ЦИФРОВИЗАЦИЯ ЭМБЛЕМ КРАСНОГО КРЕСТА, КРАСНОГО ПОЛУМЕСЯЦА И КРАСНОГО КРИСТАЛЛА

ПРЕИМУЩЕСТВА, РИСКИ И ВОЗМОЖНЫЕ РЕШЕНИЯ

ETH zürich | APL Johns Hopkins Applied Physics Laboratory

UNIVERSITÄT BONN | Australian Red Cross | MKKK

ЦИФРОВИЗАЦИЯ ЭМБЛЕМ КРАСНОГО КРЕСТА, КРАСНОГО ПОЛУМЕСЯЦА И КРАСНОГО КРИСТАЛЛА

ПРЕИМУЩЕСТВА, РИСКИ И ВОЗМОЖНЫЕ РЕШЕНИЯ

В подготовке доклада участвовали Тильман Роденхойзер (юридический советник, МККК), Мауро Виньяти (советник по новым цифровым технологиям ведения войны, МККК), Ларри Мэйби (юридический советник, Австралийский Красный Крест) и Холли Джонстон (юридический советник, Австралийский Красный Крест).

Перевод с английского.

Образец библиографической ссылки для цитирования: Цифровизация эмблем красного креста, красного полумесяца и красного кристалла: преимущества, риски и возможные решения, МККК, 2023 (на русском языке); ICRC. *Digitalizing the Red Cross, Red Crescent and Red Crystal Emblems: Benefits, Risks, and Possible Solutions,* ICRC, Geneva, 2022.

СОДЕРЖАНИЕ

ВЫРАЖЕНИЕ ПРИЗНАТЕЛЬНОСТИ

Публикация настоящего доклада — это результат двухлетней исследовательской работы и консультаций с экспертами из различных сфер и областей, проведенных под эгидой Международного Комитета Красного Креста (МККК). Выработка концепции, составление и публикация доклада были бы невозможны без участия ряда лиц и организаций.

В первую очередь мы хотели бы выразить признательность Центру кибердоверия (CECYT — совместная инициатива Цюрихского технологического института и Боннского университета) и Лаборатории прикладной физики Университета Джонса Хопкинса за работу и исследования в области технических возможностей создания «цифровой эмблемы», осуществленные на безвозмездной основе. Эти учреждения посвятили значительный объем времени и усилий разработке метода цифровой маркировки для ресурсов и данных, пользующихся защитой, а также делились специализированными знаниями и представляли свои наработки в ходе многочисленных консультаций с экспертами.

Мы также признательны членам глобальной группы экспертов, которые поделились своими знаниями и опытом в ходе серии консультаций, и хотели бы сердечно поблагодарить их за время, уделенное рассмотрению предложений, выдвинутых CECYT и Лабораторией прикладной физики Университета Джонса Хопкинса, анализу возможных решений и участию в ряде консультаций. Полный перечень экспертов представлен в приложении 1.

МККК также благодарит Австралийский Красный Крест за помощь в организации серии консультаций с экспертами из разных стран мира, целью которых было обсуждение преимуществ и рисков использования «цифровой эмблемы» как средства оповещения о правовой защите во время вооруженных конфликтов и рассмотрение потенциальных решений этой проблемы. Отличительные эмблемы — часть нашей общей культуры самоидентификации, и поэтому мы были чрезвычайно рады совместно работать над этим проектом.

Мы также хотели бы выразить благодарность за работу по подготовке настоящего доклада Тильману Роденхойзеру (юридический советник, МККК), который руководил данным проектом последние два года, а также Мауро Виньяти (советник по новым цифровым технологиям ведения войны, МККК), Ларри Мэйби (юридический советник, Австралийский Красный Крест) и Холли Джонстон (юридический советник, Австралийский Красный Крест), которые оказывали помощь в организации и проведении консультаций с экспертами. Кроме того, успешная реализация этого проекта является заслугой множества внесших свой вклад сотрудников МККК из различных отделов и делегаций, в числе которых Лоран Жизель, Венсан Граф Нарбель, Стефан Хэнкинс, Джонатан Хоровитц, Фабрис Лопер, Кубо Мачак, Седрик Мэр, Лоренцо Редалье, Виталий Савенков, Бертран Стивале и Дельфина ван Золинге, а также членов Группы МККК по содействию инновациям.

ПРЕДИСЛОВИЕ

Цифровая трансформация нашего мира оказывает влияние на ход вооруженных конфликтов, на жизнь затронутых ими людей и на деятельность тех, кто стремится облегчить причиняемые конфликтами страдания. Для гуманитарных и медицинских акторов, к которым относится и Международный Комитет Красного Креста, цифровые технологии служат источником уникальных возможностей, позволяющим эффективнее удовлетворять потребности людей в помощи. Так, мы используем спутниковые изображения для выявления людей в уязвимом положении и планирования операций по оказанию помощи. Мы анализируем огромные объемы данных для того, чтобы разыскать безвестно отсутствующих и обеспечить их воссоединение с семьей. В условиях гуманитарных кризисов мы предоставляем людям пространство в цифровых хранилищах данных, где они могут сохранить копии важнейших документов. Эксперты в области здравоохранения также широко применяют цифровые технологии в своей деятельности, например в реальном времени инструктируют медицинский персонал в учреждениях, расположенных в непосредственной близости к фронту.

Однако в последние несколько лет стало очевидно, что использование цифровых технологий, помимо огромного потенциала, имеет и свои риски. За период, прошедший с начала пандемии COVID-19, кибероперации, направленные против больниц, неоднократно становились причиной прерывания жизненно необходимого лечения и заставляли врачей и медсестер тратить драгоценное рабочее время на заполнение бумажной документации, а не на оказание помощи остро нуждающимся в ней. В начале 2022 г. выяснилось, что серверы МККК, на которых хранятся личные данные более полумиллиона людей со всего света, были взломаны в рамках крупномасштабной и высокоорганизованной кибероперации. Вследствие этого уязвимые лица — задержанные; безнадзорные несовершеннолетние; мигранты — подверглись еще большему риску. Факт утечки данных такого масштаба указывает на острую потребность активизировать нашу работу в области кибербезопасности и защиты данных, даже с учетом того, что эти направления и ранее являлись стратегически приоритетными для МККК. Для того чтобы гарантировать людям безопасность и эффективно оказывать им помощь в реальном мире, мы должны обеспечить защиту личных данных, а также доступность и неприкосновенность наших данных и систем в виртуальном цифровом пространстве.

Достижение этой цели в эпоху цифровых технологий требует от нас надежности и стремления к инновациям. Эмблемы красного креста и красного полумесяца — порой наносимые обычной краской на крышу больницы или автомобиль — давно служат знаком защиты для медицинского персонала, медицинских учреждений и оказывающих гуманитарную помощь представителей Международного движения Красного Креста и Красного Полумесяца. Это подтвердит любой делегат МККК или представитель Движения. Мне самому не раз довелось убедиться в защитном действии эмблемы во множестве опасных ситуаций: например, когда мы помогали эвакуировать гражданских лиц из окруженных районов мухафазы Дамаск (Сирия) в 2018 г., когда мы отправились в осажденный город Таиз (Йемен) в 2017 г., или во время каждой из моих многочисленных поездок в сектор Газа во время активных боевых действий 2014 и 2021 гг. и непосредственно после них.

Будет ли эта надежная и проверенная в боевых условиях эмблема применима в цифровой среде? Сможем ли мы создать инструмент цифровой маркировки ресурсов, сервисов и

данных, принадлежащих субъектам медицинской и гуманитарной деятельности? Способны ли концепции и решения, основанные на международном гуманитарном праве, эволюционировать достаточно быстро, чтобы соответствовать современному уровню развития технологий? Как добиться того, чтобы в будущем все лица, осуществляющие операции в киберпространстве, знали, что промаркированные «цифровой эмблемой» МККК компьютеры используются только в медицинских или гуманитарных целях и не должны подвергаться нападению? Для предотвращения сбоев в ИТ-системах больниц и обеспечения полной реализации потенциала гуманитарных организаций в области помощи жертвам вооруженных конфликтов и их защиты необходимы наше коллективное мышление, совместные действия и инновации. Необходимо учесть позиции всех соответствующих заинтересованных сторон. В последние несколько лет МККК работает с авторитетными исследовательскими учреждениями и многопрофильной группой экспертов из разных стран мира над изучением возможных решений и анализом преимуществ и рисков, связанных с использованием «цифровой эмблемы». Мы с гордостью представляем вам результаты нашей работы — не в знак ее завершения, но для формирования фундамента дальнейшей совместной деятельности в данном направлении.

Я приглашаю всех вас — представителей государств, членов Движения, ИТ-специалистов, занятых в секторе обеспечения безопасности, медицинском, гуманитарном и военном секторах, а также сотрудников интернет-организаций — присоединиться к обсуждению проблемы и помочь нам найти конкретные и практичные способы защитить медицинские и гуманитарные службы как в интернет-пространстве, как и вне его.

Роберт Мардини,

генеральный директор МККК

КРАТКОЕ ИЗЛОЖЕНИЕ

По мере цифровизации общества кибероперации становятся реальностью в условиях вооруженных конфликтов. Все больше государств развивают военный потенциал в киберсфере, и его использование во время вооруженных конфликтов, вероятно, будет расти. МККК уже предупреждал о возможных последствиях использования кибероперации в вооруженных конфликтах для жизни людей, особенно в результате разрушения или вывода из строя гражданской инфраструктуры с помощью киберсредств. В частности, МККК выразил обеспокоенность уязвимостью медицинских учреждений и гуманитарных организаций перед кибероперациями, поскольку и те, и другие в последние годы подвергались нападениям. Данный доклад посвящен именно этой уязвимости и способам ее устранения.

В поисках конкретных мер по практической реализации защиты, предоставляемой в киберпространстве некоторым медицинским и гуманитарным организациям международным гуманитарным правом, МККК решил изучить идею разработки нового знака, цифрового маркера или другого средства обозначения цифровых ресурсов организаций, пользующихся особой защитой, то есть так называемой «цифровой эмблемы». Идея и задача «цифровой эмблемы» имеют понятный смысл: более 150 лет отличительные эмблемы (красный крест и красный полумесяц, а впоследствии и красный кристалл) используются для передачи простого послания: во время вооруженного конфликта лица, которые их носят, или объекты и предметы, обозначенные ими, должны быть защищены от причинения ущерба. Обязательство всех воюющих сторон уважать и защищать медицинских и гуманитарных работников так же применимо к интернет-пространству, как и вне его.

С 2020 г., работая в партнерстве с Лабораторией прикладной физики Университета Джонса Хопкинса и Центром кибердоверия (CECYT — совместное начинание Цюрихского технологического института и Боннского университета), МККК ведет исследовательский проект по изучению технологической возможности разработки «цифровой эмблемы». Совместно с Австралийским Красным Крестом МККК также сформировал глобальную группу экспертов для оценки ожидаемых преимуществ и рисков, связанных с «цифровой эмблемой», а также ключевых характеристик, которыми она должна обладать. Эксперты, вошедшие в проект, представляли различные профессиональные, географические и гендерные группы. Среди участников были представители технологических компаний и компаний из сферы кибербезопасности, бывшие правительственные чиновники, специалисты, ранее занимавшиеся кибероперациями, эксперты по информационно-коммуникационным технологиям (ИКТ) из медицинской и гуманитарной сферы, специалисты с опытом работы в криминалистике и полиции, «этичные» хакеры и представители научного сообщества.

В результате исследований и консультаций МККК пришел к следующим выводам:

по мнению большинства опрошенных экспертов, ожидаемые преимущества от «цифровой эмблемы» перевешивают возможные риски.

- Основное ожидаемое от цифровой эмблемы преимущество заключается в том, что лицам, которые осуществляют кибероперации (далее — «кибероператоры»), будет легче определить пользующиеся защитой объекты и обезопасить их от нападения благодаря визуализации и практическому применению правовых мер, обеспечивающих защиту в среде ИКТ. В «тумане войны» этот дополнительный знак может принести реальную пользу. В первую очередь он усилит защиту обозначенных объектов от риска причинения вреда законопослушными операторами, а также может оказать сдерживающее воздействие на злоумышленников.

- В то же время цифровая маркировка, позволяющая идентифицировать медицинские и гуманитарные организации, рискует сделать их более подверженными вредоносным операциям. Степень серьезности риска будет зависеть от ситуации. Как обладающие большим опытом, так и не располагающие значительными возможностями операторы уже могут с легкостью идентифицировать медицинские или гуманитарные организации в киберпространстве; дополнительный риск облегчить им нападения на отмеченные соответствующим образом организации может быть относительно небольшим. Однако использование «цифровой эмблемы» может сделать их более желанными мишенями кибероперациий со стороны менее искушенных кибероператоров, которые в противном случае не смогли бы так легко их идентифицировать.
- Другой риск заключается в потенциальном неправомерном использовании «цифровой эмблемы» для ложного обозначения военной или иной инфраструктуры, не пользующейся защитой. Такой риск существует и в материальном мире, а неправомерное использование эмблемы запрещено национальным законодательством в разных странах по всему миру. Специфический риск в киберпространстве, который может привести к новым проблемам, связан со скоростью, масштабом и охватом, характерными для среды ИКТ, что может породить новые виды вредоносных операций или привести к более тяжелым последствиям их осуществления.

«Цифровая эмблема» указывает на правовую защиту; она не может считаться универсальным техническим средством решения проблем в области безопасности, с которыми в киберпространстве сталкиваются организации, пользующиеся защитой.

- Защита от вредоносных кибероперациий требует реализации мер в области кибербезопасности всеми учреждениями, пользующимися защитой. «Цифровая эмблема» не может заменить собой такие меры. Однако она может дополнить их, указывая на то, что отмеченная ею организация пользуется особой защитой в соответствии с международным правом, и ее необходимо ограждать от вреда.

Если «цифровая эмблема» будет разработана, ее должно быть просто размещать, удалять и должным образом обслуживать.

- Размещение «цифровой эмблемы» должно быть простым, а обслуживание — недорогим. Ее использование и обслуживание должно требовать минимальных ресурсов в различных регионах мира, пострадавших от вооруженных конфликтов, при этом языковые, технологические и культурные барьеры не должны служить препятствием.
- Чтобы «цифровую эмблему» можно было использовать, она должна предполагать возможность встраивания в существующую технологическую среду, а также обладать способностью отмечать различные виды ресурсов, сервисов и данных. «Цифровую эмблему» должно быть просто удалить, так как это крайне важно в свете возможных рисков в области безопасности. Кроме того, должна быть предусмотрена возможность адаптировать ее в соответствии с будущими технологическими и инфраструктурными изменениями. Например, будет важно найти технологическое решение, которое бы позволило отмечать защищенные данные в облаке.
- «Цифровая эмблема» должна использоваться под контролем компетентного органа власти любой стороны в вооруженном конфликте.

Если «цифровая эмблема» будет разработана, она должна быть «видимой», и лица, осуществляющие операции в киберпространстве, должны ее легко определять и понимать.

- Кибероператор должен иметь возможность легко определять наличие «цифровой эмблемы». Поиск и понимание «цифровой эмблемы» не должны вызывать у него трудностей.
- Операторы подчеркнули, что они должны иметь возможность проверить «цифровую эмблему», при этом не будучи идентифицированными в качестве потенциальной угрозы.
- В идеале «цифровая эмблема» должна быть частью информации, которую у системы может запросить любой кибероператор. Она должна быть видима на раннем этапе операции и должна недвусмысленным образом обозначать защиту.
- Должна быть возможность легко проверить подлинность «цифровой эмблемы». Это крайне важно для обеспечения того, чтобы такая эмблема пользовалась уважением и доверием.

Чтобы обеспечить надлежащее применение, а также предупреждать и преследовать неправомерное использование, «цифровая эмблема» должна иметь правовое обоснование, и соблюдение необходимых правовых норм должно контролироваться соответствующими органами власти.

Важное преимущество существующих отличительных эмблем заключается в том, что их форма, функция, применение и защита регулируются международным и внутригосударственным правом, а их неправомерное использование запрещено. Существуют различные варианты включения «цифровой эмблемы» в международно-правовую базу, например:

- новый Дополнительный протокол к Женевским конвенциям, признающий и регулирующий использование «цифровой эмблемы». Аналогичный подход был использован в 2005 г., когда была введена эмблема красного кристалла;
- пересмотр Приложения I к Дополнительному протоколу I, которое регулирует использование «отличительных сигналов» (световых и радиосигналов, электронного опознавания) или связи (радиосвязи, кодов). Этим способом государства воспользовались в последний раз в 1993 г.

Независимо от того, какой вариант будет выбран на международном уровне, соответствующие правовые положения должны быть включены в национальное законодательство, а органы власти государств должны будут обеспечить их соблюдение.

ПЕРСПЕКТИВЫ

Руководствуясь данными, полученными по итогам исследований и консультаций в рамках этого проекта, в основном положительными отзывами международной группы экспертов и единогласным призывом со стороны членов Международного движения Красного Креста и Красного Полумесяца (Движения) «продолжать изучение технической возможности создания „цифровой эмблемы" и оценить преимущества такой эмблемы»[1], МККК продолжит исследовательскую и консультационную работу в контексте потенциальной «цифровой эмблемы». Такая работа будет выражаться в дальнейшем осуществлении комплекса мер: от технической разработки, валидации и верификации потенциальных решений (в частности, предложенных Лабораторией прикладной физики Университета Джонса Хопкинса и CECYT) до консультаций со всеми соответствующими заинтересованными сторонами — особенно с государствами, национальными обществами Красного Креста и Красного Полумесяца (национальные общества) и интернет-организациями.

[1] См.: Council of Delegates of the International Red Cross and Red Crescent Movement, Safeguarding Humanitarian Data (resolution), CD/22/R12.

ВВЕДЕНИЕ

По мере цифровизации общества кибероперации в условиях вооруженных конфликтов становятся реальностью. Число государств, развивающих свой военный киберпотенциал, продолжает расти, в связи с чем прогнозируется повышение частоты использования такого потенциала в ходе вооруженных конфликтов[2]. В последние несколько лет МККК неоднократно выражал обеспокоенность по поводу уязвимости медицинского сектора для вредоносных кибероперацій[3]. Данный риск существует всегда, но во время вооруженных конфликтов — когда потребность в функционирующих медицинских системах и инфраструктуре максимальна — он становится особенно высоким. Кроме того, в условиях поступательной цифровизации систем и методов работы МККК и других составных частей Международного движения Красного Креста и Красного Полумесяца возникает реальная угроза того, что они подвергнутся вредоносным кибероперациям. В действительности эта угроза уже воплотилась в жизнь[4].

В связи с подобным развитием ситуации МККК в последние несколько лет привлекает экспертов в области кибербезопасности к обсуждению вопроса о том, можно ли (и каким образом) адаптировать к среде информационных и коммуникационных технологий (ИКТ) признанные на международном уровне обозначения статуса защищенного субъекта для медицинских и духовных служб в составе вооруженных сил, уполномоченных медицинских формирований, санитарно-транспортных средств и соответствующего персонала, а также для ряда гуманитарных акторов в условиях вооруженного конфликта, — к этим обозначениям относятся отличительные эмблемы красного креста, красного полумесяца и красного кристалла. В процессе поиска практических мер, позволяющих укрепить защиту, которой пользуются эти субъекты, возникла идея о создании нового обозначения, цифрового маркера или другого средства идентификации в киберпространстве[5] (далее — «цифровая эмблема»).

С 2020 г., работая в партнерстве с Лабораторией прикладной физики Университета Джонса Хопкинса и Центром кибердоверия (CECYT — совместное начинание Цюрихского технологического института и Боннского университета), МККК ведет консультационно-исследовательский проект[6] по изучению технологической возможности разработки «цифровой эмблемы». Исследовательская работа началась с изучения технических средств маркировки и опознавания цифровых ресурсов, сервисов и данных для пользующихся защитой учреждений, военных формирований и других релевантных акторов, с тем чтобы эти технические средства соответствовали характеру действий таких субъектов.

Позднее МККК при участии Австралийского Красного Креста сформировала глобальную группу экспертов, задача которой состояла в оценке потенциальных преимуществ и рисков,

---

[2] См.: UN Open-Ended Working Group, *Final Report*, 2021, para. 16; *Группа правительственных экспертов ООН по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности*. Окончательный доклад, 2021, пункт 7.

[3] ICRC, *The potential human cost of cyber operations*, 2018. В качестве примера аналогичной позиции обеспокоенности см. также: *Call by global leaders: work together now to stop cyberattacks on the healthcare sector*, Humanitarian Law & Policy Blog, 2020.

[4] См.: *МККК*. Кибератака на МККК: что нам известно, 2021.

[5] В настоящем докладе термины «киберпространство» и «среда ИКТ» используются как полностью эквивалентные.

[6] Настоящий проект был подробно описан в размещенной в открытом доступе публикации: Rodenhäuser et al, Signaling legal protection in a digitalizing world: a new era for the distinctive emblems? Humanitarian Law & Policy Blog, 2021.

связанных с «цифровой эмблемой». Результаты работы группы должны были помочь МККК принять обоснованное решение относительно того, стоит ли рекомендовать государствам дальнейшее рассмотрение этой инициативы. В течение трех месяцев были проведены консультации, участие в которых приняло 44 эксперта из 16 стран. Эксперты, вошедшие в проект, представляли различные профессиональные, географические и гендерные группы. Среди участников были представители технологических компаний и компаний из сферы кибербезопасности, бывшие правительственные чиновники, специалисты, ранее занимавшиеся кибероперациями, эксперты по ИКТ из медицинской и гуманитарной сферы, специалисты с опытом работы в криминалистике и полиции, «этичные» хакеры и представители научного сообщества. Консультации проходили в различных форматах: состоялось два пленарных совещания, семь консультаций в малых группах и ряд двусторонних дискуссий.

Цели как технологических исследований (этап 1), так и консультаций с экспертами (этап 2), заключались в следующем:

- изучение концепции «цифровой эмблемы» с операционной, технической, правовой, военной, гуманитарной и политической точек зрения;
- подробное рассмотрение преимуществ, рисков и проблем, возникающих в связи с «цифровой эмблемой»;
- определение характеристик потенциально эффективной «цифровой эмблемы»;
- проверка пригодности различных технических решений с точки зрения реализации «цифровой эмблемы».

Настоящий доклад подготовлен с опорой на материалы исследований, анализа, консультаций и дискуссий, проводившихся в ходе обоих этапов проекта силами МККК, Лаборатории прикладной физики Университета Джонса Хопкинса, CECYT, Австралийского Красного Креста и группы экспертов совместно и по отдельности. Документ содержит взвешенный обзор различных мнений о концепции и необходимых характеристиках «цифровой эмблемы», а также описывает преимущества и риски, связанные с ее использованием. Над составлением основного текста доклада работали совместно МККК и Австралийский Красный Крест, приложения были подготовлены CECYT и Лабораторией прикладной физики Университета Джонса Хопкинса. Следовательно, представленные в докладе выводы и рекомендации не обязательно отражают точку зрения тех или иных партнерских исследовательских учреждений или экспертов, принимавших участие в работе над докладом.

В главе 1 настоящего доклада излагается суть понятия «отличительные эмблемы» в соответствии с международным гуманитарным правом (МГП) и вводится концепция «цифровой эмблемы». Глава 2 содержит описание основных преимуществ, рисков и проблем, связанных с цифровой эмблемой, которые в основном были выявлены в ходе серии консультаций с многопрофильной глобальной группой экспертов. В главе 3 представлены желаемые операционные и технические характеристики «цифровой эмблемы». В главе 4 отражены результаты первичной оценки рассмотренных к настоящему времени технических решений. В главе 5 обобщены основные выводы и возможные дальнейшие действия.

ГЛАВА 1

ОТЛИЧИТЕЛЬНЫЕ ЭМБЛЕМЫ: ОПОЗНАВАНИЕ И ЗАЩИТА ВО ВРЕМЯ ВООРУЖЕННЫХ КОНФЛИКТОВ

Во время вооруженных конфликтов красный крест, красный полумесяц и красный кристалл обозначают особую защиту, которой пользуются определенные медицинские и гуманитарные субъекты[7]. Отличительные эмблемы применяются уже более 150 лет, а их вид, действие, порядок использования и характер предоставляемой ими защиты установлены широко признанными правовыми и политическими механизмами.

В идеале «цифровая эмблема» должна функционировать в рамках существующих правовых рамок: то есть ее функции и порядок применения должны соответствовать нормам МГП, регулирующим традиционные отличительные эмблемы. В разделах ниже представлен обзор правовой и политической основы, в рамках которой могла бы функционировать «цифровая эмблема».

ПРАВОВАЯ ОСНОВА

Для чего предназначены отличительные эмблемы?

Ключевая норма МГП гласит, что во время вооруженного конфликта раненые и больные лица и те кто осуществляет за ними уход — уполномоченный медицинский и гуманитарный персонал, его учреждения, формирования и транспортные средства — должны пользоваться уважением и защитой. Обязанность уважать и защищать медицинский и гуманитарный персонал и соответствующие объекты распространяется и на кибероперации, проводимые в условиях вооруженных конфликтов[8].

Отличительные эмблемы — красный крест и красный полумесяц, а впоследствии и красный кристалл — создавались как символ защиты в ходе вооруженных конфликтов, которой пользуются медицинские и духовные службы вооруженных сил, а также уполномоченный гражданский медицинский персонал, его формирования и транспортные средства. Эмблемы — это визуальное средство обозначения их защищенности в соответствии с МГП. Правовая защита, предоставляемая пользователям эмблемы, имеет юридическую силу: к субъектам, демонстрирующим отличительную эмблему, требуется в обязательном порядке проявлять уважение и предоставлять им защиту. Кроме того, «умышленное нанесение ударов по зданиям, материалам, медицинским учреждениям и транспортным средствам, а также персоналу, использующим в соответствии с международным правом отличительные эмблемы, установленные Женевскими конвенциями [1949 г.]»[9], является военным преступлением.

Эмблемы также символизируют нейтральный, беспристрастный и независимый характер

[7] Также существует отличительная эмблема в виде красного льва и солнца, которая, однако, перестала применяться на практике с 1980 г.

[8] *МККК.* Международное гуманитарное право и кибероперации во время вооруженных конфликтов, 2019; *Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности ООН.* Окончательный доклад, 2021, пункт 71(f).

[9] Ст. 8(2)(b)(xxiv) и 8(2)(e)(ii) Римского статута Международного уголовного суда (МУС).

гуманитарной деятельности составных частей Международного движения Красного Креста и Красного Полумесяца (Движение)[10].

Описанные выше цели и способы использования отличительных эмблем установлены Женевскими конвенциями 1949 г. и Дополнительными протоколами к ним 1977 г. и 2005 г., которые составляют комплексную правовую основу, регламентирующую, кто — и при каких условиях и обстоятельствах — имеет право применять такие эмблемы.

Сценарий практического использования отличительных эмблем

В ходе вооруженного конфликта между двумя вымышленными странами — Боронией и Банксией — два боронийских истребителя F-15 движутся в направлении заранее определенной военной цели. При этом пилотам неизвестно одно важнейшее обстоятельство: лица, ответственные за планирование оперативных действий, допустили ошибку и определили в качестве цели не тот объект. Вместо военного склада, который планировалось поразить, пилоты истребителей двигаются по направлению к больнице, обслуживающей 55 тыс. жителей Банксии.

Пилоты уже находятся на подлете к цели и готовятся применить управляемые боеприпасы в соответствии с заранее подготовленным перечнем объектов к поражению. Буквально за несколько мгновений до планируемого момента атаки одна из пилотов замечает в коллиматорный прицел, что на крыше объекта, обозначенного как цель, что-то нарисовано: большой красный крест на белом фоне площадью примерно 10 квадратных метров. Ей известно, что согласно международному гуманитарному праву медицинские учреждения защищены от нападений, а красный крест служит для обозначения такой защиты. Она немедленно отменяет атаку.

Какую форму имеют отличительные эмблемы?

Согласно МГП, отличительные эмблемы имеют физическую форму красного креста, красного полумесяца или красного кристалла на белом фоне. Отличительные эмблемы должны быть закреплены или изображены на поверхности защищенных объектов или учреждений или на одежде защищенных лиц, визуально обозначая защиту, которой они пользуются[11].

МГП также предусматривает возможность использования «отличительных сигналов», в том числе световых, радио- или электронных сигналов, для указания на то, что тот или иной субъект пользуется защитой[12].

Кто имеет право использовать отличительные эмблемы

Использовать такие эмблемы для обозначения особой правовой защиты, предоставляемой во время вооруженного конфликта в соответствии с МГП (то есть пользоваться «защитным действием» эмблем), разрешается следующим субъектам:

- медицинские службы вооруженных сил;
- духовный персонал и священнослужители, закрепленные за вооруженными силами;
- гражданские медицинские формирования и санитарно-транспортные средства, при наличии санкции от компетентного органа (от государства или потенциально от «вооруженной группы» во время вооруженных конфликтов);

[10] В состав Международного движения Красного Креста и Красного Полумесяца входят Международный Комитет Красного Креста, Международная Федерация обществ Красного Креста и Красного Полумесяца и все национальные общества Красного Креста и Красного Полумесяца.

[11] См.: Женевская конвенция от 12 августа 1949 года об улучшении участи раненых и больных в действующих армиях (Женевская конвенция I), ст. 38—44; Дополнительный протокол к Женевским конвенциям от 12 августа 1949 года, касающийся защиты жертв международных вооруженных конфликтов, от 8 июня 1977 г. (Дополнительный протокол I), ст. 18.

[12] См. ст. 6—9 Приложения I к Дополнительному протоколу I: правила, касающиеся опознавания, по состоянию на 30 ноября 1993 г.

- МККК и Международная Федерация обществ Красного Креста и Красного Полумесяца (Международная Федерация);
- Национальные общества, действующие под руководством медицинских служб вооруженных сил или закрепленные за таковыми.

Названные субъекты (далее — «пользующиеся защитой субъекты») могут использовать эмблему, но не обязаны этого делать. Их правовая защита от причинения вреда обусловлена МГП и не зависит от факта наличия или отсутствия отличительной эмблемы; иными словами, пользующиеся защитой субъекты не лишаются правовой защиты даже тогда, когда не используют эмблему или удаляют (снимают) ее.

В мирное время медицинские службы вооруженных сил могут прибегать к использованию отличительных эмблем в качестве меры предосторожности — так, чтобы при начале вооруженного конфликта не было необходимости их наносить (закреплять). Кроме того, составные части Движения могут использовать эмблему для опознавания своих формирований, транспортных средств, персонала и добровольцев. Подобное использование известно как «использование в целях обозначения»[13].

Кто должен обеспечивать соблюдение правовой основы, регламентирующей использование отличительных эмблем?

Регулирование, отслеживание использования и его правомерности, а также обеспечение юридической силы эмблем по всему миру не являются функциями какой-либо одной организации. Регулирование использования эмблем посредством национального законодательства, предупреждение и пресечение их неправомерного использования, а также контроль соблюдения защиты, предоставляемой эмблемами, является обязанностью каждого государства как в мирное время, так и в периоды вооруженных конфликтов[14]. В этой связи многие государства приняли комплексное законодательство об использовании отличительных эмблем и о предоставляемой ими защите или внедрили соответствующие правовые нормы в национальное законодательство и разработали нормативные акты, предусматривающие наказание за неправомерное использование эмблем[15]. Национальные общества и/или МККК могут помогать государствам в выполнении этой обязанности.

ВОЗМОЖНОСТЬ СОЗДАНИЯ «ЦИФРОВОЙ ЭМБЛЕМЫ»

В связи с тем, что отличительные эмблемы задумывались для использования в физической среде, в цифровом пространстве какие-либо отличительные эмблемы (или отличительные сигналы) отсутствуют. Тем не менее идея адаптации защитных эмблем или сигналов к условиям, созданным техническим прогрессом, не нова: МГП предусматривает возможность введения новых средств опознавания в форме «отличительных эмблем» или «отличительных сигналов», — а именно световых, радио- или электронных сигналов — для указания на то, что тот или иной субъект пользуется особой защитой в соответствии с МГП[16]. И государства уже неоднократно воспользовались такой возможностью.

«Цифровая эмблема» могла бы стать дополнительным элементом опознавания и защиты медицинских и отдельных гуманитарных акторов в условиях вооруженных конфликтов, выполняя ту же защитную функцию, что и физические отличительные эмблемы. В течение последнего десятилетия эта идея многократно обсуждалась

[13] При использовании в целях обозначения эмблема должна всегда сопровождаться полным названием соответствующей составной части Движения или его аббревиатурой и должна быть небольшого размера.
[14] См. ст. 53—54 Женевской конвенции I.
[15] Обзор таких законодательных актов см. базу данных МККК по имплементации МГП на национальном уровне (на англ. яз.): https://ihl-databases.icrc.org/applic/ihl/ihl-nat.nsf/vwLawsByCountry.xsp?xp_topicSelected=GVAL-992BU8.
[16] См. Приложение I к Дополнительному протоколу I: правила, касающиеся опознавания, 6 июня 1977 г. (по состоянию на 1993 г.).

учеными-экспертами и МККК[17].

Сценарий практического использования «цифровой эмблемы»

В ходе вооруженного конфликта между упомянутыми ранее Боронией и Банксией последняя начала разработку вредоносного программного обеспечения, которое распространяется автоматически и атакует логистическое программное обеспечение, применяемое Боронией для управления снабжением вооруженных сил. При проведении разведывательных мероприятий киберкомандование Банксии выяснило, что программное обеспечение, выбранное в качестве мишени для нападения, применяется шире, чем считалось ранее, в том числе в системах, промаркированных «цифровой эмблемой». В результате дальнейшего расследования операторы вредоносного ПО выясняют, что эти системы принадлежат больнице.

Киберкомандование Банксии осведомлено о том, что отличительные эмблемы и сигналы означают наличие защитного статуса. Обладая информацией о том, что программное обеспечение используется медицинскими формированиями (благодаря наличию «цифровой эмблемы» и результатам эффективных разведывательных мероприятий), командующий отдает программистам приказ изменить процедуры и отрегулировать киберпотенциал вредоносной программы так, чтобы она не могла причинить вреда системам, помеченным «цифровой эмблемой».

В идеале «цифровая эмблема» должна давать возможность лицам, проводящим операции в киберпространстве, маркировать или опознавать целый ряд компонентов систем, которые эксплуатируются пользующимися защитой субъектами, в том числе:

— электронные ресурсы, такие как серверы, компьютеры, смартфоны, устройства интернета вещей и сетевые устройства, эксплуатируемые пользующимися защитой субъектами;

— цифровые сервисы пользующихся защитой субъектов (например, FTP-сервер для хранения документов и VPN — технический сервис для управления электронными устройствами на расстоянии);

— данные пользующихся защитой субъектов, хранящиеся на ИТ-оборудовании/серверах/в облаке (например, данные в коммерческих облачных хранилищах), в которых могут содержаться деликатные сведения медицинского или личного характера;

— средства коммуникации (передачи данных) между пользующимися защитой устройствами и серверами (например, средства коммуникации между экипажем скорой помощи и больницей или между делегатом и штаб-квартирой МККК).

При создании нового сигнала или «цифровой эмблемы» может потребоваться дополнение действующих договоров для интеграции нового цифрового маркера в существующую правовую основу.

[17] См., например: Rauscher and Korotkov, *Working Towards Rules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace*, EastWest Institute, 2011, pp. 30-31; *Пилюгин, П. Л.* Проблемы создания технических средств контроля за соблюдением разрабатываемых норм международного права для киберпространства, Восьмой международный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности», 2014; Sutherland et al, The Geneva Conventions and Cyber-Warfare, 160 The RUSI Journal 2015; *МККК*. Международное гуманитарное право и вызовы современных вооруженных конфликтов, 2015, с. 76—77; ICRC, *The potential human cost of cyber operations*, 2018, pp. 4041; ICRC, *Avoiding Civilian Harm from Military Cyber Operations During Armed Conflicts*, 2021, pp. 27-28; Adriano Iaria, *Digital Emblems: The Protection of Health Care Facilities in the Cyber Domain in the Age of Pandemics*, Opinio Juris, 2020.

В данный момент технического решения, которое бы отвечало таким задачам и представленным в настоящем докладе дополнительным требованиям, не выявлено. Тем не менее МККК — совместно с партнерскими организациями — рассмотрел несколько потенциально применимых перспективных технических решений (см. главу 4 и приложения 2 и 3).

Краткий обзор: ключевые сведения о концепции «цифровой эмблемы»

Какие функции будет выполнять «цифровая эмблема»?

«Цифровая эмблема» будет служить для идентификации цифровых элементов (ресурсов, сервисов и данных), которые принадлежат пользующимся защитой субъектам. Она будет обозначать, что в соответствии с МГП такие субъекты не могут становиться целью нападения и должны быть защищены от причинения вреда. Она не будет обеспечивать какого-либо иного статуса с точки зрения кибербезопасности, сообщая лишь о защите от нарушения деятельности и уничтожения.

Кто сможет использовать «цифровую эмблему»?

«Цифровой эмблемой» смогут пользоваться уполномоченные медицинские и гуманитарные акторы. Порядок использования отличительных эмблем регламентирован актами международного и национального права. Применение «цифровой эмблемы» будет допустимо только для маркировки инфраструктуры или субъектов, которые пользуются особой защитой и имеют право на демонстрацию отличительной эмблемы в соответствии с МГП.

В каких ситуациях будет использоваться «цифровая эмблема»?

Отличительные эмблемы применяются в ходе вооруженных конфликтов для оповещения об особой защите, которой пользуются отдельные медицинские и гуманитарные субъекты в соответствии с МГП. Следовательно, «цифровая эмблема» не будет предназначена для маркировки медицинских и гуманитарных учреждений вне ситуаций вооруженного конфликта (за исключением использования в качестве меры предосторожности на случай начала такого конфликта). При этом стоит отметить, что члены Движения Красного Креста и Красного Полумесяца имеют право использовать эмблему в целях обозначения своей принадлежности к нему (то есть для идентификации, а не для оповещения о правовом защитном статусе) в любое время.

Как создать «цифровую эмблему»?

По состоянию на 2022 г. «цифровая эмблема» не разработана. Включение любых новых отличительных эмблем или сигналов в нормы МГП является прерогативой и задачей государств. Следовательно, согласованием вопросов о необходимости «цифровой эмблемы», форме ее технической реализации и механизмах ее внедрения на практике должны заниматься государства.

ГЛАВА 2

ОЦЕНКА ПРЕИМУЩЕСТВ, РИСКОВ И ПРОБЛЕМ, ВОЗНИКАЮЩИХ В СВЯЗИ С «ЦИФРОВОЙ ЭМБЛЕМОЙ»

Предназначение «цифровой эмблемы» можно сформулировать четко и просто: она предназначена для опознавания, а следовательно, и обеспечения защиты, ресурсов, сервисов и данных уполномоченных медицинских и гуманитарных акторов во время вооруженных конфликтов. «Цифровая эмблема» обозначает правовую защиту, другого защитного действия в отношении промаркированных ей субъектов она не имеет.

Таким образом «цифровая эмблема» не может считаться универсальным техническим средством решения проблем в области безопасности, с которыми в киберпространстве сталкиваются организации, пользующиеся защитой. Для защиты от вредоносных кибероперациий каждый пользующийся защитой субъект должен самостоятельно принять меры по обеспечению кибербезопасности. «Цифровая эмблема» не может заменить собой такие меры, она может дополнить их, указывая на то, что отмеченная ею организация пользуется особой защитой в соответствии с международным правом, и ее необходимо ограждать от вреда. Тем не менее использование «цифровой эмблемы», даже при соблюдении той защиты, на которую она указывает, не обязательно обеспечивает защиту от разного рода вреда: во время вооруженных конфликтов всегда существует риск ненамеренного нанесения ущерба медицинским или гуманитарным операторам. Так, например, несмотря на то, что стороны в конфликте должны уважать и защищать больницы, а также в любых обстоятельствах стремиться ограждать их от вреда, причинение некоторого сопутствующего ущерба четко промаркированной больнице, расположенной рядом с военной целью, на которую осуществляется нападение, не обязательно будет сочтено нарушением МГП. Кроме того, пользующиеся защитой медицинские учреждения в своей работе зависят от других объектов инфраструктуры, например систем водо- и электроснабжения. В отличие от медицинских учреждений, такая инфраструктура в общем случае не может быть отмечена отличительной эмблемой, поэтому есть риск того, что она станет целью нападения.

Одним из ключевых результатов исследовательской и консультационной работы является вывод, к которому пришло большинство экспертов: идея о создании «цифровой эмблемы» важна и целесообразна. По итогам исследований и консультаций был определен перечень основных аспектов:

- ожидаемые преимущества «цифровой эмблемы»;
- потенциальные риски, связанные с использованием «цифровой эмблемы»;
- основные проблемы внедрения «цифровой эмблемы» в практическую деятельность.

Настоящая глава, в которой обобщенно представлены преимущества, риски и проблемы, а также глава 3, которая содержит технические и операционные требования, призваны дать представление об основных вопросах, выявленных в рамках исследований и поднятых

экспертами в ходе консультационного процесса. Цель состоит в том, чтобы представить взвешенный обзор различных мнений о концепции и необходимых характеристиках «цифровой эмблемы», а также описать преимущества и риски, связанные с ее использованием. Безусловно, добиться согласия экспертов и исследователей по всем вопросам было невозможно. Кроме того, перечень аспектов и соображений, представленный в настоящем докладе, не является исчерпывающим, а выполнение изложенных здесь операционных и технических требований — не единственный способ разработки жизнеспособного технического решения.

ОЖИДАЕМЫЕ ПРЕИМУЩЕСТВА «ЦИФРОВОЙ ЭМБЛЕМЫ»

Большинство экспертов, с которыми проводились консультации в рамках этого проекта, сочли работу по созданию «цифровой эмблемы» целесообразной. Бóльшая часть экспертов придерживались мнения о том, что потенциальные преимущества «цифровой эмблемы» как средства маркировки пользующихся защитой ресурсов, сервисов и данных перевешивают потенциальные риски.

«Цифровая эмблема» может способствовать повышению уровня защиты

Как и в реальном, физическом мире, пользующиеся защитой субъекты в среде ИКТ подвержены риску стать целью или случайно пострадать от операций, направленных на нарушение деятельности или уничтожение; в среде ИКТ такую угрозу создают кибероперации. «Цифровая эмблема» обозначает, что медицинским и гуманитарным организациям нельзя причинять вред, и потенциально может защитить такие организации от ущерба, возникающего в результате вредоносных кибероперaций. Если «цифровая эмблема» поможет — пусть даже немного — сократить масштабы прямого или непреднамеренного вреда, причиняемого медицинским или уполномоченным гуманитарным акторам, ее создание и внедрение будут ценной инициативой, особенно во время вооруженных конфликтов. При этом способность «цифровой эмблемы» оказать общее положительное воздействие будет зависеть от ситуации (то есть ее нужно определять отдельно для каждого пользующегося защитой субъекта с учетом условий, в которых он действует, актуальных рисков и индивидуальных уязвимостей). При проведении любой оценки в этой связи следует принимать во внимание риск неправомерного использования «цифровой эмблемы» (см. дальнейшее обсуждение ниже).

После введения «цифровой эмблемы» кибероператорам будет легче избежать повреждения инфраструктуры, пользующейся защитой

Для кибероператоров, которые стремятся действовать в соответствии с МГП и избегать непосредственного нападения или непреднамеренного причинения вреда медицинским и гуманитарным цифровым ресурсам, сервисам или данным, «цифровая эмблема», без сомнения, будет полезна — с ее помощью они смогут лучше опознавать субъектов, пользующихся защитой, и ограждать их от нападения. Так, ее внедрение позволит кибероператорам вносить в код вредоносного программного обеспечения соответствующие ограничения, за счет которых можно минимизировать прямой или непреднамеренный вред пользующимся защитой ресурсам, сервисам и данным. Многие кибероператоры уже располагают средствами опознавания целей и потому в основном имеют представление о том, деятельностью какого рода занимается та или иная организация в среде ИКТ, или о том, какой тип систем ИКТ поражает применяемое ими вредоносное программное обеспечение. Тем не менее «цифровая эмблема» может стать дополнительным подспорьем при идентификации цифровых составных частей медицинских и гуманитарных организаций, на которые запрещено нападать. С ее помощью они смогут избежать ошибок в разведывательной деятельности (то есть удостовериться, что та или иная система принадлежит медицинскому или гуманитарному учреждению) или исправить такие ошибки.

Кроме того, можно ожидать, что в будущем кибероперации в ходе вооруженных конфликтов будут вестись с большой скоростью и в «тумане войны», и одним из способов обороны против подобных кибероперацій может стать тактика введения в заблуждение. В этих условиях риск совершения ошибок возрастает, и подобный дополнительный знак может принести реальную пользу, так же как и физические эмблемы.

Очевидно, что преимуществами, обусловленными более простым опознаванием пользующихся защитой субъектов и принятием активных мер по ограждению таких субъектов от вреда, смогут пользоваться стороны в вооруженном конфликте, стремящиеся действовать в пределах правовых норм. Высказываясь по данному вопросу, эксперты по военным тематикам подчеркивали, что при условии уважения эмблемы противоположной стороной в конфликте нет причин полагать, что преимущества использования «цифровой эмблемы» будут каким-то образом отличаться от преимуществ использования физической эмблемы[18].

«Цифровая эмблема» перенесет в среду ИКТ механизм обозначения защиты в соответствии с МГП, который лежит в основе действия существующих физических эмблем

Сегодня среди государств превалирует консенсусное мнение о том, что к использованию ИКТ применяется международное право и что «нормы международного гуманитарного права применимы только в ситуациях вооруженных конфликтов»[19]. «Цифровая эмблема», которая обретает все большую актуальность на фоне текущих многосторонних дискуссий о применимости МГП к кибероперациям, могла бы стать эффективным средством переноса в среду ИКТ и обозначения в ней той защиты, которую действующие нормы и принципы МГП предоставляют уполномоченным медицинским и гуманитарным организациям. «Цифровая эмблема» также могла бы сыграть значительную роль в адаптации существующих норм МГП к специфическим условиям, в которых осуществляются кибероперации в ходе вооруженного конфликта.

С практической точки зрения, во время вооруженного конфликта лица и организации, осуществляющие медицинскую и гуманитарную деятельность, должны пользоваться уважением и защитой. В прошлом угрозы такой деятельности имели исключительно кинетический характер, как например неправомерная бомбардировка больницы. Сегодня к угрозам кинетического характера добавился постоянно возрастающий риск проведения кибероперацій против медицинских и гуманитарных учреждений. В свете развития угроз нового типа оповещение об особой защите теперь необходимо не только в физическом пространстве (например, в форме красного креста, красного полумесяца или красного кристалла, изображенного краской на крышах зданий), но и в среде ИКТ — в форме того или иного цифрового сигнала.

---

[18] Сотрудники новостного портала BleepingComputer в 2020 г. связались с участниками различных групп, создающих программы-вымогатели, и задали вопрос о том, планируют ли они прекратить нападения на учреждения здравоохранения в период пандемии COVID-19. В ответ представители некоторых групп, в частности CLOP, DoppelPaymer, Netwalker и Nefilim, заявили, что они никогда не направляли атаки на учреждения определенных типов, в том числе на больницы и благотворительные организации, и не планируют изменять этому правилу. См.: Lawrence Abrams, https://www. bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-health-orgs-during- pandemic/, 18 March 2020.

[19] См.: *Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности ООН*. Окончательный доклад, 2021, пункты 69 и 71(f). Для того чтобы подробнее ознакомиться с принципами применимости МГП к кибероперациям, см.: *МККК*. Международное гуманитарное право и кибероперации во время вооруженных конфликтов. Изложение позиции МККК, 2019.

ПОТЕНЦИАЛЬНЫЕ РИСКИ, СВЯЗАННЫЕ С ИСПОЛЬЗОВАНИЕМ «ЦИФРОВОЙ ЭМБЛЕМЫ»

Некоторые эксперты видят в перспективе создания «цифровой эмблемы» больше рисков, чем преимуществ, в особенности в связи с тем, что злоумышленники смогут целенаправленно нападать на отмеченные такой эмблемой организации и использовать ее неправомерным образом. Такие риски следует тщательно учитывать в процессе разработки и потенциального использования любого технического решения.

Использование отличительных эмблем для обозначения статуса субъекта, пользующегося защитой, во время вооруженного конфликта несет в себе не только преимущества, но и, возможно, риски. Некоторые из рисков, выявленных в среде ИКТ, аналогичны тем, что десятилетиями существуют в физической среде, например привлечение дополнительного внимания, неправомерное использование эмблемы и создание ложного ощущения безопасности. Эти риски могут усугубляться в связи со скоростью, масштабом и широтой охвата, которые характерны для киберпространства. К примеру, промаркированные субъекты могут быть атакованы из любой точки мира, вне зависимости от физического расстояния до цели; или же атакованы массово и одновременно. Подобные риски, характерные только для киберпространства, отличаются от рисков в физическом пространстве.

«Цифровая эмблема» может упростить обнаружение медицинских и гуманитарных ресурсов, сервисов и данных

Одним из основных факторов риска, связанных с применением «цифровой эмблемы», является возможное упрощение поиска медицинских и гуманитарных ресурсов, сервисов и данных для злоумышленников. Из-за подобной простоты обнаружения такие ресурсы, сервисы и данные могут подвергнуться еще большей опасности: злоумышленники получат возможность составлять списки «беззащитных целей», нападение на которые несет в себе меньшие риски, или определять промаркированные организации как особо «ценную» мишень. В среде ИКТ степень опасности может быть еще выше, ведь частота вредоносных кибероперaций, направленных против медицинских и гуманитарных учреждений, в последние годы возрастает. В киберпространстве цифровые ресурсы, сервисы и данные могут стать целью нападения ряда акторов, — включая преступников, — которым не обязательно находиться в непосредственной близости от цели. Подобная возможность уникальна для виртуальной среды и отсутствует в реальном мире. Такое положение вещей создает еще один специфический для киберпространства риск — риск одновременного нападения на множество отмеченных соответствующей эмблемой организаций: например, если злоумышленник способен модифицировать или целенаправленно разработать вредоносное программное обеспечение так, что оно будет наносить вред всем организациям, имеющим цифровую эмблему.

Упрощение обнаружения и нападения на пользующихся защитой субъектов — это наиболее серьезный риск, который эксперты связывают с «цифровой эмблемой». Некоторые из них уточняли, что уровень этого риска, вероятно, будет варьироваться, и при его оценке нужно учитывать различные конкретные источники угрозы. В среде ИКТ уже существует множество различных методов идентификации и категоризации цифровых ресурсов, сервисов и данных. Более высокоорганизованные операторы обычно располагают возможностью опознавать медицинские и гуманитарные цифровые ресурсы вне зависимости от наличия или отсутствия «цифровой эмблемы»; «цифровая эмблема» не будет значительно упрощать достижение цели, а следовательно, не вызовет значительного повышения уровня риска, если такие операторы будут действовать злонамеренно. Менее высокоорганизованные акторы же, напротив, могут значительно активизировать свои действия в отношении субъектов, использующих «цифровую эмблему».

Необходимо помнить, что риск стать целью нападения для пользующихся защитой субъектов существует не только в среде ИКТ, но и в реальном мире. Для решения этой проблемы государства определили, что «умышленное нанесение ударов по зданиям, материалам, медицинским учреждениям и транспортным средствам, а также персоналу, использующим в соответствии с международным правом отличительные эмблемы, установленные Женевскими конвенциями [1949 г.]»[20], является военным преступлением. Если «цифровая эмблема» будет интегрирована в международно-правовую базу, эта норма также обеспечит защиту от кибератак.

Неуполномоченные акторы могут использовать «цифровую эмблему» неправомерным образом или применять ее для совершения вероломных действий

Начиная с первых дней существования отличительных эмблем государства, негосударственные субъекты и отдельные индивидуумы иногда используют их неправомерным образом для ложной симуляции статуса, предоставляющего защиту на основании МГП. Риск такого неправомерного поведения также будет существовать и в контексте действий в среде ИКТ. Любое лицо сможет неправомерным образом использовать «цифровую эмблему» для ложного сообщения о том, что оно подпадает под защиту в соответствии с МГП, с целью избежать нападения (например, за счет хранения военных данных на отмеченном эмблемой сервере или путем осуществления операций через учреждения, использующие эмблему — так, чтобы создать видимость осуществления операций медицинским или гуманитарным учреждением). «Цифровой эмблемой» могут злоупотреблять и для совершения вероломных действий (например, используя эмблему для прикрытия наступательной или преступной операции). Кроме того, в зависимости от технических характеристик решения, которое будет выбрано для разработки потенциальной «цифровой эмблемы», может существовать и техническая возможность ее неправомерного размещения на разнообразных не пользующихся защитой цифровых ресурсах, что поставит под вопрос способность эмблемы обозначать какую-либо защиту. Описанные способы неправомерного использования не только отрицательно скажутся на доверии к «цифровой эмблеме» и ее защитном действии, но и создадут для медицинских и гуманитарных учреждений риск стать целью нападения.

В случаях, когда медицинские учреждения становятся целью кинетических ударов в нарушение МГП или когда медицинский персонал подвергается неправомерному преследованию, использование «цифровой эмблемы» в медицинских устройствах или в массиве медицинских данных может упростить идентификацию и отслеживание медицинских учреждений и медицинского персонала злоумышленниками.

На самом деле, многие из этих факторов риска существуют уже несколько десятилетий, и для их устранения действуют соответствующие нормы МГП и национального законодательства многих государств. Так, согласно национальному законодательству и международному праву использовать отличительные эмблемы разрешается только определенным субъектам (см. раздел 1 выше). Любым другим лицам и организациям это делать запрещено. Кроме того, в соответствии с МГП запрещается убивать, наносить ранения или брать в плен противника, прибегая к вероломству[21]. Неправомерное и вероломное использование эмблемы является военным преступлением[22]. Для предотвращения возможного неправомерного использования эмблемы в среде ИКТ необходимо будет использовать эти правовые основы в качестве опоры

[20] Ст. 8(2)(b)(xxiv) и 8(2)(e)(ii) Римского статута МУС.
[21] МГП определяет вероломство как неправомерное использование отличительной эмблемы, чтобы вызвать доверие противника и заставить его поверить, что он имеет право на защиту или обязан предоставить такую защиту согласно нормам МГП, с целью обмана такого доверия. См. ст. 37(1) Дополнительного протокола I.
[22] См. ст. 8(2)(b) Римского статута МУС.

и соответствующим образом адаптировать их.

«Цифровая эмблема» может создавать ложное ощущение безопасности и защиты или ложное впечатление, что немаркированные субъекты не находятся под защитой

Защита медицинских и гуманитарных организаций от вредоносных кибероперациий в первую очередь требует принятия конкретных мер кибербезопасности. «Цифровая эмблема» служит лишь дополнительной мерой для обозначения правовой защиты и не может заменить собой другие действия по обеспечению кибербезопасности. Это явно следует и из практики использования отличительных эмблем в реальном мире: часто медицинское учреждение или здание, в котором размещается гуманитарная организация, бывает защищено мешками с песком или другими оборонительными приспособлениями, при этом так же будучи отмеченным отличительной эмблемой.

В связи с тем, что обеспечение безопасности в среде ИКТ требует вложения финансовых средств и наличия квалифицированных специалистов, некоторые субъекты могут полагаться исключительно на «цифровую эмблему», пренебрегая другими основными мерами обеспечения безопасности. Такая ситуация являет собой пример создания ложного чувства защищенности или безопасности. Поскольку нельзя исключить, что злонамеренные акторы могут использовать «цифровую эмблему» в целях массового нападения на пользующихся защитой субъектов, ее применение не должно снижать потребность в принятии соответствующих мер обеспечения кибербезопасности.

Для смягчения и устранения данного риска может быть принят ряд мер, например четкое информирование о том, что «цифровая эмблема» создает только *добавочную* пользу; формулирование конкретных рекомендаций относительно того, какие меры кибербезопасности следует принимать вне зависимости от использования эмблемы; а также выдвижение инициатив по наращиванию потенциала медицинских и гуманитарных организаций в области кибербезопасности.

Критически важно подчеркнуть, что отсутствие отличительных эмблем совсем не обязательно указывает на отсутствие статуса, предоставляющего защиту, или говорит о том, что субъект не пользуется особой защитой в соответствии с МГП. Кибероператоры могут халатно относиться к выполнению своей обязанности проверять правомерность нападения на цель: определив лишь факт наличия или отсутствия «цифровой эмблемы», они могут ошибочно приравнять отсутствие таковой к отсутствию правовой защиты. Тем не менее этот риск и эта проблема актуальны не только в киберпространстве. В действительности отличительные эмблемы, в том числе, вероятно, и их цифровые версии, могут лишь *отражать* или *обозначать* особую правовую защиту, а не служить ее источником. Статус, предоставляющий защиту, существует независимо от отображения той или иной эмблемы. Во время вооруженного конфликта нападение на больницу запрещено и будет рассматриваться как военное преступление вне зависимости от того, размещена ли на нем та или иная эмблема; аналогичным образом, запрещено нападать на гражданские здания, которые не являются больницами и, соответственно, не могут использовать какую-либо эмблему. МГП обязывает операторов «дела[ть] все практически возможное, чтобы удостовериться в том, что объекты нападения не являются ни гражданскими лицами, ни гражданскими объектами и не подлежат особой защите, а являются военными объектами»[23].

[23] Ст. 57(2)(a)(i) Дополнительного протокола I.

ОСНОВНЫЕ ПРОБЛЕМЫ ВНЕДРЕНИЯ «ЦИФРОВОЙ ЭМБЛЕМЫ» В ПРАКТИЧЕСКУЮ ДЕЯТЕЛЬНОСТЬ

Цифровые составные части и хранилища данных пользующихся защитой субъектов часто бывают взаимосвязаны с сетями или данными, не находящимися под защитой

В среде ИКТ сетевая инфраструктура и пространство для хранения данных часто находятся в совместном пользовании, и все большее число организаций размещает приложения и данные в облачных сервисах. Подобная ситуация создает ряд потенциальных сложностей для использования «цифровой эмблемы».

Во-первых, в идеальном исполнении «цифровая эмблема» должна давать возможность маркировать данные находящихся под защитой субъектов (и только их) в совместно используемых хранилищах, таких как облачные сервисы. Это позволит оператору исключить отмеченные эмблемой приложения или данные из целей нападения или соответствующим образом изменить код вредоносного программного обеспечения. При этом «цифровую эмблему» не следует использовать для маркировки всего облачного хранилища или сервера как находящегося под защитой (так как в обоих расположениях или в одном из них могут также быть размещены военные данные, которые потенциально превращают такие расположения в правомерные военные цели), за исключением случаев, когда такое хранилище или сервер эксплуатируются только в медицинских или гуманитарных целях. Неизбирательное использование эмблемы, при котором подобное разграничение невозможно, может привести к ослаблению обозначаемой ею защиты.

Внедрение «цифровой эмблемы» потребует принятия мер по установлению атмосферы доверия вокруг нее. Если «цифровая эмблема» будет использоваться неправомерно — или технология ее отображения будет скомпрометирована, — это может подорвать доверие, которое является фундаментом всей концепции. Для того чтобы обеспечить доверие к любой «цифровой эмблеме», ее следует разрабатывать с соблюдением принципов нейтральности и прозрачности, возможно на основе ПО с открытым исходным кодом, которое можно безопасно и просто проверить. Кроме того, порядок использования эмблемы должен быть законодательно регламентирован, а неправомерное использование должно наказываться.

Операционные системы некоторых медицинских устройств не подлежат модификации

«Цифровая эмблема» будет предназначаться для маркировки широкого спектра цифровых ресурсов, сервисов и данных, принадлежащих пользующимся защитой субъектам. В этом отношении медицинские устройства являются источником значительных сложностей. Многие медицинские устройства функционируют на основе программного обеспечения с закрытым исходным кодом, просмотреть или модифицировать который невозможно, будь то в силу *физических причин* (то есть к их программной части нельзя получить доступ), *нормативных причин* (то есть существуют ограничения, обусловленные обеспечением соответствия, сертификацией или лицензированием, которые не оставляют возможности для какой-либо модификации) или *аспектов безопасности* (для безопасной модификации такого оборудования требуется значительный объем инженерных работ). В связи с этим бывает невозможно непосредственно маркировать такие устройства «цифровой эмблемой», а значит, по состоянию на сегодняшний день *определенные* технические решения неприменимы для медицинских устройств, относящихся к названным выше категориям.

Решить эту проблему можно несколькими способами, в том числе за счет разработки «цифровой эмблемы», которую не потребуется встраивать в исходный код каждого медицинского устройства, а можно будет использовать на уровне больничной сети (к примеру, через прокси-сервер, связывающий такие устройства), или же за счет

взаимодействия с производителями устройств или органами стандартизации с целью упростить маркировку таких устройств.

«Цифровая эмблема» должна не только отвечать требованиям актуальной технологической среды, но и предусматривать возможность адаптации к перспективной инфраструктуре и технологиям для непрерывной эксплуатации

Технологии развиваются очень быстро, а потому критически важно обеспечить возможность использования «цифровой эмблемы» в будущей сетевой и технологической среде или возможность быстрой адаптации к новым условиям. В настоящее время общепринятым является мнение о том, что в будущем в медицине будут широко использоваться устройства с простой инфраструктурой, такие как компоненты интернета вещей, причем настолько широко, что медицинские и гуманитарные организации не смогут вести надлежащий учет всех используемых ими устройств. Следовательно, «цифровая эмблема» должна обеспечивать возможность одновременно опознать большое число устройств или сетей, например за счет установки на уровне прокси-оборудования и обозначения защиты всех подсоединенных к нему устройств; другими словами, «цифровая эмблема» должна быть применима в крупном масштабе.

Также нельзя забывать о том, что постоянно развивается и инфраструктура сети Интернет. Так, межсетевые протоколы (IP-адреса) в настоящее время переходят с версии IPv4 на версию IPv6. При разработке «цифровой эмблемы» следует учесть прогнозируемые изменения инфраструктуры сети Интернет и обеспечить пригодность эмблемы для использования в будущем.

Обеспечение защитного действия «цифровой эмблемы»

Медицинские и гуманитарные учреждения становятся целями намеренных вредоносных операций (таких как атаки программ-вымогателей и получение несанкционированного доступа к данным) или могут случайно оказаться мишенью вредоносного программного обеспечения, которое распространяется неизбирательно. Для того чтобы предотвращать случайное (ненамеренное) причинение вреда медицинским и гуманитарным субъектам, которые пользуются защитой, «цифровая эмблема» должна быть разработана на основе технического решения, позволяющего кибероператорам с легкостью модифицировать вредоносное ПО так, чтобы оно не причиняло вред субъектам, отмеченным эмблемой.

ГЛАВА 3

ОПЕРАЦИОННЫЕ, ТЕХНИЧЕСКИЕ И ПРАВОВЫЕ ТРЕБОВАНИЯ, КОТОРЫМИ СЛЕДУЕТ РУКОВОДСТВОВАТЬСЯ ПРИ СОЗДАНИИ «ЦИФРОВОЙ ЭМБЛЕМЫ»

Эксперты и ученые подчеркивают, что при создании любой «цифровой эмблемы» необходимо иметь четкий ответ на два вопроса: «Кто будет пользоваться такой эмблемой?» и «Какой вред она призвана предотвратить?». Кроме того, следует надлежащим образом учесть то, какие типы кибероперации обычно имеют место в условиях вооруженного конфликта, и то, какие стратегии и инструменты операторы в основном используют для идентификации целей и нападения на них. Приняв во внимание эти соображения, а также информацию о преимуществах, рисках и проблемах из главы 2, авторы настоящего доклада определили ряд операционных и технических требований в качестве актуальных при создании «цифровой эмблемы». Они были распределены по следующим категориям:

- операционные и технические требования для применения субъектами, пользующимися защитой;
- операционные и технические требования для опознания «цифровой эмблемы» кибероператорами;
- требования относительно подготовки «цифровой эмблемы» и придания ей правового статуса.

Как отмечено выше, эти операционные и технические требования не являются ни исчерпывающими, ни обязательными для разработки пригодного к применению технического решения. Тем не менее в силу того, что они были сформулированы по итогам обсуждения с разнородной группой глобальных экспертов, эти требования разумно будет принять к сведению при проведении любой оценки потенциальных технических решений.

ОПЕРАЦИОННЫЕ И ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ ДЛЯ ПРИМЕНЕНИЯ «ЦИФРОВОЙ ЭМБЛЕМЫ» СУБЪЕКТАМИ, ПОЛЬЗУЮЩИМИСЯ ЗАЩИТОЙ

Подавляющее большинство экспертов сошлись во мнении о том, что, если «цифровая эмблема» будет разработана, ее должно быть просто размещать, удалять и должным образом обслуживать. Это требование тесно связано с базовым условием — «цифровая эмблема» может обозначать защиту только в том случае, когда используется уполномоченными медицинскими и гуманитарными субъектами.

Простота размещения, удаления и обслуживания пользующимися защитой субъектами

Медицинские и гуманитарные операции в ходе вооруженного конфликта отличаются высокой сложностью, зачастую осуществляются быстро, в условиях ограниченных ресурсов и при наличии лишь базовой инфраструктуры. Кроме того, поддержка посредством ИКТ во время вооруженного конфликта чаще всего бывает ограничена, а оказывающие ее лица

располагают минимальным объемом ресурсов. Инфраструктура обычно создается стихийно и временно и может быть устаревшей, аппаратное обеспечение обычно не соответствует современным стандартам, а поиск ресурсов и управление ими часто бывают осложнены. В связи с тем, что вооруженные конфликты происходят во всех частях мира, также следует ожидать, что уровень знаний и опыта в области работы с ИКТ у местного населения, и в частности среди сотрудников медицинских учреждений и гуманитарных организаций, будет разнородным. Следовательно, размещение и обслуживание «цифровой эмблемы» должно быть низкозатратным, чтобы ее мог использовать широкий круг пользующихся защитой субъектов. Например, если для эксплуатации «цифровой эмблемы» будет необходимо сложное программное обеспечение, которое легко в развертывании, но требует значительного объема неавтоматических работ по обслуживанию, внедрять такое решение нецелесообразно. Обозначенная проблема усугубляется широким масштабом применения сетевых устройств в ходе медицинских и гуманитарных операций, в связи с чем любое решение должно быть легко масштабируемым.

Соответственно, чем более сложна «цифровая эмблема» и чем больше трудностей связано с ее размещением и обслуживанием, тем с меньшей вероятностью ее будут использовать. Поскольку удобство использования в данном случае является залогом успеха, «цифровая эмблема» должна создавать минимальную рабочую нагрузку на операционный персонал. В идеале должна быть возможность размещать «цифровую эмблему» централизованно — из столицы, главного офиса или штаб-квартиры, или же размещение эмблемы требовать лишь минимальных технических знаний от персонала, действующего на местах в районах ведения операций. Кроме того, для ее внедрения по всему миру силами экспертов в области ИКТ, представляющих медицинский и гуманитарный сектор, может потребоваться наращивание потенциала и, возможно, существенная техническая поддержка.

Кроме того, «цифровую эмблему» должно быть просто удалить. Это даст пользующимся защитой субъектам возможность выбирать — ровно так же, как в отношении физической эмблемы, — стоит ли использовать «цифровую эмблему» исходя из развития событий на местах и обстоятельств, в которых действуют эти субъекты. Простота удаления может стать одним из ключей к решению проблемы потенциальных рисков, связанных с использованием «цифровой эмблемы». При этом пользующиеся защитой субъекты должны быть осведомлены о том, что использование эмблемы в прошлом может фиксироваться в записях, а ее удаление может не приводить к исчезновению всех остаточных элементов или записей, содержащих сведения о таком использовании. Эта особенность в значительной степени роднит «цифровую эмблему» с ее физическим аналогом.

Для того, чтобы цифровую эмблему в итоговом исполнении было легче размещать, обслуживать и удалять, в потенциальном техническом решении следует эффективно применить существующие широко распространенные технологии.

«Цифровая эмблема» должна давать возможность обозначать защиту широкого спектра различных устройств

Цифровые ресурсы, данные и коммуникация пользующихся защитой субъектов могут принимать различные формы, опираться на различные типы инфраструктуры и требовать разных технических решений для идентификации и защиты. Таким образом маловероятно, что опора только на какой-либо один способ опознавания пользующихся защитой субъектов, например использование только решения на основе IP-адреса или на файловой основе, позволит сделать реальным опознавание полного спектра ресурсов, принадлежащих пользующимся защитой субъектам.

Для решения этой проблемы может потребоваться сочетание методов опознавания

пользующихся защитой субъектов. Однако это, в свою очередь, создает риск ослабления потенциального защитного действия эмблемы. У операторов не должно возникать сложностей с идентификацией и пониманием значения «цифровой эмблемы»; ее считывание и проверка не должны требовать от них чрезмерных усилий. Если разные решения будут использоваться не параллельно (в одной ситуации — одно, в другой ситуации — другое), появится риск того, что кибероператоры будут действовать, не проверив все возможные «цифровые эмблемы», и, следовательно, могут упустить сигнал о защите.

Кроме того, с учетом большого объема применяемых в медицинском и гуманитарном секторах цифровых (или связанных с цифровой средой) ресурсов, который будет лишь расти, внедрение «цифровой эмблемы» может оказаться нецелесообразным, если ее нужно будет размещать на каждом отдельном ресурсе или устройстве. Должна быть создана возможность внедрить «цифровую эмблему» на уровне сети того или иного пользующегося защитой субъекта. Задействовать такую возможность, однако, следует аккуратно, чтобы гарантировать, что к отмеченной «цифровой эмблемой» сети могут быть подключены только устройства, на которые распространяется особая защита.

«Цифровая эмблема» должна использоваться под контролем компетентного органа власти любой стороны в вооруженном конфликте

Во многих активных вооруженных конфликтах в настоящее время участвуют как государственные, так и негосударственные стороны. У каждой из сторон в определенном конфликте могут быть свои медицинские учреждения, используемые их бойцами или вооруженными силами. Также такие стороны могут управлять иными медицинскими учреждениями, которые находятся под их контролем. В соответствии с МГП, все стороны в вооруженном конфликте в целом могут использовать отличительную эмблему и разрешать ее использование. Следовательно, потенциальное технологическое решение должно быть доступно не только государствам и не должно предусматривать необходимость получать разрешение государства на его использование.

ОПЕРАЦИОННЫЕ И ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ ДЛЯ ОПОЗНАВАНИЯ «ЦИФРОВОЙ ЭМБЛЕМЫ» КИБЕРОПЕРАТОРАМИ

Поскольку обязанность уважать такую эмблему в основном — на практике и в силу необходимости — несут в основном кибероператоры, принадлежащие к той или иной стороне в вооруженном конфликте, обладающие оперативным опытом эксперты отдельно заострили внимание на том, что «цифровая эмблема» должна быть «видимой», а кибероператоры должны ее легко определять и понимать. Поиск «цифровой эмблемы» не должен создавать чрезмерную нагрузку на оператора или приводить к его идентификации как потенциального исполнителя нападения.

«Цифровая эмблема» должна быть «видимой», и лица, осуществляющие операции в киберпространстве, должны ее легко определять и понимать

Предназначение «цифровой эмблемы» — сигнализировать кибероператорам — иногда в условиях активного противостояния или в «тумане войны» — о том, что определенные субъекты пользуются особой защитой в соответствии с МГП и не должны становится целью нападения. Следовательно, такая эмблема должна быть максимально заметной, чтобы кибероператоры или вредоносное программное обеспечение, которое они используют, легко могли ее опознать.

Для этого «цифровая эмблема», как и ее физический аналог, должна быть:

- однозначной и легко заметной, чтобы кибероператорам не требовался большой объем времени и усилий для ее идентификации или создания

у вредоносного ПО функционала идентификации и предотвращения нападения на объекты с «цифровой эмблемой». В идеале она должна располагаться в том месте или процессе, которые любой оператор (или вредоносное ПО) всегда проверяет при совершении соответствующих кибероперациий, то есть не создавать дополнительный объем работы оператору, желающему проверить наличие или отсутствие «цифровой эмблемы». Один из возможных вариантов — отображать «цифровую эмблему» в перечне процессов, чтобы оператор, проверяя активные процессы, мог ее увидеть;

- легко обнаруживаемой с помощью киберинструментов (вредоносного ПО, скрипта) так, чтобы программисты могли исключить отмеченные ею организации из перечня допустимых целей, например путем создания «белого списка» защищенных IP-адресов или указания конкретного имени процесса в качестве исключения;
- однозначно распознаваемой — «цифровая эмблема» не должна затеряться в огромном потоке данных, которые циркулируют в интернете. Она должна быть разработана таким образом, чтобы операторы не могли заявить, что не заметили ее;
- легко понятной, то есть способной передать обнаружившему ее оператору необходимый сигнал независимо от того, на каком языке говорит и какими культурно-географическими характеристиками обладает оператор.

«Цифровая эмблема» должна вызывать доверие. У кибероператоров и представителей органов власти должна быть возможность проверить подлинность «цифровой эмблемы»

В контексте риска того, что «цифровая эмблема» может неправомерно использоваться для ложной маркировки субъектов, которые по сути своей являются военными или не имеют полномочий для демонстрации отличительной эмблемы по каким-либо другим причинам, а также в целях поддержания доверия к эмблеме, важно обеспечить кибероператорам возможность проверять подлинность «цифровой эмблемы». Для проверки подлинности и поддержания доверия к эмблеме можно применить ряд различных технологических решений, среди которых:

- разрешение на использование эмблемы априори со стороны соответствующего органа. Данный вариант будет целесообразен, например, в случае, когда используется решение на основе IP-адреса. В такой ситуации пользующийся защитой субъект должен запросить и получить от соответствующего органа номер IP-адреса, который будет сигнализировать о защите (подробнее см. в разделах глав 4 и 2, где говорится об эмблемах на основе IP-адреса и системы доменных имен (DNS));
- система сертификации и удостоверения, с помощью которой пользующиеся защитой субъекты будут обозначать свой статус посредством сертификатов, утвержденных авторитетным органом, например национальным или международным органом власти (см. информацию об АЦЭ в главе 4 и приложении 3). Для предотвращения подделки сертификатов или утечки личных ключей можно рассмотреть возможность использования различных технических решений, таких как краткосрочные сертификаты или система отзыва сертификатов.

Как подчеркивается ниже, такая процедура проверки должна быть простой и не должна приводить к тому, что пользующийся защитой субъект идентифицирует оператора как источник потенциальной угрозы.

Проверка наличия «цифровой эмблемы» не должна приводить к идентификации кибероператора как источника потенциальной угрозы

Кибероператоры будут готовы проверять наличие «цифровой эмблемы» в ходе разведывательных операций только в том случае, если это не приведет к идентификации их как источников потенциальной угрозы. Другими словами, если кибероператоры сочтут, что

проверка «цифровой эмблемы» приведет к их «обнаружению» (идентификации), они не будут проверять наличие или подлинность эмблемы. Риск такого «обнаружения» становится особенно высоким, если для подтверждения наличия «цифровой эмблемы» оператору нужно отправить запрос на получение конкретного файла. «Цифровую эмблему» также нельзя применять как приманку[24]: проверка наличия эмблемы не должна приводить к отрицательным последствиям для законопослушного актора.

Одним из способов решения данной проблемы может стать включение «цифровой эмблемы» в стандартную информацию, запрашиваемую настолько часто, что проверка «цифровой эмблемы» не вызовет подозрения у пользующегося защитой субъекта. Кроме того, при использовании решений на основе IP или DNS можно организовать проверку принадлежности доменного имени или IP-адреса пользующемуся защитой субъекту с помощью предоставляемого нейтральной третьей стороной перечня, который может открыть и проверить любое лицо.

Здесь необходимо напомнить о том, что отличительная эмблема или сигнал, в том числе цифровые, являются гуманитарным знаком, предназначенным для укрепления защиты медицинских и гуманитарных по своему характеру миссий. При том что идентификация исполнителей нападения, определение субъектов операций и обеспечение ответственности за противоправные действия могут вместе и по отдельности повысить уровень соблюдения МГП, содействие этому не входит в цели и задачи отличительной эмблемы.

«Цифровая эмблема» должна быть размещена по периметру или в конечных точках, а также по всей внутренней сети

Будущая «цифровая эмблема» предназначена для предотвращения кибероперaций, направленных против отмеченных ею организаций и субъектов. Кибероперации могут проводиться исключительно на сетевом уровне по периметру объекта нападения, например как в случае распределенной атаки типа «отказ в обслуживании» (DDoS-атака), подразумевающей создание такой нагрузки на ресурсы или пропускную полосу сервера, которая приводит к потере доступа к нему. Для того чтобы предотвратить подобные действия, «цифровую эмблему», обозначающую защиту ресурсов, необходимо разместить так, чтобы она была «видима» даже в том случае, если компьютерная сеть жертвы не взломана. Она должна сообщать оператору или вредоносному ПО информацию о том, что конкретная сеть пользуется защитой, еще до того, как они проникнут в эту сеть.

В ходе кибероперaций также может происходить взлом сетей. Когда оператор проникает в сеть жертвы, он часто действует внутри сети нестандартным образом, чтобы повысить результативность нападения (например, стать администратором и получить возможность более «глубокого» проникновения), или стремится получить доступ к конкретным ресурсам (получить доступ к службе каталогов Active Directory или контроллеру домена). В таком случае «цифровая эмблема» должна быть установлена на конечных точках системы (таких как ноутбуки, настольные компьютеры, виртуальные компьютеры, серверы и т. д.) и распространяться напрямую с них, чтобы обозначать их статус, предоставляющий защиту.

Для того чтобы предотвращать ошибки при идентификации или намеренное причинение

[24] «Приманка» (*англ*. honeypot, буквально — «горшочек с медом») — это механизм компьютерной безопасности, который служит для выявления и отражения попыток получения несанкционированного доступа к информационным системам, а в некоторых случаях — и для активного противодействия таким попыткам. Чаще всего «приманка» представляет собой данные (например, на каком-либо сайте сети), которые выглядят как реальный элемент сайта и содержат сведения или ресурсы, обладающие ценностью для исполнителей нападения, но на самом деле позволяют изолировать, отследить и проанализировать таких субъектов. (Wikipedia: https://en.wikipedia.org/wiki/Honeypot_(computing). В данном случае речь идет о неправомерном использовании «цифровой эмблемы» для выявления потенциальных кибероперaций.

вреда, а также иметь эффект сдерживания, «цифровая эмблема» должна легко определяться кибероператором на ранних этапах, в идеале — на периметре, то есть на внешней границе сети. Это особенно важно в свете того, что бóльшая часть кибероперaций начинается с этапа разведки, который подразумевает, среди прочего, такие мероприятия, как активное изучение или обнаружение сетевой информации, веб-сайтов или потенциальных целей. «Цифровая эмблема» должна обнаруживаться именно на этом этапе. Размещение «цифровой эмблемы» на внешней границе сети, однако, имеет свои недостатки: риск сделать пользующихся защитой субъектов более заметными для злонамеренных акторов в киберпространстве связан в основном с размещением «цифровой эмблемы» по периметру сети, а не внутри нее.

ТРЕБОВАНИЯ ОТНОСИТЕЛЬНО ПОДГОТОВКИ «ЦИФРОВОЙ ЭМБЛЕМЫ» И ПРИДАНИЯ ЕЙ ПРАВОВОГО СТАТУСА

Любое техническое решение по внедрению «цифровой эмблемы» должно пройти тестирование, прежде чем будет реализовано на практике

«Цифровой эмблемы» пока не существует, и, как показывает настоящий доклад, технические решения для реализации этой концепции должны будут соответствовать ряду требований. Вероятно, отыскать решение, которое бы одинаково полно отвечало всем требованиям, невозможно; так, решение, которое чрезвычайно сложно неправомерно использовать, вряд ли будет легко внедрить. Таким образом, особую значимость будут иметь исследование, разработка, тестирование и корректировка потенциальных решений. Очень важно будет оценить результаты такого тестирования в контексте целесообразности применения любого представленного варианта, а также связанных с ним потенциальных преимуществ и рисков (в соответствии с изложенным в главе 2).

Кроме того, в зависимости от характеристик конкретного технического решения, может потребоваться обсуждение эмблемы со специальными органами: например, с Администрацией адресного пространства Интернет (IANA) — по поводу использования выделенных IP-номеров, и с Корпорацией по управлению доменными именами и IP-адресами (ICANN) — по поводу использования выделенных доменов верхнего уровня (таких как *.emblem*).

«Цифровая эмблема» должна стать частью международной правовой базы, чтобы гарантировать ее широкое признание, известность и контроль за соблюдением норм ее использования

Важная характеристика и преимущество существующих отличительных эмблем заключаются в том, что их форма, функция, применение и защита регулируются МГП и внутригосударственным правом. Неправомерное использование отличительных эмблем запрещено и в определенных обстоятельствах уголовно наказуемо как на национальном, так и на международном уровне. Следует ожидать, что при отсутствии системы регулирования и контроля за соблюдением норм использования «цифровая эмблема» будет в меньшей степени известна, а упомянутые нормы будут соблюдаться реже. Соответственно, при создании «цифровой эмблемы» ее необходимо будет интегрировать в существующие международные и национальные правовые нормы, которые регламентируют порядок применения отличительных эмблем и сигналов. Следует обеспечить четкое регулирование и ясность таких аспектов, как круг субъектов, которым разрешается демонстрировать эмблему, допустимые цели ее использования, а также способы предотвращения и пресечения неправомерного использования. Существуют различные варианты соответствующей модификации международно-правовой базы, например:

- **новый Дополнительный протокол к Женевским конвенциям**, который, подобно действующим

нормам относительно отличительных эмблем, мог бы служить для признания «цифровой эмблемы», определения ее формы и технических особенностей, регламентации того, каким субъектам и в каких целях разрешается ее использование, а также для установления границ правомерного использования. Именно такой подход был применен при учреждении эмблемы красного кристалла в 2005 г.[25]; так как принятие нового Дополнительного протокола к Женевским конвенциям должно иметь форму заключения международного договора, его разработка, принятие и ратификация в странах по всему миру потребуют значительной дипломатической работы;

- **пересмотр Приложения I к Дополнительному протоколу I**, в котором определены «правила, касающиеся опознавания», например относительно использования «отличительных сигналов» (световые и радиосигналы, электронное опознавание) или связи (радиосвязь, использование кодов) находящимися под защитой субъектами. При разработке Приложения I к Дополнительному протоколу I государства, среди прочего, учли, что технологическое развитие может обусловить появление или необходимость в создании новых средств опознавания персонала, материалов, формирований, транспортных средств и сооружений, пользующихся защитой в соответствии с Женевскими конвенциями и Дополнительным протоколом I. Внести изменения в Приложение I можно с помощью процедуры, установленной в Дополнительном протоколе I (см. статью 98), что значительно проще принятия нового дополнительного протокола к Женевским конвенциям. Этим способом государства воспользовались в последний раз в 1993 г.;
- **специальные договоренности о «цифровой эмблеме»**: это подразумевает, что государства и, возможно, другие стороны в вооруженном конфликте могут «в любое время договариваться о дополнительных и иных сигналах, средствах и системах, которые могут облегчить опознавание и в полной мере используют технические достижения в этой области»[26]. Такой подход предлагает наибольшую адаптивность и быстроту, но при этом осложняется необходимостью добиваться соглашения между воюющими сторонами по поводу «цифровой эмблемы» после начала вооруженного конфликта и внедрять такую эмблему в условиях активных боевых действий.

После согласования всех характеристик «цифровой эмблемы» для ее успешного внедрения потребуется масштабное распространение соответствующих знаний и наращивание потенциала пользующихся защитой субъектов, имеющих право использовать «цифровой эмблемой», а также операторов, которые должны ее уважать. Нельзя ожидать, что «цифровая эмблема» будет функционировать надлежащим образом, если у упомянутых акторов не будет достаточно четкого понимания ее сути.

[25] См.: Дополнительный протокол к Женевским конвенциям от 12 августа 1949 года, касающийся принятия дополнительной отличительной эмблемы (Протокол III). Женева, 8 декабря 2005 г.
[26] Ст. 1(4) Приложения I к Дополнительному протоколу I.

ГЛАВА 4

ПЕРВИЧНЫЙ АНАЛИЗ ВОЗМОЖНЫХ ТЕХНИЧЕСКИХ РЕШЕНИЙ

На первом этапе реализации проекта «цифровой эмблемы» представители МККК совместно с учеными Центра кибердоверия и Лаборатории прикладной физики Университета Джонса Хопкинса работали над определением технических средств, с помощью которых можно маркировать и идентифицировать цифровые ресурсы, сервисы и данные пользующихся защитой субъектов (более подробную информацию см. в приложениях 2 и 3).

В ходе второго этапа проекта различные технические решения, предложенные Центром кибердоверия и Лабораторией прикладной физики Университета Джонса Хопкинса, были представлены на рассмотрение экспертов — участников консультационного процесса, которые выразили свое мнение о концепции «цифровой эмблемы». Эксперты указали на ряд аспектов относительно каждого технического решения, отметив наличие как преимуществ, так и недостатков, а также подчеркнули необходимость дальнейших исследований и тестирования. При этом подавляющее большинство экспертов сошлись во мнении о том, что лишь комбинация нескольких технических решений с наибольшей вероятностью будет отвечать всем предпочтительным критериям (см. главу 3) и может быть применена ко всем релевантным цифровым ресурсам, сервисам и данным, которыми пользуются медицинские и гуманитарные организации во время вооруженных конфликтов.

Ниже приведены соображения относительно предложенных технических решений, сформулированные по итогам выполненных до настоящего момента исследований и консультаций с экспертами.

Файловая эмблема

Данный вариант исполнения предусматривает размещение «цифровой эмблемы» в конечной точке, такой как широко известный файл, доступ к которому открывается процессам, запускаемым в рамках находящейся под защитой системы. Информирование о наличии статуса, предоставляющего защиту, может обеспечиваться либо просто за счет существования файла, либо с помощью содержащихся в нем общепринятых директив.

В общем случае файловую эмблему будет легко внедрить силами персонала, ответственного за кибербезопасность, в том числе последовательно — от системы к системе. Реализация протокола запроса, который позволит обратить внимание кибероператоров на файловую эмблему, также не представляется сложной задачей.

У данного варианта имеются и недостатки, например необходимость размещать такую эмблему на отдельных ресурсах и устройствах (которых может быть много); кроме того, на некоторых медицинских устройством с ограниченным доступом разместить файловую эмблему будет сложно, а если это все же удастся, то возникнет риск аннулирования сертификации и лицензий, выданных для таких устройств. Наименее сложную версию файловой эмблемы можно относительно легко использовать для неправомерной маркировки

инфраструктуры, которая не пользуется особой защитой. Еще один недостаток заключается в том, что файловая эмблема становится видимой только после того, как оператор проникает внутрь сети, (то есть ее нельзя обнаружить на периметре) и не может быть обнаружена сетями-посредниками (то есть с ее помощью нельзя защитить данные при передаче). Самой серьезной проблемой при эксплуатации файловой эмблемы является ее ограниченная доступность: кибероператорам придется запрашивать данные о наличии эмблемы у каждого узла сети (устройства). Если операторам придется вести активный поиск эмблемы (в конкретном файле или папке) и подвергать себя риску обнаружения после проникновения в сеть, они с меньшей вероятностью будут готовы проверять наличие «цифровой эмблемы». Следовательно, файловая эмблема должна быть максимально заметной.

Примером такого решения может служить файловая эмблема в форме конкретного процесса, который отображается в общем перечне активных процессов и, соответственно, может быть легко идентифицирован без необходимости прерывать операцию[27].

Эмблема, основанная на протоколе DNS

Эмблема на основе протокола DNS может быть реализована в форме специального ярлыка, связанного с доменным именем (например, www.icrc.*emblem*). Поскольку доменное имя ассоциируется исключительно с системами, находящимися под защитой «цифровой эмблемы», в нем будет отражена явная, считываемая «цифровая эмблема», идентифицирующая соответствующую систему.

Одним из явных преимуществ эмблемы, основанной на протоколе DNS, является то, что доменные имена считываются как человеком, так и программами и могут быть легко интегрированы в доступную глобальную инфраструктуру сети Интернет. Основанная на протоколе DNS эмблема будет также чрезвычайно удобна для ИТ-персонала находящихся под защитой субъектов, так как она распространяется на весь домен и ее не нужно размещать на каждом отдельном объекте или ресурсе. Для идентификации объекта через DNS не требуется получение доступа с целью установки или внедрения дополнительного программного обеспечения. Кроме того, очевидная и считываемая человеком эмблема будет легко заметна для оператора на самых ранних этапах контакта с соответствующей системой. В связи с тем, что распределение доменных имен регулируется на глобальном уровне, соответствующую глобальную инфраструктуру также можно использовать для предотвращения неправомерного использования за счет авторизации по принципу априори, если возникнет такая потребность.

При этом для получения основанной на протоколе DNS эмблемы лицо, желающее ее использовать, должно следовать определенной процедуре; потребуется также авторизация со стороны субъектов, не являющихся медицинскими или гуманитарными организациями, которые имеют право пользоваться такой эмблемой. Для создания механизма основанной на протоколе DNS эмблемы потребуется учреждение Корпорацией по управлению доменными именами и IP-адресами (ICANN) нового домена первого уровня с одобрения Администрации адресного пространства Интернет (IANA). Для обеспечения штатной работы данного механизма необходимо будет учредить орган, регулирующий находящиеся под защитой домены верхнего уровня и ответственный за своевременную выдачу разрешений на использование эмблемы соответствующим субъектам с соблюдением принципов беспристрастности и политической нейтральности. У находящихся под защитой субъектов должна быть возможность использовать полученное средство обозначения защиты с помощью DNS, оставаясь доступными по предыдущему адресу.

[27] Подобно тому, как пользователи обычных компьютеров для быстрого и простого отображения запущенных на них программ, фоновых процессов и приложений используют диспетчер задач Windows, кибероператоры применяют аналогичные инструменты, чтобы выяснить, какие процессы запущены на том или ином компьютере.

Потенциальным недостатком эмблемы, основанной на протоколе DNS, является невозможность ее немедленного отзыва. В связи с тем, что DNS осуществляет кэширование данных, домены могут распознаваться локально или через промежуточные распознаватели, то есть не обязательно направлять каждый запрос на полномочный сервер. У результатов такого распознавания есть определенный срок действия («время жизни»). Следовательно, при отзыве эмблемы (конкретного доменного имени) локальные результаты распознавания будут обновлены только в конце цикла обновления, а не немедленно. В этом случае возможно распознавание доменных имен, которые в действительности уже не должны распознаваться. Еще одним важным отрицательным фактором является уровень безопасности при использовании DNS, который, как считается, низок по многим аспектам. Ранее в протоколах DNS не предусматривалось каких-либо механизмов безопасности, однако Инженерный совет Интернета разработал функционал расширений безопасности системы доменного имени (DNSSEC), который опирается на технологию подписания с помощью публичных криптографических ключей. Несмотря на то что DNSSEC не используется повсеместно, крупнейшие поставщики услуг DNS-протоколирования, в том числе Google, AWS и Deutsche Telekom, приняли его на вооружение. DNSSEC обеспечивает защиту от подложных или модифицированных данных DNS, а значит и от вредоносных операций, таких как DNS-спуфинг (DNS spoofing) или «отравление кэша DNS» (DNS-cache poisoning). Таким образом, эмблема, основанная на протоколе DNS, может опираться на недавно разработанный функционал многостороннего подписания. Существует еще один недостаток использования эмблемы, основанной на протоколе DNS: при обмене данными в сети Интернет доменные имена не передаются, и системы-посредники не запрашивают DNS при перенаправлении трафика.

Эмблема, основанная на IP-адресе

Для внедрения эмблемы в таком исполнении потребуется интегрировать в IP-адрес семантические элементы, которые позволят идентифицировать как находящиеся под защитой цифровые ресурсы, так и для защищенные сообщения, передаваемые по сети. В таком случае системы, размещенные в любом месте сети Интернет, будут способны определить, связаны ли проверяемые ими системы или сообщения, передаваемые по сети, с конкретной защищенной стороной. В структуре эмблемы, основанной на сетевом адресе, могут использоваться протоколы IPv4, IPv6, специальный порт или другие элементы.

Эмблема, основанная на IP-адресе, обеспечивает простоту обнаружения как на уровне узлов (посредством ПО), так и на уровне сети (посредством роутера). С ее помощью можно идентифицировать передаваемые ресурсы и данные (то есть сообщения). Поскольку IP-адреса назначаются через глобальную систему, для предотвращения неправомерного использования эмблемы такого типа можно использовать потенциал этой системы. Основанная на IP-адресе эмблема выгодно отличается тем, что кибероператорам будет несложно направить запрос о ее наличии, ведь они в любом случае проверяют IP-адреса. Следовательно, чтобы упростить внедрение «цифровой эмблемы» и способствовать проявлению уважения к ней со стороны кибероператоров, можно прибегнуть к выделенным субсетям.

Эмблема, основанная на IP-адресе, будет функционировать в рамках уже существующей системы, которая назначает IP-адреса; этим она схожа с эмблемой, основанной на протоколе DNS. После создания выделенного диапазона IP-номеров следует заняться учреждением организации, которая будет ответственна за своевременную выдачу разрешений на использование эмблемы соответствующим субъектам с соблюдением принципов беспристрастности и политической нейтральности. Как только ответственной организации станет известно, что находившийся под особой защитой субъект утратил свой статус

защищаемого лица или что эмблема была использована неправомерно, трафик такого субъекта перестанет направляться через выделенный диапазон IP-номеров. Обычно такие изменения вступают в силу в течение 24 часов.

Неясным остается то, как IP-адреса будут распределяться в среде, где они не обязательно принадлежат конечной точке (например, в случае если у множества устройств один IP-адрес, как в механизме преобразования сетевых адресов (NAT) или в мобильной сети). Еще одним недостатком является то, что на одном сетевом адресе потенциально могут быть размещены как пользующиеся, так и не пользующиеся защитой сервисы. Значит, для IP-диапазонов, которые выделены для обозначения юридической защиты (то есть для «цифровой эмблемы»), следует ввести следующее ограничение: пользовательский доступ к ним должны иметь исключительно находящиеся под защитой субъекты. Процесс интеграции семантических элементов в IP-адреса в масштабах всемирной сети будет сложным и не обойдется без полемики.

Аутентифицируемая цифровая эмблема (АЦЭ)

Данное решение основывается на распределенной технологии с использованием цепочек сертификатов. Для того чтобы учесть разные сценарии внедрения, в механизме АЦЭ предусмотрено три уровня эмблем:

- «самоподписанные эмблемы» привязаны к публичным ключам и могут генерироваться любым субъектом;
- «эмблемы организаций» — то есть самоподписанные эмблемы, которые привязаны к реально существующим организациям, идентифицируемым по доменному имени;
- «удостоверенные эмблемы» — то есть эмблемы с более высоким уровнем аутентификации, который достигается путем их удостоверения сторонними регуляторами.

Данное решение предусматривает дистрибуцию «цифровой эмблемы» тремя способами, что позволяет охватить широкий спектр ситуаций использования и упростить идентификацию: протокол DNS применяется для маркировки публичных сетевых субъектов с именем; протокол защиты транспортного уровня (TLS) — для конфиденциальных сетевых соединений; протокол межсетевых управляющих сообщений (ICMP) — для сетевых субъектов и ресурсов без имени и для пассивных наблюдателей сетевых соединений.

Многие эксперты оценили механизм функционирования АЦЭ как детально проработанный и соответствующий критериям «цифровой эмблемы». Он обеспечит возможность широкого распространения со стороны пользователей и сделает опознавание максимально простым для операторов. Кроме того, различные уровни аутентификации позволят создать систему, которая обеспечит доверие как минимум к эмблемам организаций и удостоверенным эмблемам.

У каждого из способов распределения АЦЭ (DNS, TLS и ICMP) есть свои сильные и слабые стороны. Информация о сильных и слабых сторонах протокола DNS приведена выше. Дистрибуция АЦЭ посредством TLS может оказаться эффективной, поскольку во многих протоколах уровня приложений, таких как HTTPS, данные обычно передаются поверх TLS, и это позволяет транслировать эмблему. Реализация решения с применением TLS, однако, является относительно сложной задачей. Распределение эмблемы может осуществляться через специально созданные расширения TLS. Потенциальным эмитентам придется адаптировать свои TLS-серверы для того, чтобы обеспечить распределение эмблем. При этом для проверки таких эмблем TLS-клиенты также необходимо адаптировать, в результате чего данный вариант становится более сложным в сравнении с распределением с помощью DNS или ICMP — для них можно использовать независимые клиенты. Еще один проблемный аспект применения TLS — добавление расширений в тех случаях, когда пользующийся защитой субъект не является владельцем TLS-сервера. АЦЭ может передаваться и через другие протоколы, такие как ICMP. Информация, передаваемая по ICMP, по определению

является второстепенной, поэтому этот протокол не гарантирует надежность. Следовательно, если необходима гарантия доставки, субъекты нельзя маркировать только посредством ICMP. Тем не менее доставленный через ICMP сертификат обеспечивает аутентификацию и может предотвратить вредоносные кибероперации или уменьшить их масштаб. Дистрибуция с помощью файлов также имеет свои преимущества и недостатки; они описаны выше в том разделе, где идет речь о файловой эмблеме. С учетом преимуществ и недостатков, которыми обладают различные способы дистрибуции, будет целесообразно решение, сочетающее разные способы распространения эмблемы.

Механизм АЦЭ также предусматривает иерархию аутентификации с помощью сертификатов различного уровня, которые обеспечивают различную степень доверия. На практике даже малые организации с ограниченным потенциалом способны генерировать самоподписанные сертификаты и тем самым сигнализировать о своем статусе стороны, находящейся под защитой. Однако проверить подлинность таких самоподписанных эмблем будет сложно. Лица, которым потребуется проверить ту или иную эмблему, смогут выбрать, какому регулятору эмблем доверять (то есть считать ли достоверными самоподписанные эмблемы, эмблемы организаций или только эмблемы, удостоверенные органом, которому они доверяют). Поскольку «удостоверенные» эмблемы обеспечивают наиболее высокий уровень доверия, медицинское учреждение или аффилированный с Движением субъект, находящийся в ситуации вооруженного конфликта, должен добиться удостоверения эмблемы от релевантного (иногда де факто) регулятора в такой стране (или, среди прочего, на территории, находящейся под фактическим контролем негосударственной вооруженной группы), от других сторон в конфликте или иных авторитетных регуляторов (таких как международные организации, признанные всеми сторонами). В случае если регуляторы не удостоверяют подлинность действительных сертификатов находящихся под защитой субъектов по политическим причинам, повысить уровень доверия к статусу таких субъектов может удостоверение со стороны других авторитетных акторов, в том числе негосударственных.

Поскольку механизмом функционирования АЦЭ предусмотрены удостоверительные записи, злоупотребление эмблемой может происходить в форме выпуска поддельных сертификатов. Для того чтобы симулировать выпуск таких удостоверительных записей национальными регуляторами или международными организациями, исполнителю нападения придется взломать системы таких регуляторов и выпустить сертификаты от их имени. Проведение подобных кибероперациий, в том числе против сертифицирующих органов, является известным фактом[28]. Следовательно, следует создать децентрализованную систему отзыва, которая позволит объявлять недействительными сертификаты, выпущенные ненадлежащим образом.

Еще один повод для беспокойства — риск того, что злонамеренные операторы смогут взломать механизм АЦЭ и неправомерно его использовать. Тем не менее осуществить такую операцию будет крайне сложно, а масштаб взлома АЦЭ можно ограничить с помощью уже созданных технических решений. Представим, что в рамках операции против находящегося под защитой субъекта задачей нападающей стороны является получение непубличного ключа такого субъекта. Этот ключ затем планируется использовать, чтобы выпустить эмблему для субъекта, не имеющего права на использование «цифровой эмблемы», например для правомерной военной цели. Нейтрализовать такую угрозу можно, ограничив использование определенных ключей путем их привязки к конкретным IP-адресам: таким образом, даже если злоумышленнику удастся похитить ключ, применить его он сможет лишь в комбинации с IP-адресами субъекта, находящегося под защитой.

[28] Примерами подобных операций могут служить взломы центров сертификации DigiNotar и Comodo.

ГЛАВА 5

ОСНОВНЫЕ ВЫВОДЫ И ВОЗМОЖНЫЕ ДАЛЬНЕЙШИЕ ШАГИ

Обязанность уважать и защищать медицинский персонал и медицинские учреждения — это одна из старейших кодифицированных норм МГП. Поскольку в современных вооруженных конфликтах кибероперации проводятся все чаще, и данная тенденция будет лишь усиливаться, необходимость обеспечивать медицинским и гуманитарным организациям защиту от кибероперациий с каждым днем становится все более острой.

Универсального средства, которое во всех случаях гарантировало бы надежную защиту в среде ИКТ, не существует, но исследования и консультации продемонстрировали, что над идеей «цифровой эмблемы» стоит продолжить работу.

Основываясь на результатах исследований, проведенных Лабораторией прикладной физики Университета Джонса Хопкинса и Центром кибердоверия, а также на серии консультаций с многопрофильной группой экспертов из разных стран мира, МККК пришел к следующим основным выводам:

по мнению большинства опрошенных экспертов, ожидаемые преимущества перевешивают риски.

- «Цифровая эмблема» позволит кибероператорам легче определить пользующиеся защитой объекты и обезопасить их от нападения благодаря визуализации и практическому применению правовых мер, обеспечивающих защиту в среде ИКТ и в условиях активного ведения боевых действий (в «тумане войны»). Такая эмблема в первую очередь усилит защиту обозначенных объектов от риска причинения вреда законопослушными операторами, а также может оказать сдерживающее воздействие на злоумышленников.
- В то же время цифровая маркировка, позволяющая идентифицировать медицинские и гуманитарные организации, рискует сделать их более подверженными вредоносным операциям. Уровень такого риска будет зависеть от ситуации. Как обладающие большим опытом, так и не располагающие значительными возможностями операторы уже могут с легкостью идентифицировать медицинские или гуманитарные организации в киберпространстве; дополнительный риск облегчения им нападения на отмеченные соответствующим образом организации может быть относительно небольшим. Однако использование «цифровой эмблемы» может сделать их более желанными мишенями кибероперациий со стороны менее искушенных кибероператоров, которые в противном случае не смогли бы так легко их идентифицировать.
- Другой риск заключается в потенциальном неправомерном использовании «цифровой эмблемы» для ложного обозначения военной или иной инфраструктуры, не пользующейся защитой. Такой риск существует и в материальном мире, а неправомерное использование эмблемы запрещено национальным законодательством в разных странах по всему миру. Специфический риск в

киберпространстве, который может привести к новым проблемам, связан со скоростью, масштабом и охватом, характерными для среды ИКТ, что может породить новые виды вредоносных операций или привести к более тяжелым последствиям их осуществления.

- Для того чтобы обеспечить надлежащее применение, а также предупреждать и преследовать неправомерное использование, «цифровая эмблема» должна иметь правовое обоснование, а соблюдение необходимых правовых норм должно контролироваться соответствующими органами власти.

Подавляющее большинство экспертов сошлись во мнении о том, что, если «цифровая эмблема» будет разработана, ее должно быть просто размещать, удалять и должным образом обслуживать.

- Размещение «цифровой эмблемы» должно быть простым, а обслуживание — недорогим. Ее использование и обслуживание должно требовать минимальных ресурсов в различных регионах мира, пострадавших от вооруженных конфликтов, при этом языковые, технологические и культурные барьеры не должны служить препятствием.
- Чтобы «цифровую эмблему» можно было использовать, она должна предполагать возможность встраивания в существующую технологическую среду, а также обладать способностью отмечать различные виды ресурсов, сервисов и данных. «Цифровую эмблему» должно быть просто удалить, так как это крайне важно в свете возможных рисков в области безопасности. Кроме того, должна быть предусмотрена возможность адаптировать ее в соответствии с будущими технологическими и инфраструктурными изменениями. Например, будет важно найти технологическое решение, которое бы позволило отмечать защищенные данные в облаке.
- «Цифровая эмблема» должна использоваться под контролем компетентного органа власти любой стороны в вооруженном конфликте.

«Цифровая эмблема» должна быть «видимой», и лица, осуществляющие операции в киберпространстве, должны ее легко определять и понимать.

- Кибероператор должен иметь возможность легко определять наличие «цифровой эмблемы». Поиск и понимание «цифровой эмблемы» не должны вызывать у него трудностей.
- В идеале «цифровая эмблема» должна быть частью информации, которую у системы может запросить любой кибероператор. Она должна быть видима на раннем этапе операции и должна недвусмысленным образом обозначать защиту.
- Должна быть возможность легко проверить подлинность «цифровой эмблемы». Это крайне важно для обеспечения того, чтобы такая эмблема пользовалась доверием и уважением.

В конечном счете наиболее явным показателем любой «цифровой эмблемы» или другого сигнала о защите станет то, будут ли пользующиеся защитой субъекты применять такую эмблему на практике для маркировки своих ресурсов, сервисов и данных, ожидая что стороны в вооруженных конфликтах отнесутся к ней с уважением и что это повысит уровень безопасности. Поскольку использование «цифровой эмблемы» не обязательно, пользующиеся защитой субъекты должны самостоятельно решить, необходима ли она им. Это решение будет приниматься с учетом, кроме прочего, результатов оценки того, будут ли в конкретных условиях ожидаемые преимущества, возникающие при использовании «цифровой эмблемы», перевешивать потенциальные риски в контексте безопасности.

ПЕРСПЕКТИВЫ

Руководствуясь данными, полученными по итогам исследований и консультаций в рамках этого проекта, в основном положительными отзывами международной группы экспертов и единогласным призывом со стороны членов Движения Красного Креста и Красного Полумесяца «продолжать изучение технической возможности создания „цифровой эмблемы" и оценить преимущества такой эмблемы»[29], МККК продолжит исследовательскую и консультационную работу в контексте потенциальной «цифровой эмблемы». Такая работа будет выражаться в дальнейшем осуществлении комплекса мер: от технической разработки, валидации и верификации потенциальных решений (в частности, предложенных Лабораторией прикладной физики Университета Джонса Хопкинса и CECYT) до консультаций со всеми соответствующими заинтересованными сторонами — особенно с государствами, национальными обществами Красного Креста и Красного Полумесяца (национальные общества) и интернет-организациями.

[29] См.: Council of Delegates of the International Red Cross and Red Crescent Movement, Safeguarding Humanitarian Data (resolution), CD/22/R12.

ПРИЛОЖЕНИЕ 1

ПЕРЕЧЕНЬ ЭКСПЕРТОВ, С КОТОРЫМИ БЫЛИ ПРОВЕДЕНЫ КОНСУЛЬТАЦИИ В РАМКАХ ПРОЕКТА

ГЛОБАЛЬНАЯ ГРУППА ЭКСПЕРТОВ

ЭКСПЕРТЫ ПРИНИМАЛИ УЧАСТИЕ В РАБОТЕ ГРУППЫ В КАЧЕСТВЕ ЧАСТНЫХ ЛИЦ. ДЛЯ КАЖДОГО ИЗ ЭКСПЕРТОВ УКАЗАНА ПРОФЕССИОНАЛЬНАЯ ПРИНАДЛЕЖНОСТЬ ПО СОСТОЯНИЮ НА МОМЕНТ ПРОВЕДЕНИЯ КОНСУЛЬТАЦИЙ
ИНФОРМАЦИЯ ПРИВЕДЕНА ИСКЛЮЧИТЕЛЬНО В ЦЕЛЯХ ИДЕНТИФИКАЦИИ И НЕ ОЗНАЧАЕТ КАКОГО-ЛИБО ОДОБРЕНИЯ СО СТОРОНЫ УЧРЕЖДЕНИЙ, В КОТОРЫХ РАБОТАЮТ ЭКСПЕРТЫ

- **Абдулхаким Аджиджола**, председатель группы киберэкспертов Африканского союза, Нигерия
- **Рафаэль Арруас**, исследователь в области безопасности, Швейцария
- **Марк Барвински**, глобальный директор по кибероперациям, UBS, Швейцария
- **майор Гордон Бум**, ранее прикомандированный к Киберкомандованию ВС США, ВВС США, Соединенные Штаты Америки
- **Йонатан Бауман**, врач и исследователь в области безопасности, Нидерланды
- **Франк Калькавеккья**, специалист по информационной безопасности, Университетские больницы Женевы, Швейцария
- **Ник Карр**, глава отдела изучения киберпреступности, Microsoft, Соединенные Штаты Америки
- **Жасмин Крауфёрд-Хилл**, научный сотрудник по перспективным технологиям**,** Институт 3Ai/Центр оборонных исследований, Австралийский колледж обороны, Австралия
- **Олег Демидов**, консультант по глобальному управлению интернетом и кибербезопасности, ПИР-центр, Россия
- **Тамаш Фёльдеши**, старший специалист по безопасности, политике и качеству информации, Международная Федерация обществ Красного Креста и Красного Полумесяца, Швейцария
- **Тома Грендорж,** консультант по правовому регулированию киберпространства, Киберкомандование ВС Франции, Франция
- **Анастасия Казакова**, старший менеджер по связям с государственными органами, «Лаборатория Касперского», Россия
- **Элизабет Колэйд**, аналитик в области безопасности, Управление космической обороны, Нигерия
- **Виктория Коржук**, доцент Университета ИТМО, Россия
- **Марина Кротофил**, ответственная за разработку продукта в области кибербезопасности, Платформа интернета вещей: объединенные сетевой инфраструктурой суда, терминалы и склады, A.P. Moller, Maersk, Соединенное Королевство
- **Винит Кумар**, президент, Cyber Peace Foundation, Индия
- **Квок-Ян Лам**, профессор факультета информатики и инженерии, заместитель проректора (по вопросам стратегии и сотрудничества), Наньянский технологический

университет, Сингапур

- **Викас Махаджан**, старший специалист по информационной безопасности, Американский Красный Крест
- **Муслим Меджлумов**, директор блока управляемых сервисов, BI.ZONE, Россия
- **Елена Милошевич**, медсестра и участница сообщества I am the Cavalry, Нидерланды
- **Виктор Минин**, председатель правления Ассоциации руководителей служб информационной безопасности, Россия
- **Д-р Дай Мочинага,** старший научный сотрудник Исследовательского института Кейо, аналитик Координационного центра JPCERT и преподаватель Университета Чуо
- **Адриен Оже**, старший специалист по операциям, Институт кибермира, Швейцария
- **Кеннет Окереафор**, заместитель генерального директора по ИКТ, руководитель по безопасности баз данных и приложений, Национальная система медицинского страхования, Нигерия
- **Фолейк Олагунджу**, программный специалист в области интернета и кибербезопасности, Экономическое сообщество западноафриканских государств, Нигерия
- **Арина Пазушко**, руководитель направления развития бренда и менеджер по международным отношениям, BI.ZONE, Россия
- **Чжан Пэн**, старший научный сотрудник, Центр международного верховенства права в киберпространстве, Пекинский педагогический университет, Китай
- **Найджел Фэйр**, директор по предпринимательской деятельности, Институт кибербезопасности при Университете Нового Южного Уэльса, Австралия
- **Профессор Павел Пилюгин**, старший научный сотрудник Центра проблем информационной безопасности, Факультет вычислительной математики и кибернетики Московского государственного университета имени М. В. Ломоносова, Россия
- **Костин Райу**, директор Глобального центра исследований и анализа, «Лаборатория Касперского», Румыния
- **Тимо Шлесс**, Whiteflag Foundation, подполковник Королевских военно-воздушных сил Нидерландов; международный научный сотрудник, Колледж информации и киберпространства, Национальный университет обороны, Соединенные Штаты Америки
- **Олег Шакиров**, старший эксперт Центра перспективных управленческих решений, Россия
- **Элли Шами**, руководящий специалист по автоматизации и руководитель проектов в области кибербезопасности, Konfidas, Израиль
- **Рон Шамир**, Центр исследований в области кибербезопасности имени Федермана — Программа изучения права в киберпространстве, Еврейский университет в Иерусалиме
- **Челси Слак**, заместитель руководителя по вопросам кибероборонны, отдел новых проблем безопасности, НАТО, Бельгия
- **Тимо Стеффенс**, автор книги «Определение источников высокотехнологичных постоянных угроз» (*Attribution of Advanced Persistent Threats*), Германия
- **Викрам Такур**, технический директор, Symantec, Соединенные Штаты Америки
- **Антти Тикканен**, инженер безопасности, Snap Inc., Швейцария
- **Д-р Фитри Бинтанг Тимур**, научный сотрудник Центра стратегических и международных исследований, Индонезия
- **Анн Трико**, директор по международным связям, Национальное агентство по безопасности информационных систем, Франция
- **Тарик Тваха**, руководитель по вопросам информации, коммуникации и технологий, Кенийскиое общество Красного Креста, Кения
- **Фил Уиттакер**, руководитель по информационной безопасности, Британский Красный Крест, Соединенное Королевство
- **Маркус Уиллет**, старший консультант по кибернетике, Международный институт стратегических исследований, Соединенное Королевство
- **Д-р Данил Заколдаев**, декан факультета безопасности информационных технологий Университета ИТМО, Россия

ЭКСПЕРТЫ — ПРЕДСТАВИТЕЛИ ПАРТНЕРСКИХ ИССЛЕДОВАТЕЛЬСКИХ УЧРЕЖДЕНИЙ

ЦЕНТР КИБЕРДОВЕРИЯ (ЦЮРИХСКИЙ ТЕХНОЛОГИЧЕСКИЙ ИНСТИТУТ И БОННСКИЙ УНИВЕРСИТЕТ)

- **Д-р Дэвид Бейсин**, профессор кафедры информатики Цюрихского технологического университета
- **Лиза Гайерхас**, Институт информатики Боннского университета
- **Максимилиан Гэринг**, Институт информатики Боннского университета
- **Д-р Дэннис Джексон**, независимый эксперт
- **Феликс Э. Линкер**, кафедра информатики Цюрихского технологического университета
- **Михаэль Лиский**, кафедра информатики Цюрихского технологического университета
- **Д-р Адриан Перриг**, профессор кафедры информатики Цюрихского технологического университета
- **д-р Мэттью Смит,** профессор информатики, Институт информатики Боннского университета и Институт связи, обработки информации и эргономики Фраунгофера (Fraunhofer FKIE)

ЛАБОРАТОРИЯ ПРИКЛАДНОЙ ФИЗИКИ УНИВЕРСИТЕТА ДЖОНСА ХОПКИНСА

- **Эрин Хан**, старший научный сотрудник, Лаборатория прикладной физики Университета Джонса Хопкинса
- **Д-р Антонио де Симоне**, старший научный сотрудник, Лаборатория прикладной физики Университета Джонса Хопкинса
- **Д-р Брайан Хаберман**, старший научный сотрудник, Лаборатория прикладной физики Университета Джонса Хопкинса

ЭКСПЕРТЫ МККК И АВСТРАЛИЙСКОГО КРАСНОГО КРЕСТА

- **Лоран Жизель**, глава отдела по вооружениям и ведению боевых действий, штаб-квартира МККК
- **Венсан Граф Нарбель**, советник по стратегическим технологиям, штаб-квартира МККК
- **Стефан Хэнкинс**, юридический советник, штаб-квартира МККК
- **Джонатан Хоровитц**, юридический советник, делегация МККК в Вашингтоне, округ Колумбия, Соединенные Штаты Америки
- **Холли Джонстон**, юридический советник, Австралийский Красный Крест
- **Фабрис Лопер**, технический советник, штаб-квартира МККК
- **Седрик Мэр**, советник по цифровым технологиям, штаб-квартира МККК
- **Ларри Мэйби**, юридический советник, Австралийский Красный Крест
- **Тильман Роденхойзер**, юридический советник, штаб-квартира МККК
- **Лоренцо Редалье**, глава отдела по вопросам гуманитарной политики, делегация МККК в Москве, Россия
- **Виталий Савенков**, советник по вопросам гуманитарной политики, делегация МККК в Москве
- **Бертран Стивале**, эксперт по безопасности ИКТ, штаб-квартира МККК
- **Мауро Виньяти,** советник по новым цифровым технологиям ведения войны, штаб-квартира МККК
- **Дельфина ван Золинге**, советник по вопросам цифровых угроз, штаб-квартира МККК

ПРИЛОЖЕНИЕ 2

ТЕХНИЧЕСКИЕ РЕШЕНИЯ, ПРЕДСТАВЛЕННЫЕ ЛАБОРАТОРИЕЙ ПРИКЛАДНОЙ ФИЗИКИ УНИВЕРСИТЕТА ДЖОНСА ХОПКИНСА

ТЕХНИЧЕСКИЕ ПОДХОДЫ К ЗАЩИТЕ ЦИФРОВЫХ РЕСУРСОВ И ИНТЕРНЕТ-КОММУНИКАЦИЙ ВО ВРЕМЯ КОНФЛИКТА

Существует множество примеров проведения кибероперaций в целях нарушения работы цифровых ресурсов и связи. В киберпространстве действует широкий спектр субъектов — от пранкеров и преступников до государств. Некоторые нападения осуществляются для достижения задач того или иного государства — как в ситуациях, когда вооруженный конфликт отсутствует, например в Египте[30] и Тунисе[31] во время «арабской весны», так и в контексте вооруженного конфликта, как в Сирии[32]. Вредоносное программное обеспечение, такое как WannaCry, NotPetya или Teardrop[33], неизбирательно распространяется по всему миру, затрагивая многие отрасли, а в ряде государств — и медицинские службы.

Техническое решение для маркировки средств связи и цифровых ресурсов — «цифровая эмблема» — даст кибероператорам возможность воздерживаться от нарушения деятельности пользующихся защитой организаций. В данном материале приведены рекомендации относительно критериев оценки технических решений и описаны три подхода к созданию «цифровой эмблемы», предназначенной для обозначения статуса пользующегося защитой субъекта, которую бы узнавали и уважали участники конфликтов, осуществляющие наступательные кибероперации, а также третьи стороны.

СООБРАЖЕНИЯ ОТНОСИТЕЛЬНО РАЗРАБОТКИ ЭМБЛЕМЫ

Оценка технического решения для потенциальной эмблемы может проводиться исходя из набора желаемых критериев. Мы предлагаем оценивать варианты структуры «цифровой эмблемы» на основании следующих критериев:

---

[30] B. Woodcock, “Overview of the Egyptian Internet Shutdown,” February 2011 [онлайн-публикация]: https://www.privacywonk.net/download/Egypt-PCH-Overview.pdf; M. Richtel, “Egypt Cuts Off Most Internet and Cell Service,” The New York Times, 28 January 2011 [онлайн-публикация]: https://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html.

[31] Renesys, “77 networks out in Tunisia” [онлайн-публикация]: http://b2b.renesys.com/ eventsbulletin/2016/11/TN-1479438870.html; M. Elkin, “Tunisia Internet Chief Gives Inside Look at Cyber Uprising,” 28 January 2011 [онлайн-публикация]: https://www.wired.com/2011/01/ as-egypt-tightens-its-internet-grip-tunisia-seeks-to-open-up/

[32] Renesys, “77 networks out in Syria,” 29 November 2012 [онлайн-публикация]: http://b2b.renesys.com/eventsbulletin/2012/11/SY-1354184790.html; Akamai, “State of the Internet @ akamai_soti,” 29 November 2012 [онлайн-публикация]: https://twitter.com/akamai_soti/status/274163048263057408

[33] Teardrop — одна из разновидностей вредоносного ПО, использованная для взлома продукта Orion в ходе кибернападения на компанию SolarWinds [12].

- объем логистической и операционной нагрузки на МККК и компетентные органы власти, которые будут регулировать использование эмблемы;
- объем логистической и операционной нагрузки на находящуюся под защитой организацию;
- видимость эмблемы для третьих сторон в целях выявления случаев нарушения правил использования;
- риск несанкционированного использования, в том числе в целях совершения вероломных действий;
- совместимость с существующими подходами к ведению кибероперациий и поддержанию кибербезопасности, в том числе обеспечение возможности отслеживать враждебную киберактивность.

Угрозы нарушения деятельности субъектов, пользующихся защитой

«Цифровая эмблема» служит для обозначения субъектов, пользующихся защитой. Соотношение риска и пользы в данном случае зависит от способностей и мотивации кибероператоров. «Цифровая эмблема» дает преимущество кибероператорам, желающим не нарушать деятельность пользующихся защитой субъектов по ряду причин, например чтобы не привлекать к себе нежелательное внимание или чтобы соблюсти нормы МГП. Риск же в данном случае заключается в том, что демонстрация идентифицирующей информации в теории может сделать деятельность соответствующих субъектов целью кибернападения.

Высокоорганизованный исполнитель кибернападения может располагать множеством механизмов нарушения деятельности, которые опираются на цифровые процессы и доступ в сеть Интернет. Так, недавно группа киберпреступников осуществила серию нападений на больницы в Соединенных Штатах Америки, используя для идентификации целей нападения только размещенную в открытом доступе информацию[34]. Вне зависимости от наличия или отсутствия эмблемы, высокоорганизованный исполнитель кибернападения сможет успешно нарушить любую деятельность в интернете, за исключением наиболее технически совершенных процессов. Вероятность того, что эмблема существенно повлияет на действия высокоорганизованного кибероператора, намеренного нарушить работу медицинских организаций или деятельность МККК, низка. Государство, осуществляющее нападение на пользующийся защитой субъект в нарушение МГП, располагает разведывательным потенциалом, а также зачастую напрямую контролирует интернет-ресурсы.

Применение «цифровой эмблемы» может привести к появлению новых угроз ввиду создания средства идентификации, которое менее высокоорганизованные злоумышленники будут использовать для прицельного нападения на медицинские учреждения, их персонал и санитарно-транспортные средства. Если разместить «цифровую эмблему» на находящихся под защитой ресурсах, воюющим сторонам будет проще идентифицировать такие ресурсы. Например, это может дать кибероператорам возможность использовать «цифровую эмблему» для идентификации целей таких вредоносных операций, как, например, применение программ-вымогателей против больниц. Уровень создаваемой угрозы зависит от того, насколько идентификация соответствующих целей позволяет кибероператорам приблизиться к реализации своих намерений.

[34] R. Hattersley-Gray, “Pro-Russia Hackers Targeted More than 400 U.S. Hospitals in 2020,” 30 March 2022 [онлайн-публикация]: https://www.campussafetymagazine.com/hospital/pro-russia-hackers- targeted-400-us-hospitals/ [по состоянию на 7 апреля 2022 г.].

Эффективная реализация защитной функции
Легко обнаруживаемая эмблема способствует тому, чтобы добросовестные кибероператоры учитывали статус субъектов, пользующихся защитой, при выборе целей и выполняли свои боевые задачи, направленные против законных целей, не нарушая работу находящихся под защитой организаций.

В цифровом пространстве весьма часто проявляется проблема указания ложного источника данных. Для схожих с «цифровой эмблемой» видов цифровой информации разработан ряд эффективных методов предотвращения указания ложного источника данных, большинство из которых основываются на аттестации информации третьей стороной. Подобные методы также можно применить к «цифровой эмблеме», пускай и ценой ее усложнения. При выборе структуры «цифровой эмблемы» соотношение величины риска неправомерного использования и сложности исполнения является важным аспектом.

ТЕХНИЧЕСКИЕ ПОДХОДЫ

Лаборатория прикладной физики Университета Джонса Хопкинса рассмотрела три технических подхода к проектированию «цифровой эмблемы», которые по-разному влияют на упомянутые выше аспекты: на угрозу нарушения деятельности субъектов, пользующихся защитой, и на эффективность защиты, предоставляемой эмблемой. Влияние этих подходов также варьируется в зависимости от категории источника кибернетической угрозы.

Выделенная эмблема на файловой основе
Файловая «цифровая эмблема» сигнализирует об активном использовании эмблемы либо самим фактом существования файла, либо с помощью содержащихся в нем общепринятых директив. Когда файл «цифровой эмблемы» помещается в известное расположение внутри системы, его можно легко обнаружить любым программным обеспечением, взаимодействующим с этой системой. В качестве дополнения можно разработать простой протокол типа «запрос — ответ», который позволит запрашивать у целевой системы информацию о наличии или использовании «цифровой эмблемы».

Эмблема, основанная на протоколе DNS
Протокол DNS является ключевой составной частью глобальной распределенной инфраструктуры сети Интернет. Доменные имена — это считываемые человеком ярлыки для идентификации систем, а DNS служит для предоставления различной информации, которая привязана к ассоциированному с той или иной системой ярлыку.

Доменное имя состоит из последовательности ярлыков, выстроенных в иерархическом порядке (так, доменное имя www.icrc.org содержит три ярлыка). Для встраивания «цифровой эмблемы» в доменное имя можно предусмотреть отдельный специальный ярлык. Поскольку доменное имя ассоциируется исключительно с системами, находящимися под защитой «цифровой эмблемы», в нем будет отражена явная, считываемая «цифровая эмблема», идентифицирующая соответствующую систему.

Протокол DNS также может привязывать к доменному имени новую информацию (например, запись об использовании «цифровой эмблемы»). Направляя запрос о сетевом адресе доменного имени через DNS, программное обеспечение может также получить информацию о «цифровой эмблеме», привязанной к этому имени или сетевому адресу. Если такая запись существует, адресант запроса будет знать, что целевая система защищена «цифровой эмблемой».

Эмблема, основанная на сетевом адресе
Сетевые адреса в основном являются уникальными идентификаторами систем,

подключенных к сети Интернет. Благодаря существованию таких адресов интернет-инфраструктура может определить, какой путь нужно использовать, чтобы установить связь с целевой системой в ходе обмена сообщениями. Сетевой адрес лишь выполняет техническую функцию определения пути, в нем не содержится каких-либо глобальных семантических элементов, отражающих сведения о предназначении системы, которая использует такой адрес.

Одним из способов внедрения «цифровой эмблемы» может стать разработка механизма интеграции семантических элементов в сетевые адреса. Размещение семантических элементов в том или ином фрагменте сетевого адреса позволит создать уникальные адреса, связанные с «цифровой эмблемой», как для находящихся под защитой цифровых ресурсов, так и для защищенных сообщений, передающихся по сети. В таком случае системы, размещенные в любом месте сети Интернет, будут способны определить, связаны ли проверяемые ими системы или сообщения, передающиеся по сети, с той или иной защищенной стороной («цифровой эмблемой»).

СОБЛЮДЕНИЕ НОРМ ИСПОЛЬЗОВАНИЯ

Надлежащее использование определенных критически важных ресурсов, являющихся частью интернет-инфраструктуры, может быть обеспечено за счет внедрения процедуры утверждения по принципу априори в сочетании с публичной аттестацией (официальной сертификацией, осуществляемой нейтральной стороной) надлежащего использования. Например, один из региональных интернет-регистраторов (РИР) выделяет сетевой адрес провайдеру интернет-услуг (ПИУ). Для того чтобы указать на факт выделения, ПИУ распространяет информацию о присвоенном ему адресе. В то же время РИР аттестует факт выделения адреса через независимый канал связи. Это создает для не связанных с РИР или ПИУ третьих сторон возможность убедиться в достоверности распространяемой ПИУ информации. Сторона, принявшая решение об использовании «цифровой эмблемы», должна будет сделать официальный запрос в адрес выпускающего органа, такого как член Международной Федерации обществ Красного Креста и Красного Полумесяца. Если член одобряет запрос, он должен опубликовать подтверждающий это аттестат. Если у третьей стороны возникает потребность в проверке правомерности использования «цифровой эмблемы», она может быть удовлетворена за счет публичного заявления об аттестации.

В качестве альтернативных способов выявления неправомерного использования «цифровой эмблемы» могут выступать пассивный мониторинг или краудсорсинг. Вместо того чтобы направлять официальный запрос на использование «цифровой эмблемы», организация может тем или иным способом заявить о своем намерении использовать такую эмблему (например, с помощью глобального распределенного регистрационного журнала). Если третья сторона обнаруживает факт использования «цифровой эмблемы», она может проверить наличие записи о внедрении такой эмблемы в регистрационном журнале. Если соответствующая запись отсутствует или третья сторона считает, что эмблема использовалась неправомерно, об этом уведомляется оператор регистрационного журнала, который впоследствии несет ответственность за рассмотрение жалобы. Кроме того, субъекты могут вести поиск фактических данных о случаях использования «цифровой эмблемы» организациями без предварительного заявления о таком использовании.

ПРИЛОЖЕНИЕ 3

ТЕХНИЧЕСКИЕ РЕШЕНИЯ, ПРЕДСТАВЛЕННЫЕ ЦЕНТРОМ КИБЕРДОВЕРИЯ

АУТЕНТИФИЦИРУЕМАЯ ЦИФРОВАЯ ЭМБЛЕМА (АЦЭ)

Стремясь удовлетворить запрос МККК на разработку технических решений для внедрения «цифровой эмблемы», Центр кибердоверия (CECYT), совместное начинание Цюрихского технологического института и Боннского университета, спроектировал Аутентифицируемую цифровую эмблему (АЦЭ). АЦЭ позволяет пользующимся защитой сторонам отмечать свои цифровые ресурсы как защищенные за счет распространения криптографически подтверждаемых заявлений о защищенности и подкреплять эти заявления удостоверительными записями, выпущенными независимыми третьими сторонами.

Проектирование АЦЭ осуществлялось с опорой на результаты тщательного предварительного анализа среды, в которой она будет существовать. Перед началом внедрения «цифровой эмблемы» необходимо разрешить три вопроса второго порядка, указанных ниже.

1. «Цифровая эмблема» должна давать возможность обозначить защиту широкого спектра разнообразных организаций. Каким образом «цифровая эмблема» будет служить для опознавания пользующихся защитой организаций?
2. Как будет организовано распространение «цифровых эмблем»? Разнородность пользующихся защитой субъектов обусловливает потребность в разных способах передачи. Кроме того, следует определить каналы, дающие возможность активного распространения «цифровых эмблем».
3. На чем будет строиться доверие к «цифровой эмблеме»? Основная сложность здесь состоит в том, чтобы разработать «цифровую эмблему» так, чтобы стремящиеся проверить ее подлинность лица всегда могли убедиться в этом, даже когда система находится под воздействием того или иного источника угрозы.

АЦЭ дает следующие ответы на поставленные выше вопросы.

1. Идентификация организаций (субъектов) происходит либо по их сетевому адресу, либо по доменному имени, которые служат идентификаторами включенных в сеть процессов и устройств (объектов).
2. Распределение эмблем происходит с помощью трех разных протоколов, по возможности предоставляющих надежные гарантии безопасности и позволяющих обеспечить упрощенное распределение при меньшем уровне безопасности во всех остальных случаях. В то же время как минимум один из трех этих протоколов всегда остается доступен для любых типов субъектов, которые могут нуждаться в защите.
3. АЦЭ позволяет регуляторам криптографически удостоверить статус находящихся под защитой сторон, которые выпускают «цифровые эмблемы». В роли регуляторов,

по нашему мнению, обыкновенно будут выступать государства или наднациональные организации. Тем не менее эту роль могут выполнять и независимые организации. Проверяющие лица сами решают, каким регуляторам можно доверять. Мы рассчитываем на то, что в условиях вооруженных конфликтов проверяющие лица, действующие в соответствии с МГП, будут связаны с тем или иным государством. В таких случаях удостоверительные записи регуляторов дают проверяющим лицам возможность узнать, была ли утверждена эмблема их государством, что сводит к минимуму требования к уровню доверия.

Решения, реализованные при разработке АЦЭ, обусловливают наличие у нее многих желательных характеристик.

1. Как следует из названия, у АЦЭ можно проверить *подлинность*. Криптографические удостоверительные записи дают проверяющим лицам возможность убедиться в подлинности статуса стороны, находящейся под защитой, как такового.
2. АЦЭ позволяет находящимся под защитой субъектам *активно* распределять «цифровые эмблемы». За счет этого лица, наблюдающие «цифровые эмблемы», могут сохранить анонимность. Таким образом стремящиеся проверить подлинность АЦЭ лица могут сделать это безопасно, не рискуя быть идентифицированными как источник потенциальной угрозы.
3. АЦЭ является *распределенной*. Регуляторы независимо удостоверяют статус находящихся под защитой сторон, не сталкиваясь с необходимостью сотрудничать между собой или доверять друг другу. Это представляется чрезвычайно полезным в реалиях международной дипломатии, в которых достичь консенсуса крайне затруднительно. Пользоваться АЦЭ могут даже стороны в вооруженном конфликте. противостоящие друг другу.
4. АЦЭ *адаптивна.* Она была разработана с прицелом на совместимость со множеством разновидностей цифровых ресурсов, сервисов и данных и с учетом особенностей различных типов организаций. Более того, пользующиеся защитой стороны могут приспособить внедряемую АЦЭ под собственные нужды.
5. АЦЭ *проста* и автономна. Форма представления «цифровых эмблем» одинакова во всех интерфейсах. АЦЭ не требует обновления сетевой инфраструктуры. Способы дистрибуции АЦЭ обратно совместимы с действующими версиями клиентов, а потребность в каком-либо обновлении спецификаций или поддержке со стороны независимых субъектов, например сертифицирующих органов или интернет-провайдеров, отсутствует. Наконец, АЦЭ опирается на неоднократно испытанные и хорошо известные принципы и технологии, что способствует упрощению разработки и внедрения.

СТРУКТУРА

Рассказать о структуре АЦЭ можно на примере. Представим, что в охваченном войной регионе ведет деятельность пользующаяся защитой сторона — «Ассоциация врачей скорой помощи» (АВСП), под эгидой которой работают несколько больниц скорой медицинской помощи. Работа каждой из этих больниц связана с многочисленными цифровыми объектами.

- Персонал больницы пользуется персональными устройствами, такими как планшеты или ноутбуки, которые подключены к ИТ-инфраструктуре, в частности к базам данных, где хранятся электронные медицинские карты пациентов.
- В больницах эксплуатируется большое количество малых устройств, например устройства маршрутизации и медицинское оборудование.
- АВСП также управляет веб-сайтом, на котором используется протокол HTTPS. На веб-сайте публикуется информация о предоставляемых услугах для

общественности.

АЦЭ помогает обеспечивать защиту всех названных цифровых объектов и выполняет другие задачи. Для того чтобы инициировать распределение эмблем тем или иным цифровым объектом, системному администратору достаточно лишь установить на него клиент ПО и выполнить настройку. Если какие-либо из объектов не поддерживают установку клиента ПО или число установленных клиентов просто чрезмерно велико, АЦЭ может быть размещена, к примеру, на роутерах, чтобы статус объекта, находящегося под защитой, сообщался всем узлам в соответствующей сети.

Для создания возможности криптографической верификации заявлений о защите АВСП должна осуществить еще три действия.

1. Необходимо настроить основной веб-сайт так, чтобы его можно было использовать как платформу для идентификации самой АВСП. Идентификация будет обеспечиваться как в считываемом человеком формате — за счет публикации сведений об организации, так и в техническом смысле — посредством дистрибуции криптографических публичных ключей. Увидев эти публичные ключи, проверяющие лица смогут связать заявления о защите с конкретной пользующейся защитой стороной, в данном случае — с АВСП.
2. Следует в индивидуальном порядке связаться с двумя сторонами в конфликте: назовем эти стороны Алистаном и Бобанией. Необходимо запросить криптографические удостоверительные записи, что даст вооруженным силам обеих стран возможность определить, действительно ли публичные ключи, размещенные на веб-сайте АВСП, принадлежат АВСП — стороне, имеющей право на выпуск заявлений о том, что она находится под защитой.
3. АВСП должна привязать «цифровые эмблемы», генерируемые входящими в ее структуру субъектами, к одному из публичных ключей, размещенных на ее веб-сайте.

Для создания такой привязки АВСП необходимо выпустить промежуточные секретные ключи, например для своих сотрудников. Публичные ключи криптографически удостоверяются публичным ключом, размещенным на веб-сайте АВСП и, в свою очередь, удостоверяют публичные ключи находящихся под защитой субъектов. Подобная схема во многом напоминает цепочки сертификатов, существующие в рамках экосистемы веб-сертификатов. Все криптографические удостоверительные записи передаются на цифровые объекты и распределяются вместе с эмблемами так, чтобы стремящиеся проверить подлинность лица располагали всеми сведениями, которые нужны для составления суждения о достоверности видимой ими эмблемы.

Получив (обнаружив) «цифровую эмблему», любое проверяющее лицо — например, вооруженное формирование в составе вооруженных сил Алистана или Бобании, может проверить следующее: a) что она была выпущена АВСП и что сторона, называющая себя АВСП, действительно является таковой, и это подтверждено как (b) Алистаном, так и (c) Бобанией. Можно практически с полной уверенностью утверждать, что они будут доверять лишь своим собственным удостоверительным записям, а не записям противника.

ВАРИАЦИИ

В предыдущем разделе мы привели рекомендации по поводу того, как может быть осуществлено внедрение АЦЭ на практике. Тем не менее во время войны может потребоваться достижение компромиссов. АЦЭ можно внедрить и при меньшем уровне взаимодействия: в качестве рекомендуемых вариантов также стоит назвать удостоверительные записи, выданные третьими сторонами, централизованный веб-сайт для

пользующихся защитой сторон и даже подписи.

Без удостоверительных записей, выданных третьими сторонами, подлинность публичных ключей пользующейся защитой стороны можно проверить только с помощью идентифицирующего эту сторону веб-сайта. В связи с недостатком времени или слабым развитием сетевой инфраструктуры может возникнуть потребность обратиться к органам власти (регуляторам). Тем не менее мы должны указать на то, что пользующиеся защитой стороны могут собрать удостоверительные записи позже.

Порой даже создание централизованного веб-сайта не является осуществимым вариантом. В таких ситуациях «цифровые эмблемы» могут опираться исключительно на публичные ключи. В этом случае пользующаяся защитой сторона должна будет связаться со сторонами в конфликте, чтобы независимо сообщить им свой корневой публичный ключ.

Наконец, у пользующейся защитой стороны может в принципе не быть возможности подключить свои ресурсы к централизованному публичному ключу. В таких обстоятельствах цифровые объекты можно настроить так, чтобы они распространяли заявления о том, что находятся под защитой, без возможности аутентификации. Даже при том, что подобные неаутентифицированные заявления должны подвергаться максимально тщательному рассмотрению, они могут быть полезны в качестве временного решения, если конфликт начался неожиданно и резко. Такие заявления позволяют гарантировать, что пользующаяся защитой сторона не останется без обозначения защиты в период развертывания АЦЭ с более высоким уровнем взаимодействия.

ТЕХНИЧЕСКИЕ ПОДРОБНОСТИ

Ранее мы описали основную суть концепции АЦЭ. В этом разделе представлены подробности ее технической реализации. Он предназначен для читателей, обладающих более высоким уровнем технических знаний.

Выше мы упоминали два типа криптографических сообщений: «цифровые эмблемы» и удостоверительные записи. Далее мы будем использовать в отношении обоих типов термин «токен». Токены кодируются в форме веб-подписей JSON Web Signatures (JWS) — известного и широко используемого стандарта подписания машиночитаемых, структурированных данных. Ядром каждого токена являются данные об эмитенте, закодированные как доменное имя, которое должно указывать на веб-сайт с протоколом HTTPS. Данный веб-сайт служит местом хранения публичных ключей, как указывалось ранее. Мы называем все такие ключи *корневыми публичными ключами*.

Корневые публичные ключи удостоверяются регуляторами. В удостоверительных записях кодируется следующее заявление: «Публичный ключ К принадлежит стороне С., и сторона С имеет право на выпуск заявлений о том, что она пользуется защитой». Кроме того, в удостоверительных записях могут указываться ограничения, например границы диапазона IP-адресов, для которых разрешен выпуск эмблем. Такие ограничения нужны для того, чтобы уменьшить масштаб последствий раскрытия секретных ключей и повысить уровень доверия к удостоверительным записям. Благодаря ограничениям регуляторам не требуется вслепую доверять пользующимся защитой сторонам, выдавая им карт-бланш, позволяющий таким сторонам заявлять о защите субъектов, которые на самом деле не подлежат защите.

Удостоверительные записи третьих сторон должны храниться вместе с корневыми публичными ключами на идентификационном домене той или иной стороны.

Удостоверительные записи также можно использовать для внутреннего регулирования в системах той или иной стороны, пользующейся защитой. К примеру, такая сторона может распространять важный материал, удостоверенный одним из ее корневых публичных ключей, среди своих сотрудников. Данные промежуточные ключи могут, в свою очередь, служить для удостоверения других ключей. Таким образом создается цепочка удостоверительных записей, ведущая к важному материалу, который хранится на самих защищенных объектах. Любые удостоверительные записи, которые связывают корневой публичный ключ с публичным ключом конкретного объекта, должны отправляться вместе с «цифровыми эмблемами».

Распространение «цифровых эмблем» происходит посредством одного из трех следующих протоколов: TLS, ICMP и DNS. Мы рекомендуем по возможности использовать TLS. При использовании TLS проверяющее лицо будет точно знать, что эмблемы или удостоверительные записи не были перехвачены тем или иным противником. Если возможности применить TLS нет, в качестве альтернативы подойдет протокол ICMP. Гарантии того, что эмблема будет доставлена потенциальному проверяющему лицу, в этом случае отсутствуют, но данный протокол поддерживается практически всеми цифровыми объектами, способными запускать стек IP. Еще одним, дополнительным вариантом канала дистрибуции является протокол DNS: он не требует модификации или доступности цифровых объектов, но поддерживается не всеми типами таких объектов.

ПРИНЯТИЕ

Вкратце изложив технические подробности функционирования АЦЭ, обсудим в сжатой форме, что потребуется пользующимся защитой сторонам для принятия АЦЭ. Как указано ранее, АЦЭ не требует обновления сетевой архитектуры. Соответственно, пользующиеся защитой стороны могут внедрять ее независимо друг от друга. Тем не менее мы не ожидаем, что у таких сторон будут иметься специальные знания, необходимые для разработки и внедрения АЦЭ с нуля.

Для функционирования АЦЭ необходимо четыре вида компонентов ПО — для управления ключами и подписания удостоверительных записей, распределения эмблем, приема эмблем, а также для проверки эмблем. Программное обеспечение для распределения и приема необходимо создать для каждого из протоколов TLS, ICMP и DNS в отдельности. Мы планируем создать и протестировать соответствующие компоненты ПО в фазе прототипирования.

Положительный момент состоит в том, что их разработка может проводиться без участия пользующихся защитой сторон. Мы прогнозируем, что они будут обслуживаться как бесплатное программное обеспечение с открытым кодом. Тогда находящиеся под защитой стороны смогут свободно получать к ним доступ и использовать их в своих организационных системах, минимизируя объем работ по адаптации.

ВОЗМОЖНЫЕ РАСШИРЕНИЯ

Помимо основной структуры АЦЭ, описанной в предыдущих разделах, мы также изучаем возможность выпуска двух расширений.

Первое расширение подразумевает локальное распределение эмблем на оборудовании с включением их в процессы, запущенные на этом оборудовании, в том числе в процессы вредоносного программного обеспечения. Локальное распределение эмблем сделает технологию АЦЭ еще более вариативной. Тем не менее при локальном распределении эмблем могут возникать проблемы, которые уже были подробно изучены, но в основном на данный

момент не имеют решения. Следовательно, работа в этом направлении еще не завершена.

Второе расширение состоит в поддержке независимым образом управляемых журналов, где фиксируется история генерации центральных публичных ключей и удостоверяющих их записей. Такой подход позволит повысить прозрачность и упростит учет при использовании АЦЭ. Так, при наличии упомянутых журналов, государства не смогут создавать «фальшивые» защищенные стороны, статус которых удостоверен только ими, и использовать их для ведения вредоносных операций.

В целом основную часть структуры АЦЭ можно без проблем адаптировать к будущим изменениям. Модель обеспечения доверия к АЦЭ можно приспособить к новым средствам идентификации субъектов, находящихся под защитой, или осуществить распространение «цифровых эмблем» при минимуме дополнительных затрат, если такая необходимость возникнет в будущем.

ЦЕЛИ И ЗАДАЧИ

Международный Комитет Красного Креста (МККК) является беспристрастной, нейтральной и независимой организацией, чьи цели и задачи носят исключительно гуманитарный характер и заключаются в том, чтобы защищать жизнь и достоинство людей, пострадавших от вооруженных конфликтов и других ситуаций насилия, и предоставлять им помощь. Пропагандируя и укрепляя гуманитарное право и универсальные гуманитарные принципы, МККК прилагает все усилия к тому, чтобы предотвратить страдания людей. МККК, основанный в 1863 г., стоит у истоков Международного движения Красного Креста и Красного Полумесяца. Он направляет и координирует международную деятельность Движения по оказанию гуманитарной помощи в ситуациях конфликтов и иных ситуациях насилия.

facebook.com/icrc
twitter.com/icrc
instagram.com/icrc

МККК

Международный Комитет Красного Креста
19, avenue de la Paix
1202, Женева, Швейцария
T +41 22 734 60 01
shop.icrc.org

4649/005 05.2023 Иллюстрация на обложке: R.Banerjee/МККК