виртуальный Региональный диалог для Региона СНГ

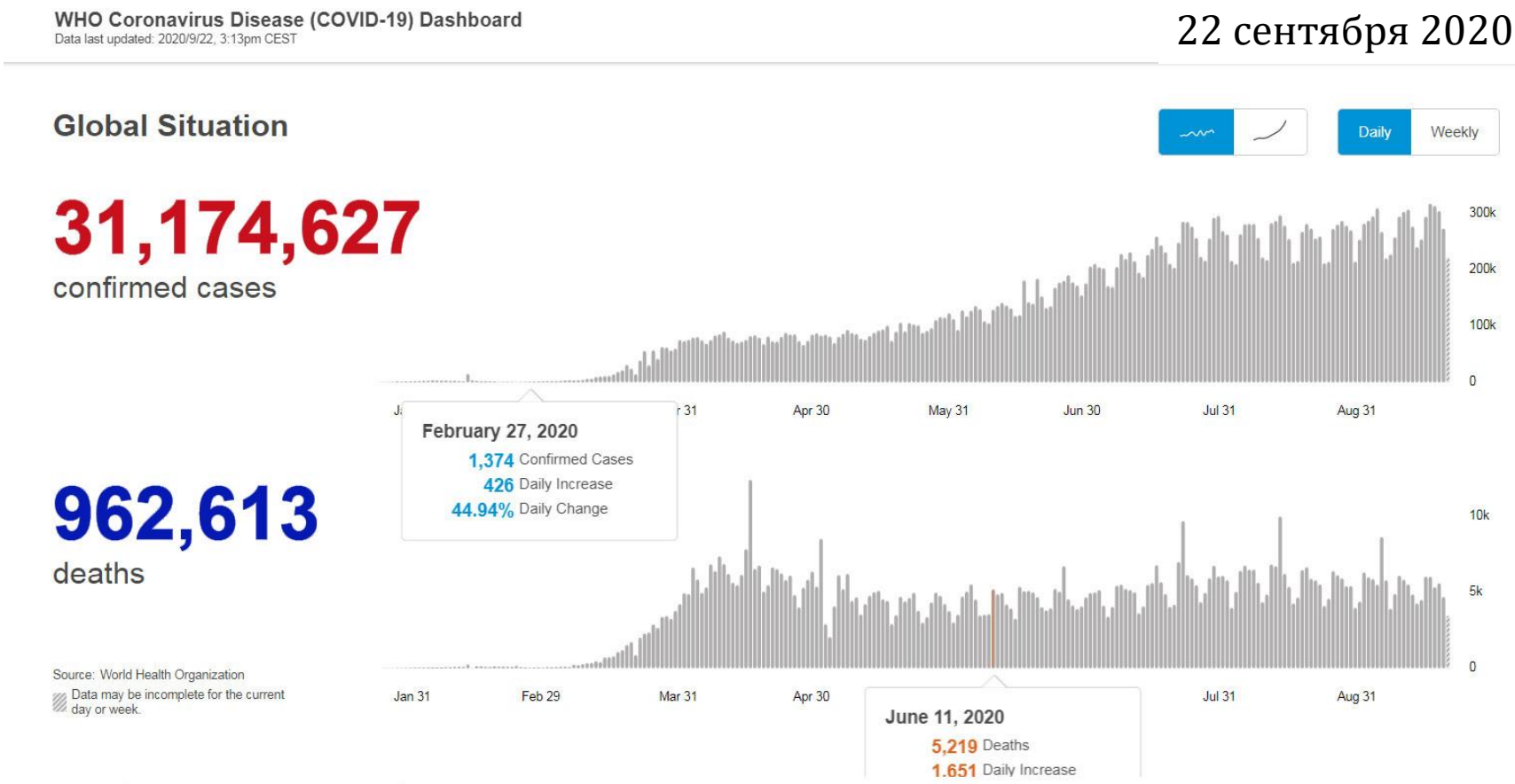
«CIRT и уроки, извлеченные из кризиса COVID-19»

Докладчик:

Эльмир Велизаде, заместитель министера

Министерство транспорта, связи и высоких технологий, Азербайджанская Республика

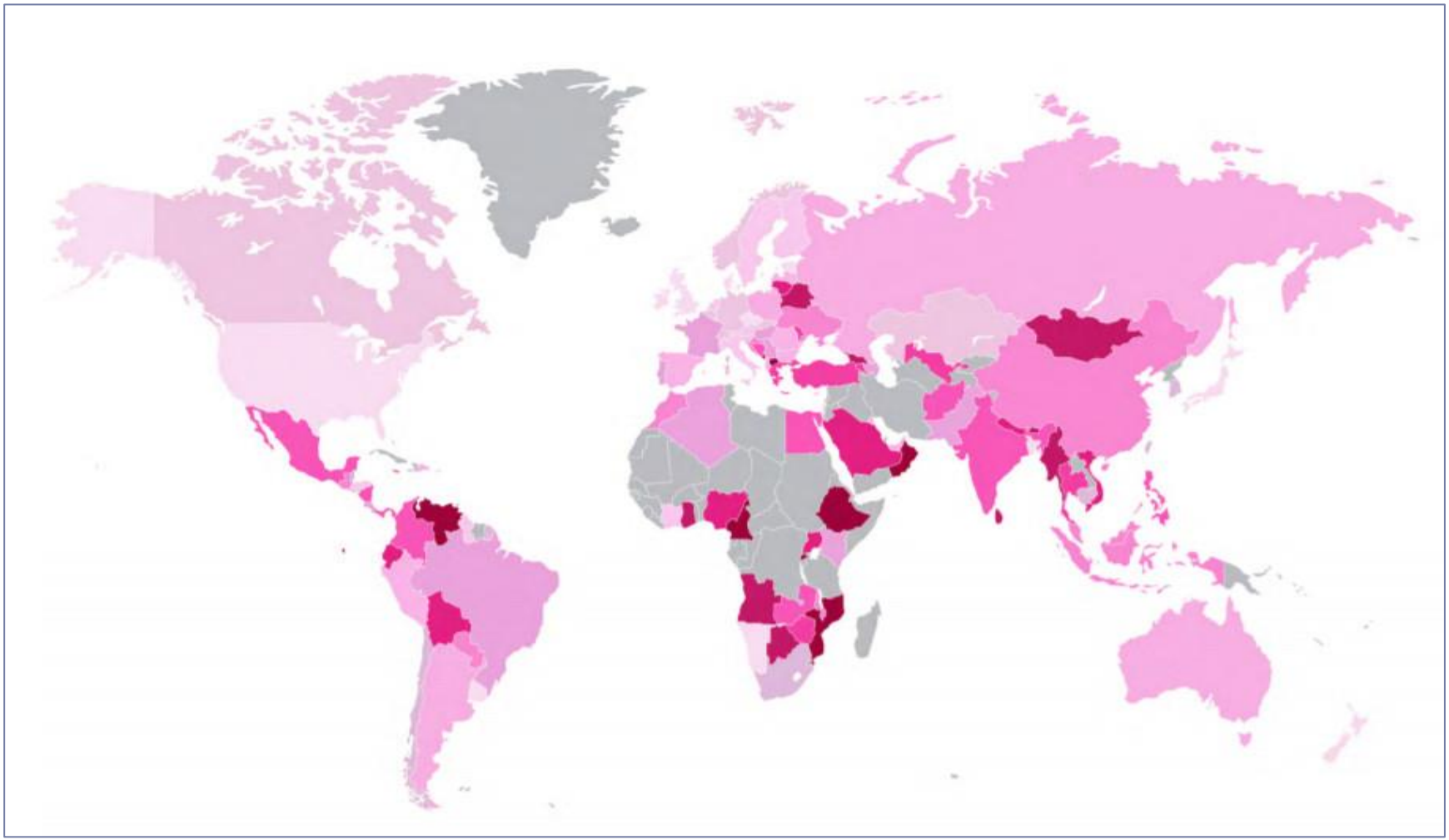
Глобальная пандемическая ситуация



COVID-19 – новая реальность жизни

- **Введение в странах ограничений на деятельность;**
- **Переход на удаленную работу;**
- **Перевод инфраструктуры на «облако»;**
- **Рост нагрузок на инфраструктуру**
- **Рост киберугроз;**
  - Распространение фишинга / вредоносного ПО с использованием тем коронавируса
  - Поддельные приложения
  - Тематические домены
  - Программы-вымогатели
  - Похитители информации
- **Атаки на отрасли;**
  - Органы государственного управления
  - Банки и финансовые структуры
  - Здравоохранение
  - Образование
  - Исследовательские институты и университеты,
  - Промышленные производственные предприятия
  - …

Карта мировых киберугроз



Источник: *Check Point Security Report 2020*

Ограничения и их последствия

- **Переход на удаленную работу;**
  - Работа из дома с использованием личных устройств
  - Использование средств видеоконференций
  - Доверие к незнакомым технологиям безопасного удаленного доступа (включая VPN)
- **Перевод инфраструктуры на «облако»;**
  - Необходимость срочного перехода
  - Возможные угрозы к корпоративным сетям
- **Рост нагрузок на инфраструктуру**
  - Увеличение интернет-трафика
  - Рост количества одновременных пользователей
  - Рост мошеннических и зловредных действий

Удаленная работа как новая норма

- В Check Point всего **за две недели 99%** сотрудников организации впервые в переехали на **работу из дома.**
- Согласно опросу **78% сотрудников** сообщили, что их **продуктивность была такой же или даже выше.**
- Согласно недавнему опросу финансовых директоров Gartner**, 74% компаний** заявили, что намерены **постоянно переводить сотрудников на работу из дома.**
- **Facebook** стала первой компанией, которая объявила, что **навсегда переведет 50%** своих сотрудников **на удаленную работу.**

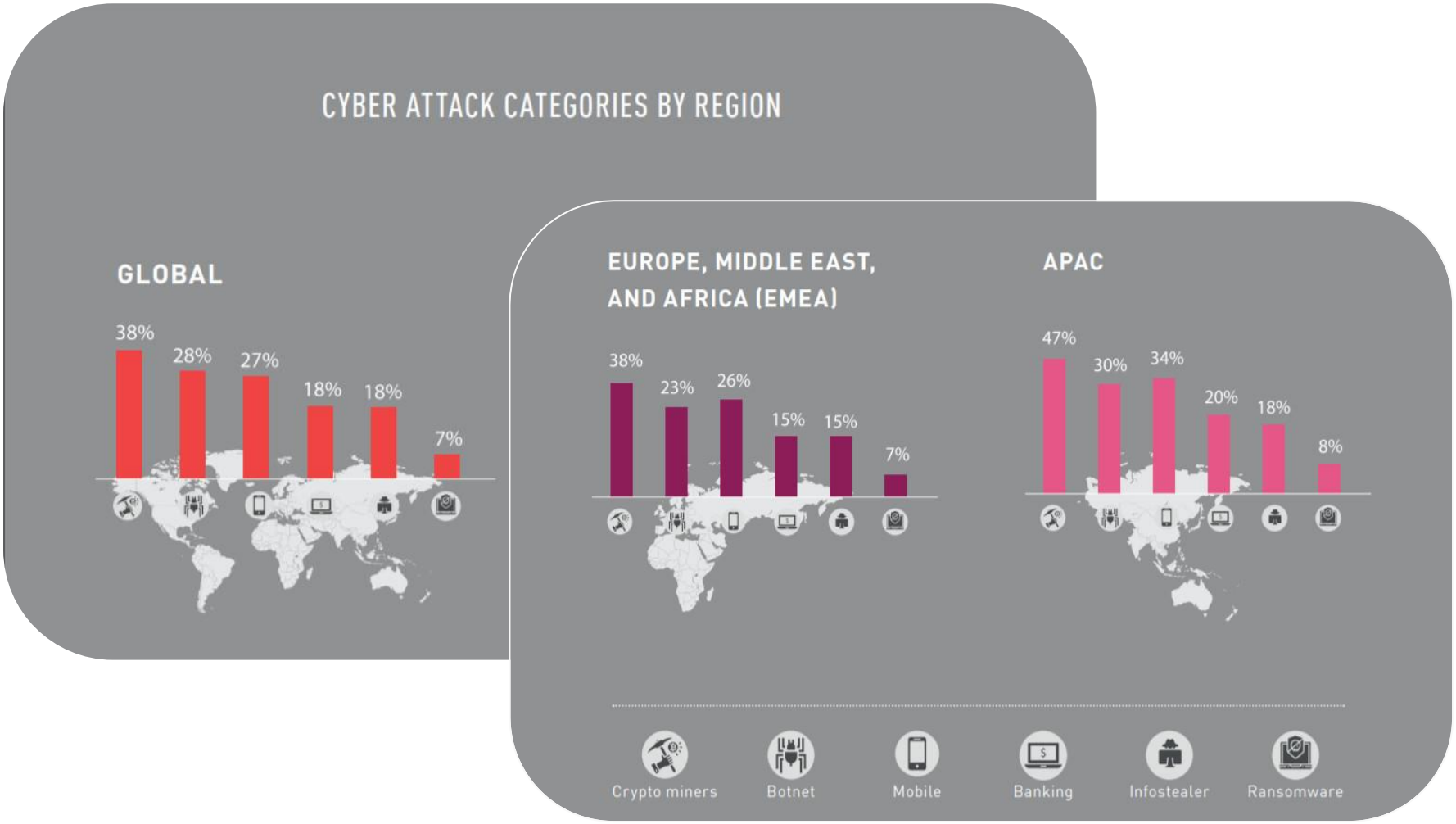
Удаленная работа

Сферы	До пандемии	В период пандемии
США	**7%** (National Compensation survey)	**64%** (Eurofound)
Европа	**до 10%** (National Compensation survey)	**40%** (Eurofound)
Желание работать удаленно	**54%** (Gallup)	**99%** (ResumeLab)
Работа на дому		**88%** (Gartner)
Желание компаний продолжит удаленную работу		**77%** (Gartner)
Запросы «как удалить вирус» увеличились		**42%** (Google Trend)
Рост потребности услугам технологических компаний (по кибербезопасности)		**83 % (36%)** (CompTIA)

Основные виды киберугроз

- Интернет-мошенничество и фишинг
- Подрывное вредоносное ПО (программы-вымогатели и DDoS-атаки)
- Вредоносное ПО для сбора данных
- Вредоносные домены
- Дезинформация и кража информации

Кибератаки



Источник: *Check Point Security Report 2020*

Кибератаки на медицинские учреждения

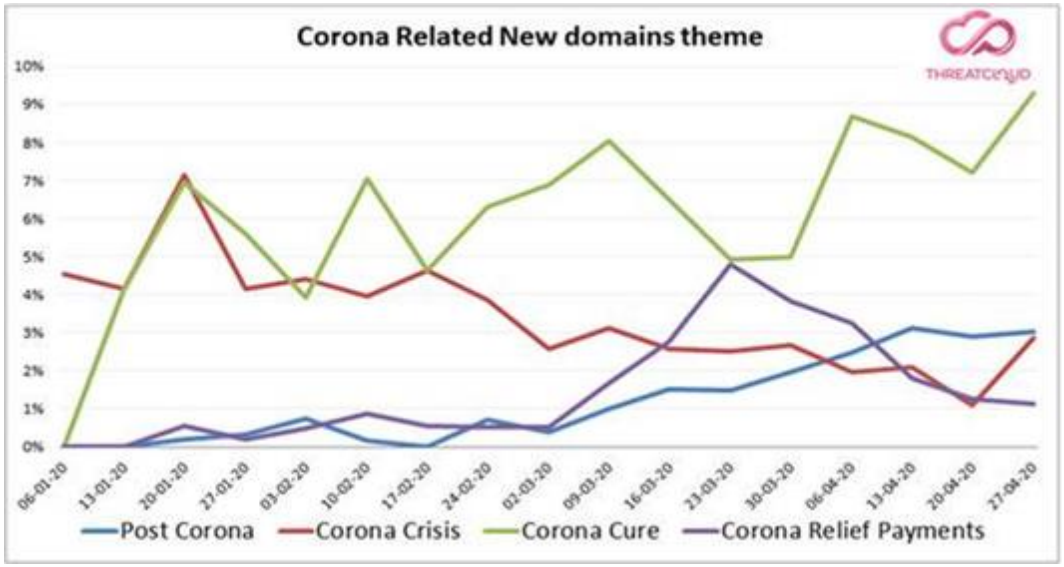
10 сентября 2020 года Университетская клиника в Дюссельдорфе (Германия) подверглась кибератаке.
В результате кибератаки был зафиксирован первый случай смерти человека, проходившего лечение в этой больнице

12 и 13 марта 2020 года Университетская больница Брно в Чешской Республике подверглась кибератаке. Во время инцидента больница была вынуждена отключить всю свою ИТ-сеть.
Больница, в которой находится одна из крупнейших в Чешской Республике центров тестирования на COVID-19, была вынуждена отменить операции и перевести новых пациентов в другие больницы

Вызовы и возможные их решения

Изме-нение	Послед-ствия	Риски	Процессы/ Технологии
Работа из дома	Мобильные и персональные устройства сот-рудников имеют доступ в служебные сети	Утечка информации (через запись клавиш, экрана ПК/ мобильника)	1. Обеспечение соответствия рабочих мест требованиям безопасности (последние исправления, антивирусы) 2. Проведение обучения пользователей (например, симуляция фишинга). 3. Защита мобильных устройств от мобильных угроз
Переход в «облако»	Быстрота развертывания в ущерб безопасности	Обычные меры безопасности могут привести к потере и манипуляциям данных	1. Инвестиции в управление облачной безопасности 2. Установка средств безопасности для контейнеров и бессерверных приложений. 3. Предотвращение угроз в реальном времени с помощью безопасности IaaS
Критичес-кая инфра-структура	Разрешение удаленного доступа к критической инфраструктуре	Нарушение критической инфраструктуры	1. Безопасность устройств «Интернета вещей» 2. Укрепление сетевой безопасности Красной командой 3. Безопасность с применением Scada
Рост сетевой нагрузки	Большая пропускная способность для обрабатываемых данных	Сбой обслуживания Остановка работы сети	1. Инвестиции в сетевую безопасность, масштабируемой по потребности 2. Должны использованы все средства защиты для сохранения непрерывности бизнеса. 3. Масштабируемый безопасность удаленного доступа

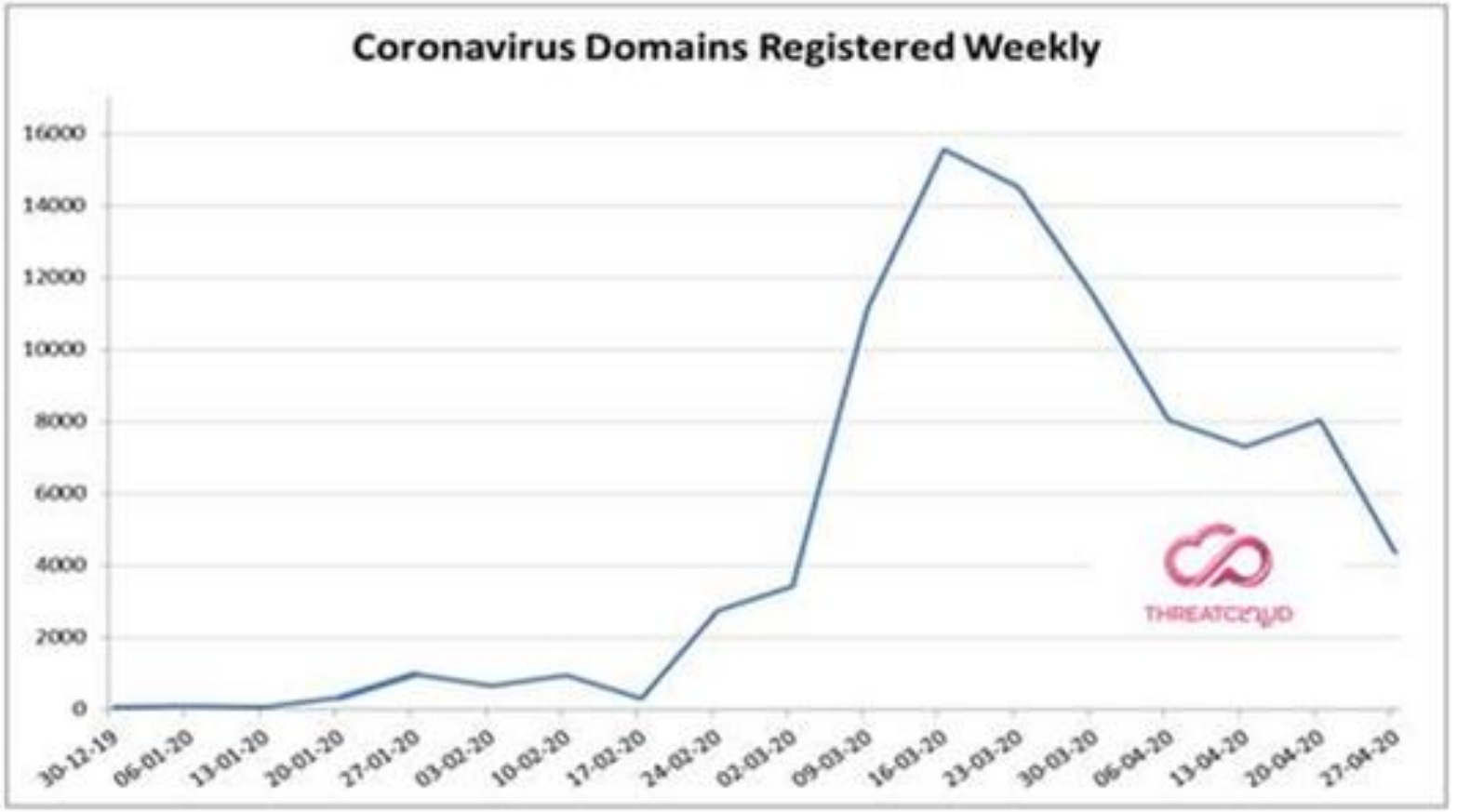
Злоупотребление доменами



Исследователи Check Point вывили зависимость между возникновением фейковых доменов и этапами вспышек эпидемии.

1. **В начале пандемии** часто встречались домены, содержащие **живые карты,** которые позволяли отслеживать распространение вируса по разным регионам. Также популярны были сайты, описывающие симптомы коронавируса.
2. **К концу марта** внимание было сосредоточено на **различных видах помощи и выплатах,** которые осуществлялись в нескольких странах.
3. **Затем** широкое распространение получили домены, связанные с **жизнью после коронавируса,** а также домены, информирующие о **второй волне эпидемии.**
4. **На протяжении всего периода** пандемии домены, связанные с **тестами и вакцинами**, остаются неугасающим трендом для злоумышленников. Их общее число продолжает расти.

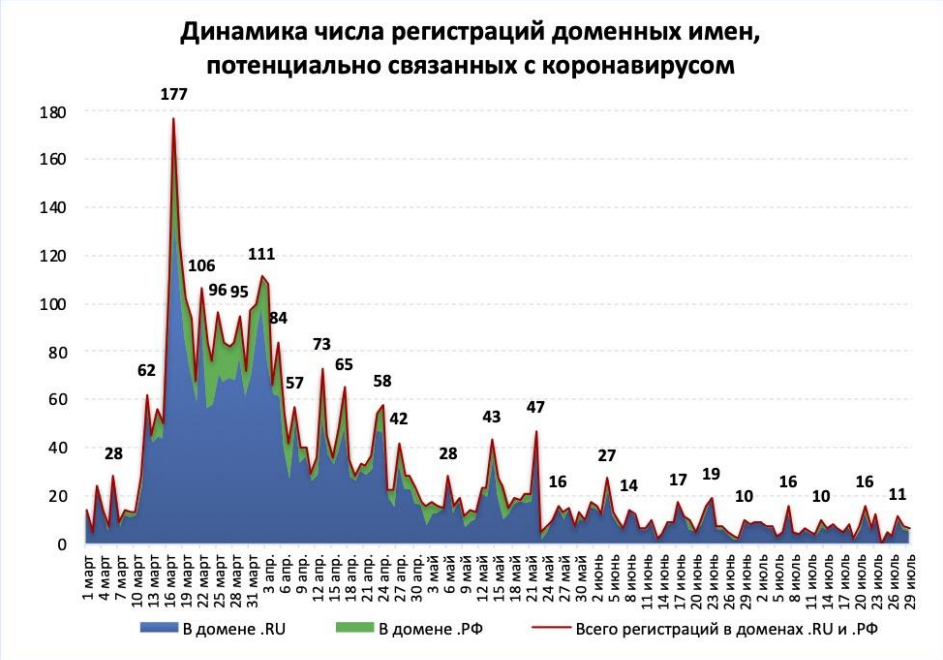
Еженедельная динамика доменов



Согласно исследователям Check Point с начала вспышки эпидемии во всем мире было зарегистрировано в общей сложности **90284 новых домена**, связанных с COVID-19. **50% из них считаются с вредоносным** содержанием.

Домены в пространстве СНГ

- По данным **Координационного центра доменов .RU/.РФ** за 7 месяцев мониторинга реестров национальных доменов (с января по июль 2020 года) в зоне .RU было зарегистрировано **3966**, а в .РФ 835 доменных имён, в которых встречаются слова «corona», «covid», «pandemia», «ковид», «пандемия», «вирус», «vaccine» и др. При этом пик «коронавирусных» регистраций пришёлся на 17 и 18 марта. Всего таких имён **в Рунете на сегодня насчитывается** 4801, и динамика их регистраций постепенно сходит на нет.
- По оценкам экспертов HostFly.by из-за пандемии цена на некоторые доменные имена **в Байнете достигла рекордных показателей в 15–35 тысяч долларов.**



Противодействие манипулированию с доменами

- **В США и Европе власти** вводят дополнительные меры, чтобы остановить массовую покупку связанных с пандемией доменных имен.
- Один из крупнейших **регистраторов доменов Namecheap запретил регистрацию доменных имён** с ключевыми словами coronavirus, covid и vaccine.
- Администратор доменной зоны Великобритании **.UK Nominet добавил все домены** с ключевыми словами coronavirus и covid **в список для рассмотрения Domain Watch** - полуавтоматической системы, которая выявляет фишинговые и другие мошеннические домены на ранней стадии.
- **Торговая площадка Dan.com сняла с продажи все "коронавирусные" домены**. По мнению её руководства, продажа таких доменов по астрономическим ценам, которые выставляют их владельцы, является неэтичной и неприемлемой.

Вредоносные типы файлов

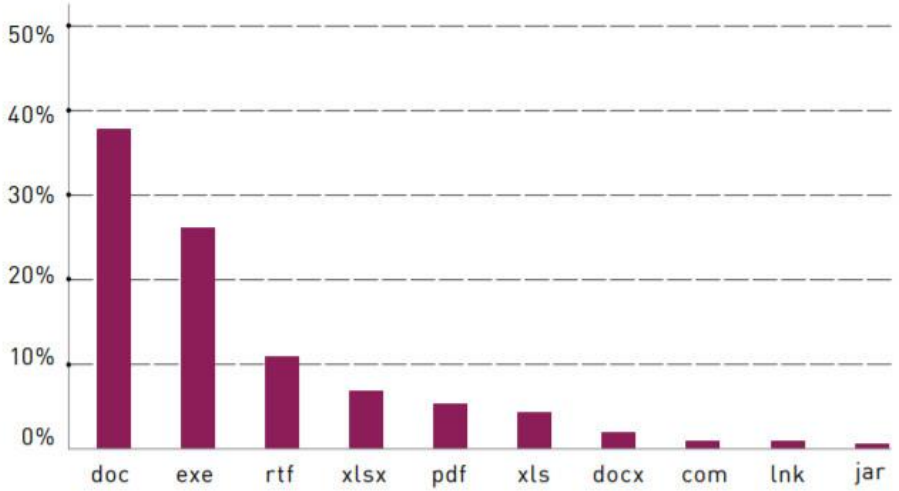


Figure 2: Email – Top malicious file types

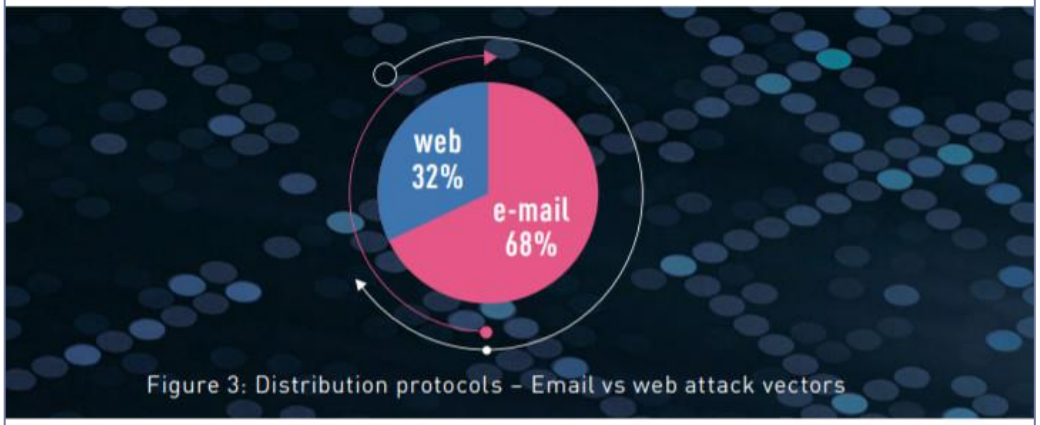


Figure 3: Distribution protocols – Email vs web attack vectors

CHECK POINT SOFTWARE
SECURITY REPORT 2020

Последствия пандемии в образовании

- Более 1,5 миллиарда детей во всем мире не посещают школы;
- Образование и социализация детей переместились в онлайн;
- Глобальная изоляция привела к выходу детей в Интернет раньше, чем можно было ожидать;
- Детям в возрасте 9 и 11 лет были предоставлены мобильные телефоны раньше, чем планировалось;
- Для родителей вопрос о том, как обеспечить безопасность своих детей в Интернете.

Задачи CERT

- **Мониторинг и анализ ситуации;**
- **Оперативность реагирования** на угрозы и инциденты;
- Проведение **информирования и просвещения**;
- Подготовка **инструкций** для противодействия, **консультации и практическая помощь**;
- **Координация взаимодействия** по инцидентам;
- **Международная координация и обмен информацией;**
- **Взаимодействие с администрациями социальных сетей** по устранению источников зловредных действий;

Мероприятия в Азербайджане (1/3)

- Были проведены **встречи** с провайдерами и операторами, **для обеспечения беспрерывности и согласованности** работы;
- Обеспечена **стабильность и безопасность** телекоммуникационной **инфраструктуры.**
- Более миллиона **учеников и студентов** перешли на **дистанционное обучение**;
- Десятки тысяч **работников** перешли **на дистанционную работу.**
- Традиционно проводимые **конференции и форумы**, различные конкурсы также проводились в **виртуальном формате.**

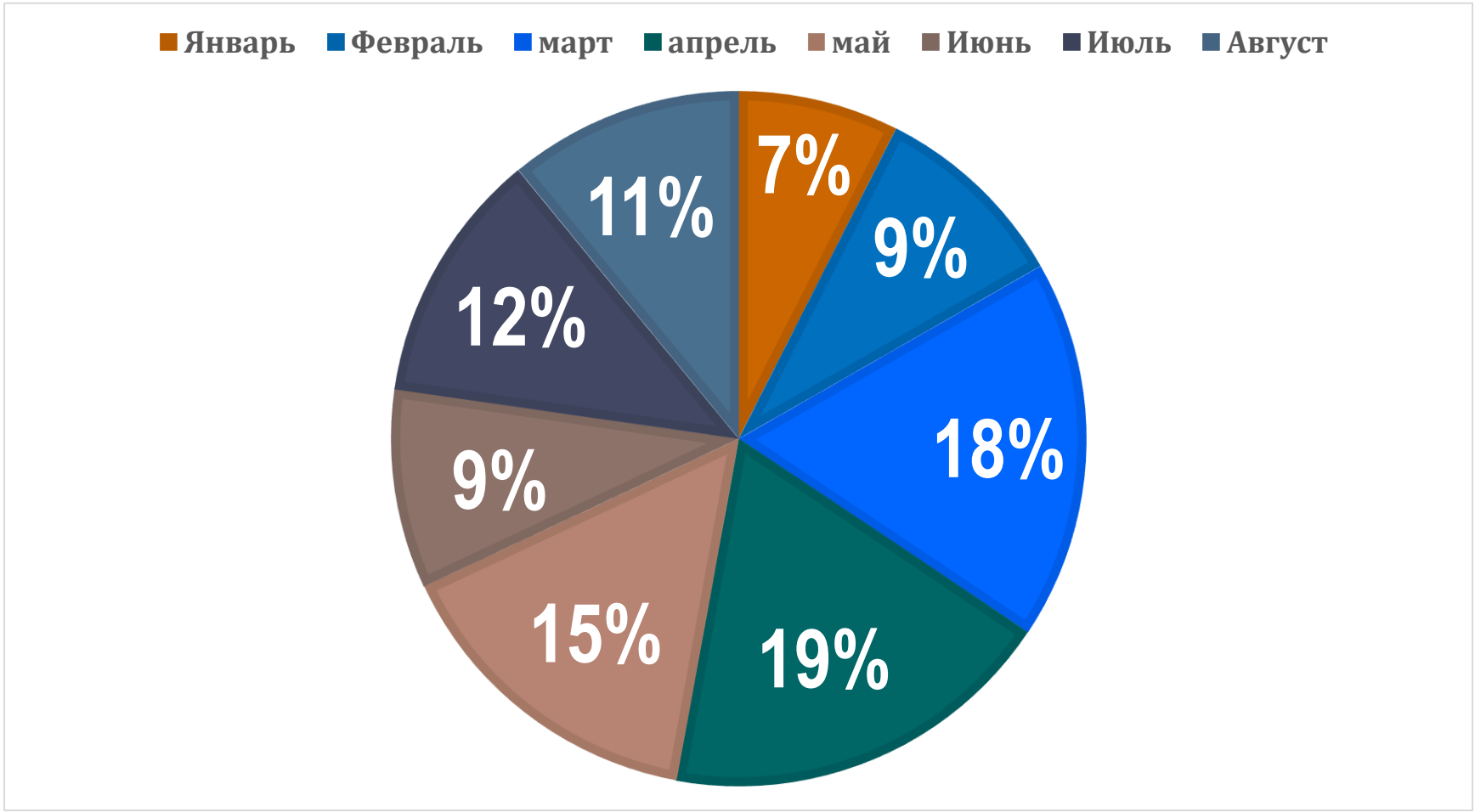
Мероприятия в Азербайджане (2/3)

- Для борьбы с пандемией были **разработаны и введены** в действие различные **информационные системы и мобильные приложения;**
- Существующие **информационные системы** были задействованы **для оперативности определения социальной помощи;**
- ИТ-сообщество инициировало создание **информационных ресурсов информативного, вспомогательного назначения;**
- Внедрены **новые электронные услуги** для обеспечения деятельности и получения необходимой помощи;
- Утверждена «**Инструкция** по кибербезопасности при удаленной работе»;
- Для различных групп населения были проведены **вебинары по кибербезопасности.**

Мероприятия в Азербайджане (3/3)

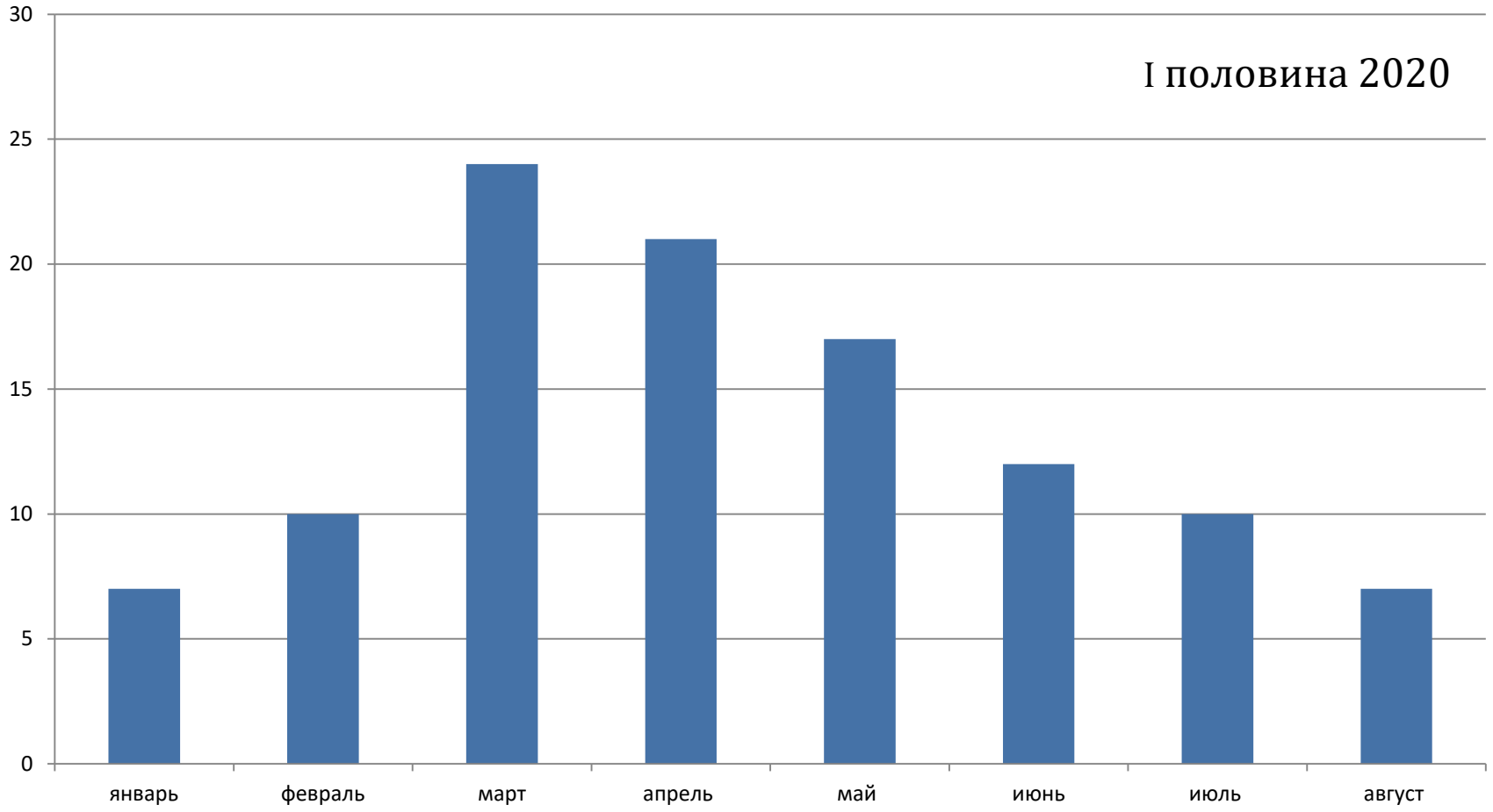
- Были расширены возможности для **заказов э-коммерции;**
- Компании, магазины перешли на расширение **онлайн заказов и доставок**;
- Была создана **локальная платформа для видеоконференций**, задействованная для государственных органов и медицинских учреждений;
- **Предотвращены функционирование фальшивых аккаунтов** государственных медицинских учреждений в социальных сетях, распространение дезинформации и фишинговых сообщений;

Статистика кибератак в Азербайджане



Источник: Служба Электронной Безопасности – cert.az

Фишинговые атаки



Будем помнить

1. **COVID-19 - крупнейшая угроза** кибербезопасности в новейшей истории;
2. **Пандемия пройдет.** А ее **последствия** на кибербезопас-ность **останутся!!!**

Благодарю за внимание