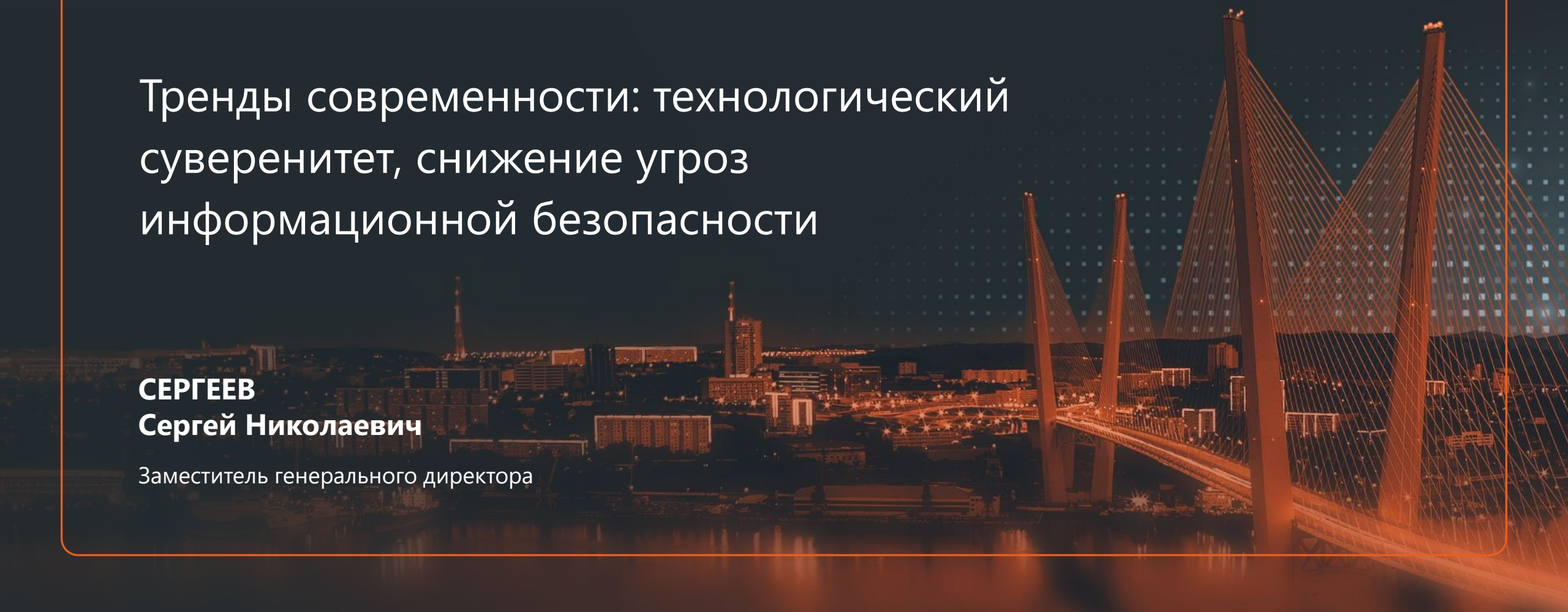
КЕЙСИСТЕМС

Тренды современности: технологический суверенитет, снижение угроз информационной безопасности



СЕРГЕЕВ
Сергей Николаевич

Заместитель генерального директора

Тренды

О текущем моменте

- **«Бум деклараций» от российских производителей** — нам обещают операционные системы, СУБД, средства управления инфраструктурой, виртуализацией, офисные приложения, ERP, управление производством и т.д.
- **Режим «сделай сам» — время дезинтеграции и нетиражируемых «зоопарков»** — на рынке еще значимое время не будет хорошо интегрированных, надежных в любой среде, широко совместимых и устойчивых к изменениям решений и технологий
- **«Цифра на всю голову»** — драматическое падение доступного для широкой массы потребителей уровня зрелости проектной практики, качества решений, профессионального уровня и опыта аналитиков, непрерывное усугубление проблемы дефицита квалифицированных специалистов

Прогнозы на 2024 год подтверждаются

- **Повышенная активность вымогателей и хактивистов:** злоумышленники продолжают уже устоявшуюся традицию вымогательства за восстановление систем и неразглашение утечек. Госсектор и связанные с ним организации традиционно в приоритете
- **Атаки на цепочки поставок:** ИТ-компании стали все чаще подвергаться атакам злоумышленников, ввиду того что подобные компании можно использовать как часть атак supply chain на те организации, которые пользуются их услугами и продуктами
- **Уязвимости в ИТ будут влиять на киберустойчивость многих отраслей:** большое количество уязвимостей в различных решениях оказывает влияние на устойчивость к кибератакам различных отраслей — от государственных организаций до сферы услуг

Информационная безопасность: о текущем моменте

КИИ

С 1 января 2025 года органам государственной власти запрещается использовать иностранное программное обеспечение на объектах критической информационной инфраструктуры

В целом готовность [средств защиты информации на объектах КИИ] можно оценивать высоко, для большинства есть аналоги. Есть технологические проблемы с высокопроизводительными средствами защиты, но для них есть нормативные акты и активно ведется совершенствование их характеристик.

Евгений Хасин, Минцифры России

Новые требования проекта приказа ФСТЭК

Требования будут предъявляться не только **для ГИС**, но **и для иных ИС** государственных органов / учреждений / унитарных предприятий

Расширение и уточнение перечня мер защиты.
Определены новые меры по защите:
- Web-приложений
- мобильных устройств
- средств контейнеризации

Формирование **Политики защиты информации:** оператор определяет **стратегию защиты информации**, содержащейся **в информационных системах оператора**

Инвентаризация информационных систем и управление их конфигурациями. Допускается использовать **автоматизированные средства сбора и хранения данных** об объектах

Новые требования проекта приказа ФСТЭК

Оператору или **ответственному лицу** предстоит **определить структурное подразделение** или назначить **отдельных специалистов**, на которых возлагаются функции **по защите информации**

С учетом структуры и состава структурного подразделения, численности специалистов по защите информации для отдельных функций по защите информации **оператор** привлекает **организации**, **имеющие лицензию** на деятельность по технической защите конфиденциальной информации

Специалисты по защите информации **должны обладать знаниями** и **умениями**, необходимыми для выполнения возложенных на них обязанностей **по защите информации**

Новые требования проекта приказа ФСТЭК

- Добавляется оценка показателей состояния защиты информации и уровня зрелости, требующая от оператора предоставления данных во ФСТЭК с определенной периодичностью
- Много требований по организации удаленного доступа, например, не допускается использование небезопасных протоколов (telnet, ldap, http, ftp, SMB v.1)
- При использовании в системе более 30 мобильных устройств обеспечивается автоматизированное управление и контроль применения мобильных устройств
- Оператор обеспечивает мониторинг информационной безопасности. По решению руководителя оператора может создаваться отдельное структурное подразделение или привлекаться подрядная организация, имеющая лицензию (с правом оказания услуг по мониторингу)

Новые требования проекта приказа ФСТЭК

- Ежегодная отправка отчета оператором о результатах мониторинга в ФСТЭК
- Должно быть обеспечено взаимодействие с ГосСОПКА и Центром мониторинга и управления сетью связи общего пользования для противодействия атакам, направленным на отказ в обслуживании

Непрерывное обеспечение информационной безопасности

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** (исследование 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

Непрерывная поддержка аттестованной ГИС

Расширенная непрерывная поддержка аттестованной ГИС

SOCRAT

SECURITY OPERATION CENTER RUSSIAN ANALYTICS TEAM

Центр мониторинга и реагирования на инциденты (SOC – Security Operation Center)

SOC RAT
SECURITY OPERATION CENTER RUSSIAN ANALYTICS TEAM

SOCRAT
SECURITY OPERATION CENTER RUSSIAN ANALYTICS TEAM

SOCRAT – ЭТО ЦЕНТР МОНИТОРИНГА, КОТОРЫЙ:

Функционирует 24×7

Является корпоративным центром ГосСОПКА класса А

Проводит периодические мероприятия в соответствии с 239 приказом ФСТЭК

Имеет гибкий подход предоставления услуг

Год создания: 2020

КАК РАБОТАЕТ 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)

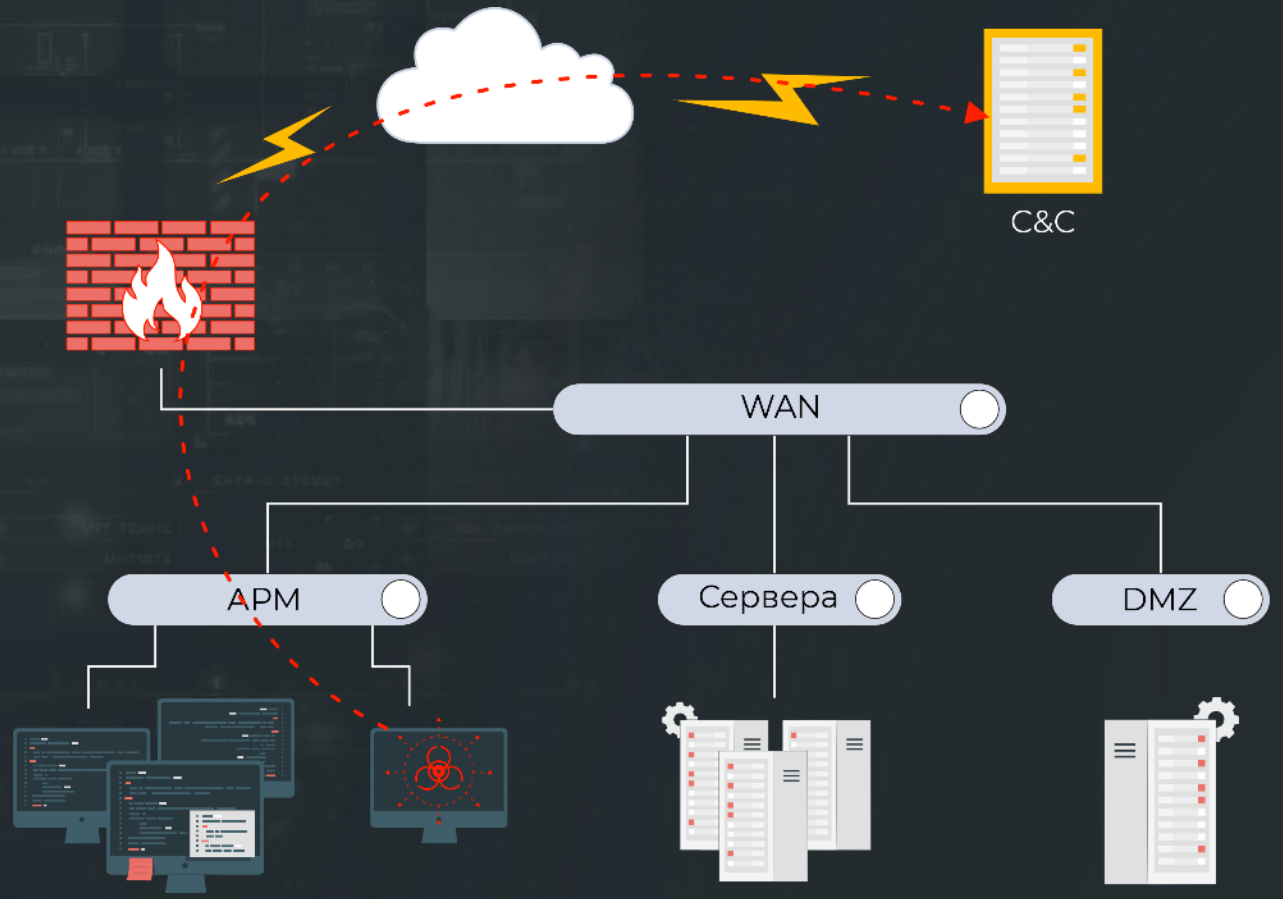
Дата выявления: 2022-03-04

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

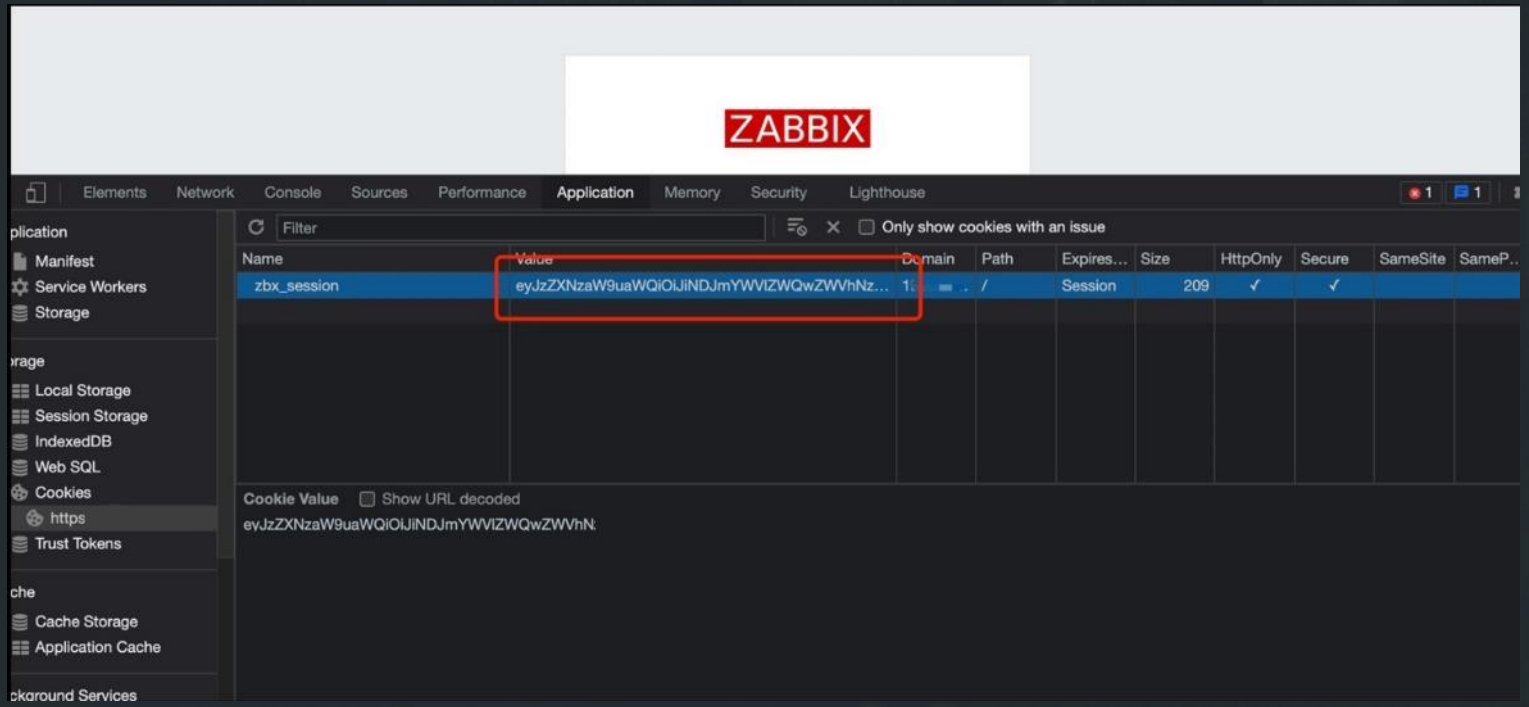
КАК РАБОТАЕТ SOCRAT

Выявления следов компрометации



КАК РАБОТАЕТ SOCRAT

Выявление атак в режиме реального времени и противодействие им



С ЧЕГО НАЧАТЬ?

ПИЛОТНОЕ ПОДКЛЮЧЕНИЕ

Вы можете бесплатно оценить качество предоставляемых услуг SOCRAT

Экосистема приложений Альфа


Здравоохранение
311 организаций
Энергетика
98 организаций
Финансы
72 организации
Высшее образование
59 организаций
Связь
49 организаций
Торговля
35 организаций
Нефтехим
31 организация
Машиностроение
29 организаций
Транспорт
28 организаций
Культура и искусство
17 организаций
Нефте- и газодобыча
8 организаций
85
субъектов
Российской Федерации
3000+
организаций
действующих пользователей
2500+
государственных
органов и учреждений
1000+
субъектов КИИ
400+
коммерческих организаций

альфа|док

Автоматизация организационных мер по защите ПДн, КИИ, ГИС

- Автоматическая разработка и актуализация комплекта документов по обработке и защите информации
- Формирование технической документации для построения системы защиты информации
- Мониторинг изменений и контроль защищенности информационных ресурсов

альфаКрипто

Автоматизация выполнения требований законодательства по учету и выдаче СКЗИ

- Автоматизация процессов учета и выдачи СКЗИ
- Существенное снижение нагрузки на сотрудников
- Выполнение требований ФСБ России
- Создание единого портала по работе с криптосредствами

альфа|коннект

Автоматизация процессов подключения пользователей к ИС и контроль выполнения ими предъявляемых требований

- Регламентация доступа пользователей
- Автоматизация контроля подключения пользователей к ИС
- Снижение риска доступа нелегальных пользователей, а также доступа с незащищенных АРМ

альфа|реестр

Учет информационных ресурсов (ИС/ГИС/ИСПДН) в регионе и сложных организационных структурах

Помогает получить информацию о системах с подведомственных учреждений

- Автоматизация процесса сбора информации об ИС/ГИС и иных типов информационных систем
- Публикация сведений реестра ИС/ГИС в интернете
- Формирование визуального ИТ-ландшафта

КЕЙСИСТЕМС

@keysystems

@ks_it

8 (8352) 323-323

info@keysystems.ru

keysystems.ru

г. Чебоксары,
ул. К. Иванова, д. 50