ГОСУДАРСТВЕННОЕ УПРАВЛЕНИЕ И ОТРАСЛЕВЫЕ ПОЛИТИКИ

DOI 10.35775/PSI.2025.118.1.015
УДК 32

В.В. КОМЕРЦОВ
старший преподаватель кафедры
информационного обеспечения ОВД РЮИ МВД России,
Россия, г. Ростов-на-Дону

О.Д. МРЫХИНА
магистрант кафедры
политологии и этнополитики РАНХ и ГС
при Президенте РФ, Россия, г. Москва

Д.К. ГРИГОРЯН
кандидат политических наук, профессор кафедры
политологии и этнополитики РАНХ и ГС
при Президенте РФ, Россия, г. Москва

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ В КИБЕРПРОСТРАНСТВЕ КАК УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

В статье рассмотрены актуальные угрозы национальной безопасности, представленные кибератаками и террористическими актами, а также взаимосвязь между кибератаками и терроризмом, определены возможные последствия для системы обеспечения государственной целостности. Проанализированы различные типы кибератак в контексте модернизации и внедрения информационно-коммуникационных технологий во все сфере общественной жизни. Подчеркивается, важность принятия мер для предотвращения кибератак как ключевых вызовов, с которыми сталкиваются граждане страны. В статье акцентируется внимание на способы обеспечения личной и государственной безопасности в контексте кибератак и терроризма.

Ключевые слова: *киберпреступность, кибератаки, национальная безопасность, кибертерроризм, компьютерные системы.*

На сегодняшний день вопрос обеспечения национальной безопасности является ключевым для любого государства мирового сообщества. В условиях быстрого распространения процессов цифровизации, информатизации общества развитие социально-политической сферы имеет прямую зависимость от темпов внедрения информационно-коммуникационных технологий во все сферы жизнедеятельности. Компьютеризация коренным образом изменила не только жизнь каждого гражданина, но и предоставила возможность для трансформации

работы институтов власти государственного масштаба. Именно поэтому ключевым направлением в вопросе обеспечения национальной безопасности является борьба с новыми видами преступлений – кибератаками, которые часто перерастают в кибертерроризм и информационные войны и могут предоставлять реальную опасность как в частном, так и в национальном масштабе.

Следует подчеркнуть, что в работах российских и зарубежных авторов, опубликованных в последние годы, освещается широкий спектр вопросов близких к данной предметной области [1; 2; 3; 4; 8; 9; 10; 13; 14; 17; 18; 19; 20; 21; 22; 23; 24].

Однако проблему информационных войн и кибербезопасности нельзя назвать однозначно исчерпанной. В силу многих объективных обстоятельств изучение обозначенной темы продолжает сохранять высокий уровень актуальности.

Сущность информационной войны состоит в том, что боевые действия происходят в виртуальном пространстве, что может затруднить отслеживание этих процессов. Различные манипуляции, которые используются в ходе такой войны, лишают человека возможности сознательно и рационально воспринимать информацию. Информационная война, это самая страшная угроза для мира в киберпространстве, сейчас хотелось бы рассмотреть ее начальные этапы, которые еще можно предотвратить [6. С. 178-183].

Кибератака – это злонамеренное действия, которое совершается при помощи компьютера, сети или электронной системы в цифровом пространстве, с целью нарушения целостности данных, раскрытия конфиденциальной информации, а также получения доступа к закрытой информации или компьютерным системам других лиц и организаций. Существует множество различных кибератак: взломы, фишинг, распространение вредоносных программ и DoS-атаки, проводимые с целью получения доступа к конфиденциальной информации или нанесении ущерба компьютерным системам ключевых институтов жизнедеятельности общества.

Взломы обычно осуществляются путем проникновения в компьютерную систему с использованием уязвимостей в ее защите. Фишинг представляет собой метод мошенничества, с целью получения доступа к личной информации пользователей путём создания фейковых интернет-сайтов, ресурсов, где пользователи указывают свои данные (номер карты, логины и пароли), после чего ими могут завладеть мошенники. Распространение вредоносных программ – это использование вирусов, червей и троянских программ, для заражения компьютеров и получения контроля над ними. DoS-атаки направлены на перегрузку серверов или сетей, чтобы привести их к отказу в обслуживании.

Несомненно, что успех кибератак зависит от того, насколько хорошо защищено информационно-технологическое поле атакуемого объекта. В настоящее время, все, от простых пользователей до крупнейших в мире IT-компаний стремятся надежную и качественную защиту своих данных в глобальной сети. Одним из самых популярных и эффективных решений является подключение специальных антивирусных программ, позволяющих преждевременно обнаружить

компьютерные вирусы, а также нежелательные программы, считающиеся вредоносными.

К сожалению, в современной реальности кибератаки стали неотъемлемой частью существования информационной сети. Согласно данным министерства иностранных дел Российской Федерации на фоне проведения СВО наша страна столкнулась с внешней агрессией наивысшего масштаба в информационном пространстве. В 2022 г. количество кибератак на Россию увеличилось на 80%. В этом году основной удар принял на себя госсектор, в особенности объекты критической информационной инфраструктуры, в то время как в прошлом году главной целью были финансовые учреждения [12].

Акты совершения DDoS-атак на государственные учреждения Российской Федерации были отмечены и в 2023 году. Как правило, DDoS-атаки усиливаются накануне или в день значимого политического или социального события. К примеру, в день начала акции «Диктант Победы» наблюдалось большое количество DDoS-атак на сервисы «Единой России». Во время выборов президента России в марте 2024 года также отмечалось большое количество попыток DDoS-атак на правительственные ресурсы. Например, атака на портал видеонаблюдения за выборами привела к его краткосрочной недоступности, указывает ведомство [26].

Кибератаки являются актуальным вызовом и угрозой национальной безопасности не только в рамках Российской Федерации, но и в контексте мирового сообщества. Особенно явно данная проблема отразилась в отношении стран запада. Так, в июле 2016 года в США хакеры атаковали серверы национальных комитетов Демократической партии США и Демократической партии перед выборами в Конгресс. Злоумышленники или, как их принято называть сегодня - хакеры взломали пароль от электронной почты кандидата Хиллари Клинтон и ее команды, получили доступ к нескольким тысячам электронных писем, семь из которых были отправлены самой Клинтон. Многие письма содержали номера кредитных карт не только членов, но и спонсоров демократической партии. А ряд документов имели гриф секретности и напрямую касались террористических атак на консульство Соединенных Штатов в Бенгази [27].

Трансформация угроз и вызовов национальной безопасности требует модернизацию методов борьбы с новыми технологическими вызовами. Как уже было отмечено, кибератаки касаются не только вопросов личных данных граждан, но и становятся угрозой для работы институтов государственной власти, затрагивая обеспечение безопасности в рамках всего мирового сообщества. Согласно данным Министерству цифрового развития, связи и массовых коммуникаций Российской Федерации в России готовится достаточное количество высококвалифицированных специалистов в сфере информационной безопасности. Однако в данный момент страна испытывает нехватку профессионалов в области информационно-коммуникационных технологий, которые будут готовы противостоять кибератакам на практике [11].

С развитием в мировой практике различных кибератак, актуальным стал вопрос о зарождении нового вида террористических атак – «кибертерроризма». Впервые данное понятие было введено в середине 1980-х годов сотрудником американского Института безопасности и разведки Бэрри Коллином. В своей работе он определяет кибертерроризм как использование высоких технологий с целью парализовать работу важнейших национальных инфраструктур, запугать правительства или гражданское население.

В российской юридической литературе этот термин практически не рассматривается, анализ кибератак российским научным сообществом только набирает свою актуальность. Так, исследователь, профессор кафедры инженерной физики В.А. Голубев понимает кибертерроризм как преднамеренную атаку на информацию, обрабатываемую компьютером, на компьютерную систему или сеть, – атаку, которая создает опасность для жизни и здоровья людей или наступление других тяжких последствий, если такие действия были совершены в целях нарушения общественной безопасности, запугивания населения или провокации военного конфликта [5].

В XXI веке кибертерроризм имеет все больший масштаб влияния: сайты и интернет-платформы, имеют возможность быстрой регистрации и ограничения доступа, а также, во избежание блокировки, часто применяется практика изменения формата и адреса интернет-ресурса. Так, согласно сведениям парламентской газеты, в 1998 году около половины террористических групп, внесенных США в список «иностранных террористических организаций», имели свои сайты. Сейчас же практически каждая террористическая группа имеет отдельные платформы в интернет-пространстве, создавая не только сайты, но и регистрируясь в популярных социальных сетях [28].

Например, запрещенные в России террористические организации «Аль-Каида», «Хезболла», «Хамас», «Организация Абу Нидаля», «Черные Тигры» (связанные с «Тиграми освобождения Тамил-Илама») не только используют киберпространство для пропаганды своих взглядов, но и в качестве оружия для нанесения ударов по объектам национальной инфраструктуры, для атак на иностранные сайты и серверы.

Киберпространство набирает все большую привлекательность для террористических группировок. Возможность быстрого доступа к конфиденциальным данным ключевых организаций власти путем взлома соответствующих интернет-ресурсов открывает широкие возможности для распространения преступной деятельности. Мотивы, составляющие основу деятельности запрещенных группировок в интернет-пространстве, чаще всего, носят финансовый характер. Как известно, у членов террористических группировок нет необходимости в приобретении оружия или специального оборудования для его производства, поэтому для проведения кибератаки необходимо устройство с доступом в интернет-пространство и покупка специализированной программы, содержащей вирус.

Ключевой причиной, по которой направление кибертерроризма набирает популярность, является анонимность проведения операций и преступных деяний. Как правило, террористы в сети действуют, используя различные псевдонимы, программы для изменения голоса. Особую популярность имеют так называемые службы VPN, которые шифруют весь трафик, заменяя IP-адрес. Это значительно упрощает жизнь преступникам и затрудняет для спецслужб обнаружение злоумышленников.

Также актуальность кибератак для террористических организаций повышает возможность проведения удаленной атаки. Находясь в любой точке не только страны, но и мира в целом, террористы могут осуществить захват и контроль информационной базы инфраструктурных объектов стратегического значения страны. Такое разнообразие гарантирует возможность нахождения уязвимых мест и обеспечения полной анонимности в ходе процесса.

Однако, самой главной причиной такого активного распространения кибератак является возможность охватить большое количество публики. Как правило, информация в сети интернет имеет огромный охват и скорость распространения, поэтому, террористические организации рассчитывают на возможность крупномасштабного распространения своей идеологии и соответствующих ценностей.

Несмотря на то, что кибертерроризм по своим мотивам схож с иными видами киберпреступлений, его дифференцирует мотив преступления. Киберпреступления обычно совершаются локально в поисках наживы: например, кража данных гражданина, с целью шантажа и вымогательства. Довольно распространенной в современном интернет-пространстве является ситуация, когда злоумышленники путем взлома веб-страниц получают конфиденциальные данные (личные фотографии или переписки), а затем, путем угрозы публикации информации в общедоступных источниках, вымогают денежные средства.

Кибертерроризм, в свою очередь, преследует более масштабные цели, носящие политический, социальный или даже идеологический характер. Зачастую они достигаются через запугивание и принуждение. Злоумышленники или группировки могут получить доступ к конфиденциальной информации государственных институтов и правительственных организаций, а также нанести вред самому главному государственному ресурсу – гражданам.

Обеспечение личной безопасности каждого гражданина страны, в том числе и подрастающего поколения, является приоритетной задачей любого государства. Одно из направлений кибертерроризма может заключаться в причинении вреда гражданам и вести к распространению культа жестокости, утрате нравственных ценностей и много другого. Это, в свою очередь, способствует активному росту правонарушений и обострению криминогенной ситуации в стране.

Одним из ярких примеров кибертерроризма является так называемая игра «Синий Кит», которая была популярна у подростков в 2016 году. Интерес к игре стал появляться по всему миру, количество поисковых запросов на нее с каждым днем возрастало в несколько раз. Для того, чтобы попасть в игру,

подростки вступали в различные сообщества в интернете, в которых изначально была возможность поиска поддержки и единомышленников в области актуальных личных проблем и переживаний. К каждому вступившему приставлялся куратор, который разъяснял правила игры и предоставлял соответствующие задания. С самого начала, чтобы подтвердить свою готовность, игроку предлагали порезать руку лезвием, вырезать надпись «море китов» или нарисовать кита. Остальные задания также были направлены на причинение вреда себе – как морального (просмотр роликов про суицид), так и физического. Финальный этап игры для всех одинаков – суицид участника в 4:20 утра. При этом, если участник пугался и пытался выйти из игры, кураторы угрожали ему. Они утверждали, что вычислили местонахождение участника по IP-адресу и получили все данные подростка. В случае, где ребенок хочет выйти из игры, кураторы обещали слить все данные в сеть и умертвить родителей подростка [7].

Данный пример подтверждает положение о том, что кибератаки и кибертерроризм имеет реальную угрозу сохранения не только личной безопасности граждан, но и безопасности государственного масштаба. Организованные кибертеррористические атаки оказывают непосредственное влияние на уровень социальной стабильности, сплоченности государства, что отражается на уровне доверия населения к действующей власти и может создать угрозу уязвимости страны перед влиянием недружественных государств.

Помимо этого, кибератаки и террористические акты могут привести к экономическим потерям. Например, кража конфиденциальной информации или нарушение работы компьютерных систем, которые способствуют остановке производства на предприятиях. Регулярное проведение подобных атак в отношении ключевых инфраструктурных предприятий страны может сказаться на темпах производства жизненно важных товаров, оказать влияние на уровне экономического роста, что создаст кризисную ситуацию национального масштаба, а также повысит возможность социальных волнений и беспорядков.

Однако, в современных условиях кибертерроризм охватывает и более значимые, тем самым, уязвимые сферы государственного развития. В условиях проведения Специальной военной операции на Украине, сопровождающейся не только реальными боевыми действиями, но и, так называемой, информационной войной, вопрос кибертерроризма и дипфейков стоит наиболее остро. В начале 2024 года спецслужбы Украины доложили о том, что взломали российскую компанию, которая обеспечивает работу информационной системы ERP [29], созданной для управления бизнес-процессами на основе единой базы данных. В этой базе хранится доступ к информации множества российских предприятий, охватывающий как сферу продовольственной безопасности, так и область военно-промышленного комплекса. Несмотря на то, что от самой компании официальной информации о проведении атаки не поступало, быстрое распространение данных в сети привело к внутренним волнениям, повышению уровня нестабильности владельцев крупных компаний.

Работа в области противодействия кибертерроризму требует не только государственного, но и мирового масштаба освещения и разработки мер. Так, в настоящий момент Российская Федерация проводит активную работу по созданию и развитию центров по центры по реагированию на киберинциденты (CERT) [30]. В 2025-2026 годах планируется открытие национального центра развития в области искусственного интеллекта и его внедрения в процесс обеспечения противодействия кибертерроризму как актуальному направлению террористических угроз. Помимо этого, 28 сентября 2018 года было подписано Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий, согласно которыми страны-участники должны обеспечить систему коллективной безопасности в области информационных технологий.

Помимо этого, в ноябре 2023 года была утверждена Стратегия развития отрасли связи до 2035 года [16]. Данная стратегия предусматривает переход на использование сертифицированных средств защиты информации в Российской Федерации. Также предусмотрено развитие государственного центра обнаружения, предупреждения и ликвидации последствий компьютерных атак. Еще одной инициативой, связанной с кибербезопасностью, является развитие единой централизованной системы защиты от DDoS-атак и других угроз.

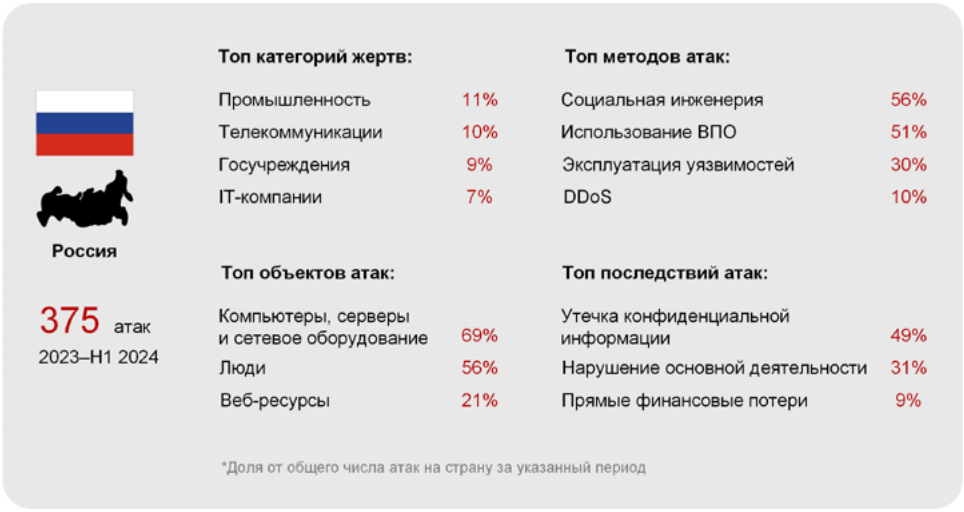
В 73% всех кибератак, произошедших в странах СНГ в 2023 и первую половину 2024 годов пришлось на Россию. Такая статистика связана с обострившейся геополитической ситуацией, сопровождающейся всесторонним давление противоборствующих стран. Российские организации становятся объектом целенаправленных чтений десятков групп, кибершпионажа, активизирующихся хактеррористов и финансово мотивированных атак.

По данным крупномасштабного исследования, проводимого российской компанией Positive Technologies, специализирующейся на разработке решений в сфере информационной безопасности, основанного на анализе международных и государственных данных, были определены основные отрасли, подвергающиеся наиболее частым атакам, а также инструментарий, составивший наибольшую привлекательность для преступных группировок (рис. 1). Так, направлениями наиболее частых атак являются промышленность (11%), телекоммуникации (10%), государственные учреждения (9%) и IT-компании (7%). Среди методов атак преобладает социальная инженерия (56%), в каждой второй атаке используется вредоносное программное обеспечение, в каждой третьей атаке злоумышленники эксплуатируют уязвимости. При использовании вредоносного ПО в 40% случаев используются инфостилеры, в 31% – трояны для удаленного управления, а в каждой четвертой атаке злоумышленники используют шифровальщики для заражения жертв. Почти каждая вторая атака (49%) приводит к утечке конфиденциальной информации, а 31% атак нарушают основную деятельность организаций [25].

Атаки на критическую инфраструктуру становятся все более распространенными и успешными. Мировая практика свидетельствует о множестве случаев

выведения из строя систем водоснабжения, энергоснабжения, производственных конвейеров, операторов связи, аэропортов, медицинских учреждений и даже атомных объектов. Конфликт между Израилем и Палестиной, а также связанные с ним события, показали, насколько уязвимы системы жизнеобеспечения перед направленным кибертерроризмом. Аналогичная ситуация сейчас наблюдается в России. По мере нарастания геополитического напряжения, количество атак на российскую критическую инфраструктуру будет только увеличиваться, независимо от их успеха.

Рис. 1. Сводная статистика по кибертеррористическим атакам в Российской Федерации



В настоящее время силы всех стран сосредоточены на принятии и реализации государственных стратегий и документов, направленных на развитие цифрового пространства и улучшение его защищенности. Однако, так как информационное пространство развивается с бешенной скоростью и каждый день появляются новые виды способы осуществления преступлений в этом пространстве, нормативно-правовая база, связанная с защитой от кибератак, все еще является неполной.

В апреле 2023 года Межпарламентская Ассамблея государств-участников СНГ приняла модельный закон «О противодействии киберпреступности» [15]. Он стал основой для совершенствования государственного законодательства в области противодействия киберпреступности. Этот закон позволит скоординировать деятельность государственных органов и повысить раскрываемость киберпреступлений. Принятие и реализация этого закона способствуют укреплению мер по защите от кибератак и повышению кибербезопасности в странах-участницах.

Таким образом, нами было выявлено, что кибератаки – неотъемлемая часть современного информационного поля. Развитие

информационно-коммуникационных технологий, несомненно, открыло новый этап развития общественной жизни, способствовало развитию цифровизации и информатизации ряда ключевых процессов государственного и мирового масштаба.

Распространение кибертерроризма связано с множеством факторов – доступностью, анонимностью, удаленностью преступных деяний. Возможность получения быстрого доступа к конфиденциальным данным повышает уровень привлекательности и распространения кибертерроризма среди террористических группировок. Такие деяния увеличивают уровень угрозы не только личной безопасности каждого гражданина, но и национальной безопасности, а также сохранения мирового правопорядка и стабильности. Согласно характеристики МВД о состоянии преступности в Российской Федерации за январь – сентябрь 2024 года, более трети преступлений совершается с использованием информационно-телекоммуникационных технологий. Таких деяний зарегистрировано на 15,3% больше, чем в январе-сентябре прошлого года [31]. В связи с этим, в условиях современного информационного поля необходима модернизация уже имеющихся и разработка новых инструментов противодействия кибератакам. Подготовка высококвалифицированных специалистов в области IT, разработка качественных антивирусных программ, способствующих защите конфиденциальных данных, принятие деклараций и стратегий противодействия киберпреступности как на уровне отдельных государств, так и в рамках мирового сообщества является необходимыми и актуальными мерами, способными создать достойный уровень противоборства преступным деяниям данного характера. Сокращение уровня киберпреступности будет способствовать дальнейшему внедрению процессов информатизации во все сферы общественного развития, позволяя раскрывать инициативы и потенциал каждого гражданина, а также увеличивая возможности эффективной работы органов государственной власти и ключевых социально-политических институтов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. **Айрапетян Д.А.** Институциональные перспективы перехода к посткапитализму: трансформация государства как субъекта власти в эпоху цифро-сетевых технологий // Вопросы политологии. 2024. № 7.
2. **Алаудинов А.А., Манойло А.В.** Когнитивная и ментальная составляющие современной гибридной войны // Вопросы политологии. 2024. № 2.
3. **Алаудинов А.А., Стригунов К.С., Гончаренко А.Р.** Структура и характеристика субъектов военного конфликта на Украине и его основные отличия от гибридных войн в Сирии и Ливии // Вопросы национальных и федеративных отношений. 2024. № 6.
4. **Бельков О.А.** Национальные интересы в координатах национальной безопасности // Вопросы политологии. 2023. № 11-2.
5. **Васенин В.А.** Информационная безопасность и компьютерный терроризм.

6. **Григорян Д.К., Кондратенко Е.Н.** Характерные черты современных информационных войн политической направленности. Издательство: Государственное и муниципальное управление. Ученые записки. 2024. № 2.
7. **Евсикова Е.В.** «Зацепинг», «спайсы» и «синий кит» глобальные угрозы современной молодежи в контексте усовершенствования административно-правовых и уголовно-правовых основ борьбы с ними // https://cyberleninka.ru/article/n/zatseping-spaysy-i-siniy-kit-globalnye-ugrozy-sovremennoy-molodezhi-v-kontekste-usovershenstvovaniya-administrativno-pravovyh-i/viewer.
8. **Жбанов А.М.** Современные тенденции политики кибербезопасности крупных держав // Вопросы политологии. 2024. № 7.
9. **Жбанов А.М.** Современное состояние киберпространства в системе обеспечения международной безопасности // Вопросы политологии. 2024. № 4.
10. **Жбанов А.М.** Практика государственно-частного партнерства в системе обеспечения политики кибербезопасности США// Вопросы национальных и федеративных отношений. 2024. № 6.
11. Заместитель главы Минцифры РФ Александр Шойтов в ходе форума «Кадры и образование по ИБ в России: настоящее и будущее», 10 марта 2023 г. // https://tass.ru/ekonomika/17234399.
12. Интервью заместителя Министра иностранных дел Российской Федерации О.В. Сыромолотова // МИА «Россия сегодня», 28 декабря 2022 года // https://www.mid.ru/ru/foreign_policy/news/1845853/.
13. **Ло Дунмэй, Ян Бо.** Российско-китайское сотрудничество в области кибербезопасности в XXI веке: возможности и вызовы // Вопросы политологии. 2023. № 11-2.
14. **Новосельский С.О., Антропова Т.Г., Гагарина И.Ю., Булавина М.А.** Особенности формирования интеллектуального капитала в России как фактора обеспечения национальной безопасности в условиях санкций // Вопросы политологии. 2023. № 9-1.
15. Постановление Межпарламентской Ассамблеи государств-участников Содружества независимых государств // https://base.garant.ru/409351058/?ysclid=m39v89ygtl354745612.
16. Распоряжение Правительства РФ от 24 ноября 2023 г. № 3339-р «Об утверждении Стратегии развития отрасли связи РФ на период до 2035 г.» // https://www.garant.ru/products/ipo/prime/doc/408020989/.
17. **Степовая Д.А.** Безопасность национального киберпространства в условиях информационно-психологического противоборства // Вопросы политологии. 2023. № 5.
18. **Сунь Сяомэн, Медведев Н.П.** Нетрадиционные угрозы безопасности и пути им противодействия в контексте международного сотрудничества // Вопросы политологии. 2024. № 5.

19. **Сурма И.В.** Вызовы и угрозы технологий искусственного интеллекта как универсального инструмента социально-политической и экономической трансформации современного общества // Вопросы политологии. 2024. № 6.
20. **Сурма И.В.** Международно-правовые особенности обеспечения кибербезопасности в условиях развития высокотехнологичной преступности // Вопросы национальных и федеративных отношений. 2024. № 7.
21. **Сурма И.В.** Кенселлинг как форма государственного кибер-остракизма // Вопросы национальных и федеративных отношений. 2024. № 6.
22. **Филатов О.В.** Подходы НАТО к обеспечению информационной безопасности: от общих киберугроз до злонамеренного использования искусственного интеллекта // Вопросы политологии. 2023. № 2.
23. **Форостянный Н.С., Тёмкина А.М.** Политический потенциал БРИКС в трансформации системы международной безопасности // Евразийский Союз: вопросы международных отношений. 2024. № 7.
24. **Чжао Лэй.** Сотрудничество в области кибербезопасности и борьбы с кибертерроризмом в рамках ШОС // Евразийский Союз: вопросы международных отношений. 2024. № 5.
25. Яна Авезова, Старший аналитик направления аналитических исследований Positive Technologies «Актуальные киберугрозы в странах СНГ 2023-2024» // https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-v-stranah-sng-2023-2024/.
26. https://www.rbc.ru/technology_and_media/23/06/2022/62b43ea09a79471246251381.
27. https://www.bbc.com/news/world-us-canada-37639370?t&utm_source=perplexity.
28. https://www.pnp.ru/politics/istoriya-kiberterrorizma-kiberterrorizm-xxi-veka.html.
29. https://lenta.ru/articles/2024/01/11/cyberwar/.
30. https://www.cnews.ru/book/RU-CERT_-_Центр_реагирования_на_компьютерные_инциденты.
31. https://мвд.рф/reports/item/56672721/.

V.V. KOMERTSOV
Senior Lecturer at the Department of
Information Support, Rostov Law Institute of the Ministry
of Internal Affairs of Russia, Rostov-on-Don, Russia

O.D. MRYKHINA
Undergraduate of the Department
of Political Science and Ethnopolitics of the Russian
Academy of Sciences and GS under the President
of the Russian Federation, Moscow, Russia

D.K. GRIGORYAN
Candidate of Political Sciences,
Professor at the Department of Political Science and
Ethnopolitics, Russian Presidential Academy of National Economy
and Public Administration, Moscow, Russia

SOCIAL ENGINEERING IN CYBERSPACE AS A THREAT TO NATIONAL SECURITY

The article examines current threats to national security presented by cyberattacks and terrorist acts, as well as the interrelationship between cyberattacks and terrorism, determining possible consequences for the system of ensuring state integrity. Various types of cyberattacks are analyzed in the context of the modernization and implementation of information and communication technologies in all areas of public life. The importance of taking measures to prevent cyberattacks as key challenges faced by the country's citizens is emphasized. The article highlights ways to ensure personal and state security in the context of cyberattacks and terrorism.

Key words: *cybercrime, cyberattacks, national security, cyberterrorism, computer systems.*