BELLSOFT


# Java технологии - Путь к Цифровому суверенитету

BellSoft 2022

www.bell-sw.com

www.libericajdk.ru

# От Java до OpenJDK

2020 **BellSoft** избрана в исполнительный комитет **Java Community Process**

**BellSoft** - участник закрытой группы по безопасности OpenJDK (**Vulnerability group**)

**1995** — Java1.0a2

**1996** — Java Development Kit (JDK) 1.0

**1997** — По контракту с Sun Microsystems

**1998** — Открыт стандарт Java Java Community Process (JCP)

**2004** — Центр разработки в Санкт-Петербурге

**2007** — Создание проекта OpenJDK

**2010** — Центр разработки в Санкт-Петербурге

**2017** — Создание компании

Oracle объявляет об изменениях лицензии Java и планах окончания поддержки Java 8

**2018** — В Топ мировых лидеров OpenJDK

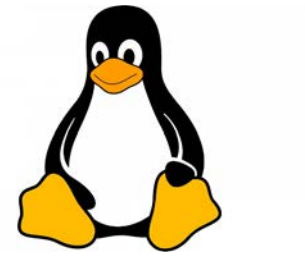
100% исходного кода Java SE открыто в OpenJDK, включая коммерческий функционал

**20+ лет опыта инженеров BellSoft в разработке Java платформы:**

BELLSOFT

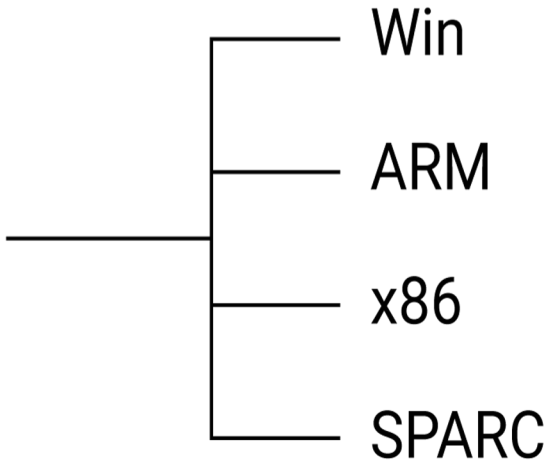
# Вклад команды в проекты с открытым кодом

Залог успеха на пути Java технологии к Цифровому и Технологическому суверенитету









# Вызовы для ИТ инфраструктуры в РФ

- **Цифровая трансформация госкомпаний 91-р (50 +) и госсектора (ФОИВ, РОИВ)**
- **Требования регуляторов к ИБ не только на бумаге**
- **КИИ и ГИС – мишень для растущего количества кибератак**
- **Санкционные риски**
- **Не допустить Цифровой паралич**

Документы:

- Директивы Правительства РФ от 14 апреля 2021 г. №3438п-П13
- Распоряжение Правительства РФ от 23.01.2003 №91-р
- Приказ Минкомсвязи России от 20.09.2018 №486 «Об утверждении методических рекомендаций по переходу государственных компаний на преимущественное использование отечественного программного обеспечения, в том числе отечественного офисного программного обеспечения»
- Приказ ФСТЭК от 25.12.2017 №239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры РФ»
- Федеральный закон от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры РФ»

# Вызовы для ИТ инфраструктуры в РФ

> Цифровая трансформация не имеет смысла, если она не основана на отечественных решениях. Она должна базироваться на отечественном программном обеспечении и аппаратных комплексах. Игнорирование российских решений – дело вредное и в какой-то степени является саботажем,

# Вызовы для ИТ инфраструктуры в РФ

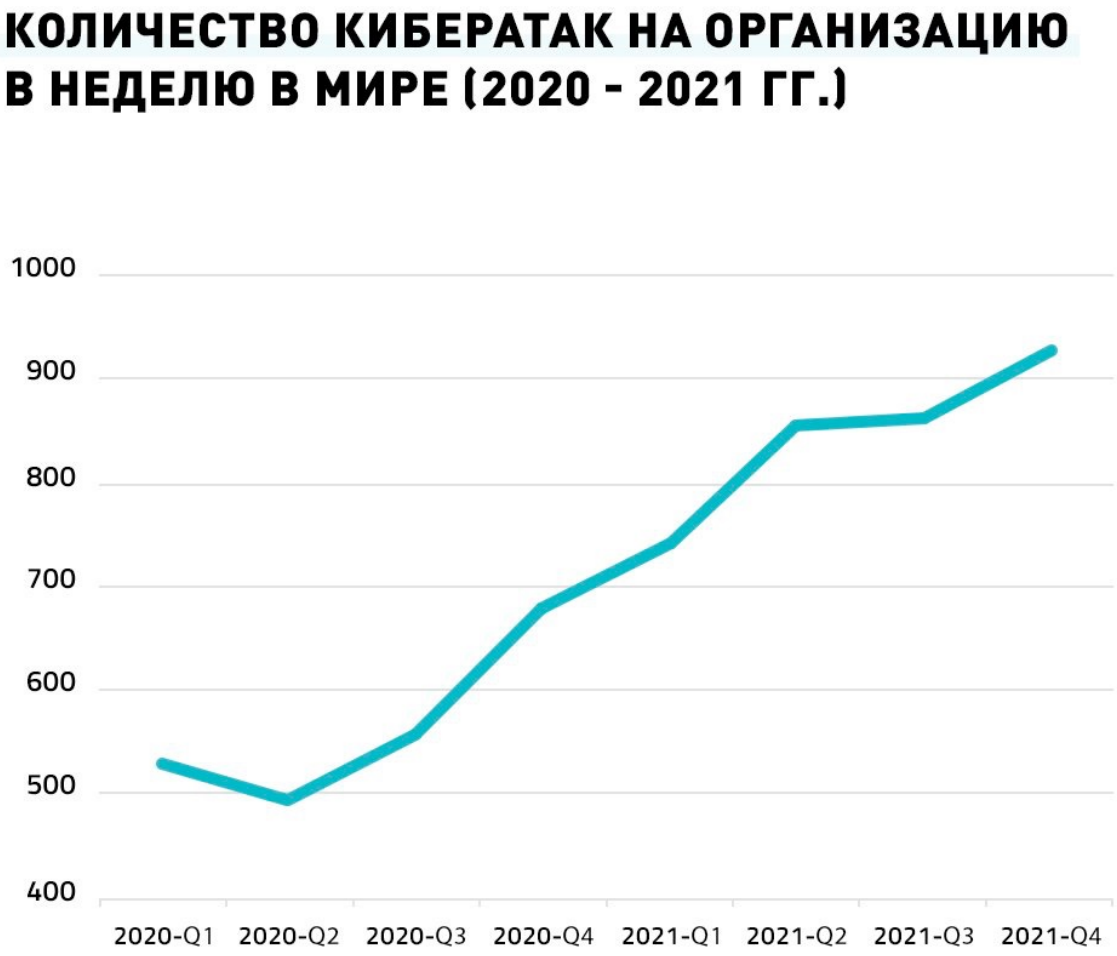
kommersant.ru

## Банкиры собрались на учения

### «Сбер» готовится к возможным технологическим санкциям

1 февраля 2022

На фоне сообщений о возможных санкционных ограничениях США по поставкам в Россию новой электроники и поддержке существующей «Сбер» провел технологические учения. На них моделировалось отключение IT-инфраструктуры банка от поддержки Microsoft, Nvidia, VMware, SAP и других компаний. Беспокойство по поводу возможных технологических санкций испытывают и в правительстве: там готовят сценарии на случай введения ограничений. Для организаций, которые еще не приступили к импортозамещению, резкий переход будет болезненным, считают эксперты.




*Источник: Check Point Research*

BELLSOFT

# Вызовы для ИТ инфраструктуры в РФ

## Киберпандемия Log4shell

В декабре 2021 года была опубликована информация об обнаружении уязвимости нулевого дня в популярной библиотеке журналирования Apache Log4j, который приводит к удаленному выполнению кода (RCE). Многие крупные компании уже сообщили, что их решения оказались уязвимы, среди них Cisco, CloudFlare, FedEx, GitHub, IBM, Apple, Amazon, Twitter, разработчик игры Minecraft и другие. Библиотека Log4j используется во многих проектах с открытым исходным кодом, к примеру Elasticsearch и Redis.

Злоумышленники начали эксплуатировать уязвимость сразу после ее публикации. Например, она уже используется для распространения банковского трояна Dridex и ряда шифровальщиков.

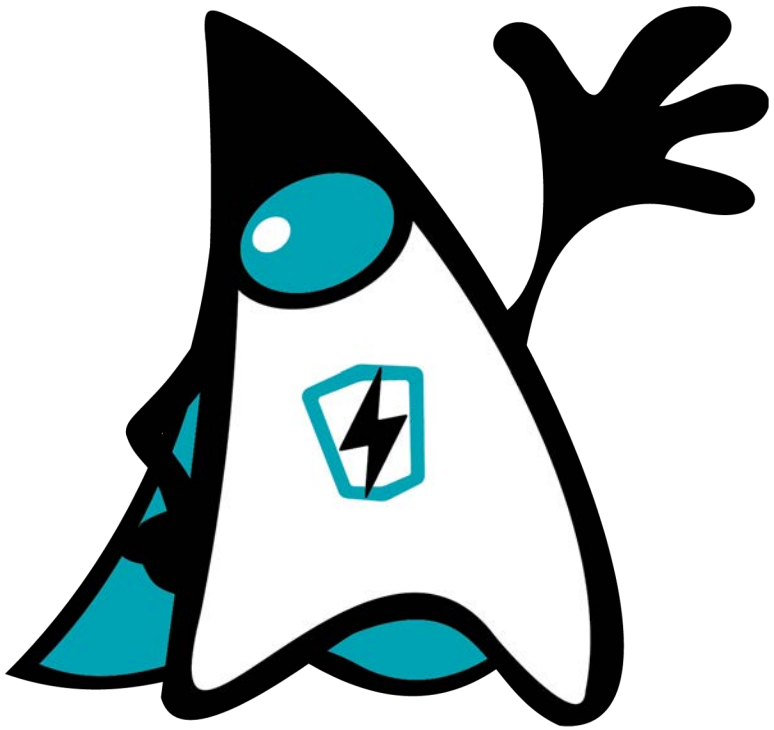
***

За всеми этими кажущимися отстраненными страшилками о гигантских утечках, зашифрованных или взломанных на продажу данных, вымогательском ПО и кибершпионаже стоят вполне понятные каждому обывателю словосочетания: нехватка топлива, отмена авиарейсов, приостановка производства и перебои с поставками продовольствия, неработающие АЗС, срыв плановых операций. А ещё десятки миллионов долларов, потерянных частными компаниями по всему миру, и уничтоженные репутации. Такова цена, которую все мы платим за небрежное отношение к информационной безопасности. Которую заплатит каждый, если отношение к важности кибербезопасности в мире не изменится в самое ближайшее время.



https://www.ptsecurity.com/ru-ru/research/analytics/informacionnaya-bezopasnost-v-2021-samye-gromkie-vzlomy-i-utechki/

# 26 лет Java - Топ технология для разработки ПО



- 12 + млрд строчек исходного кода
- 17 версий
- 4 CPU релиза в год - более 100 устранённых уязвимостей безопасности в год
- Более 1 млрд загрузок дистрибутивов JDK в год
- Java в ТОП-3 востребованных технологий (в т.ч. для КИИ, ГИС)
- Java - современная практика разработки промышленных ИТ-систем корпоративного уровня еще на 10-летия

BELLSOFT

# Java у каждого своя

## Legacy:

- Устаревшие версии JDK 1.4, 1.6, 1.7
- Вендорские сервера приложений WebLogic, WebSphere
- Редкие платформы Power, SPARC
- Скоро мы все перепишем как надо, но пока есть более срочные задачи

## Modern - microservices

- Микросервисная архитектура
- Контейнеризация
- Облака
- Native image
  - Quarkus, Micronaut, Spring Native
  - GraalVM

## Desktop:

- Толстые клиенты
- Java WebStart
- Java Applets
- JavaFX

# Java технологии
# Путь к Цифровому суверенитету

## Критерии выбора дистрибутива, “ИТ-гигиена”

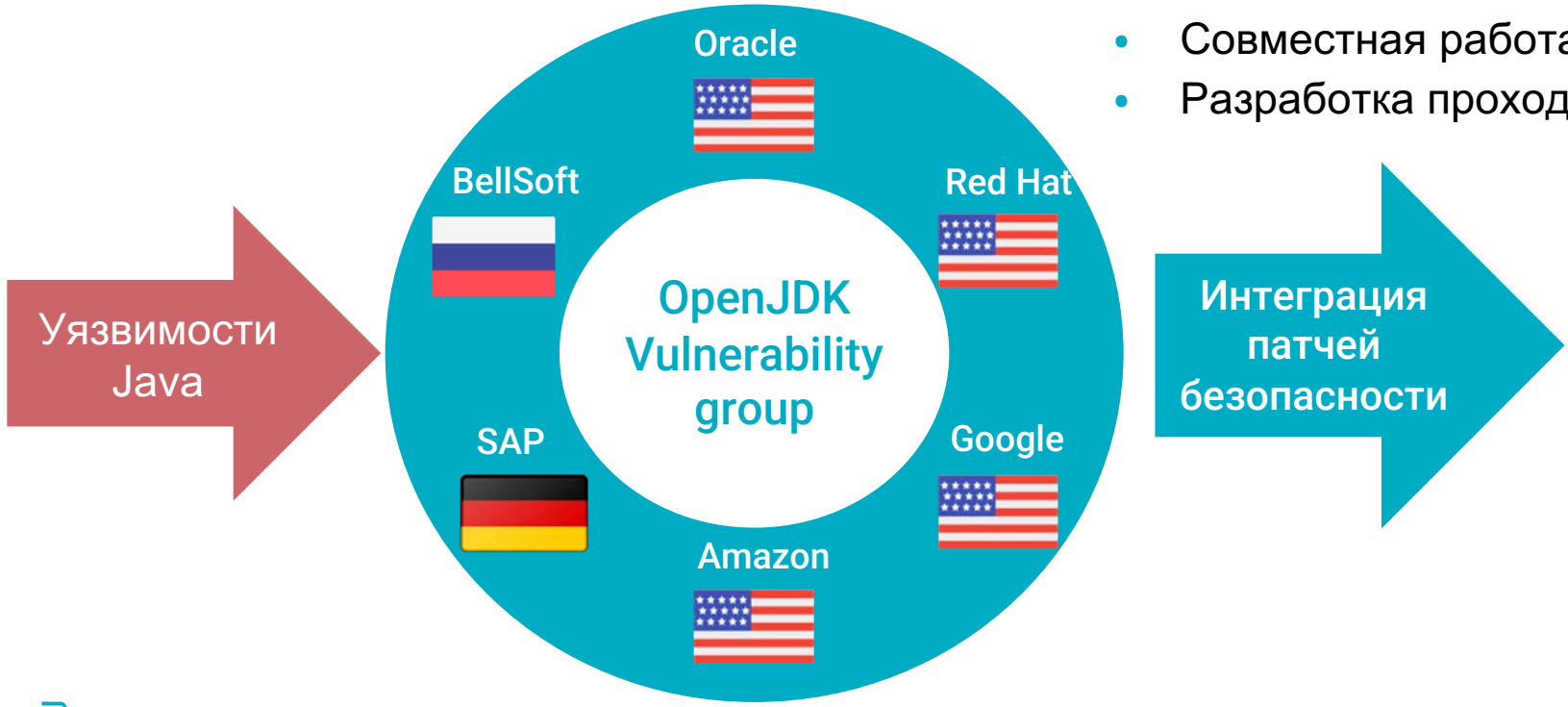
- **Своевременные обновления безопасности**
- **Поставщик ПО активный контрибьютор OpenJDK с экспертизой на уровне JVM**
- **Безопасный процесс разработки ПО / Контроль качества / Соответствие стандарту Java SE (TCK)**
- **Сертификация ФСТЭК (4УД) и Реестр Российского ПО**
- **Кросплатформенность (WORA) с фокусом на Российский стек ПО**

# OpenJDK Vulnerability group

Коллективный подход

https://openjdk.java.net/groups/vulnerability/

- Закрытая группа в OpenJDK, 11 компаний:
  - Участники OpenJDK
  - Регламент обмена конфиденциальной информацией
  - Подтвержденный опыт работы с дефектами безопасности
  - Признанные эксперты в OpenJDK и доступ к TCK
  - Для новых участников голосование (3 и более голосов)
- Отчеты о найденных уязвимостях в OpenJDK
- Совместная работа над созданием фиксов
- Разработка проходит в режиме ограниченного доступа



# Безопасный процесс разработки ПО


- **Философия:** полная автоматизация процессов, любые новые отказы подвергаются анализу, на ранних этапах работы над релизом для выявления отказов проводится анализ ошибок и рефакторинг

- **Объем работ:**
  - Legacy версии JDK (1.6, 1.7)
  - 14 стандартных платформ
  - 290 бинарных файлов
  - 192 млн результатов тестирования в рамках одного релиза
  - ПО производится в соответствии с промышленным процессом SDL

- **Тестирование:**
  - 100% TCK
  - для выявления уязвимостей
  - Регрессионное и функциональное тестирование по уровням с растущим числом прогонов
  - Регрессионное тестирование производительности
  - Стресс-тестирование (jcstress, JIT tester, Big Apps), фаззинг
  - Тесты, встроенные в популярные фреймворки (Lucene, Spring)
  - Тесты, предоставленные клиентами или встроенные в приложения (при наличии)
  - Статический анализатор SVACE от ИСП РАН

# TCK — гарантия соответствия спецификации Java SE


- Тестовая сюита TCK содержит около 140K + тестов
- Верификация сюитой TCK гарантирует соответствие зонтичному стандарту Java SE и запросам на спецификацию Java (Java Specification Requests, JSRs) конкретных версий Java
- Все сборки JDK должны быть верифицированы TCK-тестами

# Использование сертифицированной ФСТЭК Java по 4УД

ФСТЭК России

Федеральная служба по техническому и экспортному контролю

BellSoft получили решение ФСТЭК о сертификации ПО с планами закончить процесс в 1м квартале 2022 г.

Сертифицированные ФСТЭК по 4УД Java компоненты позволят компаниям сосредоточится на безопасности самих Java приложений, не погружаясь в трудоемкий и технически сложный слой JVM и сервера приложений, и использовать готовый сертифицированный кубик для своих ИТ систем, так же как и ОС.

Компании смогут проще и быстрее аттестовать:

- ГИС до 1 класса защищенности вкл-но,
- ИС ПД до 1 уровня защищенности вкл-но,
- значимые объекты КИИ 1 категории,
- АСУ ТП 1 класса защищенности.

# Кросплатформенность Java, сквозной техстек на базе Российских ИТ технологий

- Единый Реестр Российского ПО и Баз Данных
- Единый реестр российской радиоэлектронной продукции
- Системная работа направленная на совместимость стека ПО и оборудования
- Сквозной стек на отечественных технологиях от процессора до бизнес пользы
- Соответствие требованиям по созданию ГИС и работы КИИ
- Выполнение KPI по Цифровой трансформации
- Сквозной стек в т.ч на широком наборе мировых платформ

# Хватит ждать – пора действовать
# Скажи НЕТ Цифровому параличу

**TADVISER:** **Получается, что вопрос снижения зависимости от иностранных технологий в вашем случае не стоит, потому что какой-то серьёзной зависимости изначально не было?**

**ВЛАДИМИР ТРОЯНОВСКИЙ:** В целом да, но и тут мы не стоим на месте. В 2020 году, например, мы перешли с Oracle JDK на отечественный дистрибутив Java – Liberica JDK – для поддержки систем высокой доступности и безопасного процессинга. От Oracle JDK была зависимость, мы от неё ушли.



https://www.tadviser.ru/index.php/Статья:Интервью_TAdviser:_Владимир_Трояновский,_НСПК_-_об_ИТ-стратегии_и_планах_развития_российской_платежной_системы


# Свяжитесь с нами

Роман Карпов

+7 926 566 35 99
roman.karpov@bell-sw.com
https://libericajdk.ru/
www.bell-sw.com