ДЕМО-ВЕРСИЯ · БЕСПЛАТНО

Exambooster

Билеты «Стратегии информационного воздействия» — пробный билет

Один полный билет из пособия — посмотрите формат перед покупкой: обложка-конспект, тезисы для повторения и развёрнутый ответ. В полном пособии — все 30 тем собеседования (базовый блок Т01–Т07 и профильный Т08–Т30), всего 205 страниц.

НАПРАВЛЕНИЕ ПОДГОТОВКИ

41.04.05 «Международные отношения» · магистратура МГИМО

Демо-пособие · 2026

СТРАТЕГИИ ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ · БИЛЕТ Т17 · ДЕМО

Информационные войны как новый тип конфликтов. Гибридные войны

Понятие

- Тренин: с сер. 2010-х РФ–Запад ведут «настоящую информвойну»; гибридная война — «борьба без линий фронта» на стыке информационной, финансовой, технологической, экономической платформ;
- НАТО (Варшавская декларация-2016, п. 72): сочетание обычных/нетрадиционных, открытых/скрытных военных мер; единого юридического определения «гибридной войны» нет.

Российское прочтение

- Герасимов (2013): спецоперации + внутренняя оппозиция создают «постоянный фронт» + информвоздействие;
- Герасимов (2016, по Сирии): главный инструмент — цветные революции, перевороты извне через манипуляцию протестом;
- модель цветной революции (Цыганков): протестная сеть → «инцидент» → соцсети → «майдан» → перелом.

Эстония-2007 — первый прецедент

- демонтаж «Бронзового солдата» (26–27.04.2007) → хакерские атаки на госсайты и банки;
- МИД Эстонии: «нападение на европейское сообщество»; предложено приравнять кибератаки к ст. 5 НАТО;
- 2008 г. — Центр кибербезопасности НАТО открыт в Таллине.

Институты противодействия

- центры НАТО: Таллинн (киберзащита), Рига (стратком), Хельсинки (гибридные угрозы);

- Таллиннское руководство 1.0/2.0 легитимирует силовой ответ на кибератаки;
- Россия: указ №31с (2013) → СОПКА (ФСБ); закон Яровой (2016/2018).

2024–2026: позиция России

- Лавров (окт. 2024): противостояние «пока элементы гибридной войны, но всё больше переходит в прямую»;
- Грушко: «горячий театр» — Украина, «холодные» — Балканы, Балтика;
- Захарова (янв. 2026) — «полномасштабная гибридная война» Запада ради глобального доминирования.

2024–2026: инциденты и институты

- Балтика (2023–2025) — 4 инцидента с кабелями → миссия НАТО Baltic Sentry (янв. 2025);
- Польша (16.11.2025) — взрыв на ж/д, обвинение ФСБ; Молдавия/Румыния (2024) — вмешательство РФ в выборы, ИИ-дипфейки;
- штраф ЕК платформе X — €120 млн по DSA; РГОС ООН завершила мандат в июле 2025 г.

РАЗВЁРНУТЫЙ ОТВЕТ

Что это за тип конфликта и почему он новый

С начала 2010-х годов исследователи международных отношений всё чаще фиксируют, что современный мировой порядок переживает структурный кризис: механизмы, которые раньше удерживали межгосударственные конфликты в предсказуемых рамках, работают хуже, а государства и негосударственные участники получают всё больше стратегической автономии — то есть способности действовать самостоятельно, не оглядываясь на волю сильных держав. На этом фоне в политическом языке распространились понятия «постправда» (ситуация, при которой объективные факты значат для формирования общественного мнения меньше, чем эмоции и личные убеждения) и «гибридный конфликт». Сама популярность этих терминов — симптом того, что ни государства, ни исследователи не нашли твёрдой почвы для описания новой реальности: конфликт всё реже выглядит как открытое столкновение армий с ясной линией фронта, датой начала и датой окончания.

Информационная война и гибридная война — два родственных, но не тождественных понятия. Информационная война — это борьба за сознание противника: за то, как он воспринимает события, кому доверяет и какие решения готов поддержать. Гибридная война — понятие шире: сочетание информационных, военных, экономических, финансовых и технологических инструментов в единой кампании, которая балансирует на грани открытого военного столкновения, но, как правило, до него не доходит. У обоих терминов нет общепринятого юридического определения, и это не случайность: размытость границ сама служит инструментом такой войны, позволяя действовать, не пересекая порог, за которым противник получил бы законное право на военный ответ.

Откуда пришло понятие и как его сегодня определяют

Корни концепции — в дискуссиях американских военных теоретиков конца XX века. Исследователи Джон Аркилла и Дэвид Ронфельдт предложили концепцию «сетевых войн»:

будущее военного противостояния определят не армии с централизованным командованием, а сети — множество автономных или полуавтономных групп, способных действовать разрозненно или наносить массированный скоординированный удар по сигналу из центра через средства массовой информации; наглядным примером они считали восстание в мексиканском штате Чьяпас 1 января 1994 года. Тогда же полковник ВВС США Ричард Шафрански сформулировал понятие «информационной войны» — активных действий по изменению того, как противник воспринимает мир и какова его система ценностей, с целью сорвать процесс принятия им политических решений; новое понимание, в отличие от классической пропаганды, делало ставку на технологии искусственного интеллекта и автоматизацию хранения и передачи данных вплоть до теоретической возможности заблокировать всю систему государственного управления противника, что и закрепилось в американских документах 2003 и 2008 годов.

У этой рамки была и материальная, военно-техническая подоснова. Ещё в 1991 году, во время операции «Буря в пустыне», иностранные телекомпании впервые получили возможность вести репортажи из зоны боевых действий в реальном времени — возник «эффект CNN»: мировая общественность стала прямым наблюдателем войны, что ограничило возможности сторон применять пропаганду и умолчания по-старому. Доля высокоточного оружия в конфликтах выросла с девяти процентов в 1991 году до семидесяти пяти в Ираке в 2003 году, а армии всё активнее опирались на «сетецентричную войну» — объединение разведки, связи и наведения в единое информационно-управленческое поле боя. Развитие радиоэлектронной борьбы и кибероружия довершило картину: контроль над информацией стал неотделим от собственно военной борьбы.

Когда в 2010-е годы конфронтация между Россией и Западом обострилась, для неё стали использовать понятие «гибридная война» — без единого определения, но с несколькими конкурирующими. Исследователь Дмитрий Тренин говорит о конфронтации нового типа, уже не идеологической, не всемирной и не военной в первую очередь: это «борьба без линий фронта, на всю глубину человеческой деятельности» на пересечении информационной, финансовой, технологической и экономической платформ — в отличие от холодной войны 1940–1980-х годов, когда мир был расколот на два блока по принципу «или-или». НАТО (Организация Североатлантического договора) в Варшавской декларации 2016 года, пункт 72, определяет гибридную войну как ведение боевых действий, при которых государственные и негосударственные субъекты сочетают обычные и нетрадиционные, открытые и скрытные военные, военизированные и гражданские меры; тогда же киберпространство было объявлено НАТО «новой областью операций» — такой же, как воздух, суша и море. Хельсинкский центр по противодействию гибридным угрозам определяет их как методы создания уязвимостей у противника через историческую память, законодательство, поляризацию общества и технологическое отставание, а военные действия добавляются, если подрыв стабильности изнутри не удался. Американские исследователи Джеймс Мэттис и Фрэнк Хоффман в статье 2015 года предложили близкое понятие «гибридных угроз» — комплексных действий соперника, которые нельзя однозначно отнести ни к внутри-, ни к внешнеполитическим. Отсутствие единого определения признают сами западные институты — и это отражает то, что стороны конфликта заинтересованы в разной трактовке одних и тех же действий.

Российское прочтение: доктрина Герасимова и цветные революции

У этой проблемы есть российская интерпретация. В 2010-е годы российские военные аналитики фиксировали, что «конфликты нового типа» — прежде всего «арабская весна» и цветные революции — по последствиям сопоставимы с настоящей войной, хотя формально боевых действий может и не быть; пример — война в Ливии с 2011 года, где невоенные по форме средства («бесполётная зона», морская блокада, частные военные компании) привели к смене власти. Начальник Генерального штаба Вооружённых сил России Валерий Герасимов в статье 2013 года писал об асимметричных действиях — использовании сил специальных операций и внутренней оппозиции для создания «постоянно действующего фронта» на территории противостоящего государства в сочетании с информационным воздействием; этот текст на Западе стали называть «доктриной Герасимова». В 2016 году, обобщая опыт Сирии, Герасимов уточнил: главное средство «гибридных методов» — цветные революции, перевороты, организованные извне через манипуляцию протестным потенциалом населения.

В российской трактовке к «гибридным» относят прежде всего действия Запада по поддержке оппозиции на постсоветском пространстве и организации цветных революций — особенно после переворота на Украине в 2014 году. Механику такой революции детально описывает модель из пяти этапов исследователя Павла Цыганкова (сам термин «гибридная война» он не использует). Сначала формируется протестная сеть — законспирированные ячейки во главе с лидером, подготовленные через центры демократизации, с опорой на молодёжь. Затем движение выходит из подполья после «инцидента» — шокирующего события: фальсифицированные выборы в Сербии (2000), Грузии и на Украине (2004), самосожжение уличного торговца в Тунисе (2010), запустившее «арабскую весну». Далее идёт конфликтная мобилизация через соцсети («твиттерные революции»), формирование политической толпы на «майдане» и, наконец, «прорывная точка» — власть свергнута либо начинается мятеж. На примере «арабской весны» Цыганков добавляет механизм обратной связи (итеративная коррекция сценария по опыту других стран) и механизм управляемого хаоса — разрушение общественного уклада ради восприимчивости к навязываемым шаблонам; вместе они позволяют управлять нестабильностью в целом регионе. Украинскую «революцию» 2013–2014 годов автор характеризует как повторение египетского сценария свержения Хосни Мубарака, отмечая, что волна «арабской весны» дошла до пространства СНГ и остановилась у границ России.

Кейс Эстонии 2007 года: первый прецедент

Первым эпизодом, когда страна НАТО официально обвинила Россию в агрессии — пусть и в форме кибератак, — стал кризис вокруг Бронзового солдата, советского воинского мемориала в Таллине. Весной 2006 года эстонская парламентская фракция потребовала его демонтажа, требование поддержал премьер-министр Андрус Ансип, а 10 января 2007 года был принят закон «О защите воинских захоронений», узаконивший перенос. Демонтаж провели в ночь с 26 на 27 апреля 2007 года, что вызвало волнения в Таллине. На пике кризиса, 29–30 апреля, правительственные и банковские сайты Эстонии подверглись массированной атаке хакеров, в организации которой страны НАТО обвинили Россию. Уже 1 мая глава эстонского МИД Урмас Паэт заявил о «нападении на европейское сообщество», а министр обороны Яак Аавиксоо предложил экспертам НАТО приравнять кибератаки к военной агрессии — поставить вопрос о применении статьи 5 Вашингтонского договора, положения о коллективной обороне альянса, по которому нападение на одного члена НАТО

считается нападением на всех. Официально альянс обвинения не подтвердил (генсек НАТО Яап де Хооп Схеффер назвал перенос памятника «внутренним делом Эстонии»), но уже в 2008 году в Таллине разместился Центр кибербезопасности НАТО. Этот эпизод стал точкой отсчёта, после которой кибератаки начали всерьёз обсуждаться как военная угроза.

Институциональная архитектура противодействия

После эстонского прецедента западные институты начали системно выстраивать архитектуру противодействия гибридным угрозам. Ключевой элемент — сеть более чем из двадцати центров передового опыта НАТО (Centers of Excellence): Центр объединённой кибернетической защиты в Таллине (2008, ежегодные учения Locked Shields с 2010 года), Центр стратегических коммуникаций в Риге (2014–2015, публикации выраженно антироссийского характера), Центр по противодействию гибридным угрозам в Хельсинки (октябрь 2017, при участии генсека НАТО Йенса Столтенберга и верховного представителя ЕС Федерики Могерини) — именно он предложил одно из наиболее цитируемых определений гибридных угроз, приведённое выше. Параллельно формировалась правовая доктрина: Таллиннское руководство по применению международного права к киберконфликтам вышло в двух версиях (2013 — 95 правил, легитимирующих кинетический ответ на кибератаки и приравнивающих их к оружию массового поражения; 2017 — расширение на менее масштабные атаки и смежные области права). В 2015 году Евросовет создал Оперативную рабочую группу по стратегическим коммуникациям (East StratCom Task Force) для противодействия российской дезинформации, а Пентагон в сентябре 2018 года представил стратегию «Троянский конь» — использование протестного потенциала «пятой колонны» для дестабилизации в сочетании с ударами высокоточного и кибероружия. Этому предшествовала цепочка эскалационных шагов США 2013–2018 годов: отказ от соглашения о предотвращении инцидентов в сфере информационно-коммуникационных технологий, наступательная Стратегия кибербезопасности 2015 года, причисление России и Китая к «ревизионистским силам» в 2017 году.

Россия выстраивала собственный контур ответных мер. После атак на госучреждения, зафиксированных «Лабораторией Касперского», президент подписал указ №31с от 15 января 2013 года о создании государственной системы обнаружения и предупреждения компьютерных атак; на его основе в декабре 2014 года утверждена концепция СОПКА, закреплённая за Федеральной службой безопасности (ФСБ). В июле 2012 года в закон «О некоммерческих организациях» внесены поправки о статусе «иностранного агента» — реакция на риски использования «мягкой силы» внешними субъектами; летом 2018 года вступил в силу «закон Яровой» (2016), обязавший операторов связи хранить данные о передаче информации. На площадке ООН в декабре 2018 года были приняты две конкурирующие резолюции по международной информационной безопасности — российская получила заметно больше голосов, чем американская, которая предлагала создать Рабочую группу открытого состава; её организационное заседание прошло в июне 2019 года.

Новый виток: 2024–2026 годы

К середине 2020-х риторика о гибридной войне из экспертного языка перешла в официальный. Министр иностранных дел России Сергей Лавров в октябре 2024 года констатировал, что противостояние России и Запада «пока носит элементы гибридной

войны, но всё больше переходит в прямую», связывая это со стремлением США переложить основную тяжесть на европейских союзников. Заместитель главы МИД Александр Грушко описывает конфликт как гибридную войну Запада с одним «горячим» театром — Украиной — и несколькими «холодными»: Балканами (политико-дипломатическая борьба) и Балтикой с Атлантикой (ограничение доступа России к морским коммуникациям для доставки энергоносителей на Глобальный Юг). В январе 2026 года МИД России и его представитель Мария Захарова квалифицировали действия Запада как «полномасштабную гибридную войну» ради удержания глобального доминирования, а постпред России при ОБСЕ Дмитрий Полянский в мае 2026 года назвал саму организацию инструментом этой войны.

Западные страны фиксируют серию инцидентов, которые приписывают России. В Балтийском море с октября 2023 по январь 2025 года зафиксировано четыре инцидента с повреждением подводных кабелей волочением якоря (17 ноября 2024 — кабели Швеция–Литва и Финляндия–Германия; на Рождество 2024 — Estlink 2 и интернет-кабели, танкер задержан погранслужбой Финляндии); в ответ НАТО в январе 2025 года запустила миссию Baltic Sentry. В Польше 16 ноября 2025 года на железной дороге Варшава–Люблин сработало взрывное устройство под грузовым поездом; власти квалифицировали это как диверсию, возложили ответственность на российскую разведку и предъявили заочные обвинения двум гражданам Украины, работавшим, по версии следствия, на ФСБ. В Молдавии на выборах и референдуме о вступлении в ЕС (октябрь–ноябрь 2024) президент Майя Санду обвинила Россию в «беспрецедентном» вмешательстве; распространился ИИ-дипфейк, в котором Санду якобы исполняет рэп на русском. В Румынии Конституционный суд 6 декабря 2024 года аннулировал результаты первого тура президентских выборов, сославшись на кампанию влияния через сеть из порядка 25 тысяч аккаунтов в TikTok. Долгоживущая кампания «Doppelganger» (с мая 2022 года, приписывается структурам, связанным с администрацией президента России) создаёт фейковые сайты-двойники западных СМИ; в сентябре 2024 года Минюст США объявил об изъятии 32 связанных с ней доменов.

Институциональный ответ Запада расширяется: Хельсинкский центр в 2025–2026 годах определяет гибридные угрозы как скоординированные действия, эксплуатирующие пороги обнаружения и атрибуции; в декабре 2025 года Еврокомиссия впервые применила денежный штраф по закону о цифровых услугах (Digital Services Act) — оштрафовала платформу X на 120 миллионов евро сразу по трём основаниям: обманчивая платная верификация («синие галочки»), непрозрачный реестр рекламы и препятствия доступу исследователей к данным о системных рисках (включая дезинформацию). Пятилетний мандат Рабочей группы открытого состава ООН по кибербезопасности завершился в июле 2025 года рекомендацией учредить постоянный переговорный механизм — Global Mechanism. Новое технологическое измерение — искусственный интеллект: Всемирный экономический форум весной 2026 года прогнозирует, что генеративный ИИ станет определяющим фактором дезинформации в 2026 году; на выборах в Ирландии (2025) распространился дипфейк о снятии кандидата, а в Нидерландах против оппонентов использовали около 400 ИИ-изображений — регуляторы вроде Федеральной избирательной комиссии США пока не выработали единых правил. Гибридное измерение конфликтов вышло и за пределы российско-западного противостояния: в 2025–2026 годах резко интенсифицировалось давление Китая на Тайвань (свыше 3700 залётов авиации в опознавательную зону ПВО за 2025 год, задержания судов из-за подозрений в перерезании

кабелей) и на Японию — похожая модель применяется разными державами в разных регионах.

Итоги и значение

Информационная и гибридная война — не аномалия и не пропагандистский ярлык, а системная характеристика конфликтов постбиполярной эпохи, то есть эпохи после распада двухполюсного, советско-американского порядка. Понятие выросло из военной теории конца XX века — сетевых и информационных войн — и из технической революции в военном деле, но по-настоящему институционализировалось после конкретного прецедента: атаки на Эстонию в 2007 году, впервые заставившей НАТО всерьёз обсуждать кибератаки как военную угрозу. С тех пор Запад выстроил разветвлённую архитектуру противодействия — от центров передового опыта НАТО до Таллиннского руководства и закона о цифровых услугах, — а Россия сформировала собственный контур защиты, от системы СОПКА до закона Яровой.

Ключевая особенность темы — асимметрия оценок. Запад описывает Россию как агрессора в информационном и киберпространстве, приписывая ей диверсии на Балтике и в Польше, вмешательство в выборы Молдавии и Румынии, кампанию Doppelganger; российская сторона на официальном уровне — в заявлениях Лаврова, Грушко, Захаровой — описывает себя как объект «полномасштабной гибридной войны» Запада ради удержания глобального доминирования. Обе стороны сходятся в одном: конфликт не имеет чёткой линии фронта и объединяет информационные, финансовые, технологические и военные средства в единую кампанию. Отвечая на этот вопрос билета, важно показать эту двойственность понятия — теоретическую, от сетевых и информационных войн к гибридным, и политическую, во взаимных обвинениях России и Запада, — а также новейшее развитие: искусственный интеллект и дипфейки создают качественно новый инструментарий дезинформации, а распространение гибридных практик на Тайвань и Японию показывает, что это уже не специфически российско-западный, а универсальный тип конфликта современной международной системы.

EXAMBOOSTER

Понравился формат? Заберите полное пособие

В полном издании «Билеты «Стратегии информационного воздействия»» — все 30 тем собеседования (базовый блок Т01–Т07 и профильный Т08–Т30): 205 страниц в таком же формате + доступ в закрытый Telegram-канал, где каждый билет — отдельный пост с навигацией.

Купить	https://app.exambooster.ru/checkout?product=siv
Все материалы	magistratura.exambooster.ru/materialy
Telegram-канал	@mgimo_exambooster
Телефон	+7 (925) 886-41-35
E-mail	info@exambooster.ru

Цена — 8000 ₽, разовый платёж: пособие в PDF + закрытый канал.

Дмитрий Санько — основатель Exambooster, выпускник МГИМО (МЭО, 2010) и Ryerson University, ex-преподаватель МГИМО. · ИП Санько Дмитрий Сергеевич, ИНН 772854182473.