УДК 004.7

Яковицкий Сергей Анатольевич
профессор, кандидат военных наук, доцент. ФГКВОУ ВПО «Военная академия связи им. Маршала Советского Союза С.М. Буденного» Санкт-Петербург, Россия.
Yakovitsky Sergey Anatolyevich
Professor, Candidate of Military Sciences, Associate Professor. FSKVOU HPE "Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny" St. Petersburg, Russia.
Иванов Андрей Анатольевич
профессор, кандидат технических наук, доцент. ФГКВОУ ВПО «Военная академия связи им. Маршала Советского Союза С.М. Буденного» Санкт-Петербург, Россия.
Ivanov Andrey Anatolyevich
Professor, Candidate of Technical Sciences, Associate Professor. FSKVOU HPE "Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny", St. Petersburg, Russia.
Вавринюк Сергей Адамович
старший преподаватель, ФГКВОУ ВПО «Военная академия связи им. Маршала Советского Союза С.М. Буденного» Санкт-Петербург, Россия.
Vavrinyuk Sergey Adamovich
senior lecturer, FSKVOU HPE "Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny" St. Petersburg, Russia.
Ильичев Константин Федорович
служащий, ФГКВОУ ВПО «Военная академия связи им. Маршала Советского Союза С.М. Буденного» Санкт-Петербург, Россия.
Ilyichev Konstantin Fedorovich
the employee, FSKVOU HPE "Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny" St. Petersburg, Russia.

ВЗГЛЯДЫ ВЫСШЕГО ВОЕННО-ПОЛИТИЧЕСКОГО РУКОВОДСТВА ВЕЛИКОБРИТАНИИ НА ХАРАКТЕР И СОДЕРЖАНИЕ ПРОТИВОБОРСТВА В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Аннотация: *к 2025 году в стратегическом планировании Великобритании произошел фундаментальный сдвиг в понимании природы современных конфликтов, обусловленный завершением масштабной трансформации вооруженных сил по программе «Солдат будущего» («Future Soldier»). Высшее военно-политическое руководство (ВВПР) Великобритании окончательно отошло от рассмотрения информационной сферы исключительно как обеспечивающего элемента боевых действий. Согласно доктринальным документам, информационное противоборство трансформировалось в концепцию тотальной «когнитивной войны» (Cognitive Warfare), которая ведется непрерывно и не привязана к официальному объявлению войны.*

Ключевые слова: *дипфейки, кибератака, кибербезопасность, киберпространство, Когнитивная война, наука о нейронных сетях, нетрадиционные методы ведения войны, психологические операции, серая зона, операции, разведка, уязвимость.*

Abstract: *By 2025, Britain's strategic planning had undergone a fundamental shift in understanding the nature of modern conflicts, driven by the completion of a large-scale transformation of the armed forces under the "Future Soldier" program. The Supreme Military and Political Leadership The United Kingdom has finally moved away from considering the information sphere solely as a supporting element of military operations. According to the doctrinal documents, the information warfare has been transformed into the concept of total "Cognitive Warfare", which is being waged.*

Keywords: *Deepfakes, Cyberattack, Cybersecurity, Cyberspace, Cognitive Warfare, Neuroscience, Unconventional Warfare, PSYOPS, Grey Zone, intelligence, vulnerability.*

Анализ основных документов, включая отчет Палаты общин «Оборона Великобритании в 2025 году» (*UK Defence in 2025*) и профильные исследования в области военной когнитивистики, свидетельствует о том, что Лондон рассматривает способность управлять восприятием и когнитивными процессами противника как решающий фактор стратегического сдерживания и доминирования в эпоху перманентной глобальной конкуренции.

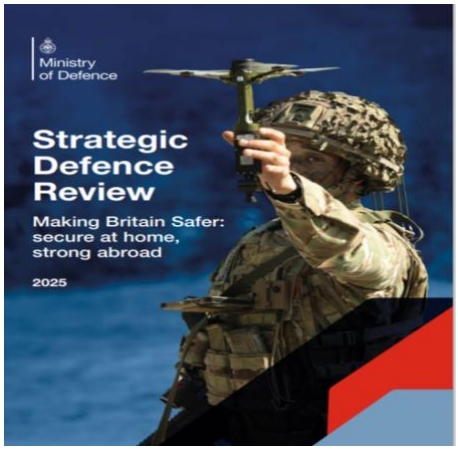

Рис. 1 Документ министерства обороны Великобритании «Обзор по вопросам стратегической обороны», 2025 г.

Важнейшей тенденцией, отмечаемой в документах министерства обороны: «Обзор по вопросам стратегической обороны» (*Strategic Defence Revie*w) (рис.1) и «Управление обороной» (*Defence Command Paper*), является перенос центра противоборства в так называемую «серую зону». Это пространство между миром и открытой войной, где агрессивные действия осуществляются ниже порога вооруженного ответа.

Британское руководство полагает, что в этой зоне информационное оружие становится основным средством принуждения. Согласно отчету «Оборона Великобритании в 2025 году», армия Великобритании адаптируется к условиям, где конкуренция идет постоянно, а понятие «тыла» отсутствует, поскольку информационному воздействию подвергается все общество.

В этой логике информация рассматривается не как инструмент коммуникации, а как функциональный аналог высокоточного оружия, способного наносить стратегический ущерб через дестабилизацию социальных институтов и потерю доверия к государственному управлению, что делает сохранение яснос-ти мышления нации приоритетом национальной безопасности.

Взгляды британских экспертов на содержательную часть информационного противоборства базируются на глубокой интеграции «нейронаук» и военных технологий. Ключевым механизмом воздействия признается не прямая пропаганда, а так называемая «когнитивная эрозия» (cognitive erosion).

Данный метод предполагает систематическое воздействие на аналитические способности целевой аудитории через фрагментацию информационных потоков. Насыщение медиапространства коротким, эмоционально окрашенным и противоречивым контентом приводит к снижению объема краткосрочной памяти и способности к долгосрочному планированию у населения противника. Как отмечается в профильных исследованиях 2025 года, целью такой тактики является создание состояния, при котором объект воздействия вынужден полагаться на примитивные, заведомо ложные алгоритмы осмысления полученной информации и навязанные извне нарративы, будучи неспособным к критической проверке фактов. Это создает эффект «иллюзорной правды», когда многократно повторенная ложь воспринимается мозгом как достоверная информация в силу особенностей нейрофизиологии памяти.

Существенной тенденцией в содержании противоборства является переход к высокотехнологичным методам манипуляции, обозначаемым термином «убеждение, управляемое событиями» (event-driven persuasion). Британское

военно-политическое руководство рассматривает возможность искусственного моделирования событий (в том числе с использованием технологий

«дипфейков» и кибератак), которые вызывают прогнозируемые эмоциональные всплески — страх, гнев или эйфорию.

В состоянии высокого эмоционального возбуждения психологические защитные механизмы личности отключаются, что позволяет внедрять необходимые поведенческие установки. В отличие от традиционной дезинформации, этот подход направлен на синхронизацию физических событий и информационных волн для достижения кумулятивного эффекта. Таким образом, *содержание современной информационной войны, по мнению Лондона, заключается в проектировании реальности, где противник, действуя в рамках навязанной ему картины мира, самостоятельно принимает решения, выгодные для Великобритании.*

В практической плоскости взгляды Лондона на информационное противоборство реализованы через масштабную реорганизацию сухопутных войск в рамках программы «Солдат будущего».

Ключевым маркером смены приоритетов стало формирование и усиление 6-й дивизии обеспечения в составе сил быстрого реагирования сухопутных войск. Соединение в официальных документах Министерства обороны позиционируется как «центр компетенций в сфере нетрадиционных методов ведения войны» (unconventional warfare). В составе этой дивизии имеются: три бригады ССО, бригада разведки, две бригады связи и бригада психологических операций (ПсО) (рис.2). Дивизия стала новым соединением, которое объединяет возможности кибероперациий, радиоэлектронной борьбы (РЭБ), информационных операций и некинетического воздействия. В соединении имеются специалисты по анализу данных, социальной инженерии и медиа-коммуникациям. Их деятельность направлена не только на противодействие дезинформации, но и на проведение наступательных операций по формированию нарративов, способных изменить волю противника к сопротивлению. Британское руководство исходит из того, что когнитивный эффект достигается через синергию: кибервойска взламывают информационные сети, а специалисты 77-й бригады ПсО наполняют эти сети

контентом, который, опираясь на когнитивные уязвимости, провоцирует нужные поведенческие реакции. Задачи 77-й бригады ПсО эволюционировали от классических психологических операций (PSYOPS) к комп-лексному управлению восприятием и поведением целевых аудиторий.

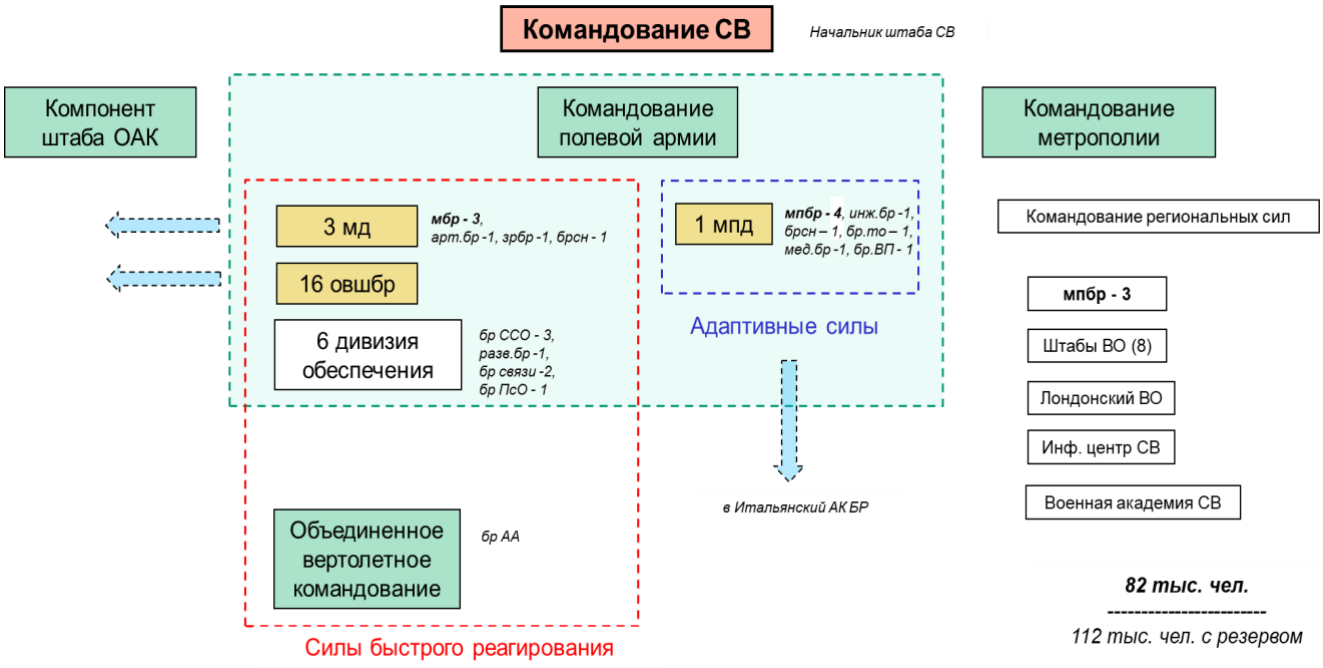

Рис.2. Место 6 дивизии обеспечения в структуре сухопутных войск Великобритании

Революционным изменением во взглядах британского истеблишмента стал отказ от разделения войны на «активную фронтовую» и «информационную». В доктрине JDP 0-20 «Сухопутная мощь» («Land Power») закреплен «маневренный подход» (manoeuvrist approach), подразумевающий атаку на уязвимости врага, а не на его сильные стороны. В современном прочтении это означает интеграцию огневого поражения с информационным ударом.

Наиболее ярко этот подход воплощен в создании в 2022 году в составе 6-й дивизии обеспечения 1-й бригады глубинной разведки и удара (1st Deep Recce Strike Brigade). Уникальность этого формирования заключается в том, что оно объединяет дальнобойную артиллерию (системы залпового огня MLRS, перспективные самоходные артиллерийские установки Archer и RCH-155) со средствами разведки и специальными подразделениями информационного

воздействия и РЭБ [1]. Четко прослеживается полный аналог создаваемым в настоящее время в сухопутных войсках США многосферным оперативным группам в соответствии с оперативной концепцией СВ США «Многосферное сражение: эволюция совместных действий различных видов вооруженных сил в XXI веке (2025–2040)» [2]. Логика созданного в Великобритании соединения продиктована стремлением к достижению так называемых «глубоких эффектов». В программе «Солдат будущего» прямо заявлена цель – удвоить долю сил, способных наносить такие удары. Под «глубоким эффектом» британские стратеги понимают ситуацию, когда физическое уничтожение командного пункта противника синхронизировано с информационной кампанией, деморализующей оставшиеся без управления подразделения.

Таким образом, информационное оружие перестает быть вспомогательным фактором обеспечения и становится частью **единого разведывательно-ударно-информационного контура**. Это позволяет достигать стратегических целей с меньшими затратами боеприпасов, поражая систему управления противника изнутри через когнитивную перегрузку и дезорганизацию.

Реализация концепции когнитивной войны невозможна без соответствующего технологического уклада. Исследования 2025 года вводят понятие «ког-нифицированных объектов» (cognified objects) – систем вооружения, которые не просто исполняют команды, но и участвуют в цикле сбора и обработки информации. Взгляды военно-политического руководства Великобритании на перевооружение армии полностью соответствуют этому тренду. Примером служит программа внедрения боевых бронированных разведывательных машин (ББРМ) семейства «Ajax». Несмотря на технические сложности реализации, британское командование рассматривает «Ajax» не как традиционное средство транспортировки пехоты или разведки, а как полностью цифровизированный узел обработки данных на поле боя. Ключевую роль играет сопряжение ББРМ «Ajax» в единый контур с беспилотными летательными аппаратами, средствами РЭБ и РЛС контрбатарейной борьбы.

Насыщение войск подобными сенсорами преследует двоякую цель. Во-первых, это обеспечивает тотальную ситуационную осведомленность, позволяющую опережать противника в цикле принятия решений. Во-вторых, массив данных, собираемый такими платформами и дополняемый роем беспилотных систем (проект «Тикила» (Tiquila) и замена комплексов «Уотчкиппер» (Watchkeeper)), служит основой для алгоритмов искусственного интеллекта. Эти алгоритмы, согласно современным британским подходам, должны выявлять склонности поведения противника и автоматически предлагать сценарии информационно-психологического воздействия. Техника перестает быть «железом» и становится интерфейсом для ведения войны в информационном пространстве, собирая контент для операций влияния в режиме реального времени.

Отдельное внимание в британских стратегических разработках уделяется автоматизации процессов воздействия. Поскольку объем информации в современном конфликте превышает человеческие возможности анализа, ставка делается на использование нейросетей и технологии больших данных (big data) для микротаргетинга. Технологическая инфраструктура, разворачиваемая в рамках модернизации армии, призвана обеспечить доставку индивидуализированного информационного сигнала до конкретного солдата или офицера противника. Это переводит противоборство на уровень «алгоритмической войны», где побеждает та сторона, чьи модели поведения целевой аудитории оказываются точнее. В этом контексте закупка новых систем связи и управления рассматривается Лондоном как инвестиция в способность навязывать свою волю через информационное доминирование, создавая для противника «туман войны» нового поколения – цифровой и персонализированный.

Общую координацию деятельности государственных организаций и частных компаний Великобритании в сфере компьютерной безопасности осуществляет ***Центр обеспечения компьютерной безопасности*** (далее – Центр), сформированный на базе центра координации безопасности

национальной инфраструктуры, службы безопасности и консультационного центра по национальной безопасности. Центр является координационным органом, главными задачами которого являются:

оценка и выявление угроз информационной инфраструктуре;

выявление и оценка уязвимости ее критических элементов;

анализ перспективных тенденций развития технологий защиты и подготовка рекомендаций по их применению.

Центр также оказывает практическое содействие национальным организациям в ликвидации последствий инцидентов, связанных с воздействием на электронные системы управления. Специалисты Центра регулярно проводят анализ безопасности компьютерных сетей государственных организаций и готовят предложения по усилению их защиты с использованием программных, аппаратных и криптографических средств. На постоянной основе осуществляется моделирование внутренних и внешних угроз информационной безопасности наиболее важных объектов национальной инфраструктуры, связанных с обеспечением бесперебойной работы транспорта, энергетических и коммуникационных сетей, системы водоснабжения, кредитно-денежных учреждений.

В условиях усиления угрозы террористических актов повышенное внимание уделяется защите сведений, которые могут быть использованы для нарушения производственной деятельности и проведения диверсий в отношении стратегических объектов. В связи с этим расширены перечни закрытой информации и намечены меры по усилению организационной и технической защиты автоматизированных информационных систем. В частности, к конфиденциальным отнесены сведения о компьютерных системах, задействованных в обеспечении безопасности технологических процессов и физической защиты ядерных и химических предприятий, а также оценки уязвимости их информационной инфраструктуры.

Список использованных источников

1. Новостной сайт НАТО и США. https://www.joint-forces.com/ Bob Morrison Scorpion cyclone 1st deep reconnai sance strike bct.
   (дата обращения 08.02.2026 г.)
2. Развертывание многосферных оперативных групп сухопутных войск США. Яковицкий С.А., Иванов А.А., Вавринюк С.А. Общество и цивилизация. 2022. Т. 4. № 3. С. 32-35.