RUDN Journal of Political Science. ISSN 2313-1438 (Print), ISSN 2313-1446 (Online) **2025 Vol. 27 No. 3 579–589**
Вестник Российского университета дружбы народов. Серия: ПОЛИТОЛОГИЯ http://journals.rudn.ru/political-science

DOI: 10.22363/2313-1438-2025-27-3-579-589
EDN: MSIFJY

Научная статья / Research article

Подходы Турецкой Республики к обеспечению цифровой безопасности и регуляции СМИ

В.А. Аватков, Л.Д. Мишин

Институт научной информации по общественным наукам Российской академии наук,
Москва, Российская Федерация
✉ v.avatkov@gmail.com

Аннотация. Турецкая Республика за последнее десятилетие продемонстрировала значительный рост влияния на мировой арене, усиление амбиций в области информационной безопасности также не обошло стороной Турецкую Республику. Турция на данный момент находится в авангарде развития цифровых и информационных инициатив среди государств Ближнего Востока. Не последнее место в новостных сводках страны занимают и новости блокировки и актов активной регуляции интернет и традиционных СМИ, которые вызывают все большую озабоченность турецкого общества. Рассмотрены исторические предпосылки, правовая база, актуальное состояние и тенденции в подходах к обеспечению цифровой и информационной безопасности Турции, а также регулятивной функции государства по отношению к интернету и СМИ. В качестве методологической основы исследования был использован кейс-стади конкретных примеров, настроивших руководство Турции на непосредственное вовлечение в процессы регулирования информационного пространства и СМИ. Помимо этого, был проведен контент-анализ, подкрепленный изучением уставных документов основных регуляторных структур Турции. В ходе работы были также изучены ключевые статьи и монографии ведущих турецких ученых в области юриспруденции, информационной безопасности и истории информационного поля страны. Выявлено, что одной из основных причин усиления контроля за информационным пространством стала нацеленность ряда кибератак на окружение президента Р.Т. Эрдогана. Вместе с тем подчеркивается, что народные волнения последних лет стали дополнительным триггером для изменения подходов к обеспечению цифровой безопасности и регулированию СМИ.

Ключевые слова: Турция, информационная безопасность Турции, цифровая безопасность Турции, безопасность Турции, внутренняя политика Турции

Заявление о конфликте интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования: *Аватков В.А., Мишин Л.Д.* Подходы Турецкой Республики к обеспечению цифровой безопасности и регуляции СМИ // Вестник Российского университета дружбы народов. Серия: Политология. 2025. Т. 27. № 3. С. 579–589. https://doi.org/10.22363/2313-1438-2025-27-3-579-589

Turkey's Strategies for Ensuring Digital Security and Regulating Media Landscape

Vladimir A. Avatkov, Lev D. Mishin

Institute of Scientific Information on Social Sciences of the Russian Academy of Sciences,
Moscow, Russian Federation

✉ v.avatkov@gmail.com

Abstract. The Republic of Turkey has demonstrated a significant increase in influence on the world stage over the past decade, and the rise of information security ambitions has not been lost on the Republic of Turkey either. Turkey is currently at the forefront of digital and information initiatives in the Middle East. Not the least place in the country's news reports is occupied by news of blocking and acts of active regulation of Internet and traditional media, which are of growing concern to Turkish society. The research paper discusses in detail the historical background, legal basis, current state and trends in approaches to ensuring digital and information security in Turkey, as well as the regulatory function of the state in relation to the Internet and media. As a methodological basis for the study, a case study of specific examples was used, setting up the Turkish leadership to be directly involved in the processes of regulating the information space and media. In addition, a content analysis was conducted, supported by a study of the statutes of the main regulatory structures in Turkey. Key articles and monographs by leading Turkish scholars in the fields of jurisprudence, information security and its history were also studied. It was revealed that one of the main reasons for the strengthening of control over the information space was the targeting of a number of cyber attacks on the entourage of President R.T. Erdogan. At the same time, it is emphasized that the unrest of recent years has become an additional trigger for changing approaches to digital security and media regulation.

Keywords: Turkey, information security of Turkey, digital security of Turkey, security of Turkey, internal policy of Turkey

Conflicts of interest. The authors declare no conflicts of interest.

For citation: Avatkov, V.A., & Mishin, L.D. (2025). Turkey's strategies for ensuring digital security and regulating media landscape. *RUDN Journal of Political Science*, 27(3), 579–589. (In Russian). https://doi.org/10.22363/2313-1438-2025-27-3-579-589

Введение: исторические предпосылки развития кибербезопасности в Турции

Турецкая Республика стала одним из первых государств Ближнего Востока, институционализировавших подразделения по обеспечению информационной безопасности [Ulas 2015: 83–93]. Одной из причин активизации повышенного

внимания государственного аппарата к развитию и становлению под централизованное управление данного ответвления национальной безопасности стала масштабная, а также самая крупная в XXI в. хакерская атака на государственные системы Турции со стороны леворадикальной группировки Redhack в 2012 г., которая с конца XX в. организовывала масштабные нападения на базы данных, критическую структуру и документы, компрометирующие определенных политических деятелей. Среди самых ярких атак необходимо отметить проникновение в сеть командования турецкой армии, а также взлом баз данных с счетами за электроэнергию граждан Турции и их полное удаление[1].

В 2012 г. группировка предприняла попытку обратить внимание на коррупционные связи семьи Р.Т. Эрдогана. Например, был получен 17-гигабайтный архив электронной почты министра энергетики и зятя президента Б. Албайрака, в котором были обнаружены следы коррупционных схем и актов кумовства[2]. Помимо этого, были опубликованы доказательства экономического сотрудничества (покупки нефти) семьи Р.Т. Эрдогана и запрещенной в России организации ИГИЛ. Данный факт был подтвержден несколькими годами позже, когда Минобороны России опубликовало доказательства закупок нефти у террористов со стороны Турции[3].

Реакция на подобные «сливы» не заставила себя долго ждать. Почти сразу аккаунты группировки во многих соцсетях были заблокированы по требованию турецких властей. Более того, ответа на представленные группировкой обвинения потребовал и Европейский Союз, после чего президент Эрдоган заявил, что готов понести ответственность, если будут предоставлены конкретные доказательства[4]. Однако конкретных обоснований европейцами предоставлено не было.

Последствием этих скандальных атак стал созыв Совета министров 20 октября 2012 г., в ходе которого было принято решение о создании Совета по кибербезопасности на платформе Министерства транспорта, морских дел и коммуникаций. Среди задач новообразованного Совета стало обеспечение мер по защите государственных учреждений и конфиденциальности от хакерских атак. С этого началась современная централизованная система обеспечения национальных интересов Турции в киберпространстве [Çakır, Taşer 2022: 346–366].

Вслед за этим последовал следующий этап институционализации инициатив по защите информационной безопасности Турции. Так, в 2013 г. была принята первая стратегия Национальной безопасности в киберпространстве, целями

[1] RedHack bu kez TRT'ye saldırdı. URL: https://www.hurriyet.com.tr/teknoloji/redhack-bu-kez-trtye-saldirdi-21088808 (accessed: 17.04.2025).

[2] RedHack madde madde anlattı: Damat Berat'ın hesabı nasıl ele geçirildi? URL: https://www.cumhuriyet.com.tr/haber/redhack-madde-madde-anlatti-damat-beratin-hesabi-nasil-ele-gecirildi-608331 (accessed: 17.04.2025).

[3] Минобороны России: Семья Эрдогана покупает краденую нефть у террористов. URL: https://www.kp.ru/daily/26465/3335897/ (дата обращения: 17.04.2025).

[4] Erdoğan'dan Redhack açıklaması. URL: https://www.sozcu.com.tr/erdogandan-redhack-aciklamasi-wp298898 (accessed: 17.04.2025).

которой были заявлены защита конфиденциальности, информации и выявление угроз в киберпространстве и внутри Турецкой Республики[5]. В 2016 г. была принята новая редакция Стратегии, которая в целом мало чем отличалась от редакции 2013 года[6]. Среди нововведений можно отметить лишь повышенное внимание к защите личных данных граждан Турции, а также усиление мер по поиску и привлечению к ответственности киберпреступников, что, по мнению составителей документа, способно обеспечить более полную безопасность национальных интересов страны. Помимо этого, существенным изменениям подверглись подходы к правам человека — акцент на методы Европейского союза в данной сфере.

Параллельно с программными документами, касающимися институционализации данного процесса, создавались и оперативные группировки из нескольких десятков до нескольких сотен человек, призванных курировать интернет- и киберпространство. Например, в 2011 г. было создано в экспериментальном формате подразделение из 200 человек, интегрированное в армию Турции. Среди задач подразделения было отражение атак на государственные и бизнес-структуры. Следует отметить, что данная инициатива была ответом на распространившийся по всему миру компьютерный вирус WannaCry[7], который не обошел стороной и Турцию.

Тем не менее данная группировка специалистов, интегрированных в армию, не смогла оказать противодействие атаке Redhack годом позднее, что вынудило турецкое руководство расширить инициативы по созданию дополнительных группировок и институционализированных подразделений. Так, вскоре после атаки Redhack был создан Командный центр киберзащиты, который годом позже был преобразован в Командование киберзащиты ВС Турции[8].

В рамках департаментов Командования киберзащиты ВС Турции выделяются следующие: правоохранительный, военный, морской, космический и комплексной обороны.

Первостепенная задача правоохранительного департамента — защита критической инфраструктуры, что было продиктовано необходимостью поставить

[5] Türkiye. Ulusal Siber Güvenlik Stratejisi. URL: http://www.bilgiguvenligi.org.tr /wp-content/uploads/2016/03/Ulusal_Siber_Guvenlik_Stratejisi.pdf (accessed: 17.04.2025).

[6] UlusalSiberGuvenlikStratejisi. URL: https://www.sbb.gov.tr/wp-content/uploads/2018/10/2016-2019UlusalSiberGuvenlikStratejisi.pdf (accessed: 17.04.2025).

[7] Турция планирует создать киберармию для защиты от хакерских атак. URL: https://news.rambler.ru/middleeast/36909963-turtsiya-planirauet-sozdat-kiberarmiyu-dlya-zaschity-ot-hakerskih-atak/ (дата обращения: 17.04.2025).

[8] ВС Турции — лидер в сфере разработок технологий кибер-защиты. URL: https://www.aa.com.tr/ru/%D0%B7%D0%B0%D0%B3%D0%BE%D0%BB%D0%BE%D0%B2%D0%BA%D0%B8-%D0%B4%D0%BD%D1%8F/%D0%B2%D1%81-%D1%82%D1%83%D1%80%D1%86%D0%B8%D0%B8-%D0%BB%D0%B8%D0%B4%D0%B5%D1%80-%D0%B2-%D1%81%D1%84%D0%B5%D1%80%D0%B5-%D1%80%D0%B0%D0%B7%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%BE%D0%BA-%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B9-%D0%BA%D0%B8%D0%B1%D0%B5%D1%80-%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D1%8B/584148 (дата обращения: 17.04.2025).

под централизованный контроль оборону от внешних кибератак после атак группировки Redhack и вируса WannaCry.

Военный департамент активно занимается продвижением наступательной стратегии, что было доказано в 2018 г. подавлением формированиями данной структуры американского ЗРК Patriot, переданного Турции Германией на хранение, располагавшегося на границе с Сирией, что стало одним из главных аргументов для последующей покупки российских систем С-400[9].

Морской департамент отвечает за безопасность инфраструктуры военных и гражданских судов, а также объектов береговой охраны. Необходимо отметить, что особенную важность данный департамент приобрел после начала активных геологоразведывательных работ Турции на шельфе Средиземного моря в рамках доктрины «Голубая Родина» [Аватков, Мишин 2024: 7–22].

Космический департамент отвечает за безопасность космических объектов и спутников. Департамент комплексной обороны специализируется на контрразведывательной деятельности, а также выявлении уязвимостей в военной инфраструктуре [Ковалев, Скипидаров 2021: 197–205].

Через несколько лет после данных первых шагов Турецкая Республика приступила к созданию центров по подготовке специалистов по обеспечению национальных интересов Турции в киберпространстве. Например, в 2016 г. на базе Командования киберзащиты был создан Центр электронной войны в Конье, целями и задачами которого заявлялись подготовка кадров к ведению боевых действий в киберпространстве, а вскоре после этого, в 2017 г., был создан Центр мониторинга киберугроз, который был нацелен на защиту внутри страны[10]. Необходимо отдельно подчеркнуть, что данная организация была отмечена в отслеживании антиправительственных комментариев и передаче информации об этом в вышестоящие органы, после чего несколько раз были заблокированы такие соцсети, как Youtube и Twitter (запрещен в России)[11].

Таким образом, можно отметить, что главным драйвером для активизации процесса выстраивания структуризации информационной безопасности Турции стал целый ряд масштабных атак на государственную систему Турции. Более того, особенный импульс это развитие получило после того, как хакеры перешли к действиям, направленным против турецкой элиты, тесно связанной с президентом Р.Т. Эрдоганом.

Масштаб организационных мероприятий по постановке сферы информационной безопасности на институционализированные рельсы сложно недооценить, однако не все из них оказывались успешными, но руководство Турецкой Республики активно извлекало уроки из каждого провала.

---

[9] Хакеры взломали зенитные ракетные комплексы Patriot. URL: https://nplus1.ru/news/2015/07/09/patriot (дата обращения: 17.04.2025).

[10] Konyanin en modern askeri tesisleri inşa ediliyor. URL: https://rayhaber.com/2024/10/konyanin-en-modern-askeri-tesisleri-insa-ediliyor/ (accessed: 17.04.2025).

[11] Турция закрыла доступ к самым популярным соцсетям. URL: https://news.ru/world/turciya-zakryla-dostup-k-samym-populyarnym-socsetyam/ (дата обращения: 17.04.2025).

Основные документы и ведомства в сфере информационной безопасности Турции

Основу правовой базы, обеспечивающей проведение политики в сфере политики безопасности страны, является Стратегия национальной безопасности, в которой пятая статья посвящена информационному ее аспекту. Данный документ обновляется каждые 5 лет, а последняя его редакция была выпущена 22 января 2025 г.[12] В данном документе особенно выделяются угрозы в киберсфере со стороны Рабочей партии Курдистана и курдских повстанцев в частности. РПК называется главной угрозой национальной безопасности в информационной сфере Турции. Вместе с этим отдельно подчеркиваются возрастающие угрозы со стороны искусственного интеллекта, который связывается со всё большей хаотичностью выстраивающегося полицентричного мира [Сбитнева 2023, 57–61].

Помимо этого, существует учрежденная правительством Организация кибербезопасности (Siber güvenlik teşkilatı), которая собирает информацию о новых угрозах и прецедентах в цифровом пространстве. Также ежегодно обновляется Национальная стратегия кибербезопасности. Последняя ее редакция была опубликована в сентябре 2024 г.[13] Среди ее ключевых положений необходимо выделить опору на цифровую безопасность в вопросах обеспечения стабильности в критической инфраструктуре, направленность на защиту человеческого капитала, а также активную защиту от всех киберугроз граждан Турецкой Республики. Следует заметить, что в данной концепции особое внимание уделяется усовершенствованию подходов к оборонительным действиям в цифровом пространстве, однако отдельно выделяется не только допустимость, но и целесообразность наступательных действий в данной сфере[14]. Первая ее формация появилась 2013 г. и называлась «Стратегия национальной кибербезопасности: план действий на 2013–2014 годы». В течение следующих она ежегодно обновлялась, однако ключевые положения документа изменениям не подвергались [Karasoy, Baboğlu 2021: 123–155].

Помимо упомянутой Организации кибербезопасности одну из ключевых ролей в защите страны от кибератак занимает Совет по цифровым технологиям и связи (Bilgi Teknolojileri ve İletişim Kurumu (BTK), который объединяет под своим началом большинство малых агентств с более узкими компетенциями. Среди основных целей организации заявлены регуляция в сферах телекоммуникации, интернета, радио и телевидения, а также обеспечение конкурентности в данных сферах и защита прав пользователей[15]. Вместе с тем подведомственные

[12] Türkiye updates National Security Policy document at first NSC meeting of 2025. URL: https://www.turkiyetoday.com/turkiye/turkiye-updates-national-security-policy-document-at-first-nsc-meeting-of-2025-109876/ (accessed: 17.04.2025).

[13] Siber teşkilat ulusal siber guvenlik strateji ve eylem plani 2024–2028. URL: https://siberteskilat.org/wp-content/uploads/2024/11/siber-teskilat-ulusal-siber-guvenlik-strateji-ve-eylem-plani-2024-2028.pdf (accessed: 17.04.2025).

[14] Ulusal siber guvenlik stratejisi 2020–2023. URL: http://www.sp.gov.tr/upload/xSPTemelBelge/files/HwolM+ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf (accessed: 17.04.2025).

[15] BTK sitesi. URL: https://www.btk.gov.tr/ (accessed: 17.04.2025).

агентства выполняют непосредственные функции защиты киберпространства. Прямым аналогом данной организации в России является Роскомнадзор, который объединяет под своим началом целую сеть агентств и ведомств.

Основным документом, регулирующим деятельность данного Совета, является четырехлетний план, в котором обозначаются основные направления деятельности организации, ее цели и задачи. Миссией организации заявлено «обеспечение преобразования в информационное общество путем создания эффективной и устойчивой конкуренции в секторе информации и связи, повышения удовлетворенности заинтересованных сторон путем защиты их прав и интересов и содействия технологическим разработкам»[16].

Взгляд руководства организации на свою деятельность, утвержденный Стратегическим планом, звучит так: «…стремление сделать нашу страну эффективной, конкурентоспособной и инновационной на международном уровне в сфере информации и связи». Важнейшими же ценностями называются «объективность и надежность, открытость и прозрачность, предсказуемость и последовательность, взаимодействие и командная работа, научная и информационная ориентация, инновации и постоянное совершенствование, эффективное использование ресурсов, социальная ответственность и отзывчивость, а также ориентация на конечного пользователя» [Aslay 2017: 24–28]. Необходимо отметить, что BTK редко непосредственно занимается блокировками и модерацией интернет-контента, делегируя данное право своим подведомственным агентствам и организациям.

Одна из них — Национальный центр по реагированию на киберпреступления Турции (Ulusal Siber Olaylara Müdahale Merkezi (USOM)), задачами которого являются следующие: выявление и анализ киберугроз; борьба с атаками на критически важные объекты; координация и информирование государственных органов; разработка локальных и национальных решений в области кибербезопасности[17]. Под эгидой USOM выпускается Стратегия защиты критической инфраструктуры, которая в целом во многом созвучна со Стратегией национальной кибербезопасности. Основной вид деятельности USOM: сканирование IP-адресов на предмет наличия проблем с кибербезопасностью [Şentürk, Zaim Çil, Sağıroğlu 2012: 112–125]. По официальным сообщениям, USOM ежесуточно предотвращает сотни крупных атак на интернет-ресурсы Турции, а также блокирует доступ вредоносным ресурсам. Только за 2023 г. было предотвращено до 140 тыс. крупных атак на ресурсы страны. Особое внимание населения, государственных структур и СМИ к деятельности USOM было привлечено после теракта спецслужб Израиля против руководства ливанской Хезболлы[18]. По за-

[16] 2024–2028 STRATEJİK PLANI. URL: https://www.btk.gov.tr/uploads/pages/yayinlar-stratejik-planlar/btk-2024-2028-stratejik-plani.pdf (accessed: 17.04.2025).

[17] USOM sitesi. URL: https://www.usom.gov.tr/ (accessed: 17.04.2025).

[18] Telsizlerin Patlamasından Sonra Değeri Daha İyi Anlaşıldı: USOM Nedir ve Tam Olarak Ne İş Yapıyor? URL: https://www.webtekno.com/usom-nedir-ne-yapar-h149265.html (accessed: 17.04.2025).

явлениям организации, были приняты все меры предосторожности, чтобы подобного не произошло в Турции.

Среди ведомств, так или иначе связанных с кибербезопасностью Турции, представлен TÜBİTAK — Совет по научным и техническим исследованиям Турции. Данная организация лишь косвенно касается кибербезопасности страны. В ее компетенции находятся научное сопровождение технического прогресса в стране. Однако данная организация активно занимается разработкой научных решений для обеспечения основных запросов правительства в сфере цифровой безопасности[19].

Наиболее известная в обществе Турции организация, которая принимает непосредственные решения по блокировке и штрафам СМИ, — RTÜK (Высший совет радио и телевидения). Среди компетенций Совета: регуляция традиционных СМИ (контроль за соблюдением законов в эфире радио и телевидения, включая лицензирование и мониторинг контента; штрафы за нарушения этических норм. Например, в 2020 г. был наложен штраф на один из телеканалов, который транслировал сериал, в котором якобы пропагандировались внебрачные отношения[20]; также с 2018 г. Совет регулирует онлайн-трансляции традиционных СМИ (в основном телеканалов); инструментарии для блокирования иностранных СМИ, если они не соответствуют законодательству (например, неоднократно подвергались блокировке каналы «DW» и «Голос Америки»[21])[22]; а также цензура определенных программ, не соответствующих традиционным ценностям Турции.

Современное состояние информационной безопасности и опыт борьбы с угрозами

На современном этапе основной фронт работы государственных структур по контролю за информационной безопасностью проходит в сфере блокировок противоправного контента, в том числе в качестве ответа на происходящие в стране социальные потрясения [Irak, Yazıcıoğlu 2012: 133]. Помимо этого, постоянно проводятся комплексные мероприятия по предотвращению кибератак на критическую инфраструктуру.

Например, в 2023 г. Турция столкнулась с несколькими крупномасштабными кибератаками, нацеленными на финансовые учреждения, телекоммуникационные сети и государственные платформы. Также среди кейсов нападений хакеров на Турцию, помимо упомянутых группировок Redhack и вируса WannaCry, важно отметить атаку на оборонный комплекс страны в 2024 г. со стороны южноазиатской группировки Bitter, нацеленной на внедрение вируса с последующим

[19] TÜBİTAK sitesi. URL: https://tubitak.gov.tr/tr (accessed: 17.04.2025).

[20] RTÜK'ten Sadakatsiz'e 'evlilik dışı ilişki' cezası. URL: https://www.gazeteduvar.com.tr/rtukten-sadakatsize-evlilik-disi-iliski-cezasi-haber-1503751 (accessed: 17.04.2025).

[21] «DW» и «Голос Америки» включены в российский реестр СМИ-иноагентов.

[22] RTÜK'ün Başvurusu Üzerine Sulh Ceza Hakimliği Dw ve Voa Türkçe Haber Sitelerine Erişim Engeli Getirdi. URL: https://www.haberler.com/guncel/rtuk-un-basvurusu-uzerine-sulh-ceza-hakimligi-dw-15050528-haberi/ (accessed: 17.04.2025).

шантажом правительства Турции[23]. Можно подчеркнуть, что интегрированные в государственные учреждения группировки, основанные на базе выводов атак 2012–2013 гг., успешно справились с минимизацией ущерба.

Что касается кейсов регуляции СМИ и интернета, то самыми известными случаями стали протесты в парке Гези в 2013 г., которые сначала разразились из-за вырубки деревьев в парке, который считался экологами жемчужиной природного достояния Стамбула. Впоследствии протесты приобрели антиправительственные очертания, в ходе которых выдвигались требования по отставке правительства Справедливости и развития и Р.Т. Эрдогана в частности. В ходе данных событий впервые в истории страны широко применялись ограничительные инструменты BTK и ее подведомственных организаций.

Например, когда протесты приняли откровенно антиправительственный характер, власти страны инициировали процесс блокировки двух крупнейших социальных сетей: Twitter и Instagram (принадлежит экстремистской организации Meta, запрещенной в России)[24]. Многие участники процесса и оппозиция обвинили правительство страны, и в частности USOM и BTK, в цензуре информационного поля. Помимо соцсетей было приостановлено вещание ряда телеканалов и запрет им на ведение трансляций с протестов. Данное решение было вынесено RTÜK, которое на протяжении нескольких лет и на сегодняшний день активно продолжает блокирующую деятельность в отношении телеканалов в ходе волнений[25].

Тем не менее данные события стали лишь прологом к активному использованию регулятивных инструментов по отношению к блокировкам социальных сетей и запретам на вещание различным телеканалам.

Наиболее красноречивым закреплением пройденных уроков протестов в Парке Гези 2013 г. стали беспорядки 2025 г., которые разразились по причине ареста мэра Стамбула из Народно-республиканской партии Э. Имамоглу по обвинению в нескольких преступлениях. Среди них значились коррупционные кейсы, а также обвинения в поддержке террористической деятельности.

По результатам данного задержания разгорелись масштабные акты гражданского неповиновения, для координации которых активно использовались соцсети. В марте 2025 г., в самый разгар протестов, были заблокированы соцсети X (запрещена в РФ), Youtube, Instagram (запрещена в РФ) и TikTok (приостановил работу в РФ)[26], что вызвало шквал негодования среди турецкой

[23] Bitter APT Targets Turkish Defense Sector with WmRAT and MiyaRAT Malware. URL: https://thehackernews.com/2024/12/bitter-apt-targets-turkish-defense.html (accessed: 17.04.2025).

[24] Twitter отказался сотрудничать с турецкими властями. URL: https://lenta.ru/news/2013/06/26/twitter/ (accessed: 17.04.2025).

[25] İstanbul Cumhuriyet Başsavcılığı, Gezi parkı olaylarıyla ilgili RTÜK'ten medya kayıtlarını talep etti. URL: https://www.ilkhaber-gazetesi.com/gundem/istanbul-cumhuriyet-bassavciligi-gezi-parki-olaylariyla-ilgili-rtuk-ten-medya-kayitlarini-talep-etti-255592 (accessed: 17.04.2025).

[26] Washington Post: Türkiye'deki protestolar gençlik içinde uyanış başlattı. URL: https://www.nefes.com.tr/washington-post-turkiyedeki-protestolar-genclik-icinde-uyanis-baslatti-27904 (accessed: 17.04.2025).

общественности, поддержанной оппозицией. Более того, судебная система страны также не нашла в данных актах противоречия закону и подтвердила их легитимность.

Заключение

Таким образом, можно подчеркнуть, что основной импульс развитию информационной безопасности и мерам по борьбе с внешними киберугрозами был придан после того, как хакеры предприняли попытку сбора компромата на ближайших сподвижников и родственников президента Р.Т. Эрдогана, который мог стать причиной для крупного международного скандала. Следует констатировать, что, в случае если бы хакеры не нацелились на личность президента, развитие данного направления как минимум бы не приняло столь быстрого характера.

Что касается работы турецких интернет и СМИ регуляторов, то импульс развития им придали опасения руководства страны вокруг возможности гибкой координации антиправительственных протестов. В 2013 г. власти страны впервые применили масштабные блокировки соцсетей, а также ограничения на телеканалы, ведшие прямые трансляции с протестов. На современном этапе, в 2025 г., данная блокирующая функция турецких государственных ведомств вышла на новый уровень, когда в одночасье в нескольких городах был отключен интернет и был ограничен доступ к некоторым социальным сетям, что, следует подчеркнуть, сыграло определенную роль в снижении протестного потенциала и возможностей оппозиции по мобилизации населения.

Поступила в редакцию / Received: 07.03.2025
Доработана после рецензирования / Revised: 21.04.2025
Принята к публикации / Accepted: 29.04.2025

Библиографический список

Аватков В.А., Мишин Л.Д. «Голубая Родина» как этап выстраивания субъектности Турции // Ближний и Постсоветский Восток. 2024. № 3 (7). С. 7–22. http://doi.org/10.31249/j.2949-2408.2024.03.01. EDN: ADZLAE

Ковалев О.Г., Скипидаров А.А. Организационно-правовые особенности построения системы кибербезопасности в зарубежных государствах (на примере модели Турецкой Республики) // Столыпинский вестник. 2021. № 3 (2). С. 197–205. EDN: BPUWCP

Сбитнева А.И. Международное сотрудничество Турции в области безопасности // Международные отношения в условиях новых угроз безопасности : сборник Международной научно-практической конференции. Москва : МГЛУ, 2023. С. 57–61. EDN: KIRXBI

Aslay F. Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi // *IJMSIT*. 2017. Vol. 1, no. 1. S. 24–28.

Çakır H., Taşer M. Türkiye'de Yapılan Siber Güvenlik Faaliyetlerinin ve Eğitim Çalışmalarının Değerlendirilmesi // Gazi Üniversitesi Fen Bilimleri Dergisi Part C Tasarım ve Teknoloji. 2022. № 11(2). S. 346–366.

Irak D., Yazıcıoğlu O. Türkiye ve sosyal medya / S Arıcıoğlu. (ed.) İstanbul : Okuyanus 2012. S. 133.

Karasoy H.A., Babaoğlu P. Türkiye'de siber güvenlik: yasal ve kurumsal altyapi // Yasama Dergisi. 2021. No. 44. S. 123–155.

Şentürk H., Zaim Çil C., Sağıroğlu Ş. Cyber Security Analysis of Turkey // International journal of information security science. 2012. Vol. 1, no. 4. P. 112–125.

Ulas G. Information Security Strategies in Turkey: Current Status, Government Policies & Recommendations // Computers & Security. 2015. No. 56. P. 83–93.

References

Aslay, F. (2017). Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi. *IJMSIT*, *1*(1), 24–28. (In Turkish).

Avatkov, V.A., & Mishin, L.D. (2024). "Mavi Vatan" as a stage of building Turkey's subjectivity. *Middle and Post-Soviet East, 3*(7), 7–22. (In Russian) http://doi.org/10.31249/j.2949-2408.2024.03.01. EDN: ADZLAE

Çakır, H., & Taşer, M. (2022). Türkiye'de Yapılan Siber Güvenlik Faaliyetlerinin ve Eğitim Çalışmalarının Değerlendirilmesi. *Gazi Üniversitesi Fen Bilimleri Dergisi Part C Tasarım ve Teknoloji, 11*(2), 346–366. (In Turkish).

Irak, D., & Yazıcıoğlu, O. (2012). Türkiye ve sosyal medya. In S. Arıcıoğlu (Ed.), *Türkiye ve sosyal medya* (p. 133). İstanbul: Okuyanus. (In Turkish).

Karasoy, H.A., & Babaoğlu, P. (2021). Türkiye'de siber güvenlik: Yasal ve kurumsal altyapi. *Yasama Dergisi*, *44,* 123–155. (In Turkish).

Kovalev, O.G., & Skipidarov, A.A. (2021). Organizational and legal features of building a cybersecurity system in foreign states (based on the model of the Republic of Turkey). *Stolypin Bulletin, 3*(2), 197–205. (In Russian) EDN: BPUWCP

Sbitneva, A.I. (2023). International cooperation of Turkey in the field of security. In *International Relations in the Context of New Security Threats, Proceedings of the International Conference* (pp. 57–61). Moscow, Moscow Linguistic University. (In Russian) EDN: KIRXBI

Şentürk, H., Çil, C.Z., & Sağıroğlu, Ş. (2012). Cyber security analysis of Turkey. *International Journal of Information Security Science, 1*(4), 112–125.

Ulas, G. (2015). Information security strategies in Turkey: Current status, government policies & recommendations. *Computers & Security, 56,* 83–93.

Сведения об авторах:

Аватков Владимир Алексеевич — доктор политических наук, заведующий Отделом Ближнего и Постсоветского Востока, Институт научной информации по общественным наукам РАН (e-mail: v.avatkov@gmail.com) (ORCID: ID 0000-0002-6345-3782)

Мишин Лев Дмитриевич — младший научный сотрудник, Институт научной информации по общественным наукам РАН (e-mail: lev.darsik@mail.ru) (ORCID: ID 0009-0003-5460-3931)

About the authors:

Vladimir A. Avatkov — Doctor of Political Sciences, Head of the Department of the Near and Post-Soviet East at the Institute of Scientific Information on Social Sciences of the Russian Academy of Sciences (e-mail: v.avatkov@gmail.com) (ORCID: 0000-0002-6345-3782)

Lev D. Mishin — Junior Researcher, Institute of Scientific Information on Social Sciences of the Russian Academy of Sciences (e-mail: lev.darsik@mail.ru) (ORCID: 0009-0003-5460-3931)