



КСБ-СОФТ – ЭКСПЕРТ В СФЕРЕ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
И ИМПОРТОЗАМЕЩЕНИЯ

О компании



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

Успешно ведем деятельность с 2014 года.

МИССИЯ КСБ-СОФТ

Мы создаем доверие в цифровом мире.



1

Аудит и исследования

- ✓ Аудит информационных систем на соответствие требованиям НПА
- ✓ Анализ уязвимостей и тестирование на проникновение
- ✓ ИТ-аудит

2

Проектирование и внедрение

- ✓ Проектирование подсистем обеспечения информационной безопасности
- ✓ Внедрение СрЗИ на всех уровнях организации

3

Сервисы сопровождения и консалтинг

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

5

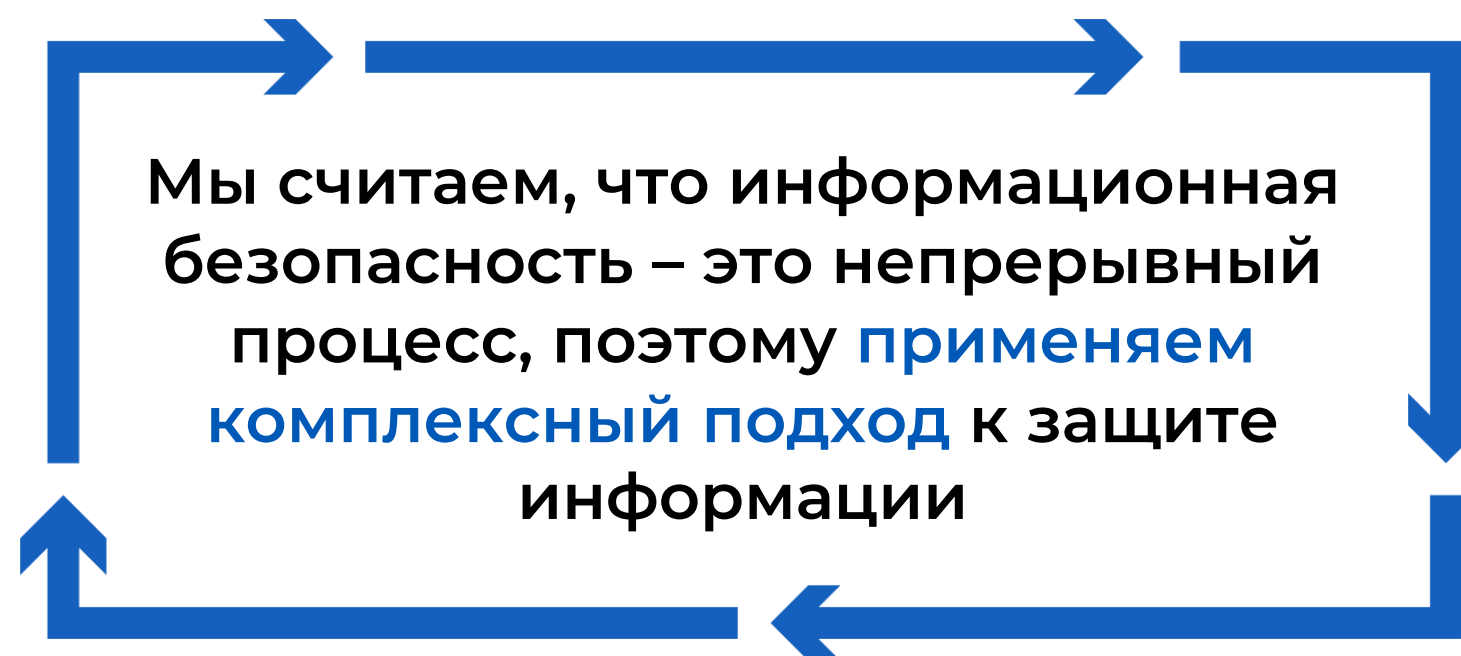
Автоматизация бизнес-процессов

- ✓ Разработка организационной и технической документации
- ✓ Контроль подключения пользователей к ИС
- ✓ Учет и выдача криптосредств
- ✓ Учет информационных ресурсов
- ✓ Автоматизация работы с инцидентами ИБ

4

Оценка соответствия

- ✓ Аттестационные испытания ИС на соответствие требованиям
- ✓ Контроль обеспечения уровня защищенности ИС



Услуги КСБ-СОФТ



1. Аудит информационных систем
2. Защита ПДн
3. Безопасность объектов КИИ (АСУ ТП)
4. Модернизация ИТ-инфраструктуры
5. Анализ уязвимостей и тестирование на проникновение (пентест)
6. Мониторинг и реагирование на инциденты ИБ – SOCRAT
7. Киберучения по информационной безопасности
8. Внедрение процессов РБПО
9. Автоматизация бизнес-процессов
10. Защита ГИС (включая требования 117 приказа ФСТЭК России)

1. Аудит информационных систем

ЗАДАЧИ

- Оценка выполнения требований законодательства (152-ФЗ, 1119-ПП РФ, приказ ФСТЭК России № 21).
- Сбор полных и достоверных сведений о защищаемой информации в организации.
- Формирование требований к системе защиты информации и ее проектирование.

КАКИЕ РАБОТЫ ВКЛЮЧАЕТ

1. Выявление и обследование бизнес-процессов, инвентаризация информационных ресурсов, оценка достаточности действующих организационно-технических мер по защите информации.
2. Моделирование угроз безопасности информации, разработка рекомендаций по выполнению требований законодательства и формирование технического задания на создание системы защиты информации.
3. Проектирование системы защиты информации.



Нефтеперерабатывающая
компания

ЗАПРОС ОРГАНИЗАЦИИ

Оценить выполнение требований 152-ФЗ в организации, разработать систему защиты информации.

РЕЗУЛЬТАТ

1. В организации с более чем 2 500 филиалами по России выявлено свыше 11 000 работников, обрабатывающих ПДн.
2. Проведена оценка действующих мер.
3. Разработаны рекомендации по защите информации.
4. Спроектирована система защиты персональных данных в соответствии с требованиями 152-ФЗ и его подзаконных НПА.

2. Защита ПДн

ЗАДАЧИ

- Выполнение требований законодательства (152-ФЗ, 1119-ПП РФ, приказ ФСТЭК России № 21).
- Защита ИСПДн и предотвращение несанкционированного доступа к обрабатываемым ПДн.
- Минимизация риска утечки ПДн и получения оборотных штрафов за утечку ПДн.

КАКИЕ РАБОТЫ ВКЛЮЧАЕТ

1. Аудит процессов обработки ПДн и разработка организационно-распорядительной документации.
2. Разработка технического проекта системы защиты ПДн.
3. Внедрение системы защиты ИСПДн и анализ уязвимостей ИСПДн.

Значимый проект



Крупная организация
в сфере гостиничного бизнеса

ЗАПРОС ОРГАНИЗАЦИИ

Обеспечить соответствие 152-ФЗ,
внедрить систему защиты ПДн.

РЕЗУЛЬТАТ

Разработана система защиты информации, которая:

1. Предотвращает несанкционированный доступ к ПДн.
2. Обеспечивает практическую безопасность и соответствие требованиям регулятора.
3. При этом сохраняет эффективность выстроенных бизнес-процессов.

3. Безопасность объектов КИИ (АСУ ТП)

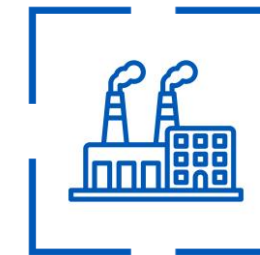
ЗАДАЧИ

- Выполнение требований законодательства (187-ФЗ и его подзаконных НПА).
- Снижение риска простоя и выхода из строя инфраструктуры объектов КИИ.
- Снижение репутационных и финансовых рисков субъекта КИИ.

КАКИЕ РАБОТЫ ВКЛЮЧАЕТ

1. Аудит и категорирование объектов КИИ, моделирование угроз.
2. Проектирование, поставка и внедрение системы защиты, разработка ОРД.
3. Организация мониторинга ИБ, взаимодействия с ГосСОПКА, техподдержка.

Значимый проект



ТЭК, энергетика, химическая металлургическая, горнодобывающая и оборонная промышленность

ЗАПРОС ОРГАНИЗАЦИИ

Обеспечить выполнение требований 187-ФЗ для значимых объектов КИИ, в том числе АСУ ТП.

РЕЗУЛЬТАТ

Проведен полный цикл работ системы защиты объектов КИИ в технологической и корпоративной сетях:

1. Аудит.
2. Категорирование.
3. Проектирование, внедрение и ввод в промышленную эксплуатацию.

3. Безопасность объектов КИИ (АСУ ТП)

3.1 Категорирование

ЗАДАЧИ

- Выполнение требований законодательства (187-ФЗ, 127-ПП РФ).
- Инвентаризация и категорирование имеющихся объектов КИИ.
- Согласование результатов категорирования с регулятором.

КАКИЕ РАБОТЫ ВКЛЮЧАЕТ

1. Аудит процессов и инвентаризация объектов КИИ с учетом отраслевых перечней.
2. Определение угроз, нарушителей, оценка критериев значимости и присвоение категории значимости.
3. Разработка документов и согласование результатов со ФСТЭК России.

Значимый проект



Ведущая энергетическая компания, реализующая один из крупнейших ресурсных проектов в России

ЗАПРОС ОРГАНИЗАЦИИ

Провести инвентаризацию ИС, АСУ ТП, ИТКС, актуализировать документацию по категорированию объектов КИИ.

РЕЗУЛЬТАТ

1. Выявлены и исправлены ошибки в инвентаризации объектов КИИ.
2. Проведено категорирование с учетом специфики ТЭК.
3. Проведено оперативное согласование результатов категорирования со ФСТЭК России.

Заказчик полностью выполнил требования в срок и без ошибок.

3. Безопасность объектов КИИ (АСУ ТП)

3.2 Проектирование

ЗАДАЧИ

- Выполнение требований законодательства (187-ФЗ, приказы ФСТЭК России № 235, 239).
- Разработка архитектуры системы защиты объектов КИИ.
- Выбор СЗИ с учетом их совместимости с инфраструктурой объекта КИИ.
- Разработка проектной и сметной документации с учетом ГОСТ-34, прохождение гос. экспертизы.

КАКИЕ РАБОТЫ ВКЛЮЧАЕТ

1. Предпроектное обследование и моделирование угроз.
2. Разработка частного технического задания, проектной, рабочей, эксплуатационной документации и ОРД.
3. Пилотирование СЗИ на стенде.

Значимый проект



Одно из крупнейших
нефтеперерабатывающих
предприятий в ЦФО России

ЗАПРОС ОРГАНИЗАЦИИ

Осуществить проектирование системы защиты для создаваемой АСУ ТП установки компримирования газов и общезаводской факельной системы, являющейся значимым объектом КИИ.

РЕЗУЛЬТАТ

1. Проведено предпроектное обследование объекта КИИ.
2. Разработана модель угроз и техно-рабочий проект на создание системы защиты объекта КИИ с учетом специфики технологических процессов АСУ ТП и отраслевых требований заказчика.

3. Безопасность объектов КИИ (АСУ ТП)

3.3 Внедрение

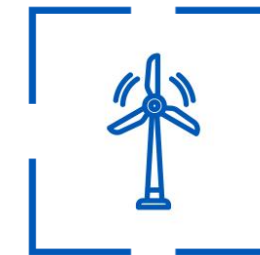
ЗАДАЧИ

- Выполнение требований законодательства (187-ФЗ, приказы ФСТЭК России № 235, № 239).
- Обеспечение устойчивого функционирования объектов КИИ при проведении в отношении них компьютерных атак.
- Снижение репутационных и финансовых рисков субъекта КИИ.

КАКИЕ РАБОТЫ ВКЛЮЧАЕТ

1. Поставка СЗИ.
2. Шеф-монтажные и пусконаладочные работы в части системы защиты объектов КИИ.
3. Проведение анализа уязвимостей объекта КИИ и испытаний системы защиты.
4. Техническое сопровождение внедренной системы защиты объектов КИИ.

Значимый проект



Одна из крупнейших ветровых электростанций России

ЗАПРОС ОРГАНИЗАЦИИ

Обеспечить комплексную защиту информации объектов КИИ ветровой электростанции.

РЕЗУЛЬТАТ

1. Внедрена, испытана и введена в промышленную эксплуатацию комплексная эшелонированная система защиты объектов КИИ
2. Обеспечено устойчивое функционирование работы объектов КИИ.
3. Достигнуто соответствие законодательству.

4. Модернизация ИТ-инфраструктуры

4.1 ИТ-аудит

ЗАДАЧИ

- Оценка эффективности и производительности ИТ-инфраструктуры.
- Анализ защищенности информационных активов и выявление уязвимостей.
- Оценка соответствия ИТ-инфраструктуры требованиям импортозамещения.

КАКИЕ РАБОТЫ ВКЛЮЧАЕТ

1. Анализ архитектуры системы, оценка ее соответствия бизнес-требованиям, выявление потенциальных рисков.
2. Комплексная оценка всех компонентов ИТ-инфраструктуры организации: серверов, сетевого оборудования, систем хранения данных, рабочих станций и ПО.
3. Подготовка рекомендаций и дорожной карты по устранению выявленных несоответствий и уязвимостей.

Значимый проект



Производственное
предприятие

ЗАПРОС ОРГАНИЗАЦИИ

Провести реорганизацию сети, настроить мониторинг событий ИБ, обеспечить защиту от угроз информационной безопасности.

РЕЗУЛЬТАТ

1. Создано более 10 сегментов сети.
2. Сервисы компании настроены по принципу минимальной необходимости.
3. Заменено ядро сетевой архитектуры.
4. Внедрена система обнаружения вторжений.

4. Модернизация ИТ-инфраструктуры

4.2 Импортозамещение

ЗАДАЧИ

- Выполнение требований законодательства (149-ФЗ, 187-ФЗ, Указ президента РФ № 166 и № 250, приказы ФСТЭК России № 117, № 21 и № 239).
- Снижение уровня зависимости от зарубежных информационных технологий.
- Повышение уровня устойчивости, надежности и безопасности информации.

КАКИЕ РАБОТЫ ВКЛЮЧАЕТ

1. Анализ текущего состояния ИТ/ИБ-инфраструктуры, определение требований и разработка архитектуры будущих решений.
2. Поставка, установка и миграция на отечественное программное обеспечение, оборудование и средства защиты информации.
3. Опытная эксплуатация, обучение персонала, консультации и проверка соответствия требованиям безопасности.

Значимый проект



Медицинский
информационно-
аналитический центр

ЗАПРОС ОРГАНИЗАЦИИ

Осуществить процесс импортозамещения ключевых компонентов инфраструктуры с соблюдением требований по защите информации в области ПДн, ГИС и ЗОКИИ.

РЕЗУЛЬТАТ

1. Спроектирована импортонезависимая ИТ-архитектура и система защиты информации.
2. Произведена замена сетевого оборудования, платформ виртуализации, системы хранения данных и операционных систем.
3. Модернизированная информационная система аттестована по требованиям защиты информации.

5. Анализ уязвимостей и тестирование на проникновение (пентест)

ЗАДАЧИ

- Выполнить требования законодательства (Приказы ФСТЭК России № 239, № 117, методические рекомендации, типовое ТЗ Минцифры).
- Получить независимую оценку эффективности системы защиты.
- Повысить уровень защищенности системы защиты информации.

КАКИЕ РАБОТЫ ВКЛЮЧАЕТ

1. Определение целей и задач (или недопустимых событий) тестирования на проникновение.
2. Имитация действий реальных злоумышленников (в рамках пентеста).
3. Отчетная документация и консалтинг по устранению выявленных недочетов.



Региональный центр
информационных
технологий и связи

ЗАПРОС ОРГАНИЗАЦИИ

Сформировать реестр недопустимых событий и провести оценку их реализации.

РЕЗУЛЬТАТ

1. Сформирован реестр недопустимых событий.
2. Проведена оценка возможности их реализации.
3. Выданы рекомендации по устранению недочетов, итоги оформлены в виде технического и аналитического отчетов.
4. Аналитический отчет направлен во ФСТЭК России.

6. Мониторинг и реагирование на инциденты ИБ – SOCRAT

ЗАДАЧИ

- Выполнить требования законодательства (187-ФЗ, приказы ФСТЭК РФ № 117, № 239, приказы ФСБ РФ в части взаимодействия с НКЦКИ (ГосСОПКА)).
- Обеспечить непрерывный контроль защищенности инфраструктуры организации.
- Своевременно реагировать на атаки и противодействовать инцидентам ИБ.

КАКИЕ РАБОТЫ ВКЛЮЧАЕТ

1. Организация процесса непрерывного мониторинга событий ИБ.
2. Проведение периодических мероприятий: инвентаризация, анализ уязвимостей, тестирование на проникновение.
3. Взаимодействие с ГосСОПКА.



Медицинский
информационно-
аналитический центр

ЗАПРОС ОРГАНИЗАЦИИ

Обеспечить непрерывную информационную безопасность ЗОКИИ, выполнить требования НПА.

РЕЗУЛЬТАТ

1. Организован непрерывный мониторинг событий информационной безопасности, позволяющий оперативно выявлять, анализировать и реагировать на инциденты ИБ.
2. Выполнены требования регулятора.
3. Обеспечено взаимодействие с ГосСОПКА.

7. Киберучения по информационной безопасности

ЗАДАЧИ

- Выполнение требований законодательства (Приказ ФСТЭК России № 117).
- Формирование компетенций по кибербезопасности.
- Отработка навыков специалистов по выявлению и реагированию на инциденты ИБ.

КАКИЕ РАБОТЫ ВКЛЮЧАЕТ

1. Организация киберполигона и подготовка сценариев атак.
2. Запуск и отработка сценариев компьютерных атак участниками киберучений.
3. Подведение итогов, разбор сценариев и формирование итогового отчета.



Региональное министерство
цифрового развития

ЗАПРОС ОРГАНИЗАЦИИ

Получить независимую оценку уровня подготовки сотрудников к выявлению и реагированию на компьютерные атаки и инциденты.

РЕЗУЛЬТАТ

1. Проведена оценка готовности участников киберучений к выявлению и реагированию на инциденты ИБ.
2. Результаты оформлены в виде отчета.
3. Отчет направлен в ГосСОПКА.

8. Внедрение процессов РБПО

ЗАДАЧИ

- Обеспечение защищенности разрабатываемого ПО.
- Обеспечение соответствия требованиям НПА, регламентирующим РБПО (ГОСТ Р 56939-2024, приказы ФСТЭК России № 117, № 239 и № 240).
- Снижение вероятности реализации угроз безопасности информации, связанных с появлением уязвимостей при разработке ПО.

КАКИЕ РАБОТЫ ВКЛЮЧАЕТ

1. Аудит процессов РБПО и формирование комплекта документации.
2. Проведение исследований безопасности ПО, направленных на выявление уязвимостей и недекларированных возможностей с формированием подробных рекомендаций по их устранению.
3. Подбор, внедрение и интеграция инструментов безопасной разработки в рамках единой платформы разработки безопасного ПО.



Компания-разработчик
в сфере электроэнергетики

ЗАПРОС ОРГАНИЗАЦИИ

Осуществить выполнение требований НПА по безопасной разработке для разрабатываемой SCADA-системы.

РЕЗУЛЬТАТ

1. Внедрены инструменты РБПО, позволяющие проводить инструментальные исследования и минимизировать риски ИБ на всех этапах жизненного цикла.
2. Сформирован комплект документации по РБПО.
3. Проведена независимая оценка выполнения требований безопасности к ПО в соответствии с Приказом ФСТЭК России № 239 (п. 29.3).

9. Автоматизация бизнес-процессов

ЗАДАЧИ

- Выполнение требований законодательства (149-ФЗ, 152-ФЗ, 1119-ПП РФ, приказы ФСТЭК России № 117 и № 21) и повышение защищенности.
- Снижение влияния человеческого фактора и минимизация ошибок.
- Экономия ресурсов за счет автоматизации рутинных процессов.

КАКИЕ РАБОТЫ ВКЛЮЧАЕТ

1. Автоматизация разработки и ведения документации по защите объектов КИИ, ПДн, ГИС, а также контроль выполнения технических мер.
2. Автоматизация контроля подключения пользователей к ИС.
3. Автоматизация процессов учета и выдачи криптосредств и учета информационных ресурсов.
4. Автоматизация работы с инцидентами.



Региональное министерство
цифрового развития, связи
и массовых коммуникаций

ЗАПРОС ОРГАНИЗАЦИИ

Автоматизировать процессы и мероприятия по ИБ на уровне региона и обеспечить выполнение организационных требований НПА по защите ГИС и ПДн.

РЕЗУЛЬТАТ

1. Внедрена комплексная система для автоматизации бизнес-процессов ИБ (SGRC) на региональном уровне в защищенном исполнении.
2. Разработана организационно-распорядительная и техническая документация по защите информации.

10. Защита ГИС (включая требования 117 приказа ФСТЭК России)

ЗАДАЧИ

- Соответствие требованиям законодательства (149-ФЗ, 152-ФЗ, 676-ПП РФ, 1119-ПП РФ, приказы ФСТЭК России № 117 и № 21).
- Защита ГИС и предотвращение нарушений их функционирования из-за кибератак.
- Выполнение требований по взаимодействию с иными ГИС.

КАКИЕ РАБОТЫ ВКЛЮЧАЕТ

1. Аудит безопасности и разработка организационно-распорядительной документации и проектов документов для корректного ввода ГИС в эксплуатацию.
2. Внедрение подсистемы обеспечения информационной безопасности, анализ уязвимостей и пентест информационных ресурсов ГИС.
3. Аттестация ГИС и обеспечение ее защиты в ходе эксплуатации.



Оператор региональной ГИС
в сфере судопроизводства

ЗАПРОС ОРГАНИЗАЦИИ

Обеспечить безопасность информации, обрабатываемой в информационных системах организации.

РЕЗУЛЬТАТ

1. В организации внедрены организационные и технические меры по защите информации.
2. Обеспечена защита информации на 140 судебных участках.
3. Разработаны мероприятия для корректного ввода в эксплуатацию ГИС и проведена аттестация ГИС и ИСПДн.

Почему КСБ-СОФТ?

- ✓ Лицензиаты ФСТЭК и ФСБ России
- ✓ Экспертиза в выполнении требований по ИБ
- ✓ Уникальная инженерная команда со знанием АСУ ТП
- ✓ Экспертиза в сфере создания систем ИБ различной сложности
- ✓ Планирование работ с учетом бизнес-процессов клиента
- ✓ Предпроектные аудиты и макетирование
- ✓ Пилотирование решений до внедрения
- ✓ Обучение специалистов по практической кибербезопасности
- ✓ Научные исследования по безопасной разработке на базе созданной в ЧГУ им. Ульянова лаборатории

С нами работают:

КОММЕРЧЕСКИЕ ОРГАНИЗАЦИИ:

- ритейл, телеком, финансы, страхование, наука

СУБЪЕКТЫ КИИ:

- энергетика, здравоохранение, ТЭК, оборонная, металлургическая, химическая промышленность, транспорт, связь

ОРГАНЫ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ:

- министерства финансов, цифрового развития, здравоохранения, труда и социальной защиты

6000+

проектов

100+

ИБ-специалистов

80+

регионов внедрения

10+

лет на рынке



НАШИ ПАРТНЕРЫ



Список партнеров регулярно обновляется.
Актуальная информация о партнерах представлена
на нашем сайте – <https://ksb-soft.ru/partnery/>

БЕЗОПАСНОСТЬ НАЧИНАЕТСЯ ЗДЕСЬ



428000, г. Чебоксары,
пр-т Максима Горького,
18 Б, пом. 9

Филиал в г. Москва:

127015, г. Москва,
ул. Бутырская, 75



info@ksb-soft.ru



ksb-soft.ru



8 (800) 333-38-72



[Телеграм-канал
«Мнение Интегратора»](#)



[Канал МАХ
«Мнение Интегратора»](#)



[Подкаст
«Голос Интегратора»](#)



[Сайт
«КСБ-СОФТ»](#)



[Сообщество ВК
«КСБ-СОФТ»](#)



[Канал Rutube
«КСБ-СОФТ»](#)