**Информация**

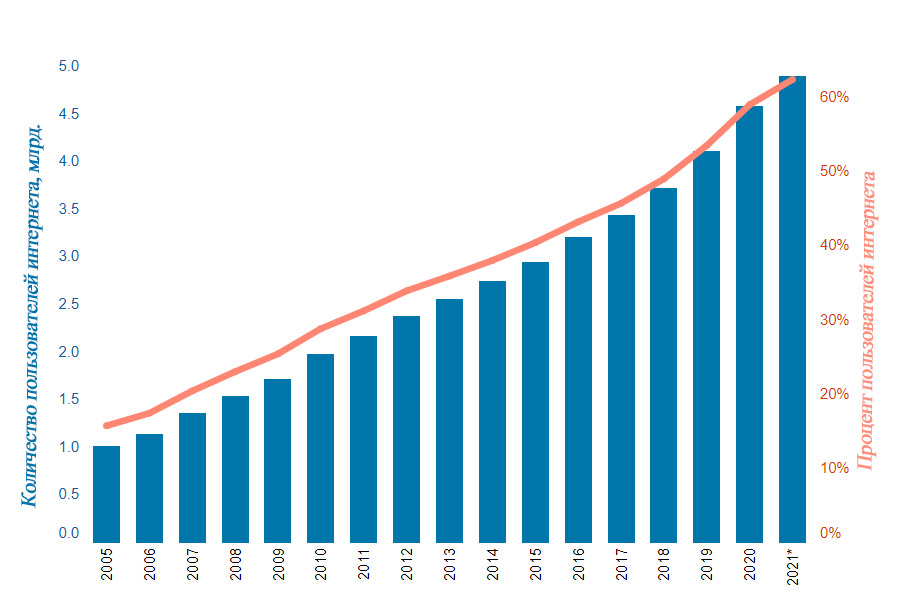
**О ситуации по кибербезопасности в мире**

*(материал ЦЭИР)*

Всемирный экономический форум *(ВЭФ)* опубликовал ежегодный отчет по кибербезопасности **«Глобальный прогноз кибербезопасности 2022 год»,** в котором обсуждаются предстоящие задачи по обеспечению цифровой безопасности.

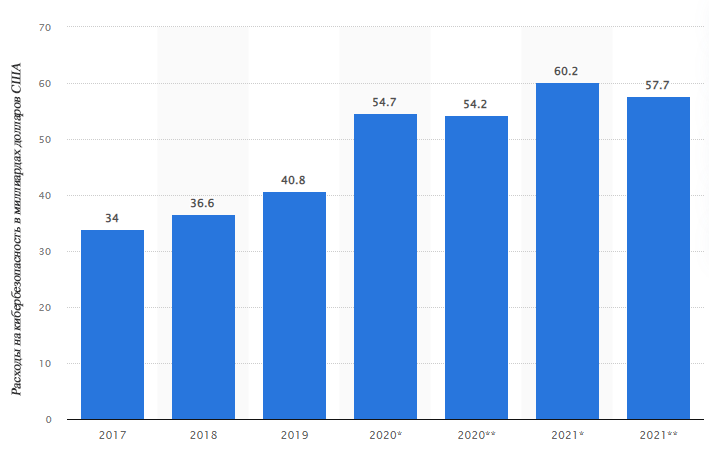
Во время пандемии цифровое использование увеличилось до **5 млрд.** пользователей по всему миру, при этом **3 млрд.** все ещё не подключены к сети интернет, **96%** из которых живут в развивающихся странах.

Причиной увеличения использования Интернета во время пандемии являются удаленная работа, дистанционное обучение, доступ к услугам, банковским операциям и покупкам.



*Справочно: Сообщается, что в Южной Корее трафик увеличился на 13%, достигнув от 45% до 60% их развернутой емкости во время пика пандемии. В Узбекистане количество пользователей Интернета превышает 27,2 млн. (78% населения), из них 25,3 млн. пользователей мобильного Интернета. 95% домохозяйств имеют доступ к мобильному интернету, а 54% домохозяйств имеют доступ к высокоскоростному интернету.*

Поскольку использование цифровых технологий продолжает расти быстрыми темпами, растет и киберпреступность. Киберпреступники используют любую возможность, чтобы использовать уязвимости против людей и организаций с помощью технологий. В отчёте ВЭФ сказано, что стоимость убытков из-за нарушений для организации составляет в среднем **3,6 млн.** долларов за инцидент. Возможно, еще большую тревогу вызывает растущая тенденция к тому, что компаниям требуется в среднем **280 дней**, чтобы выявить кибератаку и отреагировать на нее. Однако более крупные компании сталкиваются с другой проблемой – нехваткой кадров. По данным отчёта, к **2023 году** будет востребовано еще **1,8 млн** специалистов по кибербезопасности.

По данным Statista, в **2021 году** расходы на кибербезопасность во всем мире составили около **117,9 млрд** долларов, что на **8%** больше, чем в **2020** году. Gartner, техническая исследовательская и консалтинговая фирма, подсчитала, что расходы на информационную безопасность в **2022 году** составят **172 млрд.** долларов. К **2025 году** совокупные расходы могут достигать **1,75 трлн.** долларов.

Программа-вымогатель является одной из кибератак, которые больше всего беспокоят организации. Частота этого типа кибератак значительно увеличилась в первые шесть месяцев **2021** года, при этом глобальный объем атак увеличился на **151%**. В **2021 году** на каждую организацию приходилось в среднем **270** атак, что на **31%** больше, чем в **2020 году**. По данным **«Лаборатории Касперского»,** в Узбекистане ежедневно обнаруживается в среднем **67** новых инцидентов атак программ-вымогателей. Кроме того, участились случаи мошенничества, связанные с фиктивной службой технической поддержки, где жертвам сообщают, что им было предложено совершить банковские переводы на зарубежные счета или приобрести большие суммы по картам предоплаты. Убытки от таких афер составили более **347 млн.** долларов, что на **137%** больше, чем в **2020 году.**

*Справочно: Большинство пострадавших по всему миру (почти 60%) старше 60 лет, и на них приходится не менее 68% денежных потерь (почти 238 млн. долларов).*

Согласно тому же отчету, к **2025 году** к **5G** будет подключено **2,7 млрд.** устройств. С развертыванием сотовых сетей **5G** данные будут передаваться со скоростью **20 гигабит в секунду** с задержкой до **4 миллисекунд** *(для сравнения, LTE/4G задержка составляет до 20 миллисекунд)*. В то же время сети нового поколения менее централизованы и в меньшей степени зависят от аппаратного обеспечения. Это затрудняет защиту от атак и реагирование на инциденты.

Согласно Национальному индексу кибербезопасности *(NCSI)*, который ранжирует каждую страну по эффективности их мер кибербезопасности, можно выделить **5 стран** с самым высоким рейтингом — это Греция *(96,1%)*, Литва *(93,5%)*, Бельгия *(93,5%)*, Чехия *(92,2%)*.) и Эстонии *(90,9%)*. Узбекистан занимает в этом списке **87-е место** с показателем **36,6%**.

В отчете Comparitech за **2021 год** указано, что четыре страны Центральной Азии, включая Казахстан, Узбекистан и Кыргызстан, входят в число **15** наименее защищенных, а Таджикистан занимает худшее место. Эти страны также возглавили список стран с самым высоким процентом атак криптомайнеров. Страны Центральной Азии стали привлекательными местами для ферм по добыче криптовалюты из-за сравнительно низких цен на электроэнергию.

В отчете **«Обеспечение кибербезопасности в Республике Узбекистан»** от Центра кибербезопасности, что в национальном сегменте интернета выявлено более **1,3 млн.** кибератак за **2021 год.** Также Центр выявил более **17 млн.** случаев злонамеренной и подозрительной сетевой активности в национальном сегменте за тот же период. Большая часть этой активности *(76%)* приходится на участников бот-сетей, предназначенных для DOS и DDOS.

**На основании вышеизложенного предлагается принять следующие меры:**

1. Министерству по развитию информационных технологий и коммуникаций увеличить квоты приема студентов и наладить качественное образование в области информационной безопасности и кибербезопасности.

2. ГУП **«Центр кибербезопасности»** следует разработать программные средства для обнаружения криптомайнерских программ в республике или разработать меры по их предотвращению.

3. Министерству по развитию информационных технологий и коммуникаций и IT Park добавить информационную безопасность в программу **«Один миллион узбекских программистов».**

4. Министерству энергетики разработать стратегию выявления нелегальных криптовалютных ферм в стране посредством анализа данных об использовании электроэнергии.

Контактные данные:

ФИО: Утепбергенов Юнус Қутлымуратович

Должность: Ведущий научный сотрудник

Рабочий тел. : 78 150 02 02 *(450 внутр.)*

Мобильный, телеграм: 93 366-75-00

E-mail: y.utepbergenov@cerr.uz