R

WIPO
ВСЕМИРНАЯ ОРГАНИЗАЦИЯ
ИНТЕЛЛЕКТУАЛЬНОЙ
СОБСТВЕННОСТИ

WIPO/ACE/18/34
ОРИГИНАЛ: АНГЛИЙСКИЙ
ДАТА: 19 МАЯ 2026 ГОДА

Консультативный комитет по защите прав

Восемнадцатая сессия
Женева, 2–4 июня 2026 года

ВЗАИМОСВЯЗЬ МЕЖДУ ВРЕДОНОСНЫМ ПО И ПИРАТСТВОМ: ИНСТРУМЕНТЫ ОБЕСПЕЧЕНИЯ СОБЛЮДЕНИЯ ПРАВ И ВОЗМОЖНОСТИ ДЛЯ ПРИНЯТИЯ МЕР ПРАВИТЕЛЬСТВОМ

Доклад подготовила д-р Елена Блобель, директор отдела рассмотрения судебных споров Международной федерации производителей фонограмм, Лондон, Соединенное Королевство[*]*.*

АННОТАЦИЯ

В настоящем докладе рассказывается о том, как сервисы онлайн-пиратства регулярно используют обещание бесплатного доступа к защищенному авторским правом контенту для привлечения потребителей на веб-сайты, приложения и устройства, которые скрывают в себе значительные риски для них. В документе описываются типы вредоносных программ, используемых в рамках пиратской деятельности в Интернете, а также ряд инструментов правоприменения, которые могут использоваться для пресечения распространения вредоносных программ. В этом материале содержится призыв уделять больше внимания на директивном уровне взаимосвязи между вредоносным ПО и пиратством, а также множеству связанных с ними форм преступности. В заключении определяются приоритетные области для дальнейшего изучения с целью содействия принятию информированных решений лицами, ответственными за выработку политики.

[*] В настоящем документе отражена точка зрения автора, которая может не совпадать с мнениями Секретариата или государств — членов ВОИС.

I. ПОЧЕМУ ЗАЩИЩЕННЫЙ АВТОРСКИМ ПРАВОМ КОНТЕНТ ИСПОЛЬЗУЕТСЯ ДЛЯ РАСПРОСТРАНЕНИЯ ВРЕДОНОСНЫХ ПРОГРАММ?

1. Обещание доступа к бесплатному контенту, защищенному авторским правом, через онлайновые пиратские сервисы широко применяется злоумышленниками для того, чтобы заманивать потребителей на сайты, приложения и устройства, которые таят в себе различные виды вредоносных угроз для них. В этом материале описывается текущее положение дел с типами вредоносных программ, потенциальный масштаб проблемы в целом, типы существующих правоприменительных мер, а также возможности для правительств по решению данной проблемы, в том числе путем повышения осведомленности потребителей.

A. ТИПЫ ВРЕДОНОСНЫХ ПРОГРАММ, СВЯЗАННЫХ С ОНЛАЙН-ПИРАТСТВОМ

2. Исходя из опыта Международной федерации производителей фонограмм (IFPI), существует целый ряд различных типов вредоносных программ, которые можно найти на музыкальных пиратских сайтах и сервисах. Некоторые примеры вредоносных программ, связанных с пиратскими сервисами, включают:

- Программы-вымогатели доставляются через обманчивые всплывающие окна, «попандеры», требующие нажатия для воспроизведения элементы или поддельные кнопки загрузки на пиратских стриминговых и торрент-сайтах, которые шифруют файлы жертвы. Впоследствии для восстановления доступа требуется плата, обычно в виде криптовалюты.

- «Криптоджекинг», когда скрипты для добычи криптовалюты скрытно запускаются в браузере или на устройстве пользователя, потребляя при этом ресурсы компьютера и снижая производительность.

- Шпионское ПО, которое скрытно следит за действиями пользователя, считывая нажатия клавиш и учетные данные и выуживая конфиденциальную или личную информацию, такую как электронная почта, финансовая информация и фотографии.

- Трояны — это вредоносные программы, замаскированные под подлинное программное обеспечение, которые загружаются через поддельные обновления, медиаплееры или инсталляторы и создают бэкдоры или устанавливают другие вредоносные инструменты. Малвертайзинг — это агрессивная, обманчивая или навязчивая реклама, которая приводит к загрузке вредоносных программ, сбору пользовательских данных и перенаправлению пользователей на мошеннические страницы.

- Пугающие программы, имитирующие системные предупреждения и тем самым склоняющие жертв к загрузке вредоносных программ. Они распространены как на мобильных, так и на настольных пиратских сервисах.

- Инструменты для кражи учетных данных и поддельные страницы входа и оплаты нацелены на сбор имен пользователей, паролей и токенов двухфакторной аутентификации. Эти украденные учетные данные могут быть повторно использованы в учетных записях в банках или в социальных сетях, что делает возможной кражу личности, несанкционированные переводы средств и захват счетов, учетные данные также могут быть перепроданы на нелегальном рынке. Скомпрометированные учетные данные могут быть использованы для доступа к учетным записям с целью мошенничества с потоковым вещанием (т. е. для создания фальшивых потоков треков на платформах потокового вещания, не отражающих реальное потребление

фанатами), тем самым уводя доходы от законных артистов и других правообладателей.

- Вербовка ботнетов, когда одноранговые клиенты, взломанные сетевые инструменты или незаконные устройства потоковой передачи данных, предварительно нагруженные нелицензионными дополнениями, используются для проникновения в локальные сети и устройства, что приводит к их невольному пополнению ботнетами, которые координируют распределенные атаки типа «отказ в обслуживании», спам-кампании или распространение дополнительных вредоносных программ. Такие ботнеты также могут использоваться для мошенничества, включая мошенничество с потоковым вещанием.

- Угон систем доменных имен (DNS) — такие программы изменяют настройки DNS или конфигурацию браузера, чтобы перенаправить трафик на вредоносные или партнерские целевые страницы, проводя веб-запросы пользователей через контролируемые злоумышленниками сервисы.

B. МАСШТАБ ПРОБЛЕМЫ

3. На сегодняшний день миллионы пользователей Интернета по всему миру обращаются к пиратским сайтам, чтобы получить доступ к нелицензионному контенту, защищенному авторским правом. Существует значительный объем исследований, оценивающих потенциальный масштаб проблемы и риски, связанные с вредоносными программами, с которыми сталкиваются интернет-пользователи в связи с онлайн-пиратством. В целом, в докладах, посвященных преимущественно аудиовизуальному сектору, подчеркивается, что угрозы существуют в огромных масштабах по всему миру. Например:

- Потребители в Юго-Восточной Азии сталкиваются в среднем с более чем 22-кратным увеличением числа обнаружений киберугроз на пиратских сайтах по сравнению с обычными контрольными сайтами[1].

- В Индии на пиратских сайтах риск заражения устройства вредоносным ПО составляет 59%, что выше, чем на сайтах развлечений для взрослых или азартных игр, причем особенно уязвимы молодые пользователи (18–24 года)[2].

- Так называемая вредоносная реклама составляла 12% от общего количества рекламы на пиратских сайтах, принося минимум 121 миллион долларов США ежегодного дохода. Почти на 80% исследованных пиратских сайтов размещалась реклама, содержащая вредоносные программы. Посещение пиратского сайта приводит к попытке передать пользователю вредоносное ПО в среднем каждый шестой раз[3].

- Потребители в Польше в среднем в 38,5 раз чаще сталкиваются с киберугрозами на пиринговых сайтах по сравнению с обычными сайтами[4].

- Согласно одному исследованию, европейские потребители могут подвергнуться атаке уже через 71 секунду после того, как попадут на пиратские сайты, и в среднем вероятность того, что пиратские

[1] https://www.alliance4creativity.com/wp-content/uploads/2025/07/Watters-PiracyInSEA-071025-v2.pdf.
[2] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4766797.
[3] https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/Unholy-Triangle-Report.pdf.
[4] https://www.mpa-emea.org/wp-content/uploads/2024/09/Watters-Consumer-Risk-from_Piracy-in-Poland.pdf.

аудиовизуальные приложения будут предустановлены со встроенным вредоносным ПО, составляет 57%[5].

4. По другим секторам данных меньше, но соответствующие принципы в целом применимы к любым мошенническим сайтам, приложениям и устройствам, которые предлагают нелицензионный контент для привлечения пользователей, и это также подтверждается примерами в музыкальном секторе.

5. Исследование, проведенное IFPI в Латинской Америке, показало, что 33% из 174 сайтов для скачивания MP3-файлов, действующих в регионе, были связаны с распространением вредоносного ПО. Среди этих нелегальных музыкальных сайтов 17% напрямую распространяли вредоносное ПО, а еще 26% косвенно распространяли подозрительные файлы с вредоносным ПО через вторичные страницы под другими доменными именами. Это же исследование показало, что 10% нелегальных музыкальных сайтов, распространяющих вредоносное ПО, имеют собственные мобильные приложения, нарушающие авторские права, что повышает риск неправомерного доступа и кражи личных данных, а также других видов киберпреступлений. В целом, с 2018 года число случаев онлайн-мошенничества в отношении пользователей Интернета в Бразилии увеличилось на 408%, и в 2024 году было зарегистрировано 2,1 миллиона таких случаев[6].

C. КАКИЕ ИНСТРУМЕНТЫ ПРАВОПРИМЕНЕНИЯ СУЩЕСТВУЮТ ДЛЯ РЕШЕНИЯ ЭТОЙ ПРОБЛЕМЫ?

6. Существует несколько инициатив по борьбе с распространением вредоносных программ, например следующие:

- Операция Европола «Эндшпиль» — широкомасштабная инициатива, направленная на уничтожение ботнетов и связанных с ними преступных инфраструктур[7].

- Национальная лаборатория судебной экспертизы киберпреступлений при Индийском координационном центре по борьбе с киберпреступностью, которая предоставляет правоохранительным органам услуги по судебной экспертизе и анализу вредоносных программ[8].

- Центральное управление по защите прав потребителей Индии выпустило рекомендации, согласно которым цифровые платформы должны выявлять и устранять из своих интерфейсов подозрительные элементы, включая вредоносные программы[9].

7. Аналогичные инструменты должны быть легкодоступны и в других странах для борьбы с вредоносным ПО в контексте пиратства, как это видно на примере инициатив, координируемых Министерством юстиции и общественной безопасности и Лабораторией кибероперaций в Бразилии:

---

[5] https://www.aapa.eu/study-on-malware-and-audiovisual-piracy-highlights-significant-risks-to-european-consumers.
[6] https://forumseguranca.org.br/publicacoes/anuario-brasileiro-de-seguranca-publica/.
[7] https://www.europol.europa.eu/operations-services-and-innovation/operations/operation-endgame.
[8] https://education.vikaspedia.in/viewcontent/education/digital-litercy/information-security/indian-cyber-crime-coordination-centre?lgn=en.
[9] https://www.pib.gov.in/PressReleasePage.aspx?PRID=2134765. Это следует из Руководства по предотвращению функционирования и регулированию подозрительных элементов, принятого Центральным управлением по защите прав потребителей в 2023 году.

- «Операция 404», в рамках которой в течение последних шести лет было проведено семь раундов по борьбе с более чем 3 000 сайтов и мобильных приложений, нарушающих авторские права, некоторые из которых включали прямое распространение вредоносного ПО и кражу персональных данных[10].

- Операция «Перенаправление», которая была направлена на пиратские сайты, связанные с распространением вредоносного ПО (включая сайты с незаконными ссылками на музыку, сайты для копирования потоков и поисковые системы торрентов)[11]. В ходе скоординированной операции было приостановлено функционирование ряда доменов, заблокированы сайты и закрыты незаконные веб-сайты путем комбинированного применения мер по воздействию[12].

8. В дополнение к уголовным средствам защиты могут быть доступны и гражданские средства защиты. Например, недавно компания Google объявила о начале судебного процесса против операторов ботнета Badbox 2.0, который, по ее утверждению, заразил более 10 миллионов устройств, работающих под управлением программного обеспечения с открытым исходным кодом Android[13].

9. Онлайн-платформы и посредники также должны участвовать в пресечении такой деятельности. Устройства, предварительно нагруженные контрафактным контентом и вредоносным ПО, продаются на платформах электронной коммерции; мобильные приложения с вредоносным ПО доступны в официальных и нелицензированных магазинах приложений; мошеннические сайты, распространяющие вредоносное ПО, можно обнаружить с помощью поиска; а посредники, предоставляющие домены и хостинг, обеспечивают инфраструктуру, которая позволяет таким сайтам функционировать. Даже если эта деятельность запрещена соответствующими правилами и условиями, злоумышленники могут продолжать работать. Таким образом, необходимы проактивные меры, а также масштабируемые механизмы отчетности и оперативное и эффективное устранение. Существуют также независимые организации, которые предлагают каналы отчетности.[14]

D. ПОЧЕМУ ЭТО ДОЛЖНО БЫТЬ ВАЖНО ДЛЯ ПРАВИТЕЛЬСТВ?

10. Важно, чтобы вопрос о связи между онлайновым пиратством и вредоносным ПО, а также развивающиеся тенденции в этой области были доведены до сведения властей и правительств по всему миру. Использование пиратских сайтов для распространения вредоносных программ — это пример полипреступности, которая может нанести огромный вред потребителям во всем мире. Наряду с вредом, причиняемым пиратством, это представляет собой риск не только для правообладателей, но и для общества в целом.

11. Последние тенденции также показывают, что пиратские экосистемы все чаще пересекаются с более широкими формами киберпреступности и полипреступности. В частности, неофициальные экосистемы приложений, неавторизованные магазины приложений, сайты загрузки APK и другие каналы побочной загрузки часто используются для распространения приложений, связанных с вредоносным ПО, шпионскими

[10] https://www.gov.br/mj/pt-br/assuntos/noticias/operacao-internacional-contra-pirataria-tira-do-ar-675-sites-e-14-aplicativos-de-streaming.
[11] https://www.ifpi.org/brazilian-authorities-launch-operation-redirect-targeting-illegal-music-sites-responsible-for-malware-distribution/.
[12] https://www.gov.br/mj/pt-br/assuntos/noticias/operacao-redirect-bloqueia-oito-sites-piratas-de-musica-1.
[13] https://www.securityweek.com/google-sues-operators-of-10-million-device-badbox-2-0-botnet/.
[14] Например, Netbeacon предлагает канал для сообщений о злоупотреблениях в системе доменных имен: https://netbeacon.org/.

программами, кражей учетных данных, мошенничеством и другими вредоносными действиями.

12. Потребители, желающие получить несанкционированный доступ к музыкальному, аудиовизуальному контенту или трансляциям в прямом эфире, могут неосознанно устанавливать приложения вне доверенной среды распространения, подвергая устройства и персональные данные значительным рискам с точки зрения кибербезопасности.

13. Такая деятельность иллюстрирует, что пиратские сервисы могут выступать не только как механизмы нарушения авторских прав, но и как подспорье для более широкой преступной деятельности, включая фишинг, финансовое мошенничество, создание ботнетов, рекламное мошенничество и крупномасштабный сбор учетных данных.

14. В некоторых случаях злоумышленники используют спрос на популярный контент или контент, который был удален из основных магазинов приложений, чтобы заманить потребителей с целью загрузки зараженных приложений или использования мошеннических ссылок и установки поддельных обновлений программного обеспечения.

15. Дополнительным фактором роста таких рисков является все большее распространение неопубликованных на официальных платформах мобильных приложений и нелицензионных каналов распространения приложений, особенно когда недобросовестные участники могут быстро переупаковывать и затем распространять нарушающие права или вредоносные приложения вне установленных процессов проверки и безопасности. Это подтверждает необходимость скоординированного взаимодействия между правительствами, органами кибербезопасности, правоохранительными органами, онлайн-посредниками и операторами экосистемы приложений для решения проблемы более широкого общественного вреда, связанного с распространением вредоносных программ, связанных с пиратством.

16. Ожидается, что риски, связанные с вредоносным ПО на пиратских сайтах и в приложениях, будут расти, чему будет способствовать искусственный интеллект (ИИ). В недавнем отчете признается, что ИИ может дополнить и упростить совершение некоторых видов преступлений, включая распространение вредоносного ПО, благодаря своей способности сочетать более реалистичный контент с автоматизированной доставкой в большом масштабе[15]. Киберпреступность и мошенничество оказывают пагубное влияние на жертв, о чем говорилось в недавнем исследовании, опубликованном Министерством внутренних дел Соединенного Королевства[16].

II. ЗАКЛЮЧЕНИЕ

17. Взаимосвязь вредоносных программ и онлайн-пиратства должна быть изучена в большей степени, в том числе Всемирной организацией интеллектуальной собственности, для сбора соответствующих данных и информации, чтобы облегчить принятие обоснованных решений директивными органами, с целью разработки необходимых инструментов для решения любых возникающих проблем.

18. Существует ряд областей, которые можно было бы изучить подробнее, например:

- Угроза, возникающая в результате пиратства в мобильных приложениях, включая популярные приложения для обмена контентом, такие как Discord и Telegram, особенно учитывая рост потребления контента через мобильные

[15] https://cetas.turing.ac.uk/sites/default/files/2025-03/cetas_research_report_-_ai_and_serious_online_crime_0.pdf.
[16] https://www.gov.uk/government/publications/understanding-the-cyber-crime-and-fraud-victim-journey/understanding-the-cyber-crime-and-fraud-victim-journey.

устройства и более широкую доступность таких мобильных приложений из неавторизованных магазинов приложений/сайтов загрузки пакетов для Android (т. е. использование не опубликованных на официальных платформах приложений и пакетов).

- Потенциальные новые векторы угроз, создаваемые развивающимися технологиями, например использование ИИ для создания поддельных предварительных релизов или другого дипфейк-контента, который может быть использован в качестве приманки для распространения вредоносного ПО.

- Роль вредоносного ПО в полипреступности, включая распространение вредоносного ПО через устройства, предлагающие доступ к нелицензионному контенту, который затем может быть использован для сбора учетных данных или создания ботнетов для других неблаговидных целей, таких как мошенничество с потоковым вещанием.

19. Уже существует ряд инструментов и действий по обеспечению соблюдения законодательства, которые могут послужить отправной точкой для разработки передовых глобальных мер, и которые должны способствовать обсуждениям и взаимодействию с посредниками, побуждая их к более активным добровольным действиям.

20. Кроме того, постоянное повышение осведомленности и обучение потребителей на тему вреда, наносимого пиратством в Интернете, должно сопровождаться, где это возможно, соответствующими предупреждениями, связанными с риском, связанным с использованием вредоносного ПО[17].

[Конец доклада]

[17] Например, исследование, проведенное в 2023 году Ведомством интеллектуальной собственности Европейского Союза, показало, что 82% жителей Европы согласны с тем, что незаконное получение онлайн-контента сопряжено с риском столкнуться с вредными практиками, такими как мошенничество или неприемлемый контент для несовершеннолетних. Тем не менее значительно реже люди избегали нелегальных источников из-за плохого опыта, полученного ими самими или другими людьми (13% и 19%, соответственно). Однако эти причины были более убедительными с той точки зрения, чтобы побудить пользователей, намеренно пользующихся нелегальными сервисами, прекратить пользоваться пиратским контентом в Интернете (31% и 29%, соответственно). См.: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2023_IP_Perception_Study/2023_IP_Perception_Study_FullR_en.pdf.