СБЕР ТЕХ

Портфель

Кибербезопасность

Экосистемный подход

Единый портфель
Решения для защиты сервисов, интеграций и систем ИИ в едином контуре

Контроль рисков
На всех уровнях: доступ, взаимодействие систем, код и данные

Встроенная безопасность
Безопасность как часть архитектуры, а не отдельный слой

10+
лет опыта
защиты критичных систем в масштабной инфраструктуре

200+
экспертов
практиков по кибербезопасности и защите информации

Ключевые преимущества

Экспертиза практикующих специалистов
Реальный опыт защиты масштабной инфраструктуры

Безопасная разработка
Соблюдение требований ГОСТ 56939 и регуляторов

Проверенная эксплуатация
Решения используются в крупнейших инфраструктурах страны

Комплексный подход
От защиты доступа до безопасности ИИ и программного кода

Масштабируемость
Готовность к промышленной эксплуатации и высоким нагрузкам

Кому подходит

Крупный бизнес

Компании корпоративного уровня с разветвлённой инфраструктурой

Сложная интеграционная архитектура

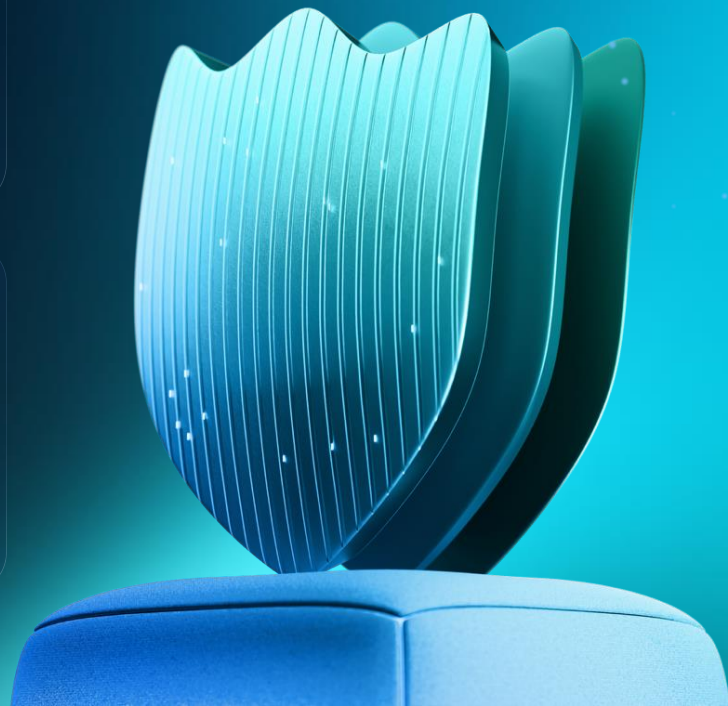
Организации с множеством взаимосвязанных систем и сервисов

Внедрение ИИ-решений

Компании, использующие искусственный интеллект в бизнес-процессах

Повышенные требования к ИБ

Бизнесы в регулируемых отраслях с жёсткими стандартами безопасности



Трёхуровневая модель безопасности

Полный контроль от проверки пользователя до защиты интеграций, кода и ИИ

Управление доступом

IAM IDM

- Аутентификация пользователей
- Управление правами доступа
- Контроль учётных записей

Безопасность взаимодействия

SOWA

- Контроль прикладных интерфейсов (API)
- Защита интеграций
- Управление обменом данными

Контроль кода и ИИ

Лаборатория проверки ПО

SOWA AI

- Безопасность систем ИИ
- Анализ программного кода
- Контроль поведения цифровых систем

Состав портфеля по кибербезопасности

Защита API и AI-security

SOWA

Контроль и защита API-трафика для интеграции внутри компании и с внешними сервисами

SOWA AI

Безопасное использование ИИ и LLM-моделей

Продукты управления доступом

IDM

Управление учётными записями для централизованного контроля доступа сотрудников к ресурсам

IAM

Сертифицированное во ФСТЭК России решение на базе Keycloak для аутентификации пользователей

Безопасность поставки ПО (DevSecOps)

Лаборатория проверки ПО

Исследование защищённости любого ПО, выявление уязвимостей, вредоносных функций и политически мотивированных внедрений

Platform V

IAM

Система управления аутентификацией пользователей

- Реализовано на базе Keycloak
- Сертифицировано во ФСТЭК

Проблемы

- Разрозненные учётные записи
- Риски несанкционированного доступа
- Сложность управления доступами

Решение

- Единый вход в системы
- Многофакторная аутентификация
- Управление ролями и сессиями
- Интеграция с каталогами пользователей

Бизнес-эффект

Централизованный контроль доступа

Снижение рисков компрометации

Ускорение подключения систем

Platform V

IAM

Пример внедрения

ИТ-компания

Данные о проекте

Переход на современный метод аутентификации, защищённый от атак на пароли

Задача

Повысить удобство и безопасность аутентификации в бизнес-системах

Решение

Platform V IAM

Включение WebAuthn, LoA-аутентификация, аутентификация по сертификатам, биометрия (отпечаток, Face ID), PIN, OTP — всё «из коробки»

Результаты

- Мгновенная аутентификация без паролей и SMS
- Единый механизм для всех корпоративных систем

100%

Готовое решение для партнёров — включается «по щелчку»

Platform V

IDM

Система управления учётными записями и правами доступа

Реализовано на базе MidPoint

Импортозамещение

- One Identity Manager
- Sail Point Identity IQ
- IBM Security Identity Manager
- Microsoft Identity Manager
- Oracle Identity Manager

Проблемы

- Избыточные права доступа
- Ручное управление учётными записями
- Отсутствие прозрачности

Решение

- Автоматизация жизненного цикла сотрудников
- Управление ролями и правами доступа
- Аудит и контроль использования доступа

Бизнес-эффект

Снижение нагрузки на ИТ-подразделения

Повышение прозрачности доступа

Соответствие требованиям регуляторов

Platform V

IDM

Пример внедрения

Крупная страховая компания

Данные о проекте

Пилотный проект
по импортозамещению
One Identity

Цитата клиента

«Отличный продукт,
который покрывает
все требования
и даже больше...»

Задача

Замена иностранного IDM-решения на отечественное с сохранением всех бизнес-требований и ростом уровня кибербезопасности

Решение

Platform V IDM

- **Пилот** на инфраструктуре заказчика с подключением промышленных целевых систем
- Развёртывание в Kubernetes

Результаты

- Гибкая кастомизация и масштабируемость
- Современная архитектура (Kubernetes-native)

100%

Полное покрытие всех текущих требований + возможности сверх ожиданий

Platform V

IDM

Пример внедрения

Банк

Данные о проекте

Полная замена legacy IBM Tivoli (СУДИР) на Platform V IDM

Миграция **350+** внутренних АС, **15 млн** управляемых учётных записей

Цитата клиента

«В процессе мы заменили много legacy-решений, обеспечивая непрерывность работы всех сервисов, и поддержали новые, повышенные требования кибербезопасности, законодательства и процессов банка»

Кирилл Меньшов, старший вице-президент, руководитель блока «Технологии» Сбербанка

Задача

- Импортозамещение
- Повышение качества управления идентификацией и доступом

Решение

Platform V IDM

в промышленной эксплуатации

- Интеграция >400 систем банка
- Автоматизация кадровых процессов с учётом совмещений и трудоустройств

Результаты

- Выдача доступов — за минуты вместо дней
- Сокращение времени на адаптацию сотрудников
- Ускорение согласования заявок
- Сокращение инцидентов ИБ

>900

систем интегрировано через Platform V IAM (в связке)

Platform V

SOWA

Мультипротокольный шлюз безопасности API

Импортозамещение

IBM DataPower

Проблемы

- Атаки через API систем
- Утечки данных
- Неконтролируемые интеграции

Решение

- Защита API от типовых атак
- Фильтрация и контроль трафика
- Управление взаимодействием сервисов

Бизнес-эффект

Снижение рисков атак

Ускорение внедрения интеграций

Снижение затрат на сопровождение

Platform V

SOWA

Пример внедрения

Финтех (топ-10 банк РФ)

Данные о проекте

Централизованная платформа безопасных внешних интеграций

Цитата клиента

«Раньше каждая интеграция — это отдельный проект с рисками и бюджетом.

Сейчас мы запускаем новые подключения за недели, а не месяцы. Это прорыв в скорости и безопасности»

Задача

Одна внешняя интеграция занимала **3–6+ месяцев** и требовала огромных ресурсов ИБ и инфраструктуры

Решение

Platform V SOWA

- Типовые безопасные коннекторы
- Единая точка контроля и аудита

Результаты

- Резкое снижение нагрузки на службу ИБ (единая точка аудита)
- Масштабируемость и гибкость: выросли в разы — типовой процесс для всех новых подключений
- Нет больше закупок серверов, лицензий и ручного управления DMZ

2–4 недели
срок реализации одной интеграции вместо 3–6+ месяцев

60-80%
снижение финансовых затрат на интеграции

Platform V

SOWA

Пример внедрения

Технологическая ИТ-компания

Данные о проекте

Централизация всего исходящего трафика

Цитата клиента

«SOWA упростила контроль исходящего трафика: валидация и мониторинг повысили безопасность и ускорили бизнес-решения»

Задача

Контроль и безопасность исходящего трафика из корпоративной сети, включая сторонние сервисы

Решение

Platform V SOWA

Как единая точка выхода:

- Валидация всех запросов
- Мониторинг
- Обнаружение аномалий

Результаты

- Автоматическая блокировка небезопасных запросов
- Прозрачная аналитика и быстрое реагирование на угрозы
- Упрощение администрирования (одна точка управления)

100%

видимость и контроль исходящего трафика

Platform V

SOWA AI

Шлюз безопасности систем искусственного интеллекта

Проблемы

- Утечки данных через модели ИИ
- Неконтролируемое использование ИИ
- Риски некорректных запросов

Решение

- Контроль запросов к моделям ИИ
- Защита от атак на модели
- Централизованный доступ к системам ИИ
- Аудит взаимодействий

Бизнес-эффект

Безопасное внедрение ИИ

Контроль использования моделей

Снижение рисков утечек данных

Хаотичная архитектура

Защищённая экосистема ИИ-трафика

Platform V

SOWA AI

Пример внедрения

ИТ-компания

Данные о проекте

Настройка API Gateway
для Open API и ИИ
с фокусом на валидацию
и безопасность

Задача

Контроль и валидация API / веб-запросов к сервисам и ИИ-агентам на корректность, безопасность и целесообразность

Решение

Platform V SOWA AI

- Валидация запросов/ответов
- Маршрутизация к inference-провайдерам
- DLP и песочница для утечек и вредоносного ПО
- AI Guardrails для ПДн и токсичного контента

Результаты

- Единый защищённый шлюз для защиты API и ИИ
- Защищённая ИИ-трансформация бизнеса
- Быстрое включение современных методов безопасности для API и ИИ
- Снижение рисков
- Анализ трафика для роста бизнеса
- Поддержка защищенной ИИ-трансформации у клиентов

Лаборатория проверки ПО

Анализ безопасности программного обеспечения по методике ФСТЭК

Проблемы

- Риски внедрения небезопасного ПО
- Непрозрачность цепочек поставки
- Скрытые уязвимости

Решение

- Статический и динамический анализ кода
- Проверка цепочки поставки ПО
- Выявление уязвимостей и недокументированных функций
- Тестирование ПО

Бизнес-эффект

Предотвращение киберинцидентов

Контроль качества программного обеспечения

Защита инфраструктуры

Влияние на доступность (A)	None (N)
Информация об эксплуатации	Эксплуатация достигается за счет создания архива с жесткой ссылкой на существующий в системе файл. При распаковке жертвой вредоносного архива и при наличии доступа к директории распаковки злоумышленник имеет доступ (чтение/запись) к целевому файлу с правами жертвы.

4. ВЕРДИКТ ЦКБСПО

Статус	☑ **Эксплуатация успешна**
	☐ **Не эксплуатируется**
Дополнительная информация	Для устранения данной уязвимости рекомендуется **удалить** пакет или **обновить до исправленной версии** (7.5.3).

5. СРЕДА ЭКСПЛУАТАЦИИ

Тип	виртуальный
Операционная система (ОС)	CentOS Stream 9
Процессор (CPU)	8 ядер (x64)
Оперативная память (RAM)	8 Гб
Жесткий диск (HDD)	256 Гб

6. ЗАДЕЙСТВОВАННЫЕ ИНСТРУМЕНТЫ

Данные об инструментах, задействованных для эксплуатации уязвимости

Задействованный POC	https://github.com/Jvr2022/CVE-2026-23745

7. ХОД ИССЛЕДОВАНИЯ

Задействованное ПО

1. node

```
[user@localhost bin]$ pwd
/home/user/node20_poc/node-v20.20.0-linux-x64/bin
[user@localhost bin]$ ./node -v
v20.20.0
```

2. tar (npm)

```
[user@localhost npm]$ pwd
/home/user/node20_poc/node-v20.20.0-linux-x64/lib/node_modules/npm
[user@localhost npm]$ ../../../bin/node ../../../bin/npm list | grep tar
├── tar@6.2.1
```

3. poc.js (код JavaScript для эксплуатации уязвимости)

```
const fs = require('fs')
const path = require('path')
const tar = require('tar')

const OUT_DIR = path.resolve('out_repro')
const SECRET = path.resolve('secret.txt')
const TAR_FILE = path.resolve('exploit.tar')
const TARGET_SYM = '/etc/passwd'
```

АНАЛИТИЧЕСКАЯ СПРАВКА О ВОЗМОЖНОСТИ ЭКСПЛУАТАЦИИ УЯЗВИМОСТИ CVE-2026-23745

Дата: 05.02.2026

Лаборатория проверки ПО

Пример внедрения

Банк

Данные о проекте

Проведение статического и динамического анализа дистрибутивов ПО для оценки уязвимостей

Цитата клиента

«Выражаем благодарность за проведённую работу – смогли вовремя закрыть задачу от своего руководства и обеспечить дальнейшее сотрудничество»

Задача

Оперативно предоставить полный анализ дистрибутива на уязвимости для оценки рисков ИБ и планирования устранения

Решение

Лаборатория проверки ПО

Сервис исследования ПО: гибридный анализ — статический и динамический — с применением проприетарных и самописных инструментов, адаптированных под инфраструктуру клиента

Результаты

- Детализированные отчёты для быстрой оценки и минимизации ИБ-рисков
- Гибкий подход к анализу, адаптированный под бизнес-процессы

1000+

исследований дистрибутивов различной сложности на конец 2025 года

Лаборатория проверки ПО

Пример внедрения

Крупная ИТ-компания

Данные о проекте

Создание портала
для доступа к отчётам
по рискам эксплуатации ПО

Цитата клиента

«Отлично, нам нравится,
очень удобный интерфейс»

Задача

Мгновенно получить сводку рисков (или их отсутствия) для ряда ПО в едином удобном формате

Решение

Портал проверенного ПО

Портал с гибкой системой поиска отчётов и ежедневным обновлением базы

Результаты

- Мгновенный доступ к готовым результатам анализа без ожидания новых исследований
- Интуитивный интерфейс для быстрого поиска и агрегации данных, упрощающий ИБ-аудит

3 600+

загруженных отчётов
на данный момент

СБЕР ТЕХ

Спасибо за внимание!

Кибербезопасность