

https://cybersecurity.analitika.kz

АКТУАЛЬНОСТЬ

Технологии в сфере кибербезопасности (информационной безопасности) в настоящее время относятся к критически важным, от развития которых зависит национальная безопасность страны и её граждан.

Технологии **непрерывно изменяются**, особый импульс скорости изменений придал ИИ. Появилось новое направление – Gen AI в кибербезопасности, объем рынка по данному сегменту в 2023 году уже составил 1,64 млрд**.** долларов США. Прогноз на 2034 год- **14,79 млрд.** долларов США, темпы роста **22,13%** *

Оказывает влияние на рынок ИБ и развитие квантовых технологий в мире. В числе 10 стратегических технологических трендов на 2025 от Gartner впервые названа **постквантовая криптография** (PQC) : защита данных, устойчивая к рискам дешифрования квантовых вычислений (QC)**.

Необходим быстрый и удобный доступ к информации о технологиях

*Источник: https://www.precedenceresearch.com/generative-ai-in-cybersecurity-market
**Источник: https://www.gartner.com/en/articles/top-technology-trends-2025

РОСТ И УСЛОЖНЕНИЕ РЫНКА

По уточненным данным Gartner, Inc. (июль 2025 года), расходы конечных пользователей во всем мире на информационную безопасность в 2024 году составили **193 млрд долларов** США, прогноз по рынку на 2025 год - **213 млрд** долларов США.
Ожидается, что к 2026 году расходы на информационную безопасность в мире увеличатся на **12,5%** и составят $ **240** млрд*.

Растет и усложняется сам рынок кибербезопасности. В ответ на новые угрозы появляются новые игроки и стартапы, обостряется конкуренция.



Необходим быстрый доступ к информации об игроках рынка и конкурентах

*https://www.gartner.com/en/newsroom/press-releases/2025-07-29-gartner-forecasts-worldwide-end-user-spending-on-information-security-to-total-213-billion-us-dollars-in-2025

ОБЩАЯ ПРОБЛЕМА ДЛЯ РЫНКА ИБ – КАДРЫ И ИХ КОМПЕТЕНЦИИ

Недостаток кадров в сфере ИБ и слабое качество их подготовки даже в экономически и технологически развитых странах

Правительство Великобритании в сентябре 2024 года объявило о планах по укреплению навыков кибербезопасности после серии громких кибератак на критически важную национальную инфраструктуру. Великобритания запустила региональную программу развития навыков для финансирования ученичества с целью создания местных каналов **подготовки экспертов по кибербезопасности** по всей стране*.

Также будет оказана поддержка компаниям, разрабатывающим **новые инструменты кибербезопасности**. Наряду с этой инициативой Innovate UK возглавляет инвестиции в размере 1,3 млн фунтов стерлингов в университеты, местные советы и предприятия с целью усиления обучения навыкам кибербезопасности*

По курсу Нацбанка РК на 15.11.2024 года данная сумма эквивалентна 817,7 млн. тенге.

*UK to unveil new cyber security skills initiative at Global Cyber Summit,18.09.2024www.verdict.co.uk/uk-to-unveil-new-cyber-security-skills-initiative-at-global-cyber-summit

ЭКСПЕРТЫ О КЛЮЧЕВЫХ КОМПЕТЕНЦИЯХ И ИНФОРМАЦИИ



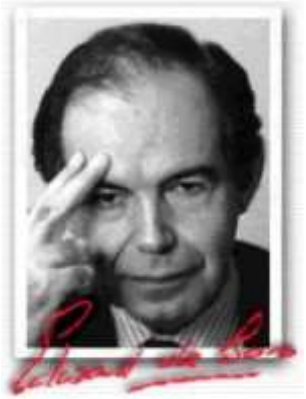
Джеффри Сэмплер,
Лондонская бизнес-школа.

Джеффри Сэмплер

«Ключевая компетенция – способность создавать новые виды бизнеса или новое конкурентное пространство:

- Интегрирование множества потоков знаний;
- Интегрирование новых знаний с традиционными;
- Новые гибридные продукты;
- Новые компетенции – новые конкурентные пространства»*.

В условиях нарастающей конкуренции необходимы новые идеи и креативные сотрудники.



Эдвард де Боно
19.05.1933-09.06.2021
Консультировал IBM, Microsoft, Apple, Пентагон

Эдвард де Боно

Латеральное мышление (lateral thinking) - метод нестандартного подхода и решения задач, способность порождать новые идеи

Для латерального мышления необходимы два условия:

1)Изобилие информации 2) Ломка стереотипов.

Брайан Трейси

«Закон интегративной сложности гласит, что компания (страна), способная интегрировать и использовать наибольшее количество информации на любом поле, поднимется на вершину этого поля».

*Джеффри Сэмплер, Стратегический менеджмент в цифровую эпоху, Курс МБА.

ПРОБЛЕМЫ РАБОТЫ С ИНФОРМАЦИЕЙ

Таким образом, информация является важнейшим фактором производства, она необходима для повышения компетенций, формирования новых идей, для принятия решений, эффективного сотрудничества и коммуникаций.



Существующие проблемы:

- Стремительный рост объемов информации в сети интернет;
- Многократное дублирование информации, порождающее информационный шум;
- Недостоверность информации в сети (случайное или преднамеренное искажение).

В таких условиях информация становится «пожирателем» трафика и времени, наблюдается парадокс: отсутствие необходимой информации при её избытке.

Рост объемов информации по кибербезопасности

По оценкам экспертов до 95 % информации можно получить из открытых источников, если грамотно организовать их изучение

Количество ответов на запросы по тематике кибербезопасности в поисковой системе Google на 03.04.2020

Поисковые запросы	Ответы в Google
Cybersecurity	292 000 000(0,45 сек)
Cybersecurity Companies	81 400 000 (0,68 сек.)
Cybersecurity Solutions	65 200 000 (0,55 сек.)
Enterprise Cybersecurity Solutions	70 300 000 (0,66 сек.)
Кибербезопасность	4 540 000 (0,42 сек)
Решения в сфере кибербезопасности	1 120 000 (0,42 сек)
Компании в сфере кибербезопасности	1 330 000 (0,44 сек)
Корпоративные решения кибербезопасности	740 000 (0,42сек)

Источник: собственные исследования



Растут непроизводительные потери времени на поиск релевантной информации

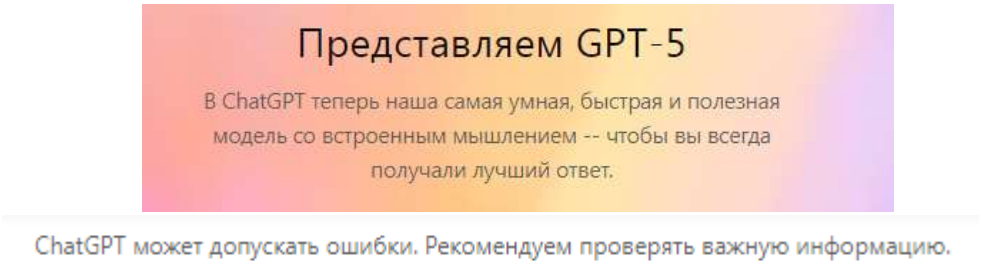
Отсутствие целостной картины ситуации на рынке

Нельзя искать то, о чём не знаешь

Через 5 лет количество ответов по запросам кратно увеличилось, так , на 05.12.2025 по запросу «Cybersecurity» получено 771 миллионов ответов (в 2020 г. –292 млн). На 20.01.2026 по запросу Cybersecurity Companies – 209 млн. ответов (в 2020 г - 81,4 млн) и т.д.

ИСПОЛЬЗОВАНИЕ ИИ (Chat GPT и др. модели)

Модели ИИ используют огромные объёмы информации и постоянно совершенствуются. Тем не менее, существующие версии LLM допускают **ошибки**, о чем предупреждают сами разработчики. Ниже представлен скрин с главной страницы последней версии Chat GPT-5, размещенной в свободном доступе 07.08.2025.



Американские эксперты о качестве данных и плохих результатах ИИ

«Данные - источник жизненной силы моделей искусственного интеллекта, они не могут быть просто средством достижения цели моделирования. Мусор на входе, мусор на выходе - давний принцип моделирования. С появлением современного искусственного интеллекта и, одновременно, огромных объемов информации, которые модели машинного обучения должны обрабатывать, стало труднее распознать логику плохих результатов»*

*Quality training data is vital for developing and deploying AI models, *https://www.verdict.co.uk/quality-training-data-ai-models/*

ИИ: СДВИГ ПАРАДИГМЫ С КОДА НА ДАННЫЕ

В отрасли информационных технологий при разработке моделей ИИ произошёл сдвиг парадигмы с кода на данные. Бывший гендиректор и основатель компании Scale AI Александр Ван ещё в 2021 году широко использовал слоган -

«данные – это новый код».

Компания на своей платформе размещала аннотированные, **проверенные человеком данные**, используя труд дипломированных специалистов и ученых ($100 за одну аннотацию). Доходы Scale AI по итогам 2024 года составили 870 млн долларов, из них 150 млн обеспечила компания Google, которая в 2025 году увеличила затраты на аннотированные данные на 33 %, выделив 200 млн долларов*.

(В июне 2025 года компания Марка Цукерберга вошла в капитал Scale AI , а основатель последней А. Ван был назначен в Meta на руководящую должность)

Компания Gartner 05.08.2025 опубликовала статью по главным инновациям в сфере ИИ в 2025 году, среди двух главных - **Готовые к использованию ИИ данные**.

«Готовые к использованию данные обеспечивают оптимизацию наборов данных для приложений ИИ, повышая точность и эффективность» **

Достоверность данных и информации выходят на первый план

* *https://www.verdict.co.uk/google-scale-ai-meta-acquisition/*

* * https://www.gartner.com/en/newsroom/press-releases/2025-08-05-gartner-hype-cycle-identifies-top-ai-innovations-in-2025

ИИ: СТРУКТУРА ДАННЫХ и ПОВЕСТВОВАНИЕ

Кроме качества данных большую роль играет их структура и формирование целостной картины, что особенно важно при отраслевом анализе.

Американский эксперт по ИИ

«При работе с данными специалисты по данным несут ответственность за обеспечение **необходимой структуры,** чтобы данные могли быть поняты целевой аудитории.
Сами по себе данные не стимулируют инновации - **важнее повествование** на основе данных, которое помогает выявить скрытые тенденции, обеспечивает персонализацию и оптимизирует процессы». *

Второй аспект использования ИИ при поиске отраслевой информации:
Эффективное использование ИИ инструментов построено на правильных формулировках запросов к модели. Появилась даже новая специальность prompt-инженеры, зарплата которых доходит до 1 млн. тенге в месяц в Казахстане и до $123 000 в год в США ($10,2 тыс. в месяц).

- По данным **Glassdoor**, средняя общая компенсация (base + бонусы) составляет около **$123 000–$123 400 в год**. Базовая зарплата — $77 000–$124 000; дополнительные выплаты — $19 000–$36 000. Все данные актуальны на апрель 2025 года. Glassdoor
- Похожий показатель представлен **Indeed**: средняя зарплата prompt-инженера — **$123 514 в год** (информация по 41 вакансии, обновление — 8 августа 2025 года). Indeed
- **NetCom Learning** указывает среднюю базу **$122 327 в год** (по данным Glassdoor). netcomlearning.com

* *Data scientists: Bring the narrative to the forefront ,17.04.2021, https://techcrunch.com/2021/04/16/data-scientists-bring-the-narrative-to-the-forefront/*

ЗАПРОСЫ К ИИ и ПРОИЗВОДИТЕЛЬНОСТЬ ТРУДА ОТРАСЛЕВЫХ ЭКСПЕРТОВ

Даже если использование инструментов ИИ и приводит к сокращению времени на поиск аналитической информации, то возникают следующие проблемы и ограничения:

1) Вопросы по достоверности информации и проблемы «галлюцинаций» у ИИ.

2) Нельзя искать то, о чем ты не знаешь (можно упустить новые технологии и компании).
3) Необходимость платной подписки для доступа к расширенному функционалу LLM.

4) Разрозненные запросы к ИИ сотрудников организации (компании) по текущим операционным вопросам не аккумулируются в корпоративную базу знаний. Одни и те же запросы могут часто повторяться разными экспертами.

5) При ротации сотрудников полученная информация, справки и отчеты, как правило, не сохраняются.

6) Сами знания и информация постоянно обновляются и требуются новые запросы к моделям ИИ.

7) И главное, **нет целостной картины развития отрасли**, в рассматриваемом случае - развития кибербезопасности в мире и в Казахстане.

ПРЕДЛАГАЕМОЕ РЕШЕНИЕ

В целях повышения конкурентоспособности Казахстана в сфере глобальной кибербезопасности и реализации целей и задач, стоящих перед государственными и частными компаниями в сфере ИБ, **приглашаем стратегических партнеров** для развития информационно-справочной системы **«Глобальный рынок кибербезопасности»** (-далее ИСС), разработанной группой компаний «LINCOMPANY» на основе авторских подходов к сбору и структурированию отраслевой информации, а также формату её представления.

В настоящее время ИСС размещена по адресу https://cybersecurity.analitika.kz и находится в закрытом доступе.

Назначение ИСС- предоставление доступа к релевантной информации по глобальному рынку кибербезопасности, мониторинг изменений глобального рынка, формирование базы знаний по кибербезопасности и применяемым технологиям.

Функциональные возможности: быстрый поиск релевантной информации по темам, компаниям и странам благодаря выстроенной трехуровневой навигации.

Развитие ИСС – на втором этапе возможно использование инструментов ИИ для актуализации новостей по разделам ИСС, на следующих этапах, после построения полной информационной модели отрасли в сети интернет, планируется формирование **отраслевой платформы по глобальному рынку кибербезопасности** с использованием ИИ на основе обучения малой языковой модели (SLM).

Разделы информационно-справочной системы





Вся экосистема глобальной кибербезопасности - в одном месте!

- Ассоциации национальные и международные;
- Госрегулирование ИБ по странам;
- Госпрограммы и стратегии по странам;
- НПА и сертификация;
- Обзоры рынка;
- Образование в сфере кибербезопасности;
- Персоны отрасли;
- Профили стран;
- Постквантовая криптография;
- Реестр компаний по странам;
- Реестр решений по кибербезопасности;
- Рейтинги страновые: GCI, NCSI;
- Статистика кибератак по странам;
- Специализированные выставки и форумы в сфере кибербезопасности
- Центры компетенций и НИИ.

Содействие реализации новой казахстанской концепции

Концепция цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023 - 2029 годы

Глава 4 «Кибербезопасность» почти полностью посвящена обзору международного опыта и завершается следующими словами:

«Для формирования государственной политики в сфере защиты персональных данных адаптируется опыт применения стандарта GDPR взятый на вооружение странами ЕС.

Также Казахстаном будет адаптирован международный опыт **формирования технологических платформ**, которые активно реализуются многие годы в Европейском союзе, Швеции, Великобритании, Австралии, Российской Федерации. Суть технологических платформ заключается в мобилизации усилий всех интеллектуальных, финансовых и иных ресурсов на приоритетных направлениях и внедрении ключевых технологий отрасли, что крайне важно при оптимизации бюджета в условиях кризиса. Таким образом, будет взят на вооружение опыт передовых ИТ- держав» *.

Разработанная информационно-справочная система может выполнять функции технологической платформы, объединяя бизнес, науку и государство

*Источник: https://www.gov.kz/legalacts/details/P2300000269?lang=ru#z169

ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ

1) Высокие позиции ИСС в поисковых запросах и в справках LLM
Так как мы интегрируем все потоки знаний в сфере глобальной кибербезопасности и организуем информацию по заданной структуре на одной интернет- площадке, это **обеспечит** хорошую выдачу ИСС в поисковых запросах и использование ресурса большими языковыми моделями (LLM) при формировании справок (есть подтверждающие факты на примере сайта КАИТК и других ресурсов, которые мы разработали и сопровождаем).
2) Повышение имиджа Казахстана на международной арене и реализация целей, поставленных Правительством , прежде всего, **повышение уровня компетенций** специалистов в сфере ИБ, информационное обеспечение по вопросам кибербезопасности, популяризация ИБ , улучшение качества взаимодействия и сотрудничества с участниками отрасли и др.
3) Повышение уровня исследовательских работ за счет генерирования новых идей и появление новых продуктов и инструментов в сфере кибербезопасности.
4) Формирование в Казахстане конкурентного в мире аналитического центра по кибербезопасности.

5) Создание условий для развития участников рынка за счет лучшего знания потребностей и эффективного продвижения своих разработок.

ИСС, размещенная в сети интернет в свободном доступе, выйдет на самоокупаемость и будет приносить доходы . Сформированные БД по кибербезопасности могут быть использованы для обучения отраслевой малой языковой модели (SLM).



Спасибо за внимание!

Насенкова Людмила **Тел.: +7(705)614-11-88**

Директор ТОО «LINCOMPANY» и ТОО «TC-Online»