МККК

ИТОГОВЫЙ ДОКУМЕНТ

ПАНЕЛЬНАЯ ДИСКУССИЯ

«Кибербезопасность в гуманитарном секторе: стратегии борьбы с онлайн–мошенничеством и имперсонизацией гуманитарных организаций»

Региональная делегация Международного Комитета Красного Креста (МККК)
в Российской Федерации и Республике Беларусь

Москва, Российская Федерация

16 сентября 2025 г.

1. РЕЗЮМЕ

Панельная дискуссия *«Кибербезопасность в гуманитарном секторе: стратегии борьбы с онлайн-мошенничеством и имперсонизацией гуманитарных организаций»* была организована Региональной делегацией МККК в Российской Федерации и Республике Беларусь 16 сентября 2025 года в рамках Международного технологического конгресса (16–18 сентября), проходившего в конгрессно-выставочном центре «Патриот» (Московская область, Россия).

В ходе дискуссии о гуманитарных последствиях кибермошенничества и различных других видов мошенничества в интернете, в том числе направленных против людей, пострадавших от конфликтов, выступили десять авторитетных представителей государственных органов Российской Федерации, экспертного сообщества, частного сектора и гуманитарных организаций. В числе участников мероприятия были представители Министерства внутренних дел (МВД) Российской Федерации, Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека, Аппарата Уполномоченного по правам человека в Российской Федерации, Центра правовой помощи гражданам в цифровой среде ФГУП «ГРЧЦ» (создан по инициативе Роскомнадзора), Российского Красного Креста, компаний «Билайн», BI.ZONE, Zecurion и Сообщества профессионалов в области приватности. В обсуждении также участвовали представители штаб-квартиры МККК в Женеве, Региональной делегации МККК в Российской Федерации и Республике Беларусь и представительства МККК в Газе.

Дискуссия была посвящена обсуждению последствий мошеннических действий, совершаемых в цифровой среде, и укреплению сотрудничества для снижения их негативных последствий для людей, в том числе пострадавших от конфликтов, и для гуманитарных организаций. В ходе обсуждения также были рассмотрены усилия и деятельность МККК, представленных российских государственных структур и технологических компаний по противодействию интернет-мошенничеству.

Докладчики описали текущую ситуацию с онлайн-мошенничеством в России и подчеркнули, что это явление распространено во всем мире. Была рассмотрена эволюция методов и средств, используемых мошенниками, а также существующие и потенциальные решения данной проблемы — технологические, законодательные и просветительские меры. Некоторые участники поделились опытом своих организаций по оказанию помощи пострадавшим от кибермошенничества и отметили, что объединение усилий поможет повысить уровень защиты людей, подверженных данным угрозам.

Мероприятие явилось эффективной площадкой для обсуждения и обмена мнениями о гуманитарных последствиях кибермошенничества и возможных путях решения данной проблемы. Оно также способствовало укреплению диалога между МККК, государственными органами, технологическими компаниями и экспертным сообществом. МККК выражает надежду, что проведенная панельная дискуссия послужит хорошим началом для постоянного и расширяющегося сотрудничества со всеми заинтересованными сторонами и компетентными органами, стремящимися минимизировать гуманитарные последствия кибермошенничества для людей, и без того находящихся в сложных жизненных обстоятельствах, и гуманитарных организаций, которые стараются им помочь.

МККК выражает признательность организаторам конгресса, в том числе Ассоциации разработчиков программного обеспечения «РУССОФТ», за приглашение провести панельную дискуссию и всем органам государственной власти и участникам дискуссии за поддержку мероприятия и выражает надежду на продолжение диалога по этой важной теме.

2. ОПИСАНИЕ ПРОБЛЕМЫ

В условиях стремительного развития новых технологий и широкого использования интернета кибермошенничество стало одной из наиболее острых угроз, влияющих на благополучие как отдельных людей, так и организаций. Масштабы проблемы вызывают серьезную обеспокоенность. Жертвами злоумышленников становится множество людей, которые теряют не только свои денежные средства, но и персональные данные, а организации — репутацию. Так, по данным Global Anti-Scam Alliance, за период с ноября 2024 по ноябрь 2025 года мошенники похитили во всем мире 442 трлн долларов США.

В России, принадлежащей к числу мировых лидеров в цифровой сфере, эта тенденция тоже прослеживается. По прогнозам специалистов Сбера, в 2025 году объем ущерба от действий мошенников может вырасти на 15% и достичь 350 млрд рублей. Уровень правовой и технологической защиты также постоянно растет, при этом ведется работа по повышению осведомленности населения о цифровых угрозах. Мошенники часто нацеливаются на наиболее уязвимые категории граждан, многие из которых уже находятся в сложных жизненных обстоятельствах и потому менее осторожны в онлайн-среде.

В 2025 году МККК зафиксировал стремительный рост числа случаев, когда жертвами мошенников в России становились люди, сталкивающиеся с последствиями конфликта, в частности семьи пропавших без вести военнослужащих. Это приносит дополнительные страдания людям, и так скорбящим по своим близким или отчаянно надеющимся на их возвращение. Еще одна тревожная и усиливающаяся тенденция состоит в том, что мошенники выдают себя за представителей гуманитарных организаций, в том числе — составных частей Международного движения Красного Креста и Красного Полумесяца, чтобы войти в доверие к своим жертвам. Такие действия серьезно подрывают доверие к гуманитарным организациям, приводя к тому, что люди могут не понимать, куда можно обратиться, не опасаясь, или кому довериться по вопросам, в решении которых им нужна помощь.

В этих условиях МККК решил организовать специализированную панельную дискуссию, в ходе которой эксперты российских государственных и частных структур могли бы обсудить актуальные проблемы и вызовы и обменяться опытом их решения.

3. ЭКСПЕРТНОЕ ОБСУЖДЕНИЕ

3.1. Точка зрения гуманитарных организаций

Во время мероприятия представители МККК выступили с докладами, в которых рассказали о том, что организация фиксирует случаи мошенничества в отношении пострадавших от конфликтов в России и Газе. Были рассмотрены инциденты, связанные с имперсонизацией гуманитарных организаций, а также меры, принимаемые для минимизации последствий кибермошенничества.

Дискуссию открыло видеообращение **Арианы Бауэр, директора Регионального управления оперативной деятельности МККК в Европе и Центральной Азии**. Она приветствовала докладчиков и аудиторию, которые собрались для обсуждения столь важной темы, объединяющей технологический и гуманитарный секторы. В своем выступлении она подчеркнула глобальный характер этого явления, отметив, что, к сожалению, мошенничество сопутствует всем конфликтам в современном мире.

Ги Брюнинкс, заместитель главы Региональной делегации МККК в Российской Федерации и Республике Беларусь, рассказал о том, как делегация работает с проблемой

онлайн-мошенничества, в частности в случаях, когда семьи пропавших без вести военнослужащих становятся мишенью для онлайн-мошенников. Так, летом 2025 года МККК зафиксировал рост числа таких случаев. Ги Брюнинкс также поделился наблюдениями и статистикой МККК относительно каналов, наиболее часто используемых мошенниками: социальные сети и мессенджеры применялись более чем в половине выявленных случаев мошенничества (54%, показатель продолжает расти), распространенным методом остаются телефонные звонки (почти 40% отмеченных случаев). Он подчеркнул, что действия мошенников делают боль семей пропавших без вести лиц еще более невыносимой. Кроме того, он отметил, что в процессе поиска близких люди нередко неосознанно подвергают себя дополнительным рискам, размещая личные данные в онлайн-группах или чатах, чтобы повысить вероятность получения информации о судьбе своих родственников. Также он описал последствия мошенничества для самой организации, включая случаи, когда злоумышленники выдают себя за представителей Красного Креста, что подрывает доверие к гуманитарной деятельности. Он рассказал и о том, какие усиленные меры МККК и Региональная делегация принимают для борьбы с такими мошенническими действиями и смягчения их последствий для людей, которым организация старается помочь. К таким мерам относятся: постоянное отслеживание ситуации в социальных сетях, оперативное и ясное донесение информации до общественности о выявленных случаях, в которых мошенники представляются сотрудниками МККК, информирование семей и партнеров МККК о мошеннических схемах такого рода, взаимодействие с платформами социальных сетей и мобильными операторами и т. д.

В своем видеообращении покидающий свой пост **глава представительства МККК в Газе Роман Парамонов** обозначил приоритетные направления работы организации в Газе и актуальность вопросов кибербезопасности. Он отметил, что мошенники активны и не стыдятся обманывать людей, находящихся в крайне тяжелых условиях. Он рассказал, что его коллеги в Газе выявляют попытки мошенников обмануть людей, живущих в ситуации интенсивного конфликта, в том числе собирая персональные данные потенциальных жертв или выдавая себя за гуманитарных работников. В качестве примера он привел случай, когда людям обещали эвакуацию из Газы за 30 000 долларов США, однако эти обещания так и не были выполнены.

Представитель Российского Красного Креста (РКК) Сергей Вильямов, директор Департамента стратегического развития и цифровой трансформации, рассказал о стратегии, разработанной РКК для противодействия мошенническим схемам, в том числе таким, при осуществлении которых мошенники выдают себя за представителей его организации. Стратегия включает в себя три основных направления. Во-первых, акцент на информировании населения об актуальных киберугрозах. Во-вторых, использование технических средств защиты. И, в-третьих, повышение внутренней культуры кибербезопасности в самой организации. Среди технических мер, принимаемых РКК, были названы: централизованное управление контентом в 85 региональных отделениях РКК, сертифицированное облачное хранение данных, двухфакторная аутентификация, использование исключительно официальных каналов связи при взаимодействии с получателями помощи. Также он представил предложения РКК по более эффективному противодействию онлайн-мошенникам, а именно:

1. создание единого децентрализованного реестра цифровых угроз для прогнозирования их дальнейшего развития;
2. создание цифрового гуманитарного ID, позволяющего понять, что вы имеете дело действительно с гуманитарной организацией;
3. создание гуманитарного киберштаба для оперативного реагирования на киберинциденты;
4. прицельное информирование уязвимых групп о существующих угрозах;

5. использование технологий искусственного интеллекта для мониторинга интернета с целью выявления мошеннического контента и его последующего удаления.

3.2. Точка зрения государственных органов

В обсуждении приняли участие представители ряда различных профильных государственных структур — от Министерства внутренних дел Российской Федерации и Центра правовой помощи гражданам в цифровой среде ФГУП «ГРЧЦ» (создан по инициативе Роскомнадзора) до Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека и Аппарата Уполномоченного по правам человека в Российской Федерации, которые рассказали о своих подходах к решению проблемы онлайн-мошенничества.

Министерство внутренних дел Российской Федерации представляла полковник юстиции **Юлия Меньщикова, заместитель начальника 2-го отдела организации расследования дистанционных хищений Следственного департамента МВД России**. Она представила аудитории статистику по онлайн-преступлениям: зарегистрировано 424 тыс. случаев, из которых 213 тыс. представляют собой дистанционное (то есть онлайн-) мошенничество, иными словами, мошенничество — это примерно половина всех киберпреступлений. Общий ущерб в 2025 году составил 119 млн рублей, из которых 111 млн рублей приходятся именно на дистанционные формы мошенничества; при этом данный показатель ежегодно растет. Она также отметила наличие обширной законодательной базы (более 100 нормативных актов, включая те, которые посвящены использованию сим-карт, утечкам данных и аренде учетных записей), что позволяет все более эффективно противодействовать подобным преступлениям. Ключевые меры реагирования государства включают пресечение деятельности мошеннических кол-центров, сотрудничество с Республикой Беларусь в данной сфере, блокировку звонков через такие приложения, как Telegram и WhatsApp, которые используются для мошеннических действий. В то же время она подчеркнула, что основное направление решения проблемы заключается во всестороннем информировании населения государственными органами, общественными организациями и средствами массовой информации о существующих угрозах. Среди препятствий для эффективной работы государства по борьбе с кибермошенничеством были также названы низкий уровень готовности иностранных криптовалютных бирж к сотрудничеству с российскими органами власти и неконструктивный подход со стороны недружественных государств.

Элина Сидоренко, член Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека, сосредоточила свое выступление на необходимости международного сотрудничества в области противодействия кибермошенничеству и выработки единого правового поля. Она отметила, что без создания «коридоров сотрудничества» невозможно привлекать к ответственности преступников, находящихся за рубежом, приведя в качестве примера конвенцию АСЕАН и Будапештскую конвенцию, посвященные одной и той же проблеме, но ратифицированные разными государствами. Именно поэтому Россия отстаивает идею подписания странами единой глобальной Конвенции ООН против киберпреступности. Она также указала на существующий разрыв между быстро развивающимися методами совершения киберпреступлений и медленной адаптацией законодательства. Кроме того, Элина Сидоренко обозначила три ключевых вызова, усугубляющие проблему: недостаточная защита данных организациями (включая гуманитарные) или их подрядчиками, неправомерное использование брендов организаций в преступных целях, применение преступниками новых технологий, таких как дипфейки, создающих дополнительные правовые и операционные сложности.

Владислав Григоров, начальник Управления защиты прав человека в уголовном процессе Аппарата Уполномоченного по правам человека в Российской Федерации, поделился опытом работы своего учреждения с обращениями граждан по вопросам онлайн-

мошенничества и представил подробную статистику по наиболее уязвимым группам населения, обращающимся в Аппарат. Согласно приведенным данным, наиболее подвержены кибератакам одинокие люди, пенсионеры (40–60 лет — 35% случаев; старше 60 лет — 32%), люди с инвалидностью и иные социально уязвимые категории граждан. Как правило, у них нет никого, к кому можно было бы обратиться за помощью или советом о том, как вести себя в таких случаях. Также было отмечено, что жертвами мошенников чаще становятся женщины (64%) по сравнению с мужчинами (36%). Среди основных трудностей в борьбе с онлайн-мошенниками он выделил отставание законодательства от развития мошеннических схем в интернете и недостаточную гармонизацию национальных правовых норм с международными.

Яков Петросян, заместитель начальника Отдела правового обеспечения и судебной практики Центра правовой помощи гражданам в цифровой среде ФГУП «ГРЧЦ» (создан по инициативе Роскомнадзора) представил деятельность своей организации, созданной в сентябре 2021 года для защиты граждан от незаконного использования цифровых данных. Он рассказал о наиболее распространенных мошеннических схемах, с которыми работает Центр при рассмотрении обращений граждан. Среди новых угроз и используемых схем были названы вредоносные программы, маскирующиеся под государственные услуги, чтобы ввести пользователей в заблуждение. Он также подчеркнул важность защиты персональных данных, поскольку их утечка в открытые источники в интернете является предпосылкой для практически любой мошеннической деятельности.

3.3. Точка зрения частного сектора

Частный сектор был представлен одним из крупнейших российских операторов мобильной связи — компанией «Билайн», одной из ведущих российских компаний в сфере кибербезопасности — компанией BI.ZONE, а также Сообществом профессионалов в области приватности — первым русскоязычным объединением специалистов по защите персональных данных.

Петр Алферов, директор по антифроду оператора сотовой связи «Билайн», рассказал об эволюции методов, используемых мошенниками, и привел статистику по жертвам мошеннических схем. Методы мошенничества постоянно развиваются: от подмены телефонных номеров до использования мессенджеров и вредоносного программного обеспечения. В 2024 году среди способов коммуникации, используемых мошенниками, телефонные звонки и мессенджеры составляли по 40%. Однако в 2025 году мошенники стали чаще использовать мессенджеры, что связано с принятием ряда законов по противодействию мошенничеству и развитием антифрод-систем банками и телеком-операторами. Он также выразил мнение, что следующий этап развития кибермошенничества будет связан с массовым распространением вирусов и вредоносных программ (вследствие ужесточения законодательства и внедрения новых защитных мер). Ежедневно компания выявляет 3 тысячи зараженных и 70 тысяч потенциально зараженных пользователей/клиентов, посещавших фишинговые ресурсы. Говоря о мерах защиты, Петр Алферов подчеркнул необходимость персонализированного подхода к защите персональных данных пользователей. Атаки мошенников становятся все более адресными и требуют соответствующих решений, иными словами, различные схемы мошенничества, направленные на разные группы населения, должны встречать соответствующие специализированные меры защиты. Во-вторых, он отметил необходимость создания интегрированной национальной антифрод-системы, которая могла бы объединять маркетплейсы, банки, социальные сети и, потенциально, гуманитарные организации. Цель такой системы — объединение всех участников цифровой экономики для обмена информацией и обеспечения более оперативного и эффективного реагирования на мошеннические атаки. В-третьих, в рамках инфраструктуры мобильного оператора разрабатывается простой и удобный сетевой антивирус, не требующий установки отдельного приложения.

В своем выступлении **Евгений Волошин, директор по стратегии BI.ZONE**, представил статистику компании по ущербу, причиненному мошенниками в России (в общей сложности 120 млрд рублей), а также обозначил основные отрасли и группы населения, чаще всего становящиеся жертвами таких преступлений. Среди наиболее пострадавших отраслей были названы государственный сектор, гуманитарная сфера и здравоохранение. Среди наиболее уязвимых возрастных групп оказалось наиболее экономически активное население (от 24 до 44 лет) и пожилые люди (у этой категории самый низкий уровень цифровой грамотности). Он также отметил, что около 9% хакеров действуют по идеологическим мотивам и наносят ущерб по политическим убеждениям и в связи с геополитической напряженностью, хотя большинство по-прежнему стремится получить финансовую выгоду. Кроме того, он подчеркнул, что международным организациям и другим государствам следует обращать внимание на положение с кибербезопасностью в России, поскольку тенденции, наблюдаемые сегодня в России и странах СНГ, могут проявиться в других регионах мира через 3–4 года. По его словам, злоумышленники, атакующие российских граждан, обладают высоким уровнем подготовки и в дальнейшем могут распространить свои методы преступной деятельности на другие страны.

Развивая мысли предыдущих докладчиков, **Алексей Мунтян, соучредитель и руководитель Сообщества профессионалов в области приватности**, представил подходы к усилению защиты данных и повышению уровня доверия в гуманитарном секторе с использованием современных ИТ-решений — технологий безопасной обработки данных. Он предложил применять четыре следующие технологии: контекстуальные идентификаторы, децентрализованную идентификацию, доказательство с нулевым разглашением, геоинформационную неразличимость. Он также отметил, что российское законодательство косвенно поддерживает принцип минимизации обработки данных для гуманитарных организаций.

3.4. Рекомендации

В завершение дискуссии **модератор Владимир Ульянов, руководитель Аналитического центра компании Zecurion**, подвел итоги обсуждения и выделил ключевые тезисы и рекомендации, которые докладчики озвучивали на протяжении всей сессии:

1. **Необходимо взаимодействие всех сторон, вовлеченных в борьбу с онлайн-мошенничеством** (законодательные органы, правоохранительные структуры, технологические компании, гуманитарные организации), в том числе на международном уровне.

2. **Особое внимание следует уделять защите персональных данных граждан**, поскольку их утечка позволяет мошенникам получать доступ к людям и осуществлять онлайн-атаки. Чтобы лишить мошенников возможности обманывать людей, необходимо должным образом защищать персональные данные.

3. **Крайне важно повышать осведомленность людей об угрозах онлайн-мошенничества**, с которыми они сталкиваются в цифровой среде, включая тех, кто уже испытывает на себе конкретные последствия конфликта, например, разыскивает пропавших без вести близких.

4. **Осведомленность и критическое мышление пользователей, подверженных данным рискам, имеют ключевое значение**. Это является необходимым условием для эффективной самозащиты в онлайн-пространстве.

5. **Своевременное развитие законодательства является критически важным**, поскольку правовое регулирование часто не успевает за постоянно меняющимися мошенническими схемами. Кроме того, для эффективной борьбы с трансграничным

онлайн-мошенничеством необходимо принятие универсальных международных норм различными государствами.

4. ЗАКЛЮЧЕНИЕ

Экспертная дискуссия по вопросам кибербезопасности в гуманитарной сфере собрала широкий круг участников, которые вместе подчеркнули необходимость комплексного подхода, предусматривающего участие различных акторов и применения разнообразных мер для эффективного противодействия онлайн-мошенничеству. Прежде всего, ключевое значение имеет междисциплинарное сотрудничество между законодательными органами, правоохранительными структурами, технологическими компаниями и гуманитарными организациями. Кроме того, приоритетом должна стать защита персональных данных, поскольку их утечки открывают мошенникам возможности для проведения таргетированных атак. Участники отметили необходимость не только внедрения технологических решений, но и проведения информационно-просветительских кампаний, направленных на повышение осведомленности населения об онлайн-угрозах. Также подчеркивалось, что правовая база должна постоянно обновляться, чтобы соответствовать быстро меняющимся и всё более изощренным мошенническим схемам. Принятие универсальных международных норм является жизненно важным условием для эффективной борьбы с трансграничной киберпреступностью, поскольку данное явление носит международный характер. Только при реализации такого многогранного подхода возможно опережать все более изощренные действия онлайн-мошенников и предотвращать страдания, которые их деятельность причиняет людям, включая тех, кто уже переживает тяжелейшие утраты, личные трагедии или занимается поиском пропавших без вести близких.

5. ПРЕСС-РЕЛИЗ МККК ОТ 16.09.2025

Гуманитарные последствия мошенничества: панельная дискуссия МККК на Международном технологическом конгрессе

Москва: 16 сентября Международный Комитет Красного Креста (МККК) провел панельную дискуссию о гуманитарных последствиях кибермошенничества, в том числе для тех, кто разыскивает близких, и семей, разлученных в результате конфликта.

Модератором дискуссии выступил Владимир Ульянов, руководитель аналитического центра компании Zecurion. В дискуссии принимали участие представители государственных органов, компаний из сектора технологий и информационной безопасности, гуманитарных и правозащитных организаций. Они обменялись взглядами по проблеме и обсудили сотрудничество для поиска решений в борьбе с мошенничеством.

Перед аудиторией, в которую входили в том числе представители Шанхайской организации сотрудничества (ШОС) и дипломатического корпуса, выступили сотрудники МВД России, Роскомнадзора, Совета при Президенте Российской Федерации по правам человека, Аппарата Уполномоченного по правам человека, Российского Красного Креста, компаний «Билайн» и BI.ZONE, Сообщества профессионалов в области приватности.

«Одной из новых особенностей нашей работы в XXI веке является то, что семьи сами используют все возможные цифровые средства для ускорения процесса розыска своих пропавших без вести родственников. Люди часто открыто делятся личными данными в группах или чатах, чтобы увеличить вероятность появления новостей об их близком человеке. А это делает их уязвимыми для мошенников», — отметил Ги Брюнинкс, заместитель главы Региональной делегации МККК в Российской Федерации и Республике Беларусь.

«Когда семьи военнопленных, пропавших без вести военнослужащих или гражданских лиц становятся жертвами мошенничества, это делает еще более нестерпимой ту боль, которую они испытывают», — добавил он.

В 2025 г. МККК зафиксировал рост числа случаев, когда жертвами мошенников в России становились люди, сталкивающиеся с последствиями конфликта, в частности семьи пропавших без вести, особенно военнослужащих. А попытки мошенников выдать себя за представителей гуманитарных организаций подрывают доверие к гуманитарным работникам и осложняют поддержку семей. Из-за действий мошенников сотрудники МККК теперь вынуждены прилагать дополнительные усилия, чтобы убедить родственников в том, что они действительно общаются с представителями МККК. Например, когда передают им долгожданные новости от содержащихся на территории Украины военнопленных, которых посетил МККК.

В записанном видеообращении директор Регионального управления оперативной деятельности МККК в Европе и Центральной Азии Ариана Бауэр отметила, что такие тенденции характерны для всех современных конфликтов: не только на территории России и Украины, но и в других регионах. А глава представительства МККК в Газе Роман Парамонов рассказал, как его сотрудники сталкиваются с попытками обмануть людей или собрать личные данные. Были случаи, когда семьи, которым пообещали эвакуацию из Газы, платили до 30 000 долларов, но эти обещания так и не были выполнены.

Юлия Меньщикова, полковник юстиции, заместитель начальника 2-го отдела организации расследования дистанционных хищений Следственного департамента МВД России, рассказала про обширную законодательную базу, которая позволяет все эффективнее бороться с такими формами мошенничества. При этом она подчеркнула, что основное направление решения проблемы лежит в области комплексного информирования населения со стороны органов государственной власти, общественных организаций и средств массовой информации.

Элина Сидоренко, член СПЧ при Президенте РФ, отметила необходимость международного сотрудничества в области противодействия кибермошенничеству и выработке унифицированного правового поля. «Без коридоров сотрудничества мы не сможем привлечь к ответственности преступников, находящихся за рубежом. Россия видит эту проблему и потому отстаивает идею подписания странами глобальной Конвенции ООН против киберпреступности», - сказала она.

Петр Алферов, директор по антифроду оператора сотовой связи «Билайн», рассказал об эволюции методов, которые используют мошенники, а также привёл статистику жертв мошеннических схем. Он поделился мнением, что следующий виток кибермошенничества будет связан с вирусами и с вредоносными программами, и подчеркнул необходимость персонифицированного подхода в том, что касается защиты персональных данных.

Евгений Волошин, директор по стратегии BI.ZONE, отметил, что международным организациям следует обращать внимание на ключевые тренды кибербезопасности, включая фишинг и телефонное мошенничество: «Тренды, которые сейчас наблюдаются в России и странах СНГ потенциально могут проявиться в других частях мира через 3-4 года».

Владислав Григоров, начальник Управления защиты прав человека в уголовном процессе аппарата Уполномоченного по правам человека в РФ, поделился опытом работы с обращениями граждан по поводу онлайн мошенничества, приведя детальную статистику по регионам. Согласно этим данным, мошенники часто выбирают себе в жертвы среди самых уязвимых, одиноких людей.

Кроме того, выступили Сергей Вильямов, директор департамента стратегического развития и цифровой трансформации Российского Красного Креста (РКК), рассказавший о стратегии выработанной РКК для противодействия мошенническим схемам, Яков Петросян, заместитель начальника отдела правового обеспечения и судебной практики Центра правовой помощи гражданам в цифровой среде, с рассказом о работе Центра и самыми распространёнными схемами мошенничества, а также Алексей Мунтян, соучредитель и руководитель «Сообщества профессионалов в области приватности», с презентацией об усилении инфоприватности в гуманитарном секторе.

Все выступающие сошлись на необходимости комплексного подхода и взаимодействия на международном уровне для выработки эффективных мер по защите от кибермошенничества.

Примечание для редакторов

1. Международный Комитет Красного Креста (МККК) — нейтральная, беспристрастная и независимая организация, чьи исключительно гуманитарные цели и задачи основываются на Женевских конвенциях 1949 г. Он помогает людям, пострадавшим от вооруженных конфликтов и других ситуаций насилия по всему миру, и делает все возможное, чтобы защитить их жизнь и достоинство и облегчить их страдания. В этой работе МККК часто сотрудничает со своими партнерами по Движению Красного Креста и Красного Полумесяца.
2. Представительство МККК в Москве (Российская Федерация) работает с 1992 г. В рамках своей деятельности МККК удовлетворяет гуманитарных потребности пострадавших в результате конфликта между Россией и Украиной, совместно со своим партнером, Российским Красным Крестом, содействуя распространению международного гуманитарного права и гуманитарной дипломатии. С 2022 г. МККК совместно с Российским Красным Крестом оказывает поддержку людям, разыскивающим своих пропавших без вести родственников.
3. Если вы разыскиваете пропавшего без вести военнослужащего, обратитесь в МККК: 8 800 600 92 69 (бесплатный номер) ; mos_tracing_services@icrc.org. Если вы разыскиваете пропавшего без вести из числа гражданского населения, обратитесь в Российский Красный Крест: 8 800 234 07 07 (бесплатный номер) ; rfl@redcross.ru
4. Международный технологический конгресс 2025 — центральное событие Российской Федерации для продвижения концепции международного сотрудничества и несырьевого экспорта как стратегии развития России.

6. ПУБЛИКАЦИИ И МАТЕРИАЛЫ ДЛЯ ДАЛЬНЕЙШЕГО ОЗНАКОМЛЕНИЯ ИЛИ ИСПОЛЬЗОВАНИЯ

6.1. Публикации и материалы МККК

- Гуманитарные последствия мошенничества: панельная дискуссия МККК на Международном технологическом конгрессе — пресс-релиз МККК
- https://t.me/mkkk_ru/1161 — публикация о прошедшем мероприятии в Telegram-канале МККК
- Круглый стол "Кибербезопасность в гуманитарном секторе: стратегии борьбы с онлайн-мошенничеством и имперсонизацией гуманитарных организаций" — анонс панельной дискуссии на сайте МККК
- https://t.me/mkkk_ru/1152 — анонс панельной дискуссии в Telegram-канале МККК
- https://www.icrc.org/en/data-protection-humanitarian-action-handbook — «Защита данных в ходе гуманитарной деятельности: руководство» (английская версия, перевод руководства на русский язык готовится к публикации)

6.2. Публикации в СМИ

- https://tass.ru/obschestvo/25073191?ysclid=mfmn5kl2pk75757859 — публикация ТАСС о прошедшем мероприятии
- https://rapsinews.ru/White_Internet_news/20250916/311153645.html — публикация РАПСИ о прошедшем мероприятии
- https://telegram.me/beeline/3110 — публикация о прошедшем мероприятии в Telegram-канале компании «Билайн»
- https://beelinenow.ru/articles/beeline-tri-napravoeniya-v-borbe-s-moshennikami/ – публикация о прошедшем мероприятии на сайте компании «Билайн»
- https://t.me/internetinsafe/4685 — публикация о прошедшем мероприятии в Telegram-канале «Белый Интернет»
- https://t.me/cryptoelina/6901 — публикация о прошедшем мероприятии в Telegram-канале «КриптоЛина»
- https://t.me/colaboratoria_edu/188 — анонс панельной дискуссии в Telegram-канале АНО «Колаборатория»
- https://vk.com/wall-231947794_33 — анонс панельной дискуссии в VK-группе АНО «Колаборатория»
- https://vk.com/sovet_po_pravam?w=wall-66412790_28738 — анонс панельной дискуссии в VK-группе Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека
- https://www.youtube.com/watch?v=bddCdY8WPx0 — анонс панельной дискуссии в YouTube-канале Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека

6.3. Фотографии и видеозапись мероприятия

- Фотографии и видеозапись мероприятия, предоставлены МККК
  Фотографии, предоставлены Организационным комитетом Международного технологического конгресса

Документ составлен Петром Лёвиным, советником по вопросам гуманитарной политики Региональной делегации МККК в Российской Федерации и Республике Беларусь, и отредактирован Рут Хетерингтон, руководителем отдела по вопросам гуманитарной политики Региональной делегации МККК в Российской Федерации и Республике Беларусь. Выражаем искреннюю благодарность всем коллегам, которые внесли свой вклад в работу над документом.