под различные цели на всех уровнях предприятия

Оценка соответствия

- ✓ Аттестационные испытания предприятия на соответствие требованиям по защите информации
- ✓ Контроль за обеспечением уровня защищенности предприятия

НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Анализ уязвимостей и тестирование на проникновение (пентест)

ЗАЧЕМ ЭТО НУЖНО

- Выполнить требования отраслевых и нормативных правовых актов
- Получить объективную независимую оценку эффективности системы защиты информации
- Получить подробные рекомендации по повышению защищенности информационной системы

ВЫПОЛНЯЕМ ВЕСЬ ЦИКЛ РАБОТ:

- Изучение объекта исследований, поиск уязвимостей информационной инфраструктуры
- Имитация атак на инфоресурсы
- Подготовка рекомендаций по устранению выявленных недостатков

Обеспечение веб-безопасности

ЗАЧЕМ ЭТО НУЖНО

- Выявить уязвимости веб-приложений и подготовить рекомендации по их устранению
- Обеспечить непрерывность процесса защиты веб-приложений
- Выполнить требования регулятора по обеспечению безопасности информационных систем, в состав которых входят веб-приложения

ВЫПОЛНЯЕМ ВЕСЬ ЦИКЛ РАБОТ:

- Сбор сведений об инфраструктуре веб-приложений
- Построение и разработка сценариев использования системы защиты веб-приложений от сетевых атак
- Техническое сопровождение системы защиты веб-приложений от сетевых атак

НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Мониторинг ИБ (SOC)

ЗАЧЕМ ЭТО НУЖНО

- Выполнить требования отраслевых и нормативных правовых актов
- Обеспечить непрерывный процесс выявления событий и инцидентов ИБ
- Своевременно реагировать и противодействовать атакам

ВЫПОЛНЯЕМ ВЕСЬ ЦИКЛ РАБОТ:

- Подключение к SOC или внедрение системы мониторинга ИБ
- Мониторинг событий и инцидентов ИБ 8/5 или 24/7
- Интеграция с ГосСопка
- Предоставление периодических отчетов и рекомендаций по результатам мониторинга ИБ

Безопасность АСУ ТП

ЗАЧЕМ ЭТО НУЖНО

- Соответствовать приказу ФСТЭК России от 14.03.2014 №31 и другим НПА в сфере ИБ АСУ ТП
- Оценить текущее состояние ИБ АСУ ТП
- Повысить уровень защищенности АСУ ТП от действий потенциального кибернарушителя
- Снизить риски простоя и выхода из строя оборудования вследствие компьютерной атаки

ВЫПОЛНЯЕМ ВЕСЬ ЦИКЛ РАБОТ:

- Аудит безопасности промышленных систем
- Разработка и внедрение комплексного решения по обеспечению ИБ промышленных систем
- Внедрение SDL, сопровождение процесса/сертификации ПО во ФСТЭК России
- Техническое сопровождение и контроль эффективности
- Мониторинг инцидентов ИБ

НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Безопасность объектов КИИ

ЗАЧЕМ ЭТО НУЖНО

- Выполнить требования законодательства по обеспечению безопасности объектов КИИ
- Организовать взаимодействие с центрами ГосСопка для обмена информацией о кибератаках
- Снизить риски выхода из строя инфраструктуры объекта КИИ
- Снизить репутационные риски субъекта КИИ

ВЫПОЛНЯЕМ ВЕСЬ ЦИКЛ РАБОТ:

- Аудит процессов и выявление объектов КИИ, подлежащих категорированию
- Моделирование угроз безопасности информации объектов КИИ
- Категорирование объектов КИИ
- Проектирование и внедрение подсистемы защиты объектов КИИ
- Внедрение SDL, сопровождение процесса сертификации ПО во ФСТЭК России
- Техническое сопровождение и контроль эффективности

НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Защита информации в ГИС
2. Обеспечение жизненного цикла ГИС
3. Защита персональных данных
4. Импортозамещение
5. Безопасная разработка
6. Защита от утечек информации (DLP)
7. Защита коммерческой тайны

КСБ-СОФТ

УСЛУГИ КСБ-СОФТ СООТВЕТСТВУЮТ ТРЕНДАМ

Мы обеспечим соблюдение всех нормативно-правовых актов:

- **Требования по защите КИИ**
  187-ФЗ, приказы ФСТЭК России №239, 235;
- **Требования по защите АСУ ТП**
  Приказ ФСТЭК России № 31;
- **Требования по противодействию киберугрозам;**
- **Требования к взаимодействию с ГосСОПКА,**
  Приказы ФСБ России
  (в части подключения к ГОССОПКА);
- **Требования по импортозамещению**
  Указ Президента № 250
- **Требования по защите ГИС**
  149-ФЗ, Приказ ФСТЭК России № 17;
- **Требования по защите ПДн**
  152-ФЗ, Приказ ФСТЭК России № 21,
  Приказ ФСБ России № 378
- **Требования по эксплуатации ГИС** 676-ПП;

И другие

НАШИ ПАРТНЕРЫ

альфа	UserGate	positive technologies
КОД безопасности	NUMA TECHNOLOGY	infotecs
kaspersky	ideco	КИБЕРПРОТЕКТ
РУТОКЕН	НАУЧНО-ПРОИЗВОДСТВЕННОЕ ОБЪЕДИНЕНИЕ РУСБИТЕХ	Эшелон комплексная безопасность

ПОЧЕМУ СТОИТ ВЫБРАТЬ КСБ-СОФТ

- На рынке ИБ с 2012 года;
- Более 80 регионов внедрения проектов
- Лицензии ФСТЭК России и ФСБ России;
- В штате специалисты с сертификатами MBA, CISM, CGEIT, CISA, PSM, OSCP.
- Возможности пилотного внедрения решений

НАШ ОПЫТ

**Нам доверяют компании
и учреждения различного профиля**:

- Роспотребнадзор РФ
- Центры информационных технологий (ЦИТ) субъектов РФ
- Министерства финансов, экономического развития, здравоохранения субъектов РФ
- Медицинские информационно-аналитические центры (МИАЦ) субъектов РФ
- Медицинские центры федерального и регионального уровня;
- Предприятия, входящие в ГК «Росатом»;

РЕАЛИЗОВАНО

> 4000

ПРОЕКТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ

НАШ ОПЫТ

2021

- Филиал Госкорпорации по ОрВД
- Областное казначейство (ПФО)
- Региональные министерства финансов
- Городской комитет по информатизации (УФО)

2022

- Промышленное предприятие Калининградской области
- Парково-развлекательный комплекс Краснодарского края
- МФЦ (ПФО)
- Региональные министерства финансов

2023

- Минфин Забайкалья
- Минфин Ульяновской области
- Судьи Саратовской области
- ЦИТ Минцифры Чувашии

НАМ ДОВЕРЯЮТ

Филиал «Аэронавигация Севера Сибири» ФГУП «Государственная корпорация по организации воздушного движения в Российской Федерации»

ФГБУ «Канал имени Москвы»

ГКУ СО «Центр обслуживания судебных участков мировых судей Саратовской области»

АО «Сахаэнерго»

Агрокомплекс имени Н. И. Ткачёва

АО «Международный аэропорт Шереметьево»

НАМ ДОВЕРЯЮТ

ФГУП «Российская телевизионная и радиовещательная сеть» (РТРС)

Минцифры Камчатского края

ДТСЗН города Москвы

Норникель

Якутскэнерго

ДИТИС ЯНАО

НАМ ДОВЕРЯЮТ

ГОБУ ЦИТ МО

ТНС энерго
филиалы в РФ

РусГидро, филиалы в РФ

Россети
филиалы в РФ

Объединенная
энергетическая
компания, АО (ОЭК)

Балтийская стивидорная
компания