

**Будущее безопасности: революция искусственного интеллекта в работе подразделений по информационной безопасности**

**Константин Саматов**

**Член Правления Ассоциации руководителей служб ИБ**

# Что такое искусственный интеллект?

**Искусственный интеллект (ИИ)** - это область науки, которая изучает, как компьютеры могут выполнять задачи, которые обычно требуют интеллекта человека.

Эта область науки включает в себя:

- машинное обучение (machine learning)
- глубокое обучение (deep learning)
- нейронные сети (neural networks)

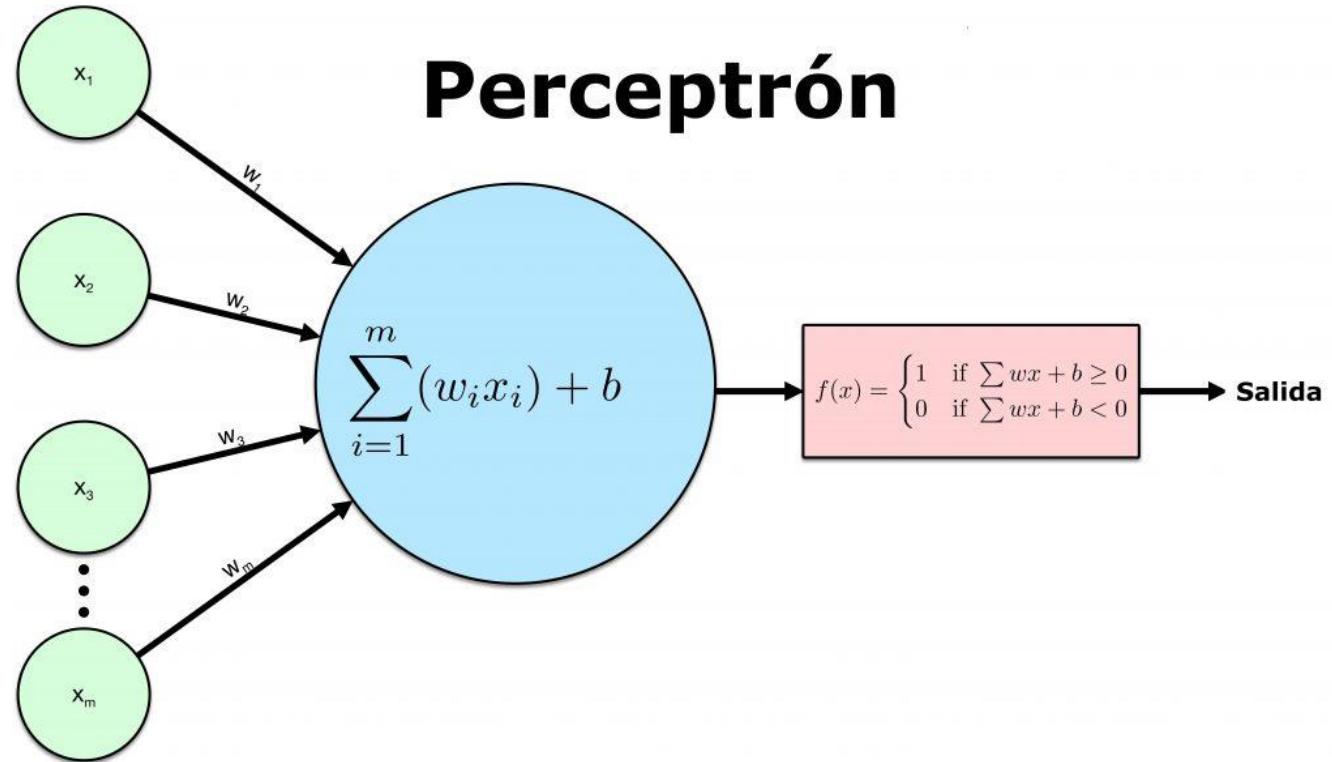




# Технологии ИИ



- Все современные технологии ИИ основаны на машинном обучении
- Искусственный интеллект - это не кибернетический разум, а система алгоритмов
- Появление искусственного интеллекта, равного человеческому (искусственного разума) в ближайшее время не ожидается



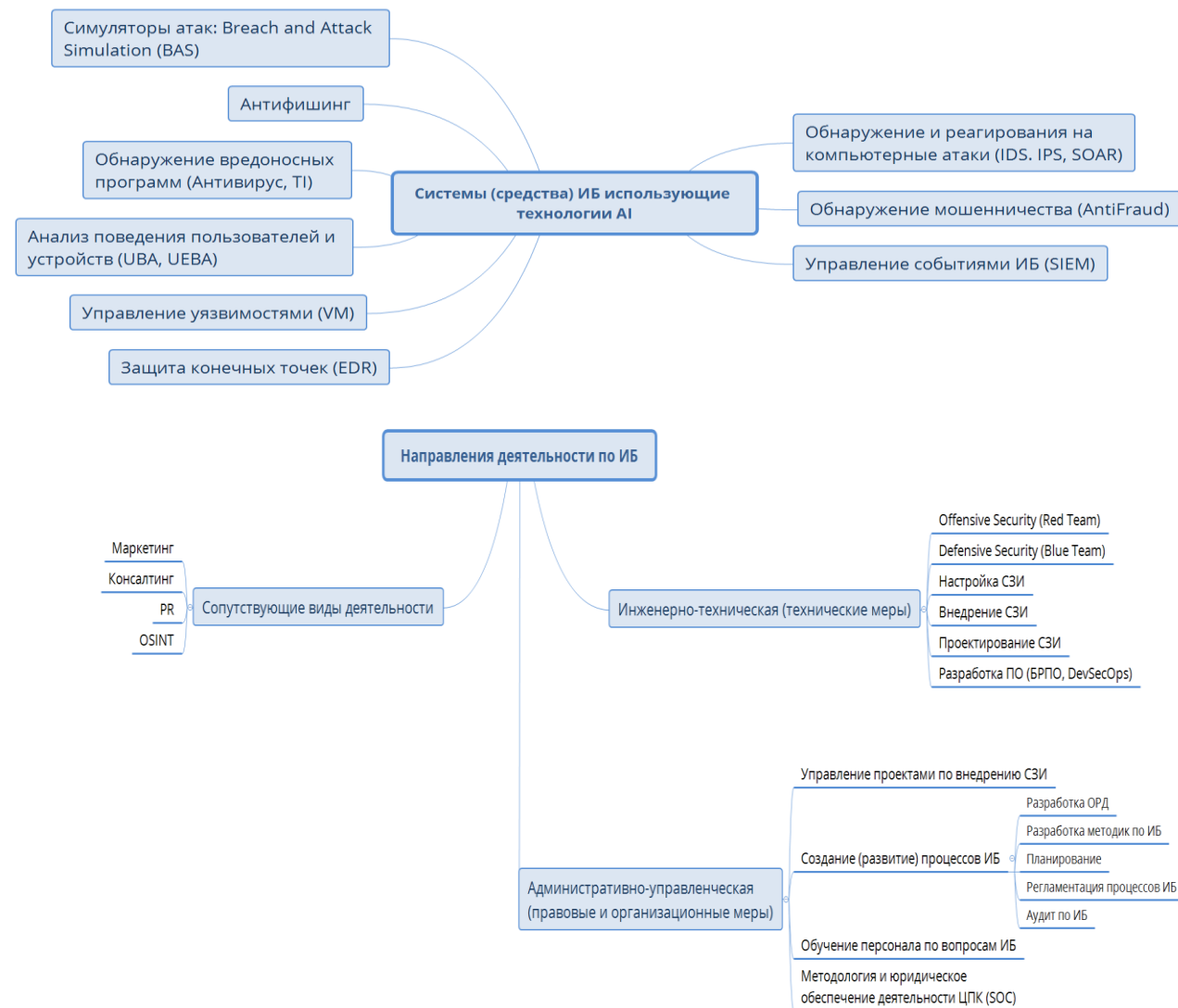
Модель перцептрона была разработана Фрэнком Розенблаттом в 1958 году.  
Это математическая модель восприятия информации мозгом

# Использование ИИ в ИБ

1. Искусственный интеллект является одним из наиболее перспективных направлений в области информационной безопасности.

2. Примеры использования ИИ в информационной безопасности:

- Обнаружение и предотвращение кибератак
- Мониторинг и защита конфиденциальных данных
- Анализ и прогнозирование уязвимостей
- Обучение персонала по ИБ



# Ключевые преимущества ИИ

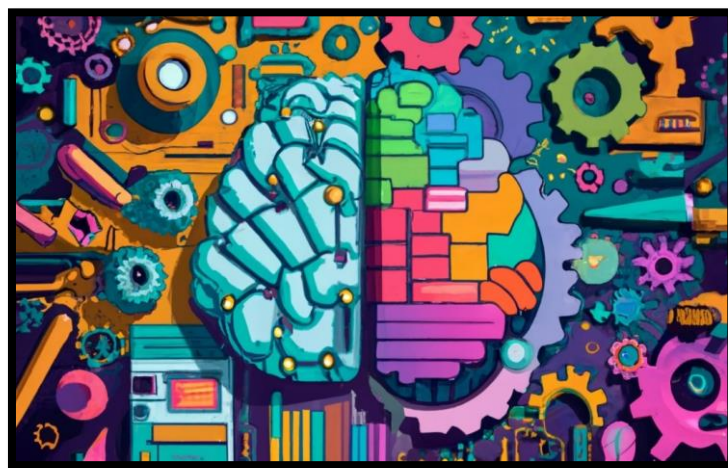
## Автоматизация и упрощение процессов

С помощью ИИ можно автоматизировать и упрощать рутинные задачи, во всех направлениях ИБ, что позволяет сократить время и улучшить качество работы



## Более эффективное обнаружение угроз

ИИ может помочь в обнаружении угроз безопасности, которые могут быть пропущены человеческим фактором. Алгоритмы машинного обучения могут анализировать большие объемы данных и выявлять скрытые угрозы

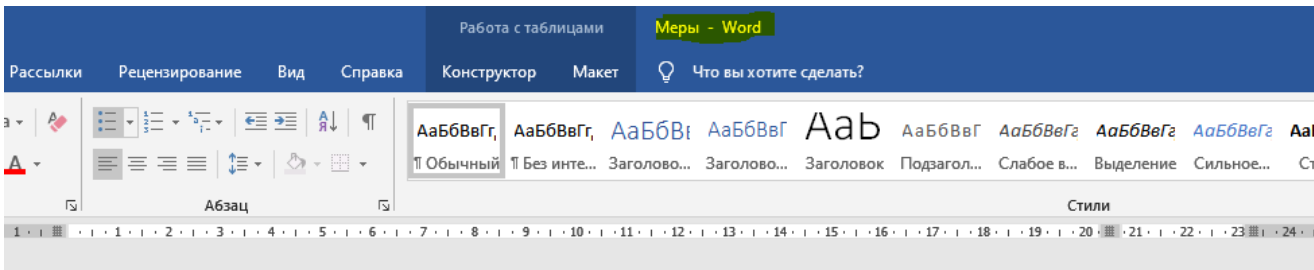


## Улучшенная реакция на кибератаки

ИИ может помочь в быстрой реакции на компьютерные атаки. Автоматические системы могут быстро определить и остановить атаку на более ранней стадии, что позволяет минимизировать ущерб для организации



# Автоматизация процессов (кейс автоматизация аудита)



<b>5. Обеспечение безопасности значимого объекта в ходе его эксплуатации (Реализация мер обеспечения безопасности)</b>	
I. Идентификация и аутентификация (ИАФ)	0,50
II. Управление доступом (УПД)	1,00
III. Ограничение программной среды (ОПС)	1,00
IV. Защита машинных носителей информации (ЗНИ)	1,00
V. Аудит безопасности (АУД)	0,00
VI. Антивирусная защита (АВЗ)	1,00
VII. Предотвращение вторжений (компьютерных атак) (СОВ)	1,00
VIII. Обеспечение целостности (ОЦЛ)	1,00
IX. Обеспечение доступности (ОДТ)	1,00
X. Защита технических средств и систем (ЗТС)	1,00
XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)	1,00
XII. Реагирование на компьютерные инциденты (ИНЦ)	1,00
XIII. Управление конфигурацией (УКФ)	0,5
XIV. Управление обновлениями программного обеспечения (ОПО)	1,00
XV. Планирование мероприятий по обеспечению безопасности (ПЛН)	0,25
XVI. Обеспечение действий в нестандартных ситуациях (ДНС)	1,00
XVII. Информирование и обучение персонала (ИПО)	0,00
XVIII. Обеспечение ИБ при использовании средств криптографической защиты информации (СКЗИ)	1,00

DOCX Меры.docx  
14.37 KB

Действуй как специалист по кибербезопасности. Проведи анализ данной таблицы и сделай выводы о реализации мер защиты

CR

На основании предоставленной таблицы можно сделать следующие выводы о реализации мер защиты значимого объекта:

1. В целом реализован достаточно широкий спектр мер защиты - 18 различных направлений. Это говорит о комплексном подходе к обеспечению безопасности.
2. Большинство мер реализованы в полном объеме и оценены максимально в 1 балл. Это касается таких важных аспектов как управление доступом, защита от вредоносного ПО, обеспечение целостности и доступности, защита информационной системы и др.
3. Однако есть и уязвимые места. Например, аудит безопасности и информирование персонала не реализованы вообще (0 баллов). А планирование мероприятий по ИБ выполнено лишь частично (0,25). Эти аспекты требуют доработки.
4. Также отмечу недостаточную реализацию таких важных мер как идентификация и аутентификация (0,5 балла), управление конфигурацией (0,5 балла).
5. В целом система защиты объекта выглядит достаточно надежно. Большинство ключевых мер реализованы. Однако существенные "дыры" в аудите, контроле конфигураций и обучении персонала заметно снижают общий уровень безопасности. Необходимо оперативно закрыть эти пробелы в первую очередь.

Вот основные выводы, которые можно сделать на основе предоставленных данных о реализации мер защиты объекта. Готов ответить на дополнительные вопросы и уточнения.

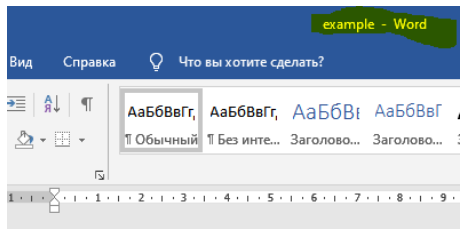
AI

Copy Retry





# Автоматизация процессов (кейс скрипт для обезличивания)



Объект «АСУТП»  
Объект «АСУТП Цеха»  
Объект «ИСПДн ЗУП»  
Объект «ИСПДн СКУД»

Чтобы проверить работу скрипта в [Google Colab](#), выполните следующие действия:

1. Откройте Google Colab.
2. Вставьте приведенный выше код в ячейку.
3. Нажмите кнопку "Выполнить".

После выполнения скрипта в документе "example.docx" появятся две таблицы с указанными вами данными.

Вот пример содержимого документа после работы скрипта:

Таблица 1

Объект 1  
Объект 2  
Объект 3  
Объект 4

Таблица 2

1. АСУТП  
2. АСУТП Цеха  
3. ИСПДн ЗУП  
4. ИСПДн СКУД

✦ Хорошо, вот скрипт для MS Word, который выполняет заданные вами условия:

Python

```
import docx

def main():
    # Открываем документ
    document = docx.Document("example.docx")

    # Получаем список параграфов документа
    paragraphs = document.paragraphs

    # Создаем таблицу для номеров объектов
    number_table = docx.Table(rows=1, cols=1)
    document.add_paragraph().add_run().add_table(number_table)

    # Создаем таблицу для названий объектов
    name_table = docx.Table(rows=0, cols=2)
    document.add_paragraph().add_run().add_table(name_table)

    # Итерируемся по параграфам
    for paragraph in paragraphs:
        # Получаем текст параграфа
        text = paragraph.text

        # Ищем все строки, начинающиеся со слова "Объект"
        for match in re.finditer("Объект (.*)", text):
            # Получаем название объекта
            name = match.group(1)

            # Получаем номер объекта
            number = len(number_table.rows) + 1

            # Добавляем номер объекта в таблицу номеров объектов
            number_table.rows[0].cells[0].text = str(number)

            # Добавляем название объекта в таблицу названий объектов
            name_table.add_row([str(number), name])

    # Сохраняем документ
    document.save("example.docx")

if __name__ == "__main__":
    main()
```

Use code with caution. [Learn more](#)



# Упрощение процессов (кейс юридический вопрос)

C

Действуй как эксперт в юриспруденции. Перепиши мне этот текст в виде таблицы. В одной колонке напиши этап принятия нормативно-правового акта в другой его описание: "V. Порядок подготовки и принятия нормативных правовых актов Министерства при осуществлении нормативного регулирования в установленной сфере деятельности"

5.1. Нормативные правовые акты издаются Мини Федерации в виде в соответствии с утвержденны федеральных органов государственной власти и Департамент, осуществляющий подготовку про департаментами с привлечением при необходи заинтересованными департаментами проекты и представлению в Юридический департамент, к надлежащим оформлением и своевременным н: Министерство юстиции Российской Федерации В целях обеспечения возможности проведения департамент, осуществляющий подготовку про направления указанного проекта на рассмотрен сайте regulation.gov.ru в информационно-телек



Этап принятия нормативно-правового акта	Описание
Подготовка проекта нормативного правового акта	Департамент, осуществляющий подготовку проекта нормативного правового акта, разрабатывает его в соответствии с планами разработки нормативных правовых актов Министерства. При необходимости к разработке проекта привлекаются специалисты научных и иных организаций.
Согласование проекта нормативного правового акта	Проект нормативного правового акта согласовывается с заинтересованными департаментами Министерства, а также с федеральными органами исполнительной власти, органами государственной власти субъектов Российской Федерации, общественными объединениями и иными заинтересованными лицами. В случае необходимости проект нормативного правового акта проходит независимую антикоррупционную экспертизу.
Размещение проекта нормативного правового акта на regulation.gov.ru	Проект нормативного правового акта размещается на сайте regulation.gov.ru в информационно-телекоммуникационной сети "Интернет" не менее чем на 7 дней для проведения независимой антикоррупционной экспертизы, а также для общественного обсуждения.
Подписание нормативного правового акта	Проект нормативного правового акта подписывается Министром или лицом, исполняющим его обязанности.

Export to Sheets



# Риски и вызовы

## Недостатки ИИ в ИБ

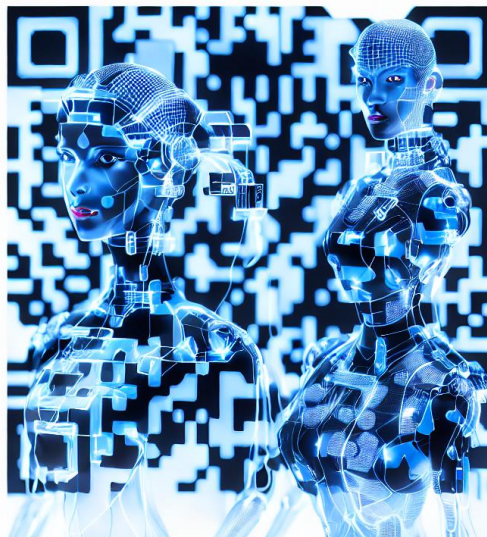
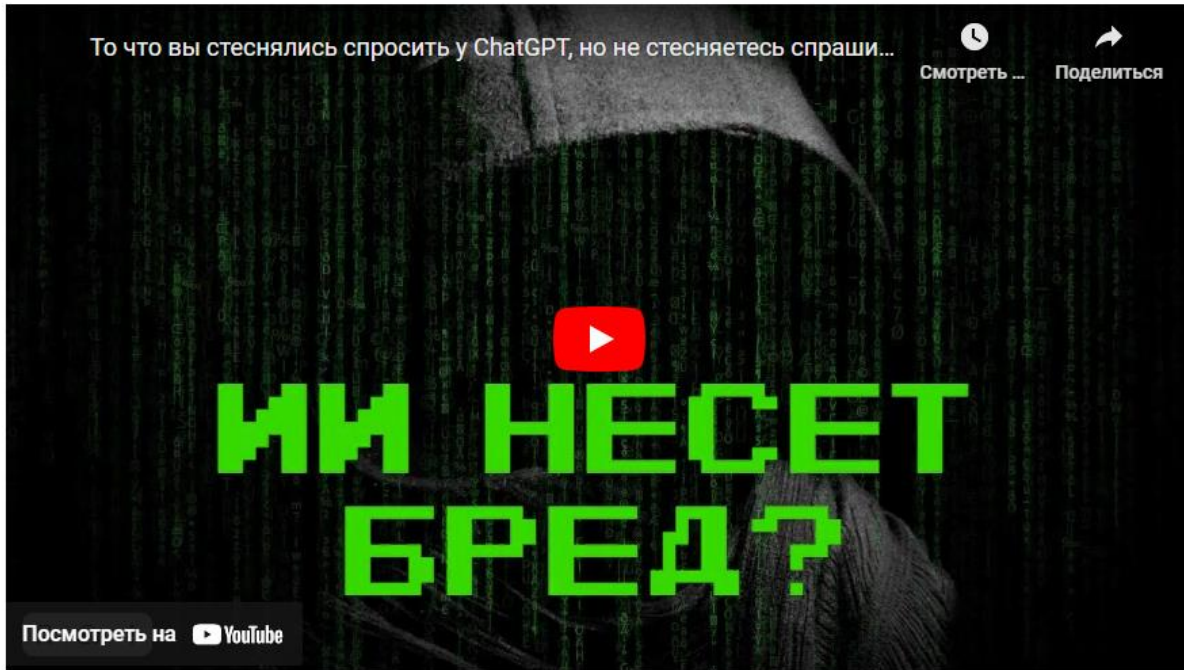
*Недостаточная точность:* ИИ может допускать ошибки, особенно если его алгоритмы не обучены правильно

*Недостаточная прозрачность:* Иногда трудно понять, на чем основаны «выводы» ИИ, что может затруднить их проверку и обнаружение ошибок

*Ограниченность:* ИИ может быть ограничен в своих возможностях, особенно если он не имеет доступа к достаточному количеству данных или если его алгоритмы не соответствуют конкретным потребностям безопасности



# Недостатки ИИ



ChatGPT bot

Кто такой Константин Саматов? 18:48 ✓

Константин Саматов - это российский кинорежиссёр и продюсер. Он известен своей работой в киноиндустрии, включая создание фильмов и других произведений. Информация о нём может быть распространена в социальных сетях, на сайтах киностудий или в профессиональных публикациях. 18:49

**GIGA CHAT**

Новый чат

Все чаты Избранные

FAQ

Bard (Experiment)

See the latest updates to the [Elastic Labs Hub](#)

New chat

Специалист по информацион...

Порядок механизмов SIEM-сист...

Кибербезопасность: основные...

Show more

Кто такой Константин Саматов?

Константин Саматов – российский специалист в области информационной безопасности и защиты данных. Он работает в этой сфере более 20 лет и имеет богатый опыт в различных областях, включая техническую безопасность, аналитическую работу, управление проектами и обучение.

Константин родился в Екатеринбурге и окончил Уральский государственный педагогический университет по специальности **Информатика**. После окончания университета он начал работать в сфере безопасности, сначала в качестве сотрудника службы безопасности, а затем в качестве руководителя отдела информационной безопасности.

За время своей работы Константин участвовал в разработке и реализации проектов по обеспечению информационной безопасности для различных компаний и организаций, включая государственные органы, банки, предприятия и образовательные учреждения. Он также является автором нескольких книг и статей по информационной безопасности.

Константин является активным сторонником популяризации информационной безопасности в России. Он **ведет блог**, где делится своими знаниями и опытом с широкой аудиторией. Также он регулярно выступает на конференциях и семинарах, рассказывая о современных угрозах информационной безопасности и способах их защиты.



# Риски и вызовы

## Риски использования ИИ в ИБ

*Нарушение конфиденциальности:* Использование ИИ может привести к утечке конфиденциальной информации.

*Возможность злоупотребления:* ИИ может быть использован злоумышленниками для создания новых видов кибератак и других угроз безопасности данных.

*Недостаточная защита:* приложение (модель) ИИ может быть уязвим к атакам и другим угрозам безопасности.

**Подробнее:** OWASP Top 10 for Large Language Model Applications (OWASP Top 10 для приложений с большими языковыми)  
<https://owasp.org/www-project-top-10-for-large-language-model-applications/>





# Будущее информационной безопасности

## **Автоматизация и оптимизация процессов**

С помощью ИИ можно автоматизировать рутинные задачи и оптимизировать процессы, что позволит специалистам по ИБ сосредоточиться на более сложных и важных задачах

---

## **Развитие кибератак и усиление защиты**

С развитием технологий кибератаки становятся все более сложными и усовершенствованными. В будущем ИИ будет использоваться для создания более эффективных систем защиты и противодействия киберугрозам

---

## **Использование больших данных**

Использование ИИ позволит анализировать и обрабатывать большие объемы данных, что поможет выявлять уязвимости и предотвращать кибератаки.



# Будущее информационной безопасности: кадры (персонал)

Жопотолог  
(Prompt Engineer)



Data Scientist







**Спасибо за внимание!**