



Кибербезопасность объектов КИИ: насущные проблемы и пути их решения

Спикер:

- Татьяна Егорова – заместитель руководителя департамента интеграционных решений по вопросам промышленной кибербезопасности, КСБ-СОФТ;





Системный интегратор
в сфере информационной
безопасности и импортозамещения
информационных технологий



Входим в ГК «Кейсистемс»



Лицензиат ФСТЭК России

Лицензиат ФСБ России

Проекты компании курируют опытные
ИБ-специалисты, аккредитованные
по международным сертификациям
OSCP, CISM, CGEIT и CISA.

80+

регионов
внедрения

4000+

реализованных
проектов

НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ

03



1 Домен «Непрерывная безопасность. SOCRAT»

Услуги центра мониторинга SOCRAT
Тестирование на проникновение (Pentest)
Анализ уязвимостей
Защита порталов (WAF)
Внедрение SIEM

2 Домен «Промышленность. Субъекты КИИ»

Безопасность объектов КИИ
Безопасность АСУ ТП

3 Домен «Безопасная разработка»

Аудит безопасности ПО
Внедрение процессов безопасной разработки (SDL)
Сертификация продуктов

4 Домен «Органы власти. ГИС»

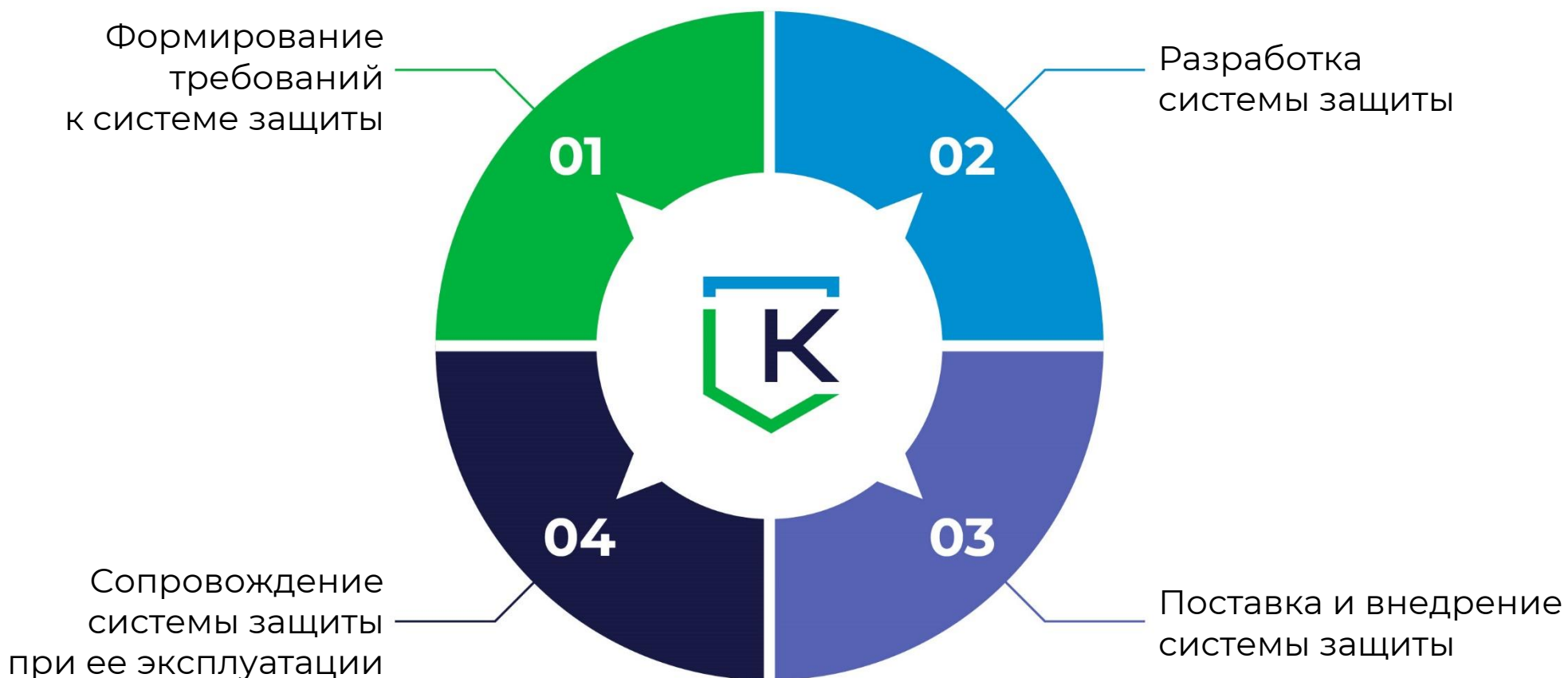
Защита информации в ГИС
Обеспечение жизненного цикла ГИС (676 ПП)
Инвентаризация ГИС и контроль подключения
(Экосистема Альфа)

5 Домен «Коммерция. Защита ПДн и коммерческой тайны»

Защита персональных данных
Защита коммерческой тайны
Защита от утечек информации (DLP)

6 Домен «ИТ-интеграция»

Импортозамещение
Внедрение ИТ-продуктов



ПОРТФОЛИО В ЧАСТИ ПРОМЫШЛЕННОЙ БЕЗОПАСНОСТИ ЗА 2023 Г.

06

Сфера: энергетика.

Конечный Заказчик: ПАО «Россети» и его филиалы.

Объекты защиты: АСУ ТП электрических подстанций 500 кВ, 330 кВ, 220 кВ

Работы: проектирование СИБ, пусконаладочные работы СИБ

Сфера: топливно-энергетический комплекс.

Конечный Заказчик: ООО «Арктик СПГ 2», АО «Верхнечонскнефтегаз» (ПАО «НК «Роснефть»)

Объекты защиты: АСУ по управлению электроснабжением, пожарной сигнализации и управления пожаротушением

Работы: проектирование СИБ, пусконаладочные работы СИБ

Сфера: транспорт.

Конечный Заказчик: ФГБУ «Канал имени Москвы»

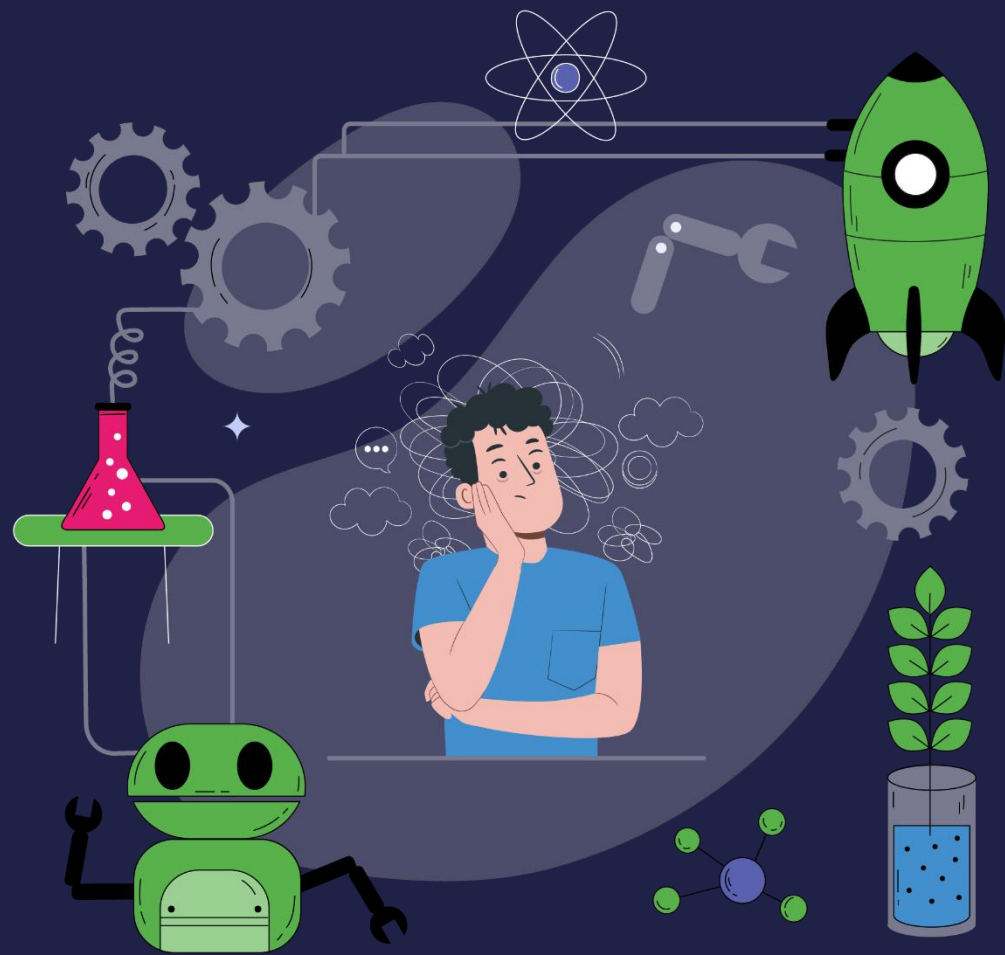
Объекты защиты: АСУ телемеханики, контроля шлюзования, судопропуска и т.д.

Работы: проектирование СИБ

НАСУЩНЫЕ ПРОБЛЕМЫ

07

- Отсутствие осознанного подхода по созданию СОИБ ОКИИ
- Раздел ИБ по «остаточном принципе»
- Коммуникации внутри субъектов КИИ
- Средства защиты информации
- Импортозамещение



ОТСУТСТВИЕ ОСОЗНАННОГО ПОДХОДА ПО СОЗДАНИЮ СОИБ ОКИИ

08



Подходы и способы реализации СОИБ имеют разнородный характер даже в рамках одного холдинга, группы компаний



К подрядчикам не предъявляются требования по ИБ



Не проводится обучение персонала правилам ИБ



Организационные меры разрабатываются не в полном объеме



Мероприятия, прописанные в ОРД, не выполняются



Нехватка специалистов ИБ

РАЗДЕЛ ИБ ПО «ОСТАТОЧНОМУ ПРИНЦИПУ»

09



Отсутствие проектного подхода к созданию системы ИБ



Проблемы с выделением бюджета на работы по ИБ



При проектировании АСУ ТП
Заказчики забывают заложить
требования по ИБ



Не выстроены процессы по ИБ



СОИБ не закладывается на стадии
проектирования АСУ ТП, в результате
чего СЗИ внедряются уже в рамках
функционирования АСУ ТП



Долгое согласование заявок
на проведение работ

КОММУНИКАЦИИ ВНУТРИ СУБЪЕКТОВ КИИ



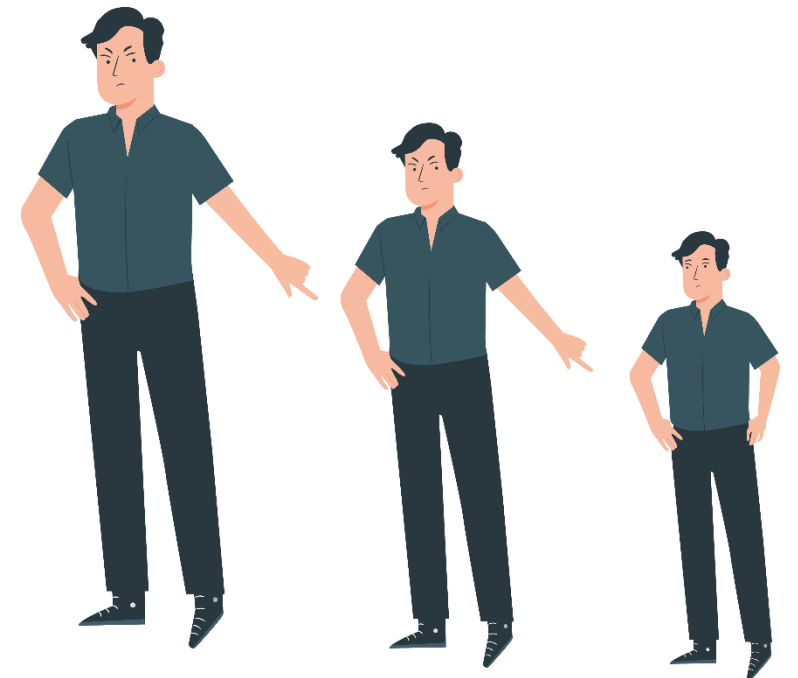
Недостаточное взаимодействие специалистов из разных служб/отделов (АСУ, связь, ИБ и т.д.)



Перекладывание ответственности



Низкая осведомленность персонала в вопросах ИБ



СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

11



На рынке мало СЗИ
в промышленном
исполнении



СЗИ должным образом
не пилотируются перед
внедрением



Перегруженная техподдержка
производителей



Политика лицензирования
СЗИ без учета специфики сферы

ИМПОРТОЗАМЕЩЕНИЕ

12



Отсутствие отечественных аналогов ПО и оборудования для АСУ ТП



Большинство АСУ ТП продолжает работать на уязвимых версиях ОС



Устаревшее ПО и оборудование АСУ ТП не совместимы с современными СЗИ

ВЫПОЛНЕНИЕ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА В ЧАСТИ КИИ

13



Седьмой год продолжаются бесконечные споры в части выделения ОКИИ, подлежащих категорированию и определения критических процессов



Субъекты КИИ стремятся уйти от категории значимости ОКИИ



В некоторых отраслях недавно опубликованные типовые перечни ОКИИ вызывают вопросы у субъектов КИИ



Отсутствует методический документ по выполнению требований 239 приказа ФСТЭК России



Обеспечение полноценного мониторинга ИБ и подключение к ГосСОПКА откладывается в долгий ящик



В НПА отсутствуют требования к подрядчикам в сфере КИИ



СО СТОРОНЫ СУБЪЕКТОВ КИИ:

- 1) Формирование осознанности первых лиц и персонала субъектов КИИ в части важности обеспечения ИБ
- 2) Выстраивание процессов внутри субъектов КИИ, прозрачное распределение ответственности
- 3) Регулярное обучение персонала правилам безопасной работы



СО СТОРОНЫ РЕГУЛЯТОРОВ:

- 1) Методические документы и публичные мероприятия по разъяснению требований НПА
- 2) Упрощение/ускорение процедуры сертификации СЗИ
- 3) Закрепление в НПА требований к подрядчикам в сфере КИИ



СО СТОРОНЫ ВЕНДОРОВ, ИНТЕГРАТОРОВ:

- 1) Более внимательное отношение к особенностям сферы
- 2) Оперативная и качественная техподдержка интеграторов
- 3) Постоянный обмен опытом, организация практических бесплатных вебинаров с разборами кейсов в части ИБ

ЧТО ТАКОЕ РАЗРАБОТКА БЕЗОПАСНОГО ПО (SSDLC)

15



SDLC (Software Development Lifecycle)

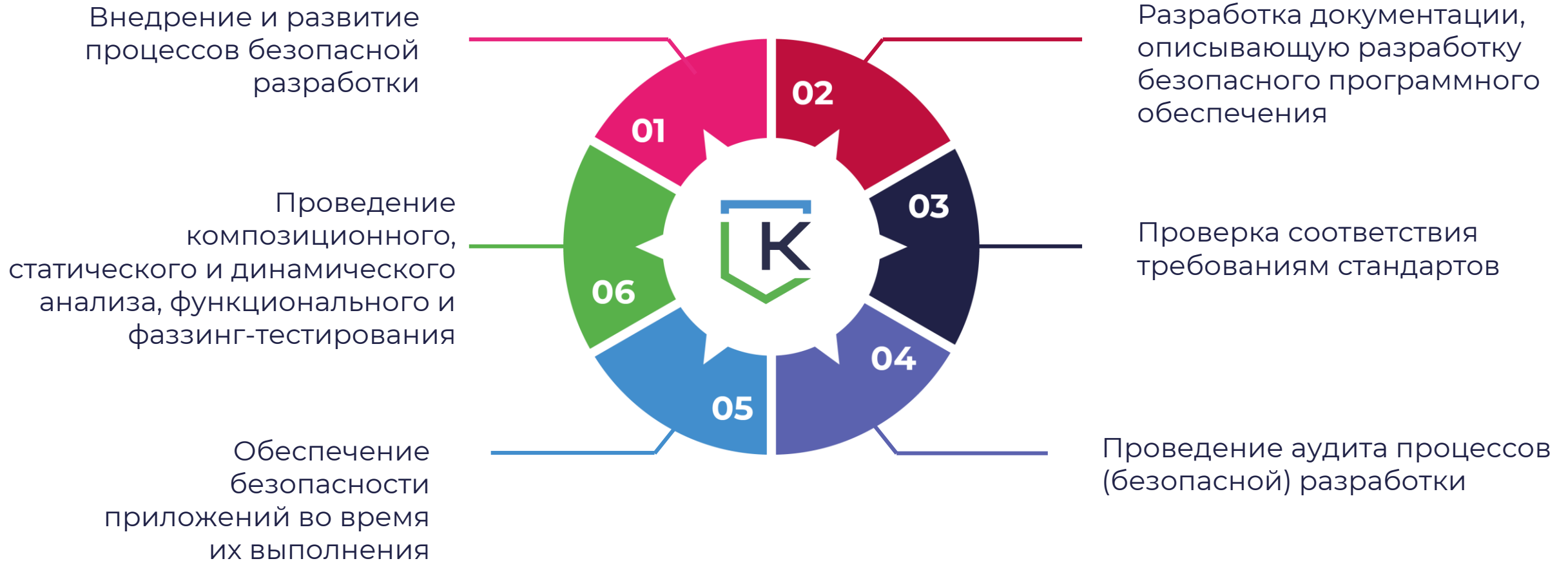
Жизненный цикл разработки ПО. SDLC подразумевает действия и задачи, которые осуществляются в ходе разработки ПО. В SDLC нет анализа безопасности разрабатываемого продукта.

SSDLC (Security Software Development Lifecycle)

Набор процедур безопасной разработки ПО, позволяющий обнаруживать и устранять уязвимости на ранней стадии, до публикации релиза продукта.

ЦЕНТР ЭКСПЕРТИЗЫ ПО БЕЗОПАСНОЙ РАЗРАБОТКЕ КСБ-СОФТ

16





SOCRAT – ЭТО ЦЕНТР МОНИТОРИНГА, КОТОРЫЙ:

Функционирует **24x7**

Является корпоративным
центром **ГосСОПКА** класса **A**
(<https://gossopka.ru/lists/centers/>)

Проводит периодические
мероприятия в соответствии
с **239** приказом **ФСТЭК**

Имеет **гибкий подход**
предоставления услуг

Год создания: **2020**

С ЧЕГО НАЧАТЬ?

18

ПИЛОТНОЕ ПОДКЛЮЧЕНИЕ

Вы можете бесплатно оценить качество предоставляемых услуг **SOCRAT**

Мониторинг: **8x5**

Время реагирования – **24 часа** с момента обнаружения

Ограниченный состав подключаемых ресурсов

Длительность пилота – **1 месяц**

+

Возможность пропилотировать **MP SIEM**

Демостенд



Пилот



Серверы



Консультации



Компания КСБ-СОФТ оказывает полный комплекс услуг по защите объектов КИИ

Мы поможем Вам защитить данные и выполнить требования НПА



Безопасность объектов КИИ

Выявление и категорирование объектов КИИ, разработка и внедрение комплексного решения по обеспечению безопасности значимых объектов КИИ, организация взаимодействия с центром ГосСОПКА, анализ уязвимостей и пентест



SOCRAT - центр мониторинга и реагирования на инциденты информационной безопасности

Мониторинг и предотвращение атак на начальных стадиях, либо выявление следов проникновения

[просмотреть вебинар](#)



Импортозамещение

Решение задач импортозамещения в соответствии со стратегией развития информационного общества в Российской Федерации

ПК АльфаДок. Автоматизация процессов по защите информации



- Разработка и актуализация документации, журналов
- Учет защищаемых ресурсов и средств защиты информации
- Моделирование угроз безопасности и определение мер по защите информации
- Оценка защищенности систем, анализ уязвимостей
- Категорирование объектов КИИ с разработкой документации в соответствии с приказом ФСТЭК России № 239
- Планирование деятельности, оценка готовности к проверкам
- Учет и реагирование на инциденты информационной безопасности

Работайте с нами!



<https://ksb-soft.ru/>



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



8 800 3333-872



info@ksb-soft.ru



Телеграм-канал
«Мнение интегратора»

