Как непрерывно обеспечивать информационную безопасность в ГИС. Новые предложения ГК «Кейсистемс»

Сергеев Сергей Николаевич

Заместитель генерального директора ООО «Кейсистемс»

Шипицын Михаил Юрьевич

Заместитель генерального директора ООО «КСБ-СОФТ»

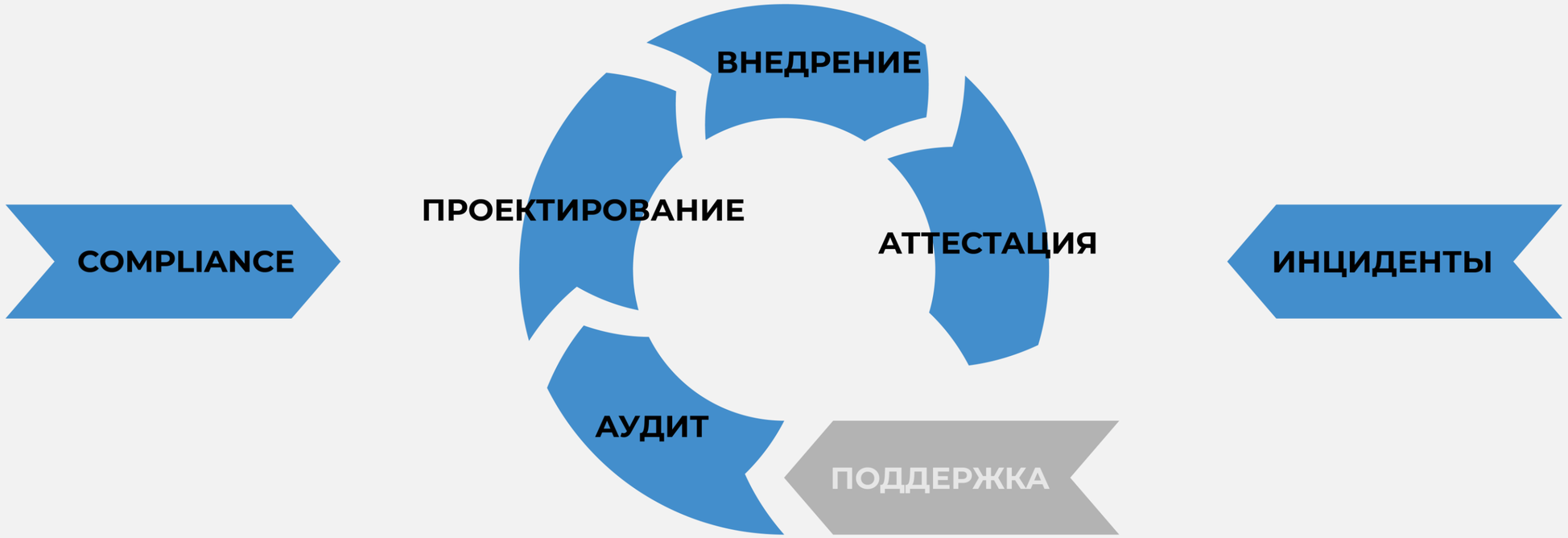
О чем сегодня поговорим?

1 Информационная безопасность как сервис

2 Центр мониторинга SOCRAT

3 Экосистема Альфа

Технологический суверенитет и ИБ



1. Часто поддержка НЕ осуществляется
2. Дорогая процедура аттестации

Истории мира ИБ

- Мы давно импортозаместились. А информационная безопасность?
  Эмм… безопасность?
- Сейчас мы купим 100 отечественных ОС и сразу внедрим их без проблем…
- У нас уже 5 лет аттестована ГИС, все под защитой. А как же периодические мероприятия? Какие такие мероприятия, есть же действующий аттестат!
- У нас есть ViPNet\Континент\др. МЭ, враг не пройдет! Как зашифровали базу?
  Как они обошли наш МЭ?
- Что это значит злоумышленник сидел в нашей инфраструктуре полгода?
  Он что читал мои письма?
- Да я всего лишь файл из письма открыл, оно же от главного бухгалтера.
  Как Она в отпуске в Тайланде без доступа к интернету?…
- У нас уже куплена и работает SIEM система, да-да и IDS\XDR\NAT, все уже есть.
  Что значит смотрят ли Ваши сотрудники события в SIEM системе, а зачем?
  Мы для чего её покупали, чтобы еще туда смотреть и выявлять инциденты?!

Предпосылки непрерывной безопасности

1

Внедрение импортонезависимого оборудования и ПО (железо, СУБД, виртуализация, ОС, офис, резервное копирование, прикладное ПО и пр.)

vs Защищенный хостинг

2

Требования НПА в ГИС (аудит, инвентаризация, учет СКЗИ, 676 ПП, ПОИБ ГИС, анализ уязвимостей, аттестация, техподдержка)

3

Подключение внешних пользователей (регламентация доступа, VPN, контроль актуальности версий и сроков действия СЗИ)

4

Цифровой документооборот (сокращение бумаги, цифровая среда доверия, адаптация БП, прозрачная цепочка движения и подписания, дистанционное подписание, юридическая значимость)

Предпосылки непрерывной безопасности

5

Техподдержка как сервис (обновление СЗИ, актуализация ОРД, обучение, настройка СЗИ, поддержка при проверках регуляторов)

6

Проактивная защита от киберугроз (исследования кода прикладного ПО, безопасность контейнеров, защита веб-приложений, анализ сетевого трафика, управление уязвимостями)

7

Мониторинг и реагирование на инциденты ИБ (инвентаризация ресурсов, учет инцидентов, реагирование, расследование, периодический анализ уязвимостей, подключение к ГОССОПКА)

Сервисная модель обслуживания: «Непрерывная поддержка аттестованной ГИС»

Порядок действий:

- проводим ревизию аттестованной ГИС;
- готовим индивидуальное предложение;
- вы получаете предсказуемый бюджет на поддержку.

Качество информационной безопасности

Расход на аттестацию и поддержку ГИС

Состав «Непрерывной поддержки аттестованной ГИС»

Что входит в «Базовую непрерывную поддержку аттестованной ГИС»:

- Актуализация документации;
- Дистанционная конфигурация\настройка СЗИ;
- Пересмотр модели угроз;
- Пересмотр проектного решения;
- Контроль защищенности, либо повторная аттестация;
- Консультации при проверках.

Что может входить в «Расширенную непрерывную поддержку аттестованной ГИС»:

Базовый пакет +

- Обновление СЗИ при выходе новых версий;
- Очная Конфигурация\настройка СЗИ;
- Периодический анализ уязвимостей;
- Периодическое тестирование на проникновение (Pentest);
- Защита контейнеров;
- Поддержка WAF, VM, NTA и др.

Новые требования регуляторов

- Перечни типовых ОКИИ
- Запрет на иностранные СЗИ с 1 января 2025 (указ № 250)
- SDL ГОСТы
- Две методики оценки ФСТЭК
- Изменения ПДн (ФЗ № 266-ФЗ)
- [планы ФСТЭК] обновить 17 приказ

Обзор писем

1	Атака через поставщика
2	Письма ФСТЭК
3	SDL
4	Отечественное ПО
5	Защита WEB

КСБ-СОФТ

Непрерывная поддержка аттестованной ГИС

Расширенная непрерывная поддержка аттестованной ГИС

SOC RAT
SECURITY OPERATION CENTER RUSSIAN ANALYTICS TEAM

SOC RAT
SECURITY OPERATION CENTER RUSSIAN ANALYTICS TEAM

SOCRAT – ЭТО ЦЕНТР МОНИТОРИНГА, КОТОРЫЙ:

Функционирует 24x7

Является корпоративным центром ГосСОПКА класса А

Проводит периодические мероприятия в соответствии с 239 приказом ФСТЭК

Имеет гибкий подход предоставления услуг

Год создания: 2020

КАКИЕ ВОЗМОЖНОСТИ ОТКРЫВАЮТСЯ ПРИ ПОДКЛЮЧЕНИИ К SOCRAT

Выявление и устранение потенциальных векторов атак

BDU:2022-01141
CVE-2022-27228

Уязвимость модуля «vote» системы управления содержимым сайтов (CMS) 1С-Битрикс: Управление сайтом связана с возможностью отправки специально сформированных сетевых пакетов. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, записать произвольные файлы в уязвимую систему

Уязвимое ПО:
- (1С-Битрикс: Управление сайтом), до 22.0.400 (vote)

Дата выявления: 2022-03-04

Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10)
Критический уровень опасности (базовая оценка CVSS 3.0 составляет 9,8)

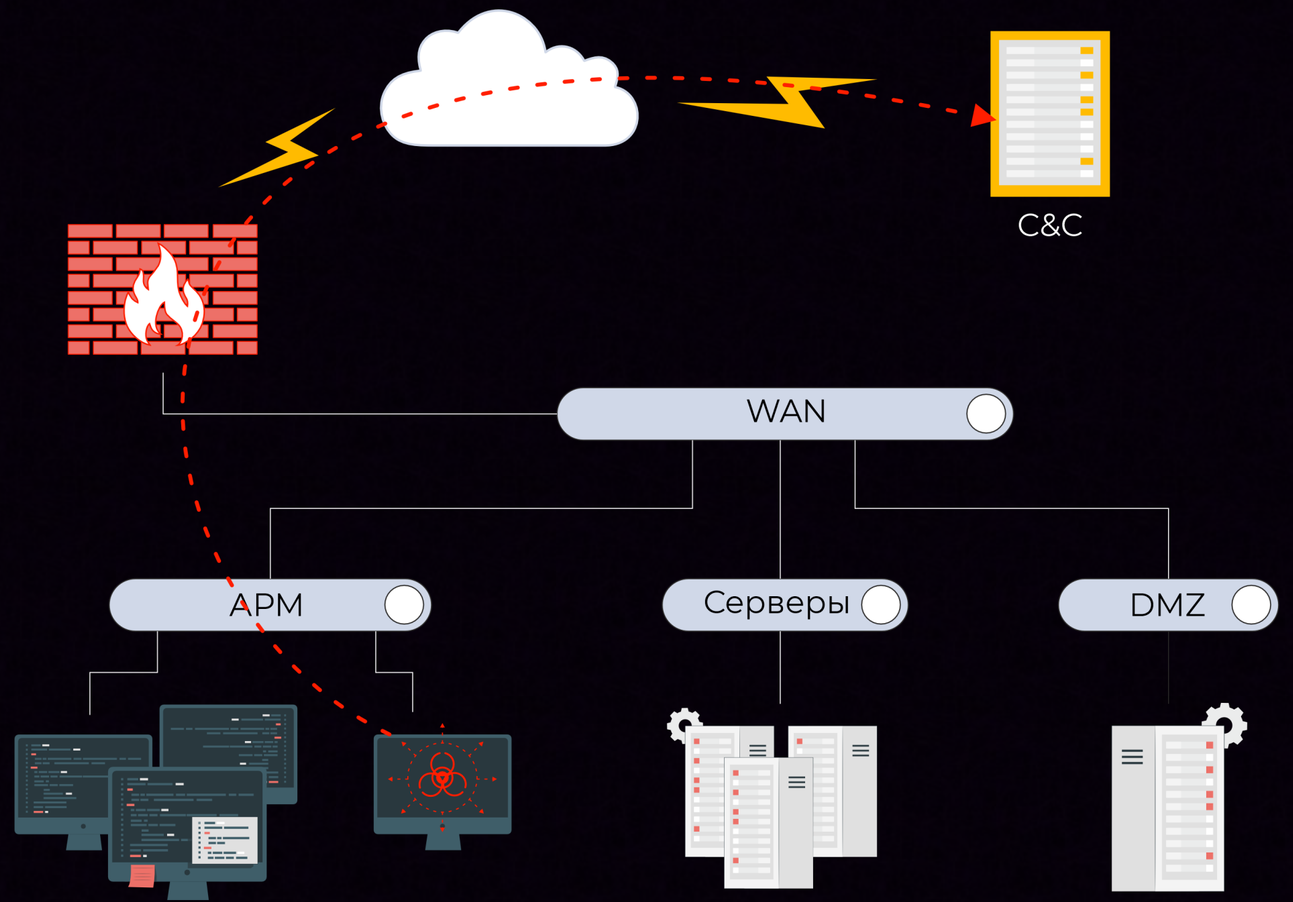
Проверка эффективности системы защиты

Index of / employee_data

Name	Last modified	Size	Description
Parent Directory		-	
List_of_employee_jan_2022.csv	2022-01-31 23:50	1632K	
List_of_employee_feb_2022.csv	2022-02-28 23:50	1428K	
List_of_employee_mar_2022.csv	2022-03-31 23:50	1816K	

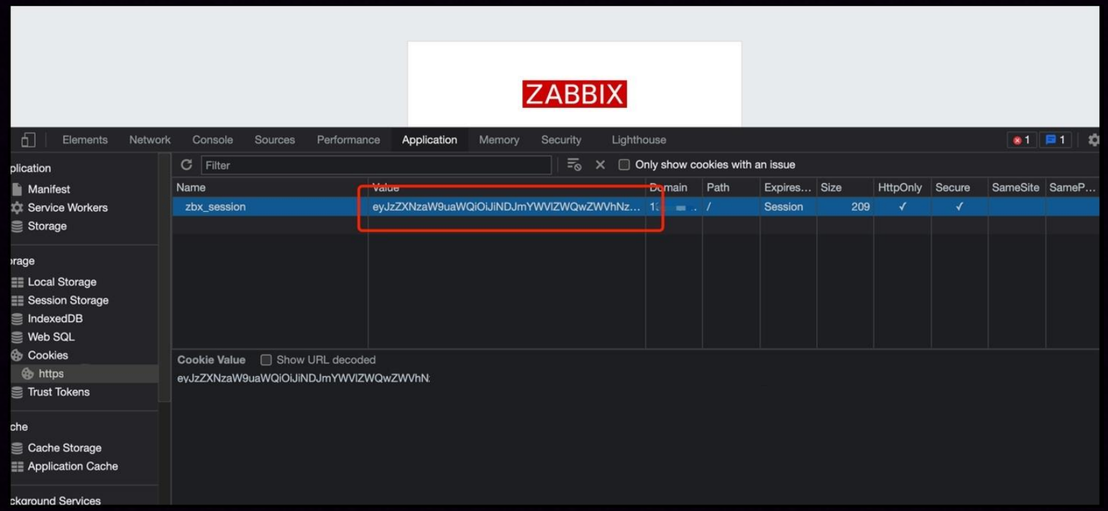
КАКИЕ ВОЗМОЖНОСТИ ОТКРЫВАЮТСЯ ПРИ ПОДКЛЮЧЕНИИ К SOCRAT

Выявления следов компрометации



КАКИЕ ВОЗМОЖНОСТИ ОТКРЫВАЮТСЯ ПРИ ПОДКЛЮЧЕНИИ К SOCRAT

Выявление атак в режиме реального времени и противодействие им



КАКИЕ ВОЗМОЖНОСТИ ОТКРЫВАЮТСЯ ПРИ ПОДКЛЮЧЕНИИ К SOCRAT

Помощь в выполнении требований НПА

С ЧЕГО НАЧАТЬ?

ПИЛОТНОЕ ПОДКЛЮЧЕНИЕ

Вы можете бесплатно оценить качество предоставляемых услуг SOCRAT

НЕМНОГО ОБ ИНСТРУМЕНТАХ: ЭКОСИСТЕМА АЛЬФА

альфа|док

- Учет ГИС, ИТ-активов и СЗИ, входящих в состав ГИС
- Классификация ГИС и ИСПДн
- Моделирование угроз, определение требований по защите ГИС и ПДн
- Разработка документации по защите ГИС, ПДн
- Выполнение требований по обработке ПДн
- Контроль корректности и достаточности применения СЗИ, сроков действия лицензий, сертификатов, аттестатов

альфа|коннект

- Создание цифровых регламентов по подключению пользователей к ГИС
- Автоматизация процесса подачи и обработки заявок на подключение пользователей
- Контроль выполнения требований по подключению к ГИС
- Ведение реестра пользователей

альфа|крипто

- Учет СКЗИ в соответствии с требованиями ФСБ России
- Автоматизация процесса выдачи СКЗИ
- Контроль сроков действия лицензии и сертификатов

БОЛЬШЕ ТОЧНОСТИ, МЕНЬШЕ ЗАТРАТ: АВТОМАТИЗАЦИЯ ПРОЦЕССОВ УЧЁТА И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННЫХ РЕСУРСОВ КЕМЕРОВСКОЙ ОБЛАСТИ – КУЗБАССА

Результаты:

К началу 2024 года оцифровка процессов ведения реестра ИС/ГИС, подключения пользователей, заключения ИТ-соглашений позволила достичь следующих показателей эксплуатации платформы:

- объединено 1746 организаций (3716 пользователей);
- сформировано 14958 заявок от пользователей на услуги;
- переведено в электронный вид 42 процесса.

Отзыв Министерства цифрового развития и связи Кузбасса:

«Внедрение информационной системы «Реестр государственных информационных систем Кемеровской области – Кузбасса», основанной на экосистеме «Альфа», позволил кратно снизить трудозатраты специалистов Минцифры Кузбасса при рассмотрении заявок на подключение к государственным информационным системам и иным информационным системам, находящимся в ведении Министерства. Перевод в электронный вид процесса учёта информационных систем реализовал возможность в кратчайшие сроки инвентаризировать не только государственные информационные системы, но и иные информационные системы региона».

ЭФФЕКТИВНЫЙ ПОДХОД К УЧЁТУ И ВЫДАЧЕ КРИПТОСРЕДСТВ В МИНИСТЕРСТВЕ ФИНАНСОВ ЧЕЛЯБИНСКОЙ ОБЛАСТИ: АВТОМАТИЗАЦИЯ ДЛЯ ОПТИМИЗАЦИИ ПРОЦЕССОВ

Результаты:

Внедрение приложения АльфаКрипто позволило Министерству:

- автоматизировать процессы учёта, выдачи СКЗИ и создания сопроводительной документации при работе с криптосредствами;
- в разы увеличить скорость выдачи криптосредств и сократить время ожидания для клиентов. Система автоматически генерирует лицевые счета и при необходимости даёт сотруднику возможность вносить необходимые правки. Операторы больше не тратят время на создание документации и перенос сведений в журналы. Сотруднику ОКЗ нужно всего 10 минут, чтобы принять пользователя, выдать криптосредство и собрать необходимые подписи. Также ОКЗ может контролировать внутренний учёт обращавшихся ранее за выдачей криптосредств организаций.

Работайте с нами!

КСБ-СОФТ

1) Заполните анкету
2) Подключайте нашу «Непрерывную поддержку аттестованной ГИС»
3) Подключайте бесплатный пилот SOCRAT
4) Обращайтесь и мы поможем

Сайт компании
КСБ-СОФТ

Телеграм-канал
«Мнение Интегратора»

Подкаст
«SOCRAT за стеклом»

8 800 3333-872

+7 (8352) 322-322

info@ksb-soft.ru