Научная статья
УДК 34
NIION: 2022-0089-4/25-329
MOSURED: 77/27-031-2025-04-329
EDN: https://elibrary.ru/EKWXLF

Противодействие вербовке граждан Российской Федерации в сети Интернет спецслужбами Украины для совершения противоправных деяний

Анатолий Васильевич Богданов[1], Олег Васильевич Кудин[2]
[1,2] Московский университет МВД России имени В.Я. Кикотя, Москва, Россия
[1] bogdanov.a.v58@mail.ru
[2] Kudin.mpf@yandex.ru

Аннотация. Исследуются методы и технологии вербовки спецслужбами граждан России, а также предлагаются меры противодействия этой деятельности. Рассматриваются такие инструменты, как психологическое давление, пропаганда, финансовые стимулы и дистанционные методы вербовки через Интернет, включая OSINT и телефонный терроризм. Особое внимание уделено деятельности ЦИПсО (Центра информационно-психологических операций) Украины, который специализируется на гибридной войне. Анализируются принципы выявления фейковых материалов и подчеркивается важность информированности и бдительности для предотвращения вербовки.

Ключевые слова: вербовка, специальные службы, психологическое давление, пропаганда, OSINT, телефонный терроризм, ЦИПсО, гибридная война, фейковые материалы, противодействие

Для цитирования: Богданов А. В., Кудин О. В. Противодействие вербовке граждан Российской Федерации в сети Интернет спецслужбами Украины для совершения противоправных деяний // Судебная экспертиза и исследования. 2025. № 4. С. 16–21.

Original article

Countering the recruitment of citizens of the Russian Federation on the Internet by the special services of Ukraine to commit illegal acts

Anatoly V. Bogdanov[1], Oleg V. Kudin[2]
[1,2] Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot', Moscow, Russia
[1] bogdanov.a.v58@mail.ru
[2] Kudin.mpf@yandex.ru

Abstract. The methods and technologies of recruitment by the special services of Russian citizens are being investigated, as well as measures to counter this activity are proposed. Tools such as psychological pressure, propaganda, financial incentives, and remote recruitment methods via the Internet, including OSINT and telephone terrorism, are considered. Special attention is paid to the activities of the CIPsO (Center for Information and Psychological Operations) of Ukraine, which specializes in hybrid warfare. The principles of detecting fake materials are analyzed and the importance of awareness and vigilance to prevent recruitment is emphasized.

Keywords: recruitment, special services, psychological pressure, propaganda, OSINT, telephone terrorism, CIPsO, hybrid warfare, fake materials, counteraction

For citation: Bogdanov A. V., Kudin O. V. Countering the recruitment of citizens of the Russian Federation on the Internet by the special services of Ukraine to commit illegal acts. Forensic science and research. 2025;(4):16–21. (In Russ.).

В современном мире средства массовой информации (СМИ) и интернет-ресурсы стали основными средствами воздействия на общественное сознание, в особенности на мировоззрение несовершеннолетних, молодежи и пожилых людей. Влияние СМИ и информационно-телекоммуникационных технологий (ИТТ) на указанную категорию не всегда носит созидательный характер в процессе формирования ценностных ориентиров.

Один из важнейших национальных интересов, обозначенный Стратегией национальной безопасности Российской Федерации — это развитие безопасного информационного пространства, защита граждан от деструктивного информационно-психологического воздействия.

Деструктивные силы и спецслужбы Украины и Запада провокационно воздействуют на сознание и поведение граждан России.

С началом конфликта между Россией и Украиной информационное пространство стало ареной масштабной борьбы за умы и действия людей. Спецслужбы Украины активно используют Интернет как средство ведения кибервойны, одной из целей которой является вербовка российских граждан для проведения акций, сбора разведданных, диверсий и других противоправных деяний.

90 млн человек ежедневно пользуются мессенджерами в России.

Главная угроза — то, что эти действия происходят удаленно, как правило, анонимно, что затрудняет их выявление и нейтрализацию.

В современных условиях сложной внешнеполитической ситуации вопрос пресечения размещения в информационно-телекоммуникационной сети Интернет сведений, оказывающих дестабилизирующее воздействие на социальную, экономическую сферу, а особенно на граждан, а также в связи с проведением специальной военной операции (СВО), особенно актуален.

Когда Вооруженные силы Российской Федерации проводят специальную военную операцию на Украине, это не только война, которая ведется на поле боя, это, прежде всего и борьба за умы и сердца миллионов граждан России и Украины в сети Интернет.

Используя методы социальной инженерии и искусственного интеллекта, преступники легко завоевывают доверие тех, кто совсем не привык жить в мире цифровых угроз, вербуя граждан России и мигрантов для совершения преступлений.

На сегодняшний день новости о задержании россиян за сотрудничество со спецслужбами Украины уже не вызывают удивление после начала СВО.

Россиян задерживают в разных городах, таких как республика Крым, городах: Нальчик, Дивногорск, Челябинск, Новосибирск, Москва, Махачкала, Дербент, Ростов-на-Дону. По указанию украинских телефонных мошенников россияне поджигают военкоматы, транспортно-информационную структуру, банкоматы. В 2023 и в 2024 гг. были зафиксированы несколько десятков таких случаев по всей стране.

Со стороны Украины в отношении России работает около 400 колл-центров. Киберугрозы продолжают расти как в объеме, так и в сложности.

Основная проблема заключается в использовании ВСУ и связанными с ними структурами (такими как ЦИПсО) методов психологического воздействия, пропаганды, финансовых стимулов и дистанционных технологий для вербовки российских граждан. Это создает угрозу не только для безопасности отдельных лиц, но и для стабильности общества и государственной безопасности.

Недостаточная осведомленность граждан о таких методах делает их уязвимыми для манипуляций, что требует детального анализа и выработки стратегий противодействия.

Вербовка — это комплекс разнообразных агентурно-оперативных и поисковых мероприятий, направленных на завлечения интересующего спецслужбу лица, к сотрудничеству с ними, для выполнения определенных задач разведывательного характера, диверсионных и террористических действий.

Основной целью вербовки российских граждан спецслужбами Украины является создание осведомительной сети и использование ее для следующих задач:

♦ подрыва внутренней стабильности России, через провоцирование насилия, террористических актов, диверсий, саботажа и т. д.;

♦ сбор сведений о действиях Вооруженных сил РФ, силовых структур, систем энерго- и водоснабжения, транспортные сети;

♦ кибершпионаж и хакерские атаки на важные объекты: госпорталы, системы энерго- и водоснабжения, здравоохранение, транспортную инфраструктуру;

♦ влияние на общественное мнение путем подкупа блогеров, распространения фейков, создания иллюзии массового недовольства;

♦ формирование «сети сочувствующих», которые изнутри страны распространяют украинскую националистическую или антироссийскую повестку;

♦ спецслужбы Украины заинтересованы не только в активных действиях агентов, но и в вербовке «спящих ячеек», которые могут быть активированы при необходимости.

Человек, который попал на манипуляционный ресурс, не может остановиться. Момент, когда он начинает выполнять задания кураторов, можно назвать точкой невозврата.

В Международной конвенции о борьбе с вербовкой, использованием, финансированием и обучением наемников, принятой резолюцией 44/34 Генеральной Ассамблеи от 4 декабря 1989 г. закреплено в ст. 5 п. 2: «Государства-участники не вербуют, не

используют, не финансируют и не обучают наемников для цели противодействия законному осуществлению неотъемлемого права народов на самоопределение, признанного международным правом, и принимают в соответствии с международным правом надлежащие меры по предотвращению вербовки, использования, финансирования или обучения наемников для этой цели».

Отрицая и не придерживаясь данной Международной конвенции, Украинские специальные службы систематически нарушают ее в отношении граждан Российской Федерации и лиц, проживающих на территории Российской Федераций. Спецслужбы вербуют в свои ряды граждан России всех возрастов, начиная с детей и заканчивая пенсионерами, и не собираются останавливаться на этом.

Украинские вооруженные силы и спецслужбы активно используют различные методы пропаганды и психологического воздействия для вербовки российских граждан и мигрантов. Они распространяют ложную информацию о ситуации в Украине, создают негативный образ России и используют психологические приемы для манипуляции сознанием людей.

Кроме того, проводятся мероприятия по мобилизации и рекрутированию граждан России в вооруженные силы Украины. Организуются специальные рекрутинговые кампании, проводится обучение и подготовка новобранцев, а также предоставляется материальная поддержка в виде денежного вознаграждения, специальных средств, вооружения (в основном иностранного производства), разных веществ, транспорта и т. п. Всем этим занимается **Центр информационно-психологических операций (ЦИПсО);** он является частью украинских сил специальных операций. В отличие от обычных войск, которые ведут бои с помощью оружия, ЦИПсО специализируется на информационной (гибридной) войне и психологическом давлении на противника.

Для привлечения российских граждан в ряды украинских вооруженных сил предоставляются финансовые стимулы, такие как высокие заработки, дополнительные пособия и премии за выполнение определенных задач.

Украина также использует дипломатическое воздействие, включая убеждение дипломатических представителей России в других странах о важности перехода на сторону Украины.

Вооруженные силы Украины могут применять психологическое давление на российских граждан, чтобы заставить их изменить свое мнение и присоединиться к украинским вооруженным силам. Это может включать угрозы, шантаж или другие методы воздействия на психику личности. Главная опасность вербовки заключается в том, что человеку очень сложно распознать, что его вербуют. Вербовка редко начинается с прямого предложения. Она выстраивается поэтапно и может длиться месяцами.

Существует несколько этапов вербовки лиц:

- 1 этап: зондирование;
- 2 этап: знакомство или установление доверия;
- 3 этап: обещания;
- 4 этап: группа риска (эмоционально и психологически подавленные лица);
- 5 этап: текстовые задания («Напиши надпись», «Размести листовку», «Сделай фото военкомата» и т. д.).

Методы вербовки ЦИПсО российских граждан и меры противодействия.

1. Одним из распространенных методов дистанционной вербовки является OSINT. OSINT — Opensourceintelligence. Разведка по открытым источникам. Эта разведывательная дисциплина зародилась в США еще в начале второй мировой войны. И не секрет, что современные американские соцсети и поисковые системы созданы, в том числе и с использованием военных патентов. С помощью слитых баз данных россиян в сети Интернет спецслужбы Украины имеют доступ к номерам, персональным данным, месту жительства, месту работы, хобби, религиозных убеждений и т. п., что в последствии дает им возможность оказывать на россиян давление и манипулировать ими, делая из них «ракету дистанционного управления».

2. Размещение материалов о потерях личного состава и военной техники РФ на популярных сайтах, видеохостингах и других сервисах в качестве рекламы, часто с демонстрацией трупов убитых солдат в текстовой, фото или видео форме. Проводится с целью устрашения и деморализации российских военнослужащих, их родственников и других граждан. Необходимо игнорировать, по возможности, не просматривать.

3. Телефонный терроризм включает в себя следующие действия:

♦ отправка SMS-сообщений с угрозами, недостоверной информацией, призывами к сдаче в плен и т. п.;

♦ звонки с анонимных номеров, сопровождающиеся угрозами;

♦ звонки с целью шантажа и предложения выкупа пленных военнослужащих и их родственников, захваченных спецслужбами Украины;

♦ звонки с ложными сообщениями о гибели близких родственников в зоне СВО, с целью оказания психологического давления;

♦ использование вышеуказанных методов через мессенджеры, возможно с использованием фото и видеоматериалов;

♦ иные подобные действия.

4. Цель проведения акции — манипуляция. Рекомендуется игнорировать ее. Не вступать в диалог, не принимать во внимание содержание сообщения.

Противник привлекает профессиональных психологов, способных убедить любого человека. Необходимо немедленно прекратить контакт и добавить звонившего (писавшего) в черный список. После этого следует сообщить командиру или компетентным органам.

5. Угроза распространения или публичное распространение персональных данных военнослужащих, должностных и гражданских лиц, активно выражающих свою патриотическую позицию. Цель проведения данной акции — запугивание, убеждение к сотрудничеству или вовлечение в другую незаконную деятельность. Все это рекомендуется игнорировать. Важно помнить, что любое взаимодействие с противником является незаконным. Если у вас есть информация о таких фактах, необходимо сообщить командиру воинского подразделения или компетентным органам.

6. Отправка фотографий школы, где учится ребенок, или фотографий дома, входной двери квартиры, где живет семья, другому члену семьи участника СВО считается доказательством того, что «диверсанты» нашли семью военнослужащего. В таких случаях обычно поступают угрозы убийства родных, если военнослужащий откажется дезертировать или сдаться в плен. В этом случае необходимо сразу доложить командиру и сообщить в компетентные органы о произошедшем.

7. При захвате старшего офицера или офицера спецназа, они могут быть склонены к сотрудничеству с помощью различных методов воздействия на тело и психику с целью сделать их участниками постановочных материалов информационно-психологического воздействия. Например, пленный офицер может в видеообращении заявить, что его захват является вымыслом, и даже утверждать, что он сам захватил солдата противника, указывая при этом название.

Цель проведения таких действий — дезинформировать командование в своей или соседней зоне ответственности, а также привлечь их в засаду. Если обнаружены подобные материалы, необходимо учитывать возможность проведения такой операции и немедленно доложить командованию или сообщить в компетентные органы населенного пункта, где он находится, и просить о помощи.

8. Создание и реклама информационного ресурса в Интернете, организующего городские игры и квесты по принципу AlternateRealityGames (ARG). Основной принцип ARG — TINAG (Thisisnot a game — «Это не игра»), предполагает, что игра должна быть неразличима от реальности. Участники ARG узнают правила постепенно, взаимодействуя с персонажами игры через общение в сети. Хотя игры в альтернативной реальности проходят в основном в Интернете, они могут переходить в реальный мир, например, при сборе игроков в определенном месте для получения информации. В таких играх участвуют «кукловоды» — организаторы, предлагающие игрокам разгадывать загадки и выполнять задания с материальным вознаграждением. В частности, на Донбассе проводилась подобная операция под названием «Молодежное движение «Рейв». По началу задания для участников были разные, в основном безобидные. Сфотографировать рассвет около стадиона «Донбасс-Арена» или магазин «Авоська», затем — автомобиль «Урал» (а они на Донбассе только армейские), место нахождения воинской части в своем районе, якобы для того, чтобы показать, что ВСУ обстреливают не ее, а мирные дома школы, детские сады и т. п. Эти фотографии игроки отправляли организаторам «игры», тем самым совершая тяжкие преступления, сами того не понимая.

Основные принципы выявления фейкового материала:

♦ необходимо определить, какая сторона получит выгоду от публикации данного материала;

♦ необходимо обратить внимание на первоисточник — информационный ресурс, на котором этот материал был опубликован изначально. Часто фейки публикуются анонимными источниками, информационными ресурсами без истории, безликими или фейковыми аккаунтами в социальных сетях, враждебными информационными ресурсами или ресурсами, которые маскируются под российские. Иногда враждебные официальные СМИ могут быть первоисточниками, но это редкость. Еще реже враждебные дип-фейки могут появиться на некоторых российских информационных ресурсах, администраторы которых не проверили материал должным образом;

♦ фейковые материалы создаются таким образом, чтобы их опровержение было невозможно, сложно или требовало больше времени, чем распространение и внедрение фейка. Поэтому люди на видео могут быть сняты в масках, скрывать лица от камеры или их лица просто неразличимы (например, из-за ракурса или плохого качества видео). Очень редко такие материалы могут быть сняты с открытыми лицами, но это возможно.

Противник также избегает характерных черт и ориентиров, которые могут указывать на место съемки (например, линии электропередач, узнаваемые строения, украинская минеральная вода на фоне и т. д.);

♦ необходимо применить логику. Задать себе вопрос: «Логично ли то, что я вижу?». Для простоты можно представить себя на месте людей на видео и представить, как бы мы себя вели в подобной ситуации;

♦ очень редко в постановочных материалах используются профессиональные актеры. Это позволяет распознать фейк по неестественным или наигранным фразам и движениям людей на видео;

♦ часто в постановочных видео добавляются дополнительные фоновые звуки (стрельба, взрывы, звуки разбивания посуды или стекла, шум автотранспорта, движение военной техники, детский плач и т. д.). Без опыта и специального оборудования можно распознать подделку по разнице в громкости звуков.

Киберпреступники Украины и западных специальных служб придумывают все новые и новые схемы обмана и шантажа, при этом обещают баснословные выигрыши и легкие заработки с одной целью — выманить деньги у доверчивых граждан, особенно у пенсионеров и молодых людей, и затем их провоцируют на совершение преступлений.

По-прежнему среди ключевых задач органов внутренних дел это противодействия преступлениям в сфере информационных технологий. Это колоссальный объем преступлений и колоссальный объем пострадавших и задержанных.

Украинские националисты активно использовались в прошлом и используются спецслужбами Запада и США в настоящее время для подрывной деятельности против Российской Федерации. Западные и американские спецслужбы отводят им определенную роль и в своих агрессивных планах на будущее против России. В Украине и за ее пределами продолжают активную деятельность русофобские центы и организации украинских националистов, состоящие на службе у разведок Запада и США, готовящихся к диверсионно-террористическим актам и вербовке наших граждан для совершения преступлений.

Националистические элементы проживают как в Украине, так и в разных субъектах России, но все они вынашивают замыслы в создании «самостийной» Украины и проведении подрывной деятельности против России.

Проведенное исследование демонстрирует, что вербовка российских граждан для совершения преступлений представляет собой системную угрозу, реализуемую через комплекс методов гибридной войны — от психологического давления и пропаганды до цифровых технологий (OSINT, ARG-квестов) и прямого шантажа. Противодействие требует многоуровневого подхода: ужесточения законодательства, усиления киберзащиты, международного сотрудничества и, главное, повышения медиаграмотности населения. Ключевым фактором устойчивости общества является способность граждан распознавать манипуляции, а государства — оперативно нейтрализовать угрозы, сочетая правовые, технологические и просветительские меры. Только такая стратегия позволит эффективно защитить национальную безопасность в условиях эскалации информационных войн. Националисты Украины всегда выражали свое недовольство к Российской Федерации.

В современном мире идет жесткая конкуренция, агрессивная борьба за влияние на умы людей.

Библиографический список

1. Резолюция Генеральной Ассамблеи ООН 44/34 от 4 декабря 1989 г. «Международная конвенция о борьбе с вербовкой, использованием, финансированием и обучением наемников» // СПС «КонсультантПлюс».

2. Петров С. А. Методы информационно-психологического воздействия в современных конфликтах // Национальная безопасность. 2023. № 4. С. 45–58.

3. Смирнова Е. В. OSINT-технологии в гибридных войнах: угрозы и противодействие // Вестник МГИМО. 2022. № 3. С. 112–125.

4. Ионов В. Преступники поневоле? Как россиян втягивают в предательство // Щит и меч. 2025. 23 окт.

5. URL: https://www.mid.ru/ru/

6. URL: https://www.cert.ru

Bibliographic list

1. UN General Assembly Resolution 44/34 of December 4, 1989 «International Convention on combating the Recruitment, Use, Financing and Training of Mercenaries» // LRS «ConsultantPlus».

2. Petrov S. A. Methods of information and psychological impact in modern conflicts // National Security. 2023. No. 4. P. 45–58.

3. Smirnova E. V. OSINT technologies in hybrid wars: threats and counteraction // Bulletin of MGIMO. 2022. No. 3. P. 112–125.

4. Ionov V. Involuntary criminals? How Russians are being dragged into betrayal // Shield and sword. 2025. October 23.

5. URL: https://www.mid.ru/ru/

6. URL: https://www.cert.ru

Информация об авторах

А. В. Богданов — доцент кафедры оперативно-разыскной деятельности и специальной техники Московского университета МВД России имени В.Я. Кикотя, доцент;

О. В. Кудин — доцент кафедры оперативно-разыскной деятельности и специальной техники Московского университета МВД России имени В.Я. Кикотя, доцент.

Information about the authors

A. V. Bogdanov — Associate Professor of the Department of Operational Investigative Activities and Special Equipment of the Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot', Associate Professor;

O. V. Kudin — Associate Professor of the Department of Operational Investigative Activities and Special Equipment of the Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot', Associate Professor.

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

Contribution of the authors: the authors contributed equally to this article. The authors declare no conflicts of interests.

Статья поступила в редакцию 05.11.2025; одобрена после рецензирования 12.11.2025; принята к публикации 19.11.2025.

The article was submitted 05.11.2025; approved after reviewing 12.11.2025; accepted for publication 19.11.2025.