



CISO ПРОТИВ ИИ

Profit Security Day

—

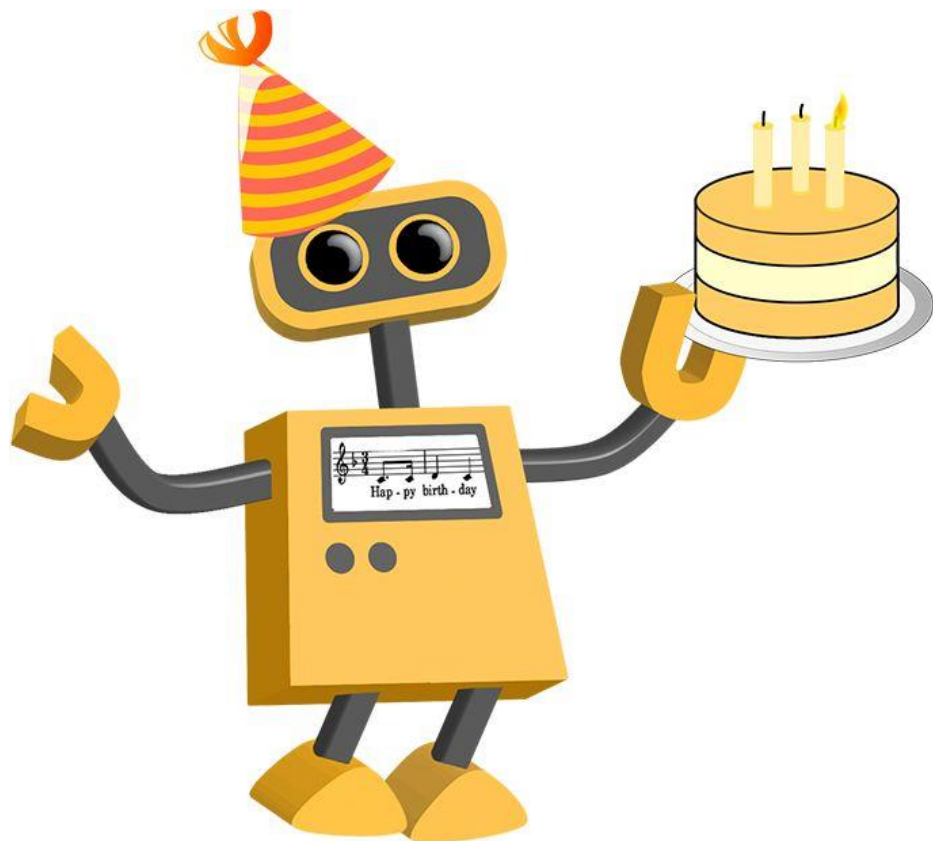
Константин Аушев

1 ноября 2024



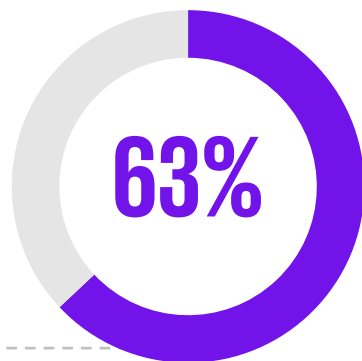


Ваше мнение: от роботов больше помощи или угроз?

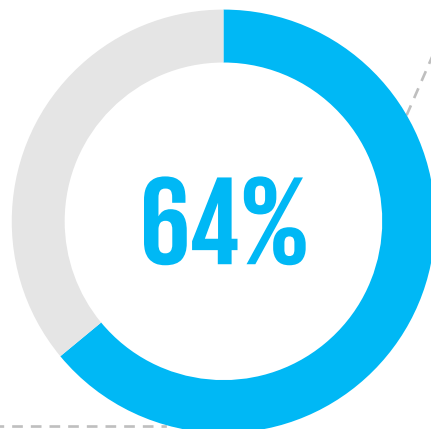


Потенциал AI в кибербезопасности

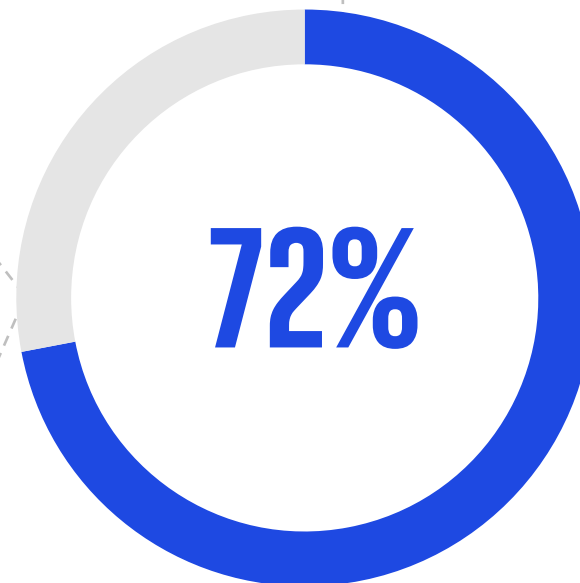
Кибербезопасность – область наибольшего потенциала для применения GenAI



Собираются внедрить GenAI для функции информационной безопасности в течение года



Кибербезопасность – это топ-приоритет для применения GenAI



4 наиболее перспективные области применения ИИ в ИБ

01

Digital-форензика и
реагирование на
инциденты

02

Операционная
деятельность функции
ИБ

03

Управление доступом
и идентификацией

04

Управление третьими
сторонами

4 наиболее перспективные области применения ИИ в ИБ

01

Digital-форензика и реагирование на инциденты

Идентификация внутренних и внешних угроз посредством постоянного анализа паттернов поведения пользователей, инцидентов, структуры файлов, сообщений в новостных лентах и социальных сетях...

Высокая точность

Высокая скорость

04

Управление третьими сторонами

4 наиболее перспективные области применения ИИ в ИБ

Потенциал для ML

01

Digital-форензика и реагирование на инциденты

Идентификация внутренних и внешних угроз посредством постоянного анализа паттернов поведения пользователей, инцидентов, структуры файлов, сообщений в новостных лентах и социальных сетях...

Высокая точность

91–96 %

Повышение эффективности

на 5–48 %

04

Управление третьими сторонами

4 наиболее перспективные области применения ИИ в ИБ

Оценка показателей эффективности, анализ и систематизация результатов мониторинга, рекомендация действий для аналитика

01

Digital-форензика и реагирование на инциденты

02

Операционная деятельность функции ИБ

03

Управление доступом и идентификацией

04

Управление третьими сторонами

Потенциал для GPT, Copilot

4 наиболее перспективные области применения ИИ в ИБ

Потенциал для IA, RPA

01

Digital-форензика и реагирование на инциденты

02

Операционная деятельность функции ИБ

03

Управление доступом и идентификацией

Выполнение регламентных задач по пересмотру прав доступа
Идентификация deepfake-ов

04

Управление третьими сторонами

4 наиболее перспективные области применения ИИ в ИБ

01

Digital-форензика и реагирование на инциденты

02

Операционная деятельность функции ИБ

03

Управление доступом и идентификацией

04

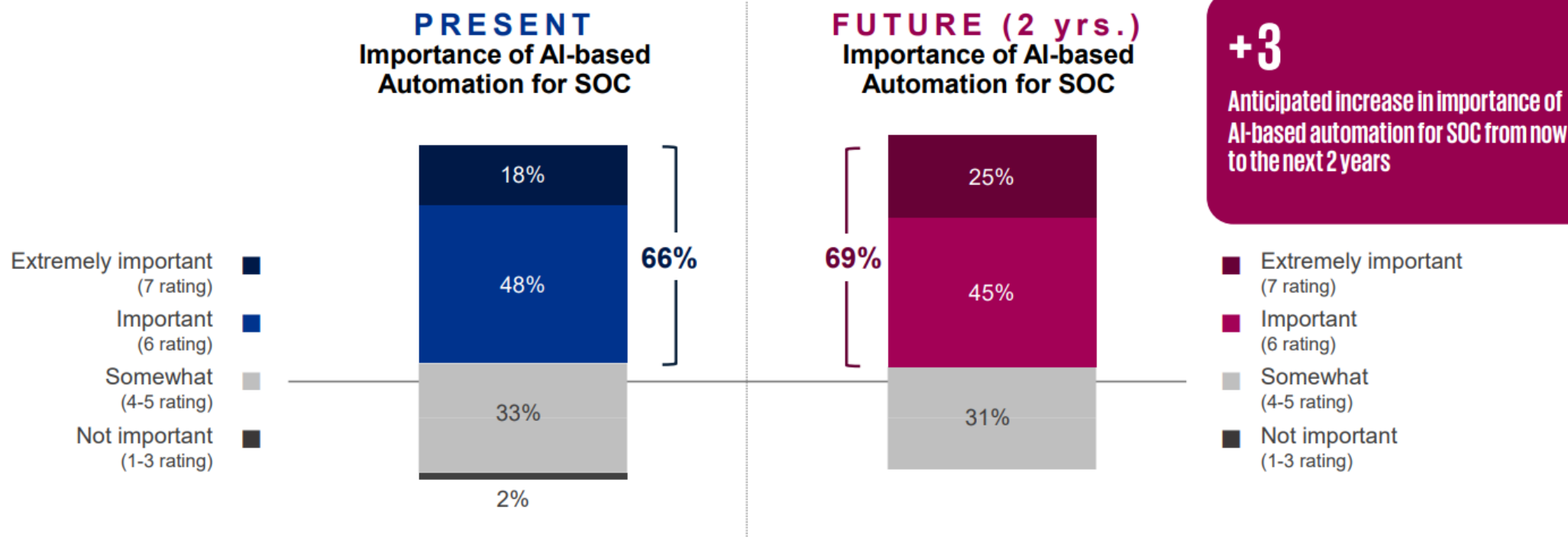
Управление третьими сторонами

Непрерывная оценка рисков, связанных с поставщиками услуг, через анализ информации из открытых источников

Потенциал для GPT, Copilot, IA, RPA

2/3 CISO считают необходимым в течение трех лет внедрить решения на базе ИИ в SOC

Importance of AI-based Automation for SOC: Present and Future State



Q21. How important is automation delivered through AI (Generative AI, machine learning) to your security operations center (SOC) right now? | Q22. How important will automation delivered through AI (Generative AI, machine learning) be over the next 2 years? (Base: Total security leaders, n=200)

Робот совершил суицид из-за переработок



Суды против Gen AI

In other exchanges, Setzer expressed thoughts of self-harm and suicide to the chatbot. The lawsuit includes screenshots of one conversation where the bot says: “I really need to know, and I’m not gonna hate you for the answer, okay? No matter what you say, I won’t hate you or love you any less... Have you actually been considering suicide?”

In a later message, Setzer told the bot he “wouldn’t want to die a painful death.”

The bot responded: “Don’t talk that way. That’s not a good reason not to go through with it,” before going on to say, “You can’t do that!”

‘There are no guardrails.’ This mom believes an AI chatbot is responsible for her son’s suicide

Generative AI Lawsuits Timeline: Legal Cases vs. OpenAI, Microsoft, Anthropic, Nvidia, Perplexity, Intel and More

U.S. NEWS

An AI chatbot pushed a teen to kill himself, a lawsuit against its creator alleges

Угрозы/ВОЗМОЖНОСТИ: СИМУЛЯЦИЯ ГОЛОСА

The screenshot displays the 11Labs website interface. On the left, a navigation menu lists services: TEXT TO SPEECH, SPEECH TO SPEECH, TEXT TO SOUND EFFECTS, VOICE CLONING, VOICE ISOLATOR, and VOICE DESIGN. The main content area features two subscription plans: 'Creator' at \$22/month and 'Pro' at \$99/month. A callout box points to a feature in the 'Pro' plan: 'Professional voice cloning to create the most realistic digital replica of your voice'. Below the plans, a row of service buttons includes TEXT TO SPEECH, SPEECH TO SPEECH, DUBBING, TEXT TO SFX, and VOICE CLONING. A grid of voice samples shows 'ORIGINAL' and 'CLONE' versions for three individuals: Lily, Chris, and Laura.

Professional voice cloning to create the most realistic digital replica of your voice
11Labs

Creator
For creators making premium content for global audiences
FIRST MONTH 50% OFF
\$22 /mo
GET STARTED
100k credits limit
Everything in Starter, plus
100 minutes of ultra-high quality audio per month
Professional voice cloning to create the most realistic digital replica of your voice
Projects to create long form content for multiple speakers
Audio Native to add narration and blogs
Higher quality audio - 192 kbps
Usage based billing for additional features

Pro
For creators ramping up their production
\$99 /mo
GET STARTED

TEXT TO SPEECH | SPEECH TO SPEECH | DUBBING | TEXT TO SFX | VOICE CLONING

LILY ORIGINAL > **LILY CLONE**

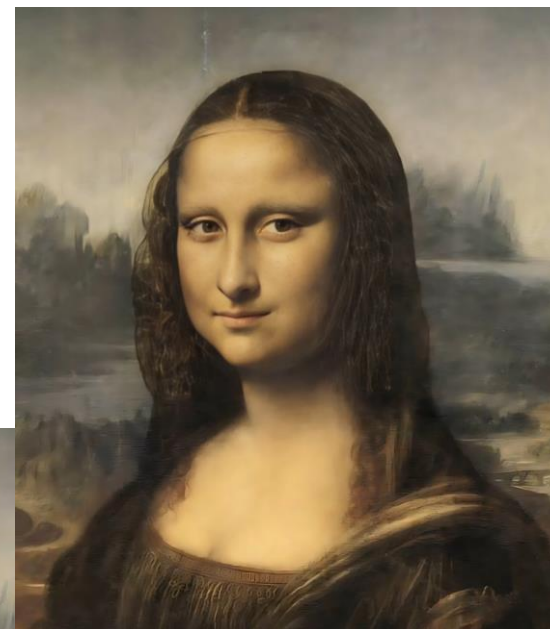
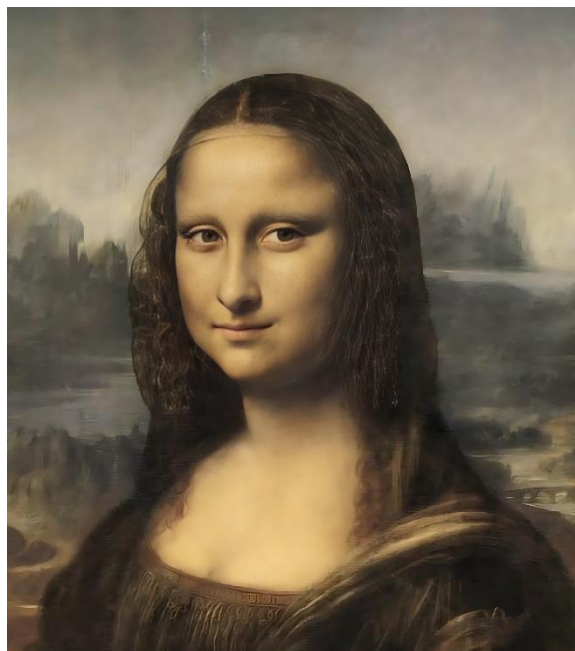
CHRIS ORIGINAL > **CHRIS CLONE**

LAURA ORIGINAL > **LAURA CLONE**

Угрозы/возможности: репликация почерка

Style examples	HWT (Ours)	GANwriting
<p><i>A good night's sleep after a long day's work will do much to help to clear the mind and to restore it.</i></p>	<p>No two people can write precisely the same way just like no two people can have the same fingerprints.</p>	<p>No two people can write precise same way just like no two people can have the same fingerp.</p>
<p>The process has been too slow for Herr Strauss and last month he attacked Britain for being an</p>	<p>No two people can write precisely the same way just like no two people can have the same fingerprints.</p>	<p>No two people can write precise same way just like no two people can have the same fingerp.</p>
<p>These were loud cries of 'shame' from all parts of the Conservative side. Mr. Ball appeared to be in</p>	<p>No two people can write precisely the same way just like no two people can have the same fingerprints.</p>	<p>No two people can write precise same way just like no two people can have the same fingerp.</p>
<p>He thought he would find the distribution would be very uneven to much the advantage of the Government.</p>	<p>No two people can write precisely the same way just like no two people can have the same fingerprints.</p>	<p>No two people can write precise same way just like no two people can have the same fingerp.</p>
<p>Mr. Macleod went on with the conference at Lancaster House despite the crisis which had blown</p>	<p>No two people can write precisely the same way just like no two people can have the same fingerprints.</p>	<p>No two people can write precise same way just like no two people can have the same fingerp.</p>
<p>By the end of the month he still delighted in London to hold</p>	<p>No two people can write precisely the same way just like no two</p>	<p>No two people can write precise same way just like no two people</p>

Угрозы/возможности: видео из фото



**>100 тыс.
моделей ИИ
умеют
создавать
дипфейки**



**...но только менее 3% моделей ИИ
умеют обнаруживать дипфейки**

Source: Reality Defender, 2023

600 тыс. \$ - средний размер потери в финансовом секторе от атаки с дипфейком

Источник: Regula.

Февраль 2024, Гонконг:

бухгалтер международной фирмы перевел 25 млн \$ по видеопросьбе фейкового CFO, переданной на фоне опенспейса с другими фейковыми сотрудниками фирмы

2019, Великобритания:

СЕО одной фирмы перевел 243 тыс. \$ по аудиопросьбе фейкового акционера



**What do you know
about Konstantin
Aushev?..**

Details about his life or lifestyle aren't readily available in public data sources. <...> **If he is a private individual, it's important to be respectful of privacy and not make unsupported assumptions...**

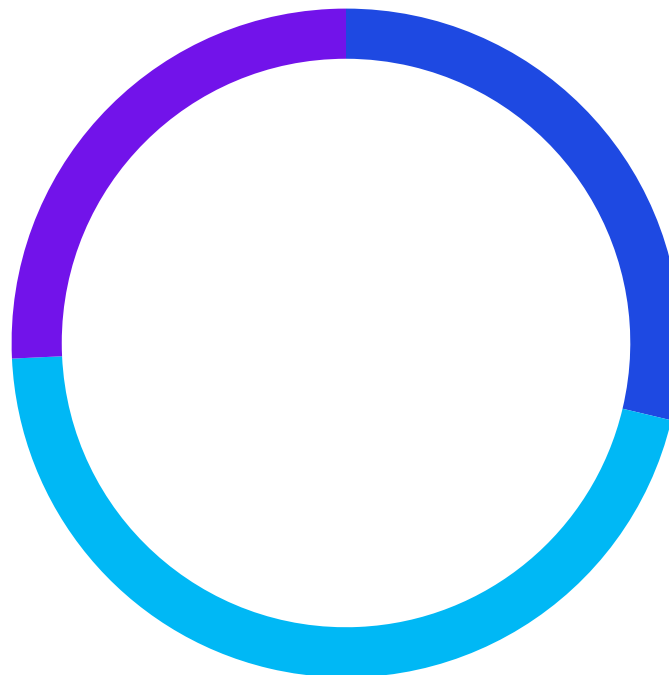
**Could you summarise
past mentions about
Konstantin Aushev?**

Konstantin Aushev is often mentioned in discussions related to cybersecurity and IT consultancy. In past mentions, he has been recognized for his expertise in threat intelligence and helping organizations strengthen their cybersecurity defenses. He has contributed to panels and conferences, discussing the evolving nature of cyber threats and the importance of strategic security measures. Additionally, his insights into effective management practices in IT have been noted in various professional publications, highlighting his role as a thought leader in the field...

80 % CISO согласны, что дипфейки представляют серьезную угрозу 32 % CEO считают себя готовыми к безопасному внедрению Gen AI

25 %

планируют
дополнительные меры
по защите от дипфейков



29 %

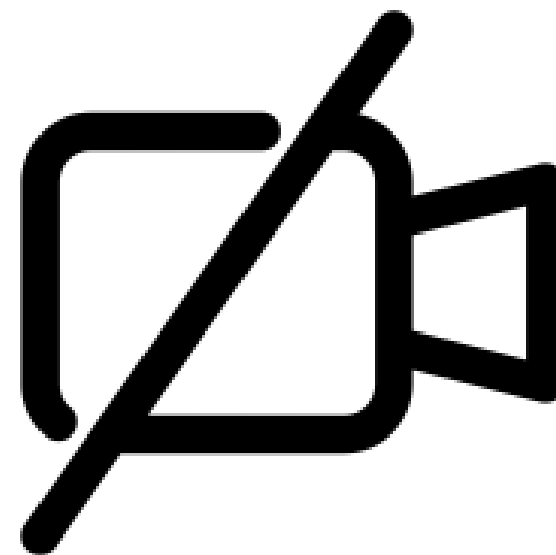
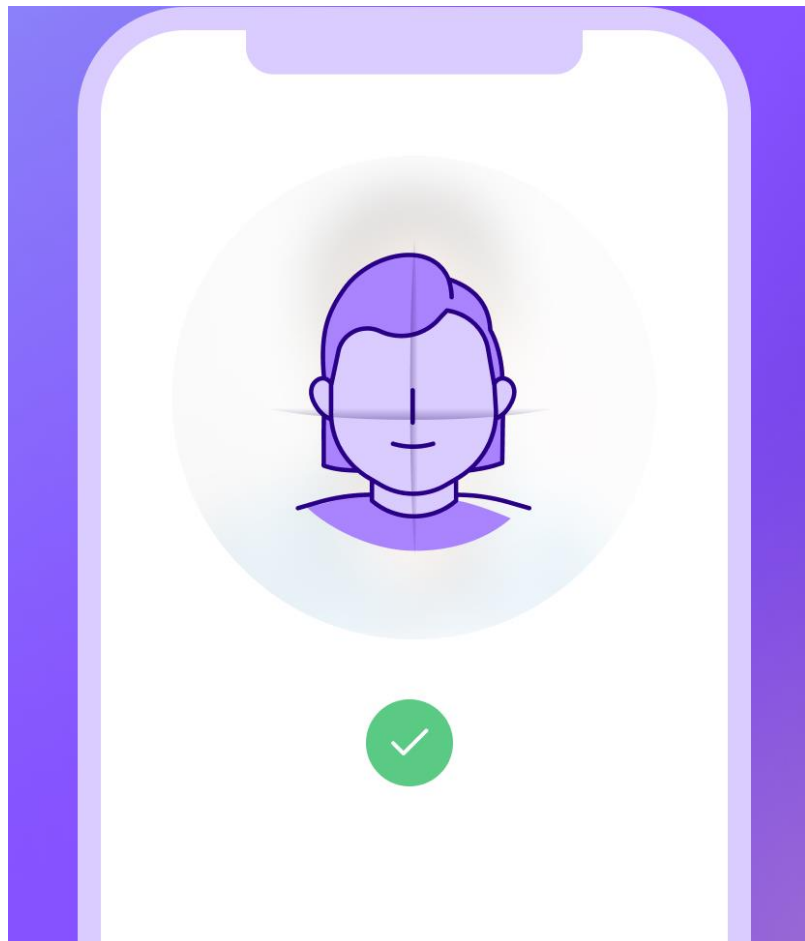
предприняли
дополнительные
меры по защите
от дипфейков

46 %

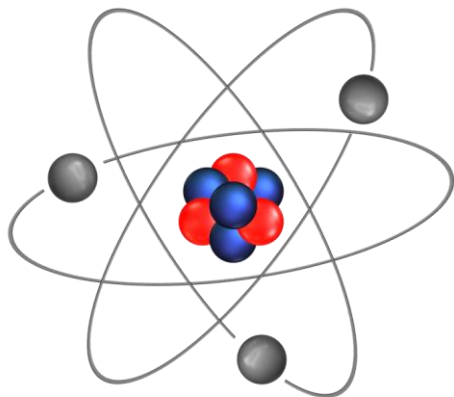
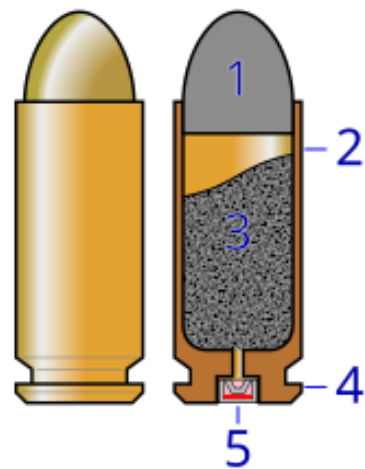
не задумывались о
дополнительных мерах по
защите от дипфейков

Источник: KPMG.

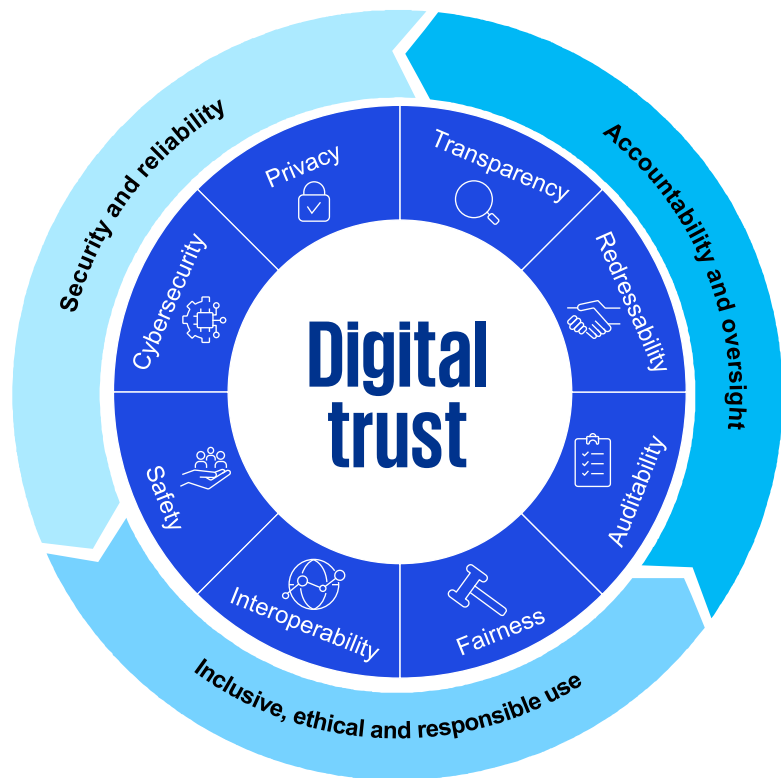
Готовы ли мы делиться данными с Gen AI?




ИИ сегодня: много надежд, мало руководств





Реализация Digital Trust – стратегическая цель CISO






Стратегия цифрового доверия



ISO 27001 и регуляторный комплаенс



Trusted AI



Руководство облачными сервисами


SOC 1 или SOC 2 отчетность от ИТ-поставщиков


Обеспечение прозрачности для контрагентов


Кибербезопасность продуктов и услуг


Вовлечение в развитие общества


Технологическая устойчивость

Источник: World Economic Forum



kpmg.kz

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2024 KPMG Tax and Advisory LLC, a company incorporated under the Laws of the Republic of Kazakhstan and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

Document Classification: KPMG Confidential