Борьба с киберпреступностью

Наша цель — защищать мир от киберпреступлений. Эффективное противостояние киберпреступности требует объединения усилий всего общества, поэтому мы сотрудничаем с правоохранительными органами и вносим вклад в совершенствование законодательства в этой сфере.

Ключевые документы

- Внутренняя политика «Лаборатории Касперского», определяющая работу с запросами правоохранительных органов[1] (утверждена в сентябре 2021 года топ-менеджерами Компании).
- Соглашение с Интерполом о совместной борьбе с киберпреступлениями.
- Меморандумы о сотрудничестве с различными агентствами по кибербезопасности и правоохранительными органами.

Как мы сотрудничаем с правоохранительными организациями

Большинство кибератак совершаются злоумышленниками или хакерами с целью получения финансовой прибыли. Однако их мотивы могут быть также личными или политическими. Киберпреступления совершают частные лица и организации, которые используют продвинутые методики и хорошо подкованы технически.

Киберпреступления приводят к серьезным последствиям как для компаний, так и для частных лиц. В основном это финансовый ущерб, а также утрата доверия и репутационные потери. Киберпреступность не знает границ, и ни одна страна или организация не может справиться с ней в одиночку. Эта задача требует всестороннего подхода и объединения усилий.

Правоохранительные органы нередко обращаются за консультациями к IT-компаниям, которые обладают высоким уровнем экспертизы в области кибербезопасности. «Лаборатория Касперского» активно помогает в исследовании киберпреступлений. При этом мы очень серьезно подходим к вопросу прозрачности в совместной работе — у нас есть четкий порядок работы с запросами от правоохранительных органов, который регулируется внутренней политикой, и критерии для юридической проверки каждого запроса. Если запрос не соответствует нашим критериям, мы можем отклонить его или оспорить. Важно отметить, что мы не предоставляем доступ к нашей инфраструктуре или данным.

[1] Processing Law Enforcement and Government Requests for Disclosure of Data.

Задача

Содействие в исследовании киберпреступлений

Киберпреступность не имеет границ, поэтому «Лаборатория Касперского» регулярно участвует в операциях и исследованиях, проводимых совместно с глобальным сообществом специалистов по IT-безопасности, международными организациями, такими как Интерпол, правоохранительными органами и центрами реагирования на компьютерные инциденты. Для исследования киберпреступлений мы предоставляем нашу экспертизу и необходимую техническую информацию, регулярно проводим тренинги.

Решения

Защищаем киберпространство вместе с Интерполом

В 2014 году мы начали сотрудничество с Интерполом, подписав первое соглашение о совместной борьбе с киберпреступлениями. В 2019 году мы заключили новое соглашение на пять лет, которое предусматривает значительное расширение сферы нашего взаимодействия.

Наша поддержка Интерпола

- Делимся экспертной информацией о новейших видах вредоносных программ и методах кибератак.
- Участвуем в совместных операциях по всему миру для выявления и пресечения киберпреступлений.
- Проводим обучающие программы в области кибербезопасности и консультируем сотрудников Интерпола и других правоохранительных органов.

Как мы помогали Интерполу в 2022–2023 годах:

- наши специалисты содействовали Интерполу в проведении операций Africa Cyber Surge и Africa Cyber Surge II, нацеленных на борьбу с киберпреступностью на Африканском континенте;
- под эгидой Интерпола мы организовали обучение более 100 представителей правоохранительных органов из разных стран по направлениям «Реакция на инциденты» и «Анализ вредоносных программ»;
- Виталий Камлюк, руководитель Глобального центра исследований и анализа угроз в Азиатско-Тихоокеанском регионе «Лаборатории Касперского», выступил с докладом на международной конференции по кибербезопасности INTERPOL Global Cybercrime Conference (IGCC) 2023. Он представил обзор крупнейших в мире эпидемий компьютерных червей и описал меры, которые были приняты для борьбы с ними.

Поддерживаем международную кооперацию

«Лаборатория Касперского» тесно сотрудничает с многочисленными международными организациями и правоохранительными органами, участвуя в совместных операциях, исследованиях киберугроз, кибердипломатии, содействуя развитию открытого и безопасного интернета.

33
международных и российских партнера по защите киберпространства

>10
меморандумов о взаимопонимании заключено с международными организациями и правительственными учреждениями

>60
организаций участвуют в обмене новыми вредоносными самплами[1]

Например, в рамках альянса No More Ransom, который был создан совместно с Европолом и другими партнерами, мы помогаем жертвам вредоносных программ-вымогателей в 30 странах восстановить свои зашифрованные данные, не выплачивая выкуп. За семь лет работы этот альянс помог примерно 2 млн пользователей по всему миру восстановить свои данные.

Наши партнеры в борьбе с киберпреступностью и содействии устойчивому развитию цифрового пространства

- Интерпол
- Альянс No More Ransom
- Коалиция против сталкерского ПО (Coalition Against Stalkerware)
- Женевский диалог (Geneva Dialogue)
- Парижский призыв к доверию и безопасности в киберпространстве (Paris Call for Trust and Security in Cyberspace)
- Совет Европы
- Cybermalveillance.gouv.fr (GIP ACYMA) (Франция)
- Renaissance Numérique (Франция)
- World Internet Conference (член Экспертно-консультативного комитета высокого уровня)
- China Industrial Control System CERT (отраслевой партнер)
- Промышленный консорциум интернета вещей (Industry IoT Consortium, США)
- Международный союз электросвязи
- Международная организация по стандартизации (ISO)
- Альянс по защите детей в цифровой среде (Россия)
- АНО «Цифровая экономика» (Россия) и многие другие

Мы также охотно делимся нашей экспертизой в сфере кибербезопасности, выступая на крупных конференциях и мероприятиях, таких как RSA Conference и Virus Bulletin, публикуем информацию в собственных блогах и проводим бесплатные вебинары по кибербезопасности. Кроме того, в 2023 году мы расширили функционал бесплатных сервисов на портале Kaspersky Threat Intelligence, который позволяет найти информацию о киберугрозах в режиме реального времени.

В 2022–2023 годах в рамках борьбы с киберпреступностью «Лаборатория Касперского» расширяла сотрудничество с международными и национальными организациями, в частности подписала ряд важных соглашений, включая соглашения о сотрудничестве с национальными центрами по кибербезопасности, а также меморандумы о сотрудничестве с Университетом Корё, Советом по кибербезопасности ОАЭ и Министерством образования Италии.

В рамках Всемирной конференции в области интернета в Китае Компания получила награду World Leading Technology за разработку решения Kaspersky Automotive Secure Gateway, а глава Компании Евгений Касперский был удостоен звания Special Contributor за заслуги в продвижении глобального сотрудничества в области кибербезопасности.

В 2023 году «Лаборатория Касперского» получила награду Alliance of Public Private Cybercrime Stakeholders (основан под эгидой Сил полиции Сингапура) за вклад в формирование киберустойчивого мира.

Помимо этого, Компания занималась формированием отзывов и предложений к проекту всеобъемлющей международной конвенции о противодействии использованию информационных технологий в преступных целях, которая разрабатывается под эгидой ООН. Мы также направили свои предложения в рамках инициативы ООН «Глобальный цифровой общественный договор» с акцентом на вопросы повышения цифровой грамотности.

В 2022–2023 годах наши эксперты принимали участие в многочисленных форумах и конференциях по кибербезопасности, среди которых были:

- Рабочая группа открытого состава ООН по ИКТ (в ходе неформального диалога под эгидой председателя Рабочей группы);
- Пятые межсессионные консультации Спецкомитета ООН по разработке всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях;
- Африканский форум по управлению интернетом;
- Сессия по цифровой безопасности в рамках инициативы ООН «Глобальный цифровой общественный договор»;
- Рабочие группы «Женевского диалога»;
- Международная конференция Интерпола по кибербезопасности;
- Форум ООН по управлению интернетом;
- Формат B20 (Business 20) в рамках G20.

Кроме того, мы сотрудничаем с другими IT-компаниями по всему миру путем обмена образцами вредоносного ПО (более 60 компаний).

[1] Образец вредоносного ПО.

Задача

Улучшение законодательной базы

Современные технологические вызовы требуют более гибкого и адаптивного законодательства. Злоумышленники постоянно совершенствуют свои методы, поэтому законы должны позволять эффективно реагировать на новые угрозы. Кроме того, совершенствование законодательства помогает стандартизировать правовые механизмы на мировом уровне, обеспечивая более эффективный обмен информацией и экстрадицию преступников.

Решения

Совершенствуем законодательство в сфере борьбы с киберпреступностью

«Лаборатория Касперского» постоянно участвует в разработке законодательства, политик и других документов, направленных на обеспечение кибербезопасности в мире. Наши эксперты делятся своими знаниями и опытом в области защиты критической инфраструктуры, борьбы с киберпреступностью, а также защиты данных и других смежных тем. Поскольку регулирование в сфере кибербезопасности ужесточается во многих странах, мы все чаще получаем запросы от национальных, региональных и международных организаций на предоставление экспертной помощи. Некоторые из таких экспертных материалов доступны в нашем блоге о политике кибербезопасности.

Мы регулярно обмениваемся информацией с заинтересованными сторонами по вопросам кибербезопасности и киберпреступности на уровне ООН. В частности, начиная с 2020 года мы активно участвуем в неформальном диалоге ООН под эгидой председателя Рабочей группы открытого состава по кибернормам[1] (РГОС), где обсуждаются различные вопросы в сфере кибербезопасности, меры по повышению доверия в киберпространстве и развитие компетенций. В отчетном периоде Компания участвовала в двух встречах, на которых презентовала свои предложения в области использования ИИ с акцентом на кибербезопасность, а также комментарии к ежегодному отчету РГОС.

Наш вклад в борьбу с международной киберпреступностью

Участвуем в операции Africa Cyber Surge

Индустрия информационной безопасности в Африке не так хорошо развита, как в других регионах, поэтому ее страны более уязвимы для кибератак. Чтобы помочь Интерполу бороться с киберпреступностью в Африке, «Лаборатория Касперского» предоставила ему данные об угрозах в ходе операции Africa Cyber Surge.

Первая часть операции проходила с июля по ноябрь 2022 года и включала серию оперативно-разыскных мероприятий против злоумышленников. Вторая часть — Africa Cyber Surge II — началась в апреле 2023 года и продлилась четыре месяца, охватив 25 африканских стран.
Вместе с другими партнерами Интерпола «Лаборатория Касперского» передала международному агентству индикаторы компрометации (IoC), включая информацию о вредоносных серверах, фишинговые ссылки и домены, а также мошеннические IP-адреса.

Что в результате?

Благодаря помощи «Лаборатории Касперского» следователям удалось обнаружить скомпрометированную инфраструктуру и задержать злоумышленников, подозреваемых в совершении киберпреступлений в Африке. В результате операции были арестованы 14 человек, а также выявлена сетевая инфраструктура, с которой связаны финансовые потери более чем на $40 млн.

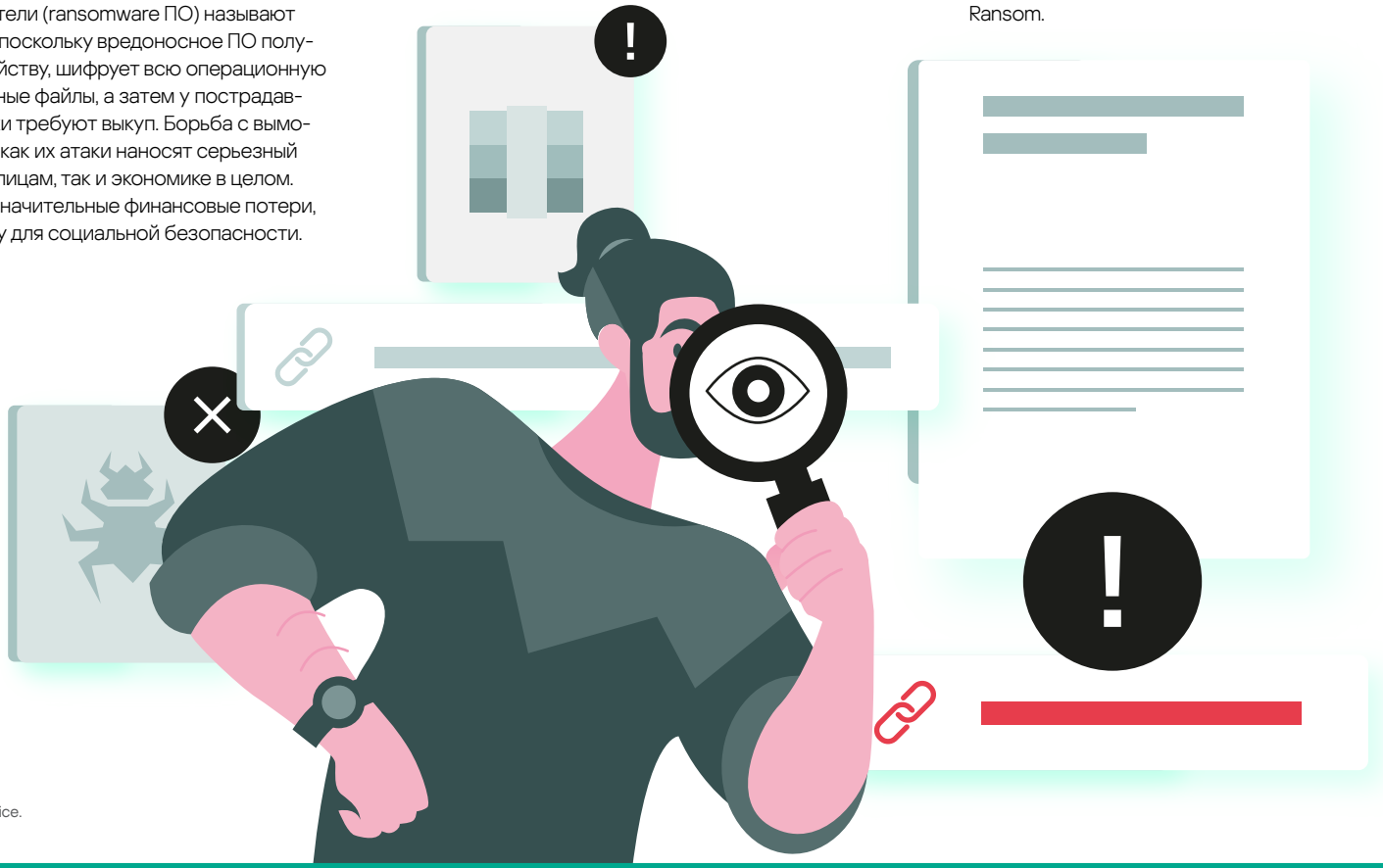
«Операция Africa Cyber Surge II помогла усилить борьбу с киберпреступностью в странах-участницах, а также укрепить партнерские отношения между ключевыми заинтересованными сторонами, такими как отделы по реагированию на компьютерные инциденты и интернет-провайдеры. В дальнейшем это будет способствовать снижению глобального влияния киберпреступности, а также защите сообществ в Африканском регионе».

Юрген Шток,
Генеральный секретарь Интерпола

Задача

Защита пользователей от программ-вымогателей

Программы-вымогатели (ransomware ПО) называют шифровальщиками, поскольку вредоносное ПО получает доступ к устройству, шифрует всю операционную систему или отдельные файлы, а затем у пострадавших злоумышленники требуют выкуп. Борьба с вымогателями важна, так как их атаки наносят серьезный ущерб как частным лицам, так и экономике в целом. Они могут вызвать значительные финансовые потери, а также несут угрозу для социальной безопасности.



[1] Ransomware-as-a-Service.

Решения

Раскрываем схемы атак, анализируем инструменты злоумышленников и обновляем собственные утилиты для дешифровки в рамках инициативы No More Ransom.

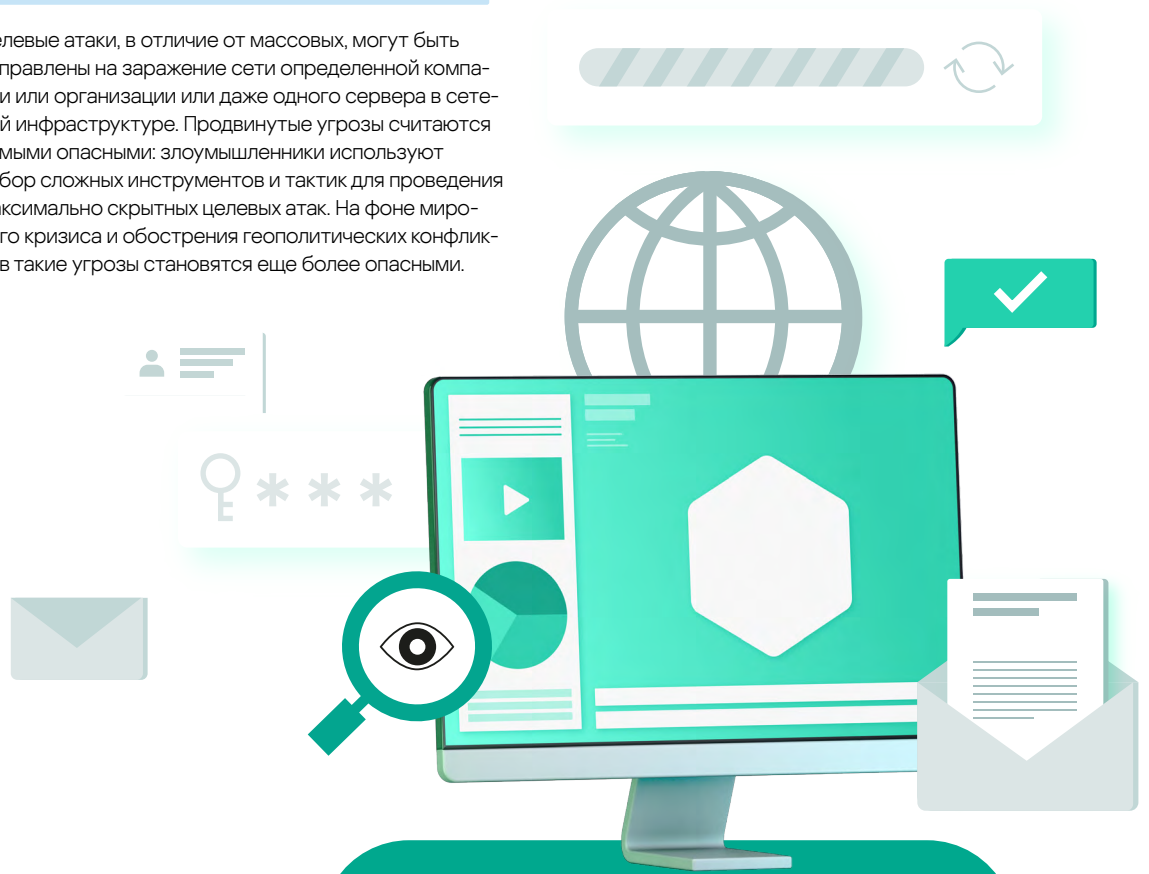
В отчетном периоде «Лаборатория Касперского»:

- обнаружила и помогла обезвредить атаки шифровальщиков с применением эксплойта нулевого дня (написанного для использования уязвимости, о которой еще не знает разработчик). В числе мишеней были предприятия малого и среднего бизнеса на Ближнем Востоке, в Северной Америке, а ранее и в азиатских регионах;
- обновила инструмент расшифровки для жертв программы-шифровальщика Conti. «Лаборатория Касперского» обновила общедоступный инструмент расшифровки на портале Noransom для версии, которая использовалась для атак на коммерческие компании и государственные учреждения;
- проанализировала билдер Lockbit 3. Lockbit — один из самых распространенных типов шифровальщиков. Он распространяется среди партнеров по модели RaaS[1], предлагая участникам до 80% от суммы выкупа. В сентябре 2022 года произошла утечка билдера Lockbit 3, позволяющего любому пользователю сконструировать свою собственную версию программы-шифровальщика. Глобальная команда реагирования на киберинциденты «Лаборатории Касперского» проанализировала билдер, чтобы разобраться в методологии конструирования шифровальщика и определить возможности для дополнительного анализа. Этот инструмент позволял любому создать свою собственную версию программы-вымогателя.

Задача

Исследование целевых (таргетированных) атак и продвинутых угроз

Целевые атаки, в отличие от массовых, могут быть направлены на заражение сети определенной компании или организации или даже одного сервера в сетевой инфраструктуре. Продвинутые угрозы считаются самыми опасными: злоумышленники используют набор сложных инструментов и тактик для проведения максимально скрытных целевых атак. На фоне мирового кризиса и обострения геополитических конфликтов такие угрозы становятся еще более опасными.



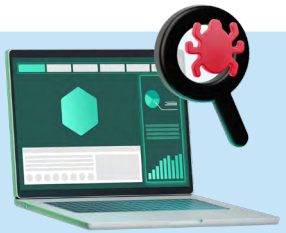
Решения

Эксперты глобального центра исследований и анализа угроз (GReAT) «Лаборатории Касперского» и команда Kaspersky Cyber Threat Intelligence пристально следят за множеством APT-групп, анализируют текущие тренды и прогнозируют развитие ландшафта киберугроз, чтобы оставаться на шаг впереди злоумышленников и обеспечивать безопасность клиентов «Лаборатории Касперского».

Примеры кибергруппировок, за которыми велось наблюдение, и их атак.

- **Разбор угроз группы Cuba Ransomware**. В 2023 году «Лаборатория Касперского» опубликовала результаты исследования нового киберинцидента с участием Cuba. Это группа вымогателей, которая атаковала многие компании по всему миру, в том числе торговые, логистические, финансовые, государственные учреждения и промышленные предприятия в Северной Америке, Европе, Океании и Азии. Наши эксперты разобрали историю, а также техники, тактики и процедуры известной кибергруппы.
- **Ошибки группы Andariel и новое семейство зловредов**. Эксперты «Лаборатории Касперского» обнаружили новый инструмент в арсенале кибергруппы Andariel, которая входит в состав Lazarus. Это троянец удаленного доступа, который получил название EarlyRat. Зловред может попадать на устройство через уязвимость, найденную с помощью эксплойта Log4j, либо через ссылки в фишинговых документах.
- **Новая группа GoldenJackal**. Данная группа ведет свою деятельность с 2019 года и обычно атакует правительственные и дипломатические организации на Ближнем Востоке и в Южной Азии. Эксперты «Лаборатории Касперского» начали следить за этой группой в середине 2020 года. Ее главная особенность — специфический набор зловредных имплантов, которые распространяются через съемные диски и используются для контроля целевых компьютеров, извлечения данных, кражи учетных записей, сбора информации о локальной системе и действиях жертвы в интернете, а также для создания и отправки снимков экрана.
- **Кибергруппа ToddyCat усложняет свои кампании кибершпионажа**. Эксперты «Лаборатории Касперского» рассказали о новом наборе вредоносных инструментов, о программах, используемых для кражи и эксфильтрации данных, а также о методах, применяемых этой активной группой для перемещения в инфраструктуре и проведения шпионских операций.

Итоги работы по направлению борьбы с киберпреступностью



С ноября 2022 года по октябрь 2023 года[1] наш веб-антивирус заблокировал

112 922 612

уникальных вредоносных объектов.

В целом за этот период решения «Лаборатории Касперского»:

- отразили 437 414 681 вредоносную атаку, которые проводились с интернет-ресурсов, размещенных в различных странах мира;
- обнаружили 106 357 530 уникальных вредоносных URL, на которых происходило срабатывание веб-антивируса;
- отразили атаки шифровальщиков на компьютерах 193 662 уникальных пользователей;
- предотвратили атаки майнеров на 1 140 573 уникальных пользователя;
- заблокировали попытки запуска вредоносного ПО для кражи денежных средств через онлайн-доступ к банковским счетам на устройствах 325 225 уникальных пользователей.

В этих результатах — вклад четырех наших подразделений: Лаборатории исследования киберугроз (AMR), Центра исследований безопасности промышленных систем и реагирования на инциденты информационной безопасности (ICS CERT), команды расследования компьютерных инцидентов и команды Глобального центра исследования и анализа угроз (GReAT).

Наши планы на 2024 год

- Участие в формировании правового поля по борьбе с киберпреступностью.
- Обучение и повышение квалификации экспертов, проведение тренингов по актуальным темам в области кибербезопасности.
- Сотрудничество с внешними организациями и установление партнерских отношений с государственными учреждениями для обмена информацией о киберугрозах.
- Регулярное обновление ПО и технологий для надежной защиты от последних угроз.

[1] См. отчет «Лаборатории Касперского»: https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2023/11/28132907/KSB_statistics_2023_ru.pdf.