КИБЕРБЕЗОПАСНОСТЬ НА МЕСТАХ

РЕШАЕТ ЛИ МАССОВЫЙ ПЕРЕХОД НА ГИСЫ ПРОБЛЕМУ УГРОЗ И КАКИЕ ВОЗМОЖНОСТИ ПРИ ЭТОМ СОЗДАЮТСЯ?

НАИБОЛЕЕ РАСПРОСТРАНЕННЫЕ КИБЕРУГРОЗЫ

Атаки на отказ в обслуживании (DDoS)

используются для перегрузки серверов государственных платформ, что приводит к сбоям в их работе

Фишинг и социальная инженерия

направлены на получение доступа к конфиденциальной информации через обман сотрудников и граждан

Эксплуатация уязвимостей программного обеспечения

использование незащищенных мест в коде систем, что позволяет злоумышленникам проникать в защищенные сети

Целенаправленные атаки (APT)

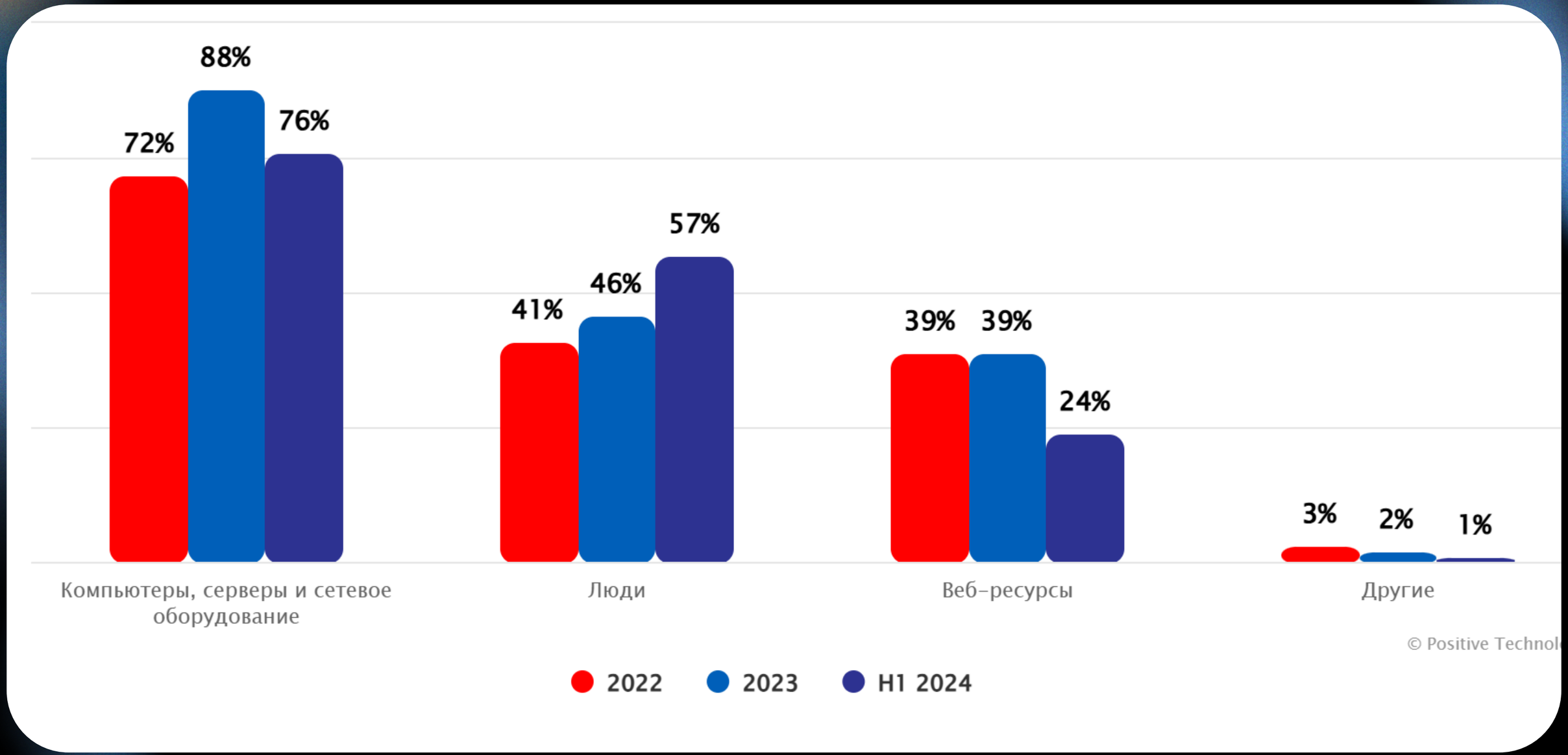
долгосрочные кибератаки со стороны организованных хакерских группировок, часто поддерживаемых государствами

Вредоносное ПО и вирусные атаки

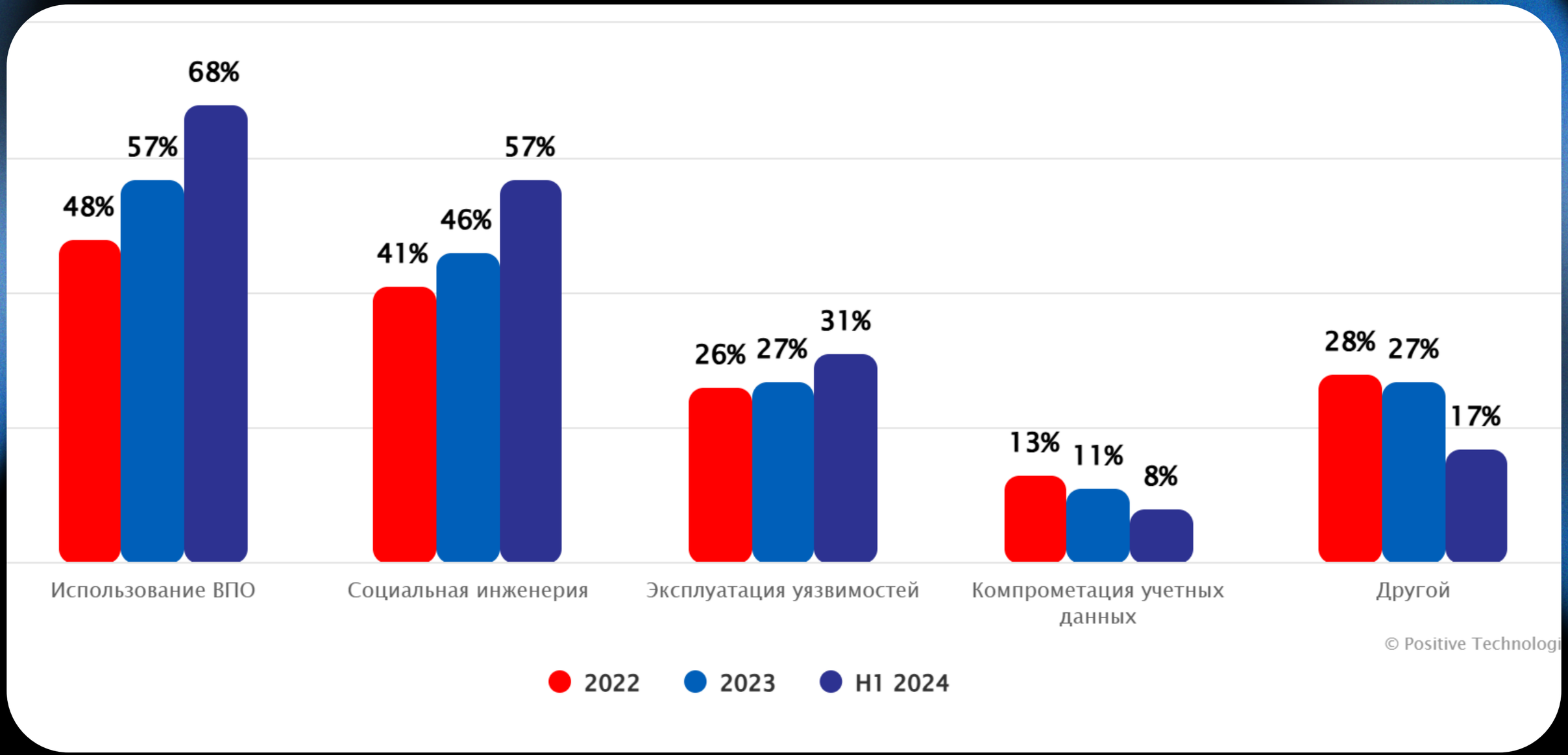
внедрение троянов, программ-вымогателей (ransomware) и шпионского ПО с целью кражи данных или блокировки доступа.

ДОЛЯ АТАК НА ОРГАНИЗАЦИИ

ОБЪЕКТЫ АТАК



МЕТОДЫ АТАК


68%
57%
48%
57%
46%
41%
31%
27%
26%
13%
11%
8%
28%
27%
17%
Использование ВПО
Социальная инженерия
Эксплуатация уязвимостей
Компрометация учетных данных
Другой
© Positive Technologi
2022
2023
H1 2024

НОВЫЕ ВОЗМОЖНОСТИ

Повышенная безопасность

стандартизированные протоколы устраняют разрозненность в подходах к киберзащите

Более эффективное реагирование на угрозы

централизованный контроль позволяет быстрее выявлять атаки и координировать защитные меры

Снижение зависимости от зарубежных ИТ-компаний

уменьшает риски, связанные с использованием иностранного ПО

Экономия ресурсов

унификация технологий снижает затраты на поддержку разрозненных систем

Упрощение регулирования

ГИС позволяют государству более эффективно контролировать обработку данных

Передовые технологии для усиления защиты данных

Квантовая криптография

Технология блокчейн

Системы поведенческого анализа

Биометрическая аутентификация

Облачные технологии с усиленной защитой

НОВЫЕ РИСКИ

Централизованные системы как главная мишень атак

взлом может привести к компрометации огромных объемов данных

Внутренний саботаж

сотрудники, имеющие доступ к критически важной информации, могут злоупотреблять этим

Монополизация управления и зависимость от единого оператора

сбой или ошибка в системе могут парализовать работу государственных сервисов

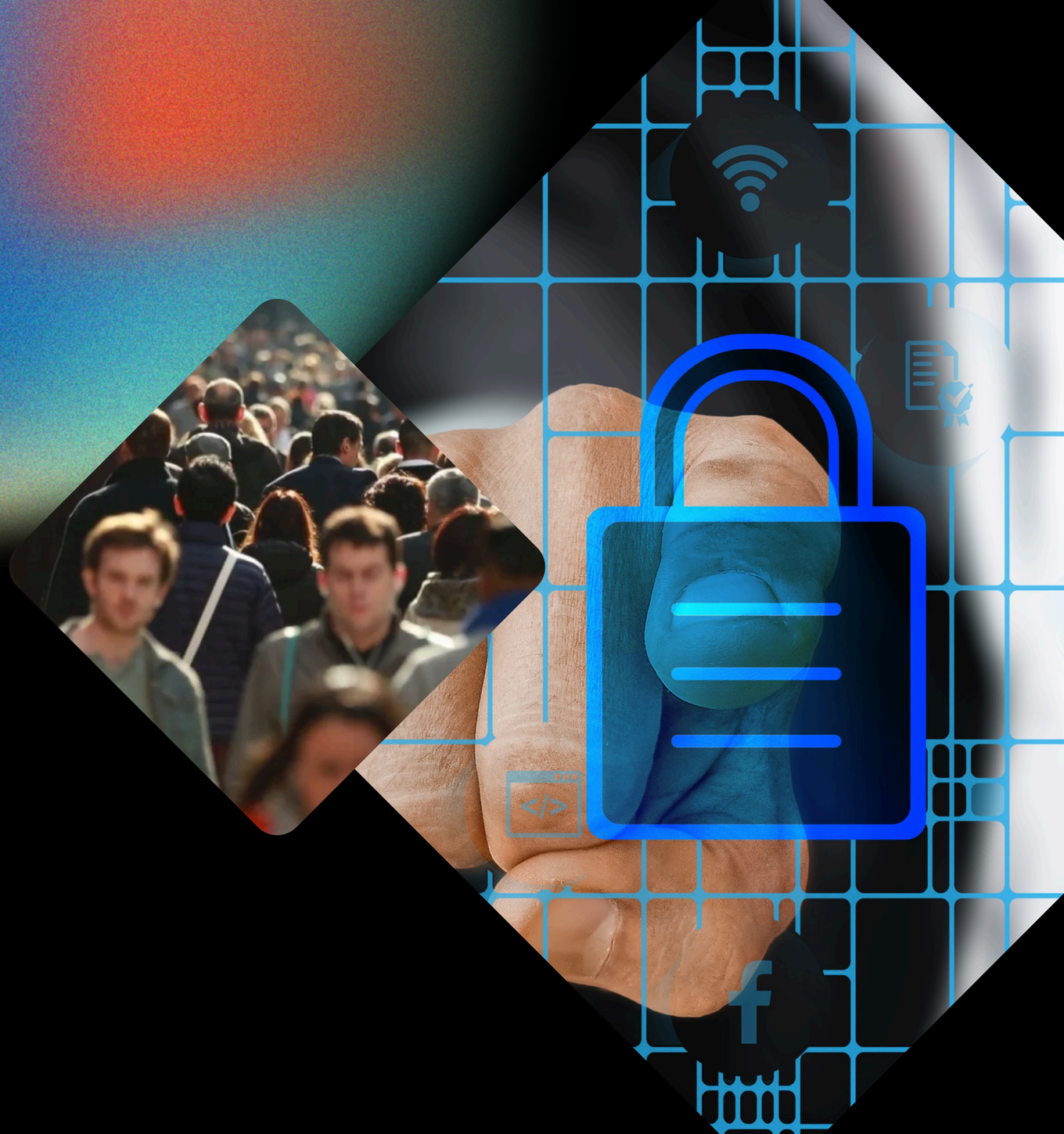
Сложность модернизации

обновление таких систем может происходить медленнее, чем в частном секторе

Правовые и этические вопросы

централизация данных вызывает опасения в отношении конфиденциальности и возможного неправомерного использования информации

Внедрение ГИС также повышает удобство для граждан. Возможность быстро получать государственные услуги в цифровом формате делает взаимодействие с государством проще и прозрачнее. Например, реестры недвижимости или кадастры становятся более защищенными от манипуляций, что снижает уровень коррупции.



ЗАКЛЮЧЕНИЕ

Массовый переход на государственные информационные системы укрепляет национальную кибербезопасность, но требует комплексного подхода. ГИС централизуют управление, унифицируют защиту и снижают зависимость от зарубежных технологий. Однако концентрация данных увеличивает риски атак и требует усиленной защиты.

СПАСИБО ЗА ВНИМАНИЕ