

Технологический суверенитет со стороны кибербезопасности

Артем Зиненко

Лаборатория Касперского

PRO
автоматизацию



Rockwell Automation



SIEMENS



BOSCH

Schneider Electric

Honeywell

UNISOC

AVEVA

gemalto
security to be free

Итэлма
Электронные решения



ELTEX

EMERSON

FLEXERA
SOFTWARE

MOXA

SAPERION

WAGO



CODESYS

PcVue Solutions

Telit Cinterion

OPC
FOUNDATION

kraftway

Примеры, как не нужно делать



Все ли продукты в Реестре¹ - российские?

¹ Реестр российского ПО <https://reestr.digital.gov.ru/>

Запись в Реестре российского ПО

Наименование	Правообладатель / Производитель	Классы ПО/ПАК	Дата включения в реестр	№ реестровой записи
[REDACTED]	[REDACTED]	12.20 Информационные системы для решения специфических отраслевых задач 04.04 Среды разработки, тестирования и отладки	[REDACTED]	[REDACTED]

Запись в Реестре российского ПО

Об установлении **запрета** на допуск программного обеспечения, происходящего из **иностранных** государств



МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

№ [REDACTED]

Москва

О формировании и ведении единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств – членов Евразийского экономического союза, за исключением Российской Федерации

В соответствии с пунктами 25, 26 Правил формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств – членов Евразийского экономического союза, за исключением Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» (далее – Правила), и на основании решения Экспертного совета по программному обеспечению при Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации (далее – Экспертный совет) от 31 мая 2021 г.

12.20
Инфор
специ
0.04
Среды

Анализ продукта

```
$ head -n10 ./ReadmeP006.txt
```

```
=====
Patch P006 "DECEMBER-2021" for WinCC OA Version 3.18      December 2021
=====
```

```
Summary:
```

```
=====
```

Siemens SIMATIC
WinCC OA

```
Enhancements and bugfixes for WinCC OA.
```

Известные уязвимости Siemens

CVE-2022-33139, CVSSv3: 9.8

The following versions of SIMATIC WinCC OA, a SCADA HMI system, are affected:

- SIMATIC WinCC OA v3.16: All versions
- SIMATIC WinCC OA v3.17: All versions
- **SIMATIC WinCC OA v3.18: All versions**

Известные уязвимости Siemens в БДУ ФСТЭК

Главная / Список уязвимостей

ФИЛЬТРАЦИЯ

Контекстный поиск по названию уязвимости

Введите слово или словосочетание

Производитель ПО **Siemens AG**

Тип ПО

Программное обеспечение **SIMATIC WinCC OA**

Аппаратная платформа

Версия ПО

Статус уязвимости

Доп. параметры

Диапазон дат

Уязвимости, связанные с инцидентами ИБ

Год добавления

По Вашему запросу найдено 11 записей

Выводить по: 10, 20, 50, 100 Сортировка: Элементы с 1 по 10 из 11

BDU:2024-04186	Уязвимость сетевого программного обеспечения Siemens, связанная с чтением за границами памяти, позволяющая нарушителю вызвать отказ в обслуживании	14.05.2024
BDU:2022-07414	Уязвимость приложения контроля лицензий CodeMeter, связанная с чтением данных за границами буфера в памяти, позволяющая нарушителю раскрыть защищаемую информацию или вызвать отказ в обслуживании	10.06.2021
BDU:2022-03715	Уязвимость SCADA-системы SIMATIC WinCC, связанная с возможностью использования аутентификации на стороне клиента, позволяющая нарушителю повысить свои привилегии	21.06.2022
BDU:2021-02031	Уязвимость сетевого программного обеспечения Siemens, связанная с отсутствием кавычек в написании элементов или путей поиска, позволяющая нарушителю выполнить произвольный код с повышенными привилегиями	10.06.2020
BDU:2019-01778	Уязвимость программного обеспечения Siemens, связанная с недостаточной проверкой вводимых данных, позволяющая нарушителю вызвать отказ в обслуживании	09.04.2019
BDU:2019-00765	Уязвимость программного обеспечения криптографической библиотеки OpenSSL, связанная с некорректной работой механизма «error state», позволяющая нарушителю передавать незашифрованные конфиденциальные данные по сети	07.08.2018
BDU:2018-01125	Уязвимость TCP-сервера SCADA-системы SIMATIC WinCC OA, позволяющая нарушителю повысить свои привилегии	11.09.2018
BDU:2014-00393	Уязвимость автоматизированной системы управления технологическими процессами SIMATIC WinCC OA, позволяющая злоумышленнику обойти файловую систему без прохождения процедуры аутентификации в контексте текущего пользователя	06.02.2014

Известные уязвимости вендора в БДУ ФСТЭК

10

[Главная](#) / Результаты поиска по запросу: [REDACTED]

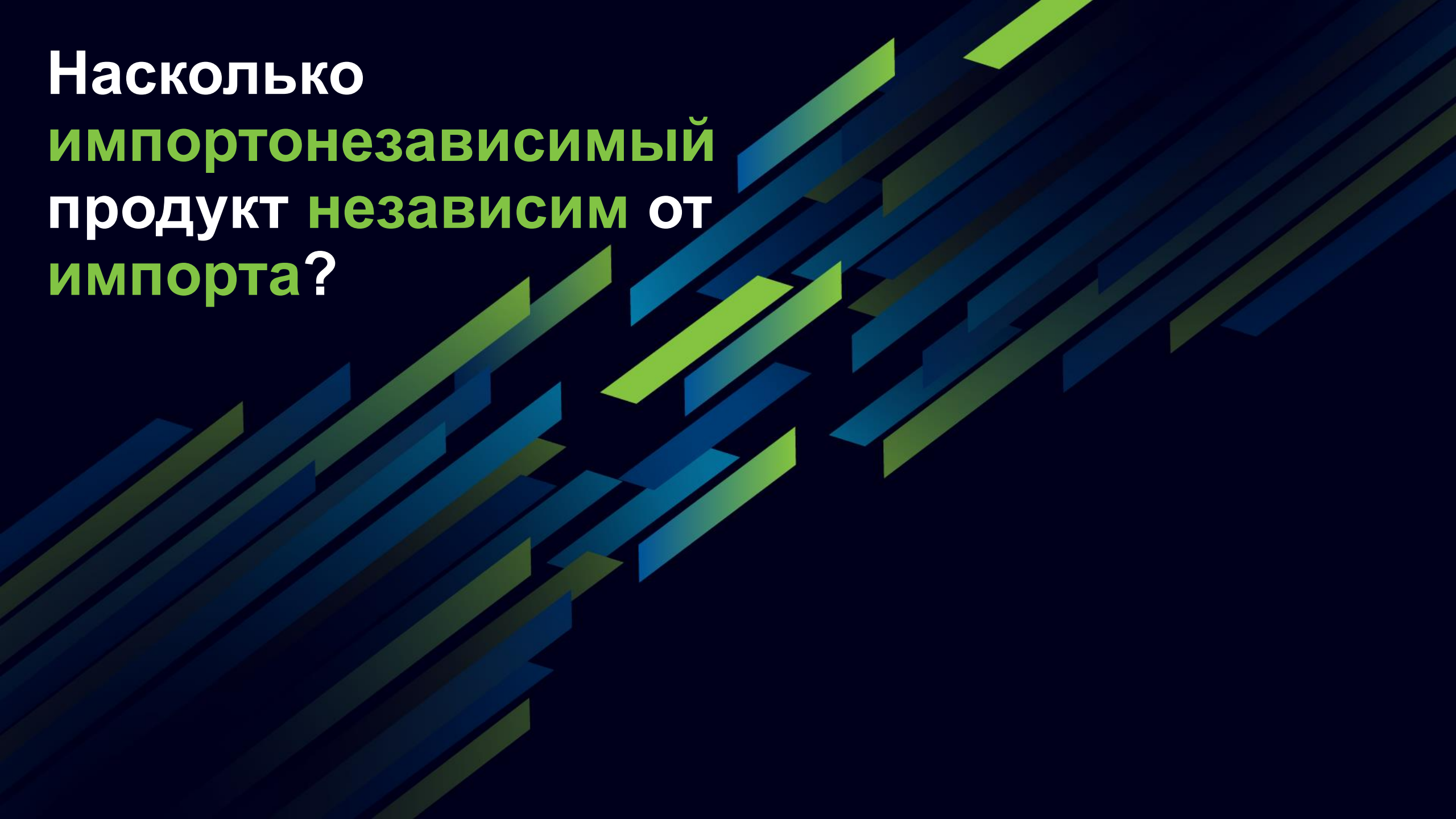
[REDACTED]

Результаты поиска по запросу: [REDACTED]

Выводить по: [10](#), [20](#), [50](#), [100](#)

Поиск не дал результатов.

Насколько
импортонезависимый
продукт независим от
импорта?

The background of the slide features a series of parallel, diagonal stripes in various shades of blue and green, creating a sense of movement and depth against a dark background.

Импортонезависимый продукт?

Программное обеспечение блока внесено в реестр отечественного ПО.

Операционная система на базе ядра Linux.

Аппаратная часть выполнена на импортонезависимой электронно-компонентной базе (материковый Китай).

материковый Китай

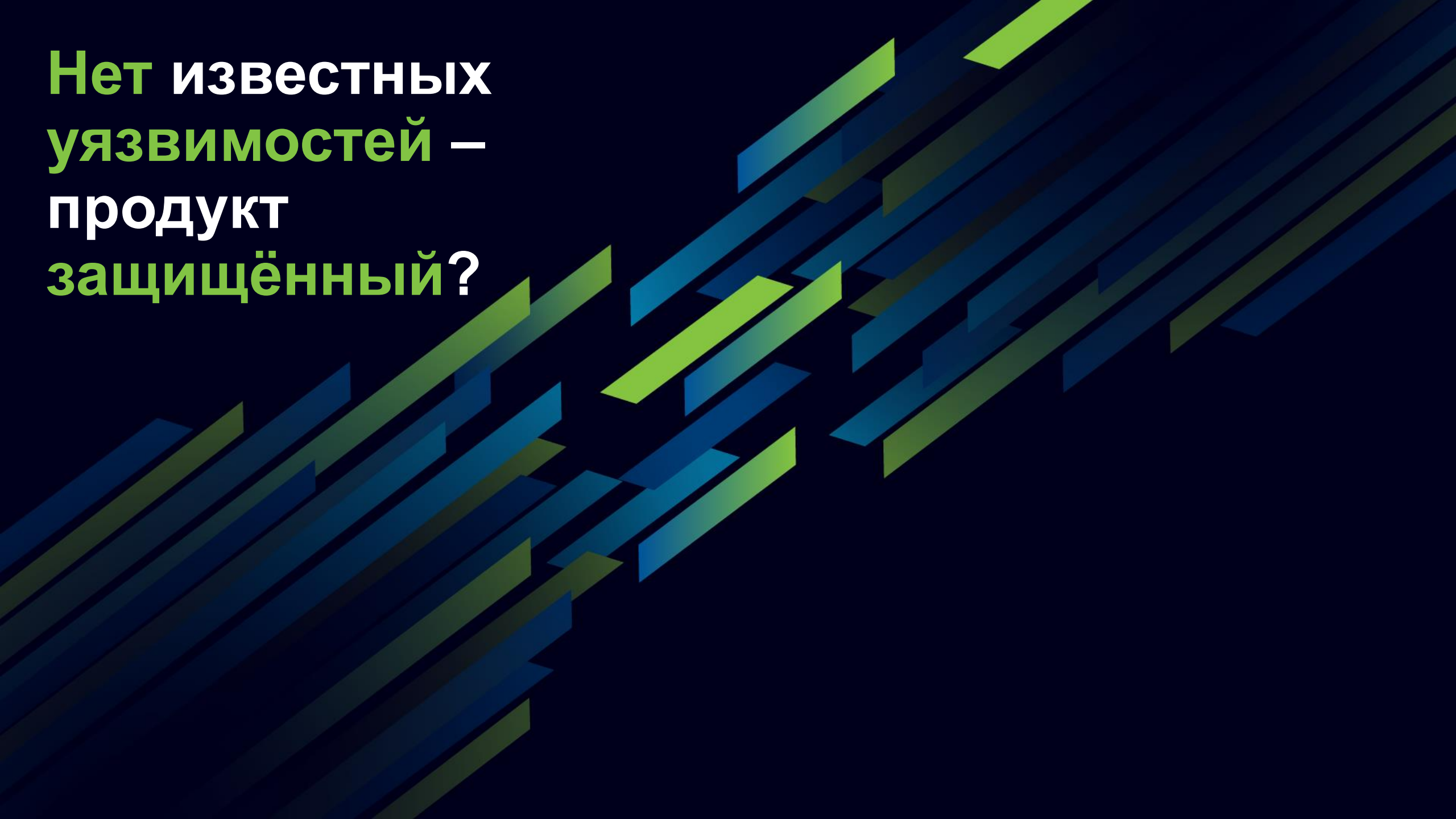
История одной уязвимости



Общение с вендором

*Based on our internal risk assessment, ... we have decided **not to publish any fix** for the listed issues ...*

**Нет известных
уязвимостей –
продукт
защищённый?**

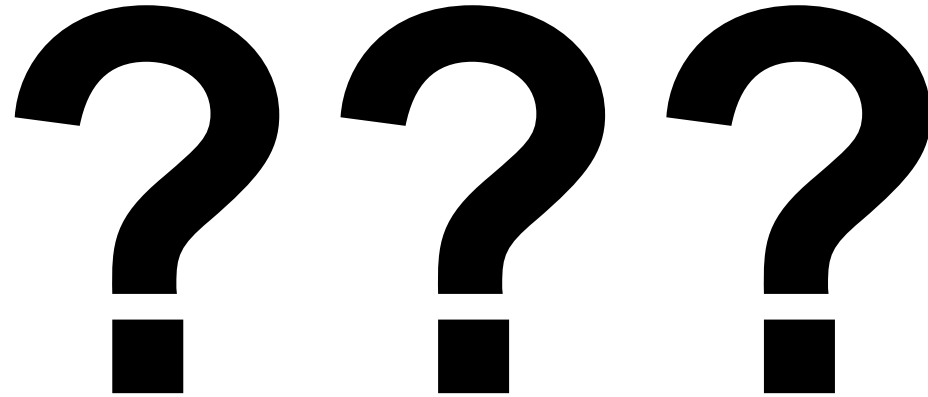
The background of the slide features a series of parallel, diagonal stripes in various shades of blue and green, creating a sense of depth and movement. The stripes are arranged in a way that they appear to recede into the distance, with some stripes being more prominent than others. The overall effect is a modern, geometric pattern.

Нет известных уязвимостей для продукта в БДУ



Сведения об уязвимостях в Банке данных угроз безопасности информации не обнаружены

Аудит продукта



потратили на поиск **критической уязвимости** в продукте
(удаленное выполнение произвольного кода)

1 час

потратили на поиск **критической уязвимости** в продукте
(удаленное выполнение произвольного кода)

Информация о НОВЫХ УЯЗВИМОСТЯХ

The background of the slide is a dark blue gradient. It features a series of diagonal, overlapping stripes in various shades of blue and green, creating a sense of depth and movement. The stripes are oriented from the bottom-left towards the top-right.

Подход большинства вендоров



Что делать?

The background of the slide is a dark blue gradient. It is decorated with numerous diagonal stripes of varying lengths and colors, including shades of blue, teal, and light green. These stripes are arranged in a way that creates a sense of depth and movement, appearing to recede into the distance from the bottom left towards the top right.

Что делать вендорам?

- **Внедрять** современные практики **безопасной разработки**
- **Проводить** регулярный **аудит** безопасности своих продуктов
- **Уведомлять пользователей** продуктов о проблемах в безопасности
- **Управлять** уязвимостями в используемых **внешних компонентах**
- Создать канал для **приема информации** о проблемах в безопасности от **внешних исследователей**

Что делать компаниям?

- При выборе новых продуктов уделять внимание **уровню зрелости** вендора с точки зрения безопасности
- **Проводить** независимый **аудит** безопасности используемых продуктов
- **Управлять уязвимостями** в используемых продуктах
- При внедрении требовать **передачи** всех **артефактов**, необходимых для **работы** продукта
- Выстраивать **архитектуру** систем с использованием подходов **эшелонированной защиты** (Defense in Depth) и **нулевого доверия** (Zero Trust)

Положительные изменения



Спасибо за
внимание!

kaspersky

Артем Зиненко

Artem.Zinenko@kaspersky.com

 **PRO**
АВТОМАТИЗАЦИЮ

