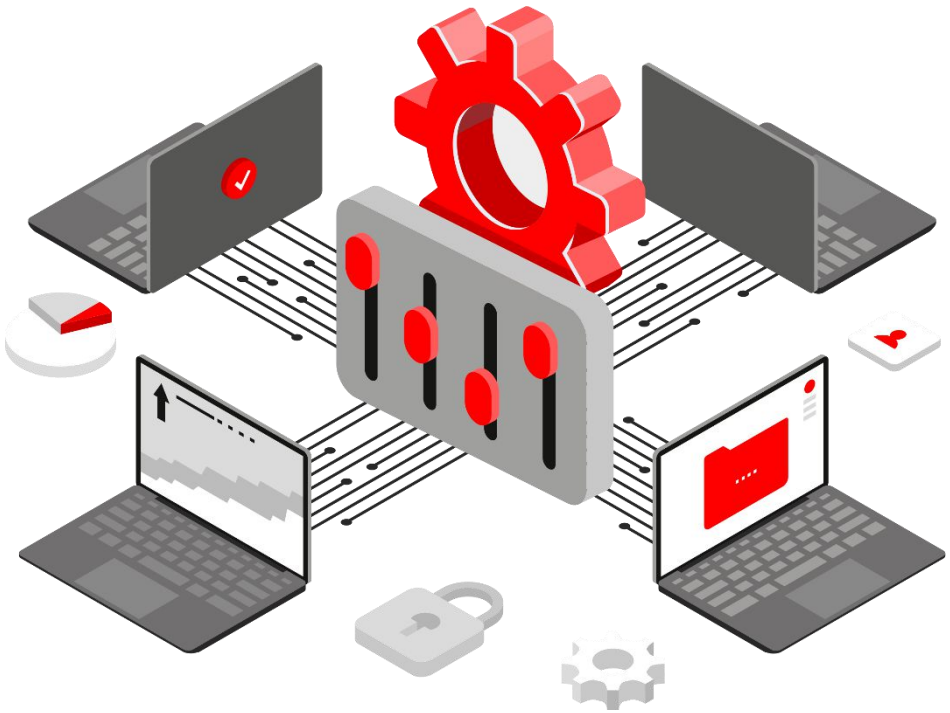
SPACE·BIT

X·CONFIG

Система управления уязвимостями конфигураций программного обеспечения



www.spacebit.ru

Уязвимости, связанные с человеческим фактором

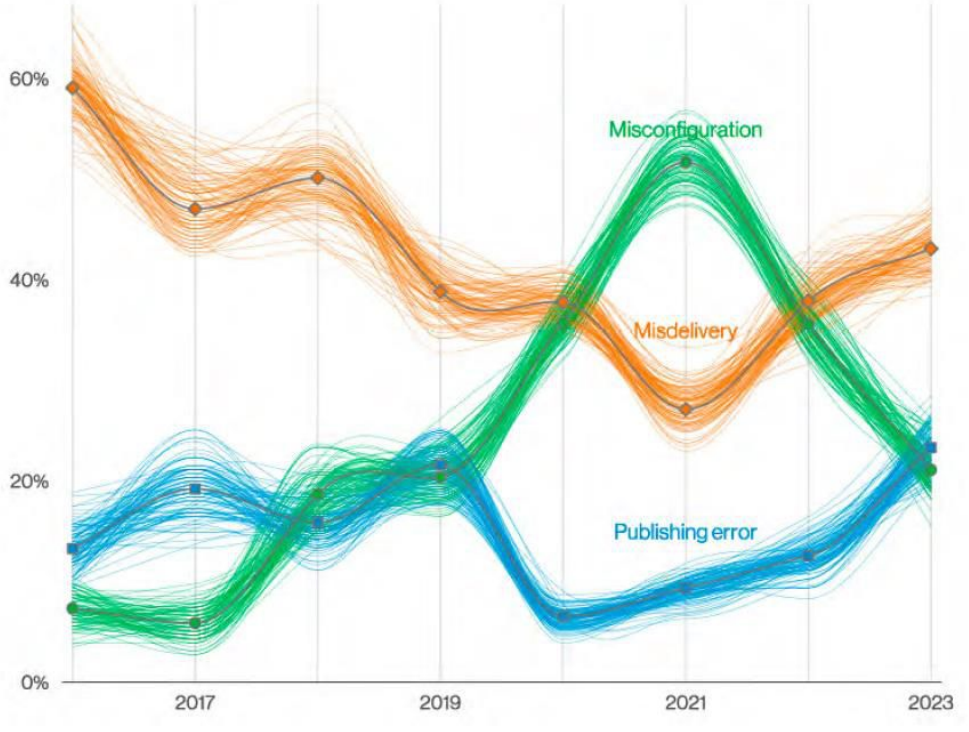


Figure 41. Action varieties over time in Miscellaneous Errors breaches

- **Небезопасные настройки**
- **Ошибки при доставке данных**
- **Ошибки при публикации**

(c) Data Breach Investigations Report, Verizon, 2023

Управление уязвимостями в информационных системах

Категория уязвимости	Распространенные методы предотвращения уязвимостей данной категории	Зона ответственности
Уязвимости проектирования	▪ Моделирование угроз и нарушителей ▪ Включение требований безопасности в задание на создание системы	Разработчик
Уязвимости реализации	▪ Анализ безопасности исходного кода приложений ▪ Тестирование безопасности при приемке системы ▪ Устранение выявленных уязвимостей уровня реализации	Разработчик
Уязвимости конфигурации	▪ **Разработка и применение стандартов безопасной конфигурации** ▪ **Периодическое тестирование безопасности** ▪ **Периодическое сканирование уязвимостей** ▪ **Установка обновлений безопасности, устраняющих известные уязвимости**	**Потребитель**

ЛЮБАЯ СИСТЕМА, ДАЖЕ НЕ ОБЛАДАЮЩАЯ УЯЗВИМОСТЯМИ УРОВНЯ ПРОЕКТИРОВАНИЯ И РЕАЛИЗАЦИИ, ПРЕДСТАВЛЯЕТ СОБОЙ СУЩЕСТВЕННУЮ УГРОЗУ БЕЗОПАСНОСТИ, ЕСЛИ ОНА НЕ СКОНФИГУРИРОВАНА ДОЛЖНЫМ ОБРАЗОМ

Этапы работ по управлению уязвимостями

(с) Руководство по организации процесса управления уязвимостями в органе (организации), ФСТЭК, 17 мая 2023 г.

Требования регуляторов (профили стандартов безопасного конфигурирования)

- Торговые предприятия
- Финансовые учреждения
- Разработчики ПО и аппаратного обеспечения для этих областей
- Сервис-провайдеры

PCI DSS

- Здравоохранение
- Наука
- Транспорт
- Связь
- Энергетика
- Финансовый сектор
- Топливно-энергетический комплекс
- Атомная энергетика

КИИ (ФЗ-187)

- Финансовые и страховые организации

Банк России (ГОСТ Р57580.1 2017)

X-CONFIG

Система управления уязвимостями конфигураций информационных ресурсов. Решение позволяет выстроить постоянный процесс управления конфигурациями программного обеспечения и снизить риски ИБ, связанные с некорректной настройкой ПО.

X-Config необходим, если:

- **Отсутствует актуальная информация** о состоянии конфигураций ПО с точки зрения ИБ
- В результате аудита **образуется большой объем неструктурированных и неприоритизированных данных**
- **Большая нагрузка на ИТ и ИБ-службы** в результате отсутствия выстроенного процесса
- Используемые **групповые политики не закрывают проблему**, необходим контроль

Возможности X-Config

Обеспечение соответствия требованиям и лучшим практикам конфигурации ПО
Система отслеживает соответствие ресурсов требованиям регуляторов, а также лучшим общепризнанным практикам безопасного конфигурирования

Приоритизация несоответствий по степени критичности
Система автоматически расставляет приоритеты для ликвидации выявленных уязвимостей и отслеживает их устранение

Инвентаризация ресурсов сети
Система проводит инвентаризацию защищаемых машин, в рамках которой определяются: тип аппаратного обеспечения, платформа (ОС), установленное ПО, обновления, открытые сетевые порты

Организация процесса управления уязвимостями конфигураций ПО
Система выстраивает рабочий процесс по управлению конфигурациями ПО на основе политик ИБ, проверяет ресурсы, контролирует фактическое закрытие уязвимостей и формирует отчеты

Формирование корпоративных политик безопасного конфигурирования
Механизм профилирования позволяет вносить изменения в готовые стандарты в соответствии с внутренними политиками

Оптимизация для применения в крупных разветвленных инфраструктурах
Сеть коллекторов позволяет масштабировать сбор информации о конфигурациях до необходимой производительности

Ролевая модель взаимодействия

Администратор X-Config	Главный офицер безопасности	Офицер безопасности	ИТ специалист
управляет всеми настройками и пользователями системы	утверждает профили стандартов безопасного конфигурирования	наполняет реестр ресурсов, заводит задачи, создает профили проверки	на основе отчетности организует работы по устранению уязвимостей

Преимущества X-Config

Поддержка лучших практик безопасного конфигурирования и богатая собственная экспертиза

Проработанная регулярно расширяемая **библиотека готовых стандартов** с информацией по каждой настройке

Гибкое профилирование стандартов, учитывающее неоднородность и индивидуальность каждой инфраструктуры

Безагентная технология не требует установки дополнительного ПО и более безопасна

Возможность кастомизации решения с учетом бизнес-задач, а также индивидуальной разработки стандартов

Возможность интеграции с другими средствами защиты информации (SIEM, IRP, SOAR, CMDB)

Масштабируемость для обслуживания десятков тысяч хостов в рамках одной инсталляции системы

Полностью **российская разработк**а (номер в Реестре российского ПО 7045), техподдержка и сопровождение проектов от вендора

Стандарты безопасного конфигурирования (СБК)

Системное ПО:

Windows:

- Windows Server 2012/2016/2019/2022
- Windows 10/11

***NIX:**

- Astra Linux SE/CE
- РЕД ОС
- ОС Альт
- ОС Атлант
- AlterOS
- CentOS 7/8
- Ubuntu 18/20/22
- RHEL 7/8
- Debian 10/11/12
- OpenSUSE
- FreeBSD 12/13/14

Прикладное ПО:

Веб-серверы:

- Nginx/Angie PRO
- Microsoft IIS
- Apache HTTP Server

Контейнеры сервлетов:

- Apache Tomcat 9/10

Почтовые серверы:

- Microsoft Exchange Server
- Postfix/RuPost

СУБД:

- PostgreSQL/Postgres Pro
- Microsoft SQL Server
- Oracle DB
- Apache Cassandra

Офисное ПО:

- Microsoft Office

Веб-браузеры:

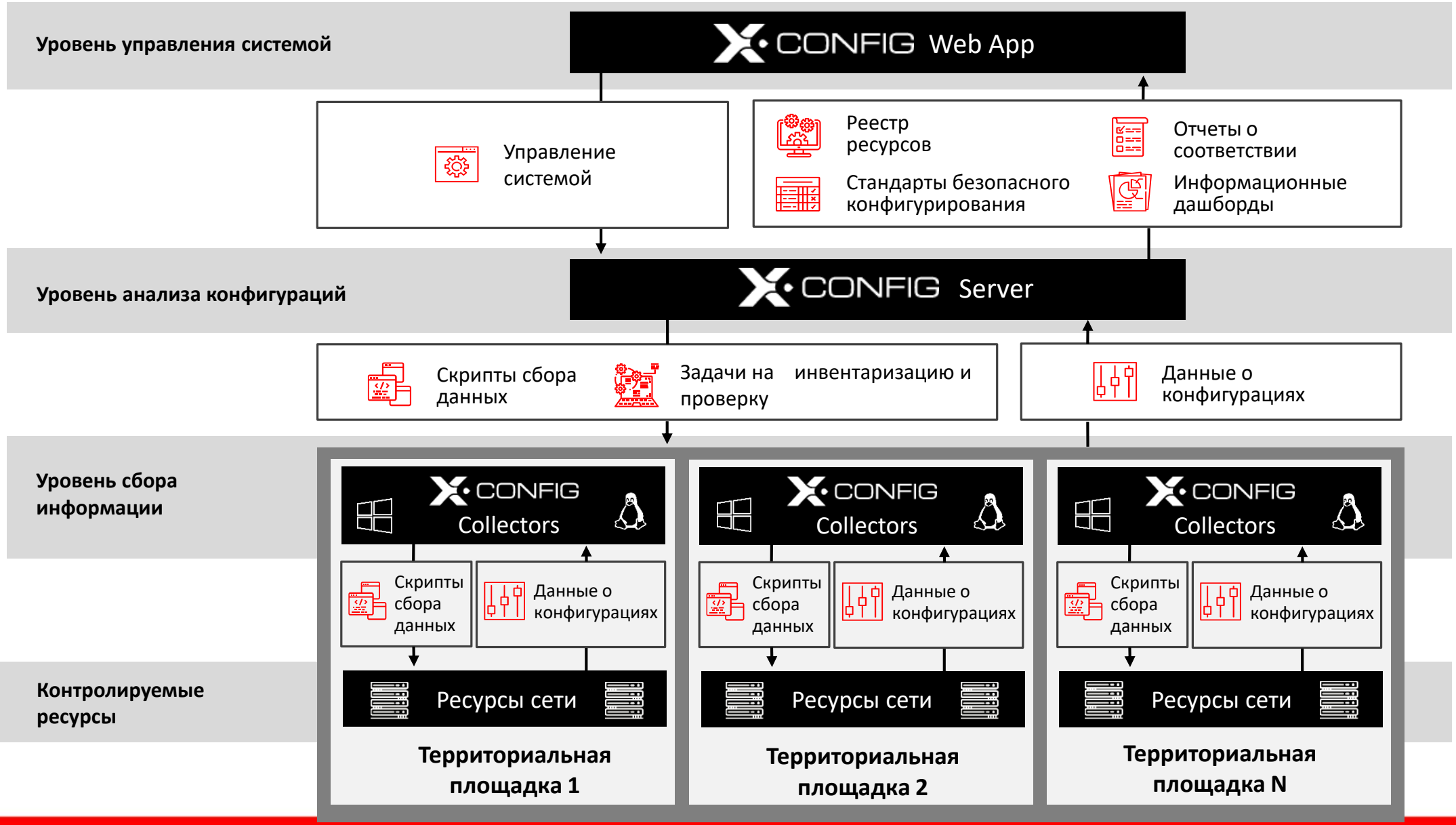
- Google Chrome
- Microsoft Edge
- Internet Explorer 11
- Яндекс.Браузер
- Mozilla Firefox

Системы виртуализации:

- Docker
- VMware ESXi

Сетевые устройства:

- Код Безопасности
- Элтекс
- Usergate
- Cisco


Уровень управления системой
CONFIG Web App
Управление системой
Реестр ресурсов
Отчеты о соответствии
Стандарты безопасного конфигурирования
Информационные дашборды
Уровень анализа конфигураций
CONFIG Server
Скрипты сбора данных
Задачи на инвентаризацию и проверку
Данные о конфигурациях
Уровень сбора информации
CONFIG Collectors
Скрипты сбора данных
Данные о конфигурациях
Ресурсы сети
Территориальная площадка 1
Территориальная площадка 2
Территориальная площадка N
Контролируемые ресурсы

Системные требования

X-Config App:

- Веб-браузер
- Разрешение: 1366x768

X-Config Server:

- OS: ОС с Docker
- CPU: 6 Cores
- RAM: 12 GB
- HDD : 200 GB

Collector:

- OS: Linux / Windows Server
- CPU: 1/2 Core
- RAM: 2/4 GB
- HDD: 50/80 GB

Стек технологий:

- Java 11, Spring
- React
- NodeJS
- Nginx
- PostgreSQL
- MongoDB

Установка:

- Docker
- RPM
- DEB

О компании Spacebit

Spacebit - российский разработчик современных программных продуктов в области информационной безопасности. Компания создает эффективные инструменты, помогающие бизнесу и государственным организациям различного масштаба повышать уровень защищенности ИТ-инфраструктуры и автоматизировать процессы управления ИБ.

SPACE-BIT

Решения

X-CONFIG

Система управления уязвимостями конфигураций информационных ресурсов

X-CONTROL

Система управления жизненным циклом средств криптографической защиты информации

SpaceView

Система мониторинга и реагирования на инциденты информационной безопасности

Наши преимущества

Российская разработка
все продукты создаются на территории РФ и включены в Реестр отечественного ПО

Универсальность применения
решения подходят для любых организаций вне зависимости от отрасли и масштаба

Простота развертывания и обслуживания
продукты быстро интегрируются в ИТ-инфраструктуру и легко поддерживаются

Гибкость и масштабируемость
системы масштабируются и кастомизируются под бизнес-требования заказчика

Политика лицензирования
модель лицензирования позволяет подобрать оптимальное решение для каждой компании

Оперативная техподдержка
специалисты помогут решить любые вопросы по настройке, эксплуатации и обновлению систем

Наши партнеры

Контакты

SPACE·BIT

www.spacebit.ru

info@spacebit.ru

+7 (495) 989-90-01