ИНФОРМАЦИОННАЯ ВОЙНА ЗАРУБЕЖНЫХ ГОСУДАРСТВ С ЦЕЛЬЮ ВОЗДЕЙСТВИЯ НА СИСТЕМУ И ВОЙСКА СВЯЗИ ВС РФ

Вавринюк С.А.[1]

DOI: 10.24682/3034-4050-2024-3-20-25

Ключевые слова: *противоборство, информационные операции, киберпространство, контрразведка, критически важные технологии, национальная безопасность, разведывательное сообщество, стратегия, угрозы, уязвимость, система и войска связи.*

Цель работы: *формулирование понятия «информационная война» применительно тезиса воздействия на систему и войска связи, а также выработка контрмер на такое воздействие.*

Метод исследования: *сравнительный анализ*

Результаты исследования: *Результаты затрагивают несколько ключевых аспектов и подчеркивают важность противодействия факторам ведения информационной войны: 1. Успешные операции по распространению дезинформации могут привести к снижению доверия к официальным источникам информации, что ослабит моральный дух войск. 2. Прямые атаки на систему связи может нарушить координацию действий между подразделениями, что приведет к снижению оперативной готовности и эффективности выполнения задач. 3. Повышение осведомленности о возможностях киберугроз может привести к улучшению мер безопасности и позволит выявить новые уязвимости в системах. 4. Информационные войны могут изменить подходы к ведению военных операций, акцентируя внимание на информационном превосходстве, как ключевом элементе стратегии. 5. Необходимость противодействия информационным атакам может стимулировать развитие новых технологий и методов защиты информации. 6. Успешные информационные операции могут изменить баланс сил на международной арене, вызывая ответные действия со стороны других стран.*

Научная новизна: *исследование и объединение знаний из различных областей знаний, предложения мер защиты от информационных атак и повышения устойчивости систем связи и управления.*

Введение

Учитывая характер и движущие силы конфликтов начала XXI века, основными средствами их разрешения могут стать невоенные и, прежде всего, информационные способы воздействия. Развитие мирового сообщества наглядно демонстрирует, что в последнее время критически важным государственным ресурсом, оказывающим все большее влияние на национальную безопасность, становится информация, циркулирующая в автоматизированных системах управления и связи. Данные системы являются неотъемлемым компонентом структуры управления государством, экономикой, финансами и обороной. Ускоренное развитие компьютерных технологий не только в значительной мере способствовало повышению эффективности их функционирования, но и открыло дополнительные возможности для преднамеренного деструктивного воздействия на них противостоящей стороны.

Кроме этого, имеет место информационно-психологическое воздействие, которое представляет собой целенаправленное производство и распространение специальной информации.

Информация является важнейшим атрибутом процесса управления войсками и оружием. На всех этапах исторического развития военного дела она выступает как объект ожесточенной борьбы. Информационная борьба велась практически во всех войнах. Еще в VI–V веках до н. э. известный китайский полководец и военный теоретик Сунь-Цзы в своем трактате о военном искусстве писал: «…самая лучшая война — разбить замыслы противника; на следующем месте — разбить его союзы; на следующем месте — разбить его войска».

Таким образом, на современном этапе научно-технического развития на смену концепции «тотальной войны», которая может привести к глобальной катастрофе, вошла концепция цивилизованной «информационной войны» (ИВ).

Целевой задачей данной статьи является формулирование понятия «информационная война» применительно тезиса воздействия на систему и войска связи, а также выработка контрмер на такое воздействие.

[1]Вавринюк Сергей Адамович, старший преподаватель 45 кафедры, ФГКВОУ ВПО «Военная академия связи им. Маршала Советского Союза С.М. Буденного», г. Санкт-Петербург. E-mail: logoshik@mail.ru

1. Формулирование термина «информационная война» с точки зрения воздействия на систему и войска связи

Решающее значение борьбы за информационное превосходство для геополитического соперничества было так или иначе понято специалистами в конце 70-х — самом начале 80-х гг. XX века. В это время произошел перелом в оценках значимости информатизации руководителями государств-лидеров научно-технического прогресса. Были приняты первые государственные программы информатизации общества и вооруженных сил (ВС), которые по своей сути были направлены на наращивание усилий по достижению превосходства в информационной сфере.

Доктринальная проработка вопросов ведения информационного противоборства (ИП) в США началась сразу же по завершении операции «Буря в пустыне» в Персидском заливе (1991 г.), в которой американскими ВС были впервые применены новейшие информационные технологии. Основные принципы ведения информационной войны (ИВ) применительно к ВС были сформулированы в секретной директиве министерства обороны США от 21 декабря 1992 г. № TS 3600.1 «Информационная война». В директиве были сформулированы основные положения стратегии ИП. **В этом документе ИВ определялась как самостоятельный вид оперативного обеспечения** (комплексное информационное воздействие на системы государственного и военного управления противника и системы связи).

По мнению американских аналитиков, ИВ состоит из действий, предпринимаемых для получения *информационного превосходства, под которым понимается достижение военно-стратегического преимущества за счет более высокого, чем у противника, информационного потенциала, который позволяет держать противника в постоянном напряжении, одновременно повышая боевую устойчивость собственных сил*.

В директиве перед объединённым штабом комитета начальников штабов (КНШ) и штабами видов ВС ставились задачи по разработке военного аспекта новой концепции. Эта работа была завершена к концу 1993 г. и нашла своё отражение в секретной директиве (меморандуме) председателя КНШ ВС США № 30–93. В ней достаточно «аморфные» исходные положения концепции ИВ были трансформированы в концепцию **«Борьбы с системами управления»**, сущность которой определялась как «комплексное проведение по единому замыслу и плану ПсО, мероприятий по маскировке, РЭБ и физическому уничтожению пунктов управления и систем связи противника с тем, чтобы лишить его информации, вывести из строя или уничтожить его системы управления, одновременно защитив свои от аналогичных действий». Позднее военное руководство было вынуждено существенно расширить изложенный в директиве перечень целей проведения информационных операций (ИО).

С выходом в свет данной директивы в ВС США началась активная реорганизация существующих и создание новых организационно-штатных структур, предназначенных для решения задач планирования, моделирования и осуществления действий по борьбе с системами управления от стратегического до оперативно-тактического звеньев ВС. К концу 1998 г. были созданы соответствующие структуры в аппарате министра обороны и КНШ, а также во всех видах ВС США.

Согласно концепции информационной войны США оставляют за собой право на превентивные действия в киберпространстве в отношении враждебных государств в случае, если их политика угрожает или в обозримом будущем будет угрожать национальным интересам США. Кроме того, США также оставляют за собой право на адекватный ответ в случае нападения на информационные системы из кибернетического пространства, а не будут ограничиваться юридическими вопросами и слушаниями в суде по факту нарушения защиты информационных ресурсов [4].

Рис.1. Современные руководящие документы США в области информационной безопасности

В марте 2023 года принята новая «Национальная стратегия кибербезопасности США» вместо аналогичной 2018 года (Рис. 1).

В целом, анализ руководящих документов США в области ИП показывает, что все они направлены на обеспечение главенствующей роли США во всех сферах деятельности мирового сообщества и носят явно наступательный, агрессивный характер.

Итак, в соответствии с перечисленными руководящими документами, **информационная война — это комплексное воздействие на систему государственного и военного управления противостоящей стороны, ее политическое и военное руководство, которое уже в мирное время приводило бы к принятию благоприятных для США (стран блока НАТО) решений, а в ходе войны полностью парализовало бы всю систему управления противника. Одновременно с этим предусматриваются меры противодействия аналогичным акциям противника, защита своих систем управления от несанкционированного использования, изменения режима функционирования и физического разрушения**.

Война, как таковая не мыслима без проведения операций. **Информационная операция** — действия, предпринимаемые с целью затруднить сбор, обработку передачу и хранение информации информационными системами противника при защите собственной информации и информационных систем.

Таким образом, особое внимание уделим составным частям информационной войны, касающихся системы и войск связи: **психологические операции; электронная война; дезинформация; меры безопасности, прямые информационные атаки**.

Психологические операции — это программы действий и/или программы подготовки продукции, которые влияют на оценки, мнения и эмоции иностранных объектов воздействия с задачей формирования поведения, отвечающего целям внешней политики США и замыслу соответствующих командиров на стратегическом, оперативном и тактическом уровнях.

К основным средствам ведения психологических операций можно отнести:

- печатные материалы – листовки, плакаты, информационные бюллетени, средства их производства и распространения;
- средства массовой информации – газеты, радио, телевидение, новостные сайты и агрегаторы новостей в сети Интернет;
- интернет-ресурсы: специально созданные сайты и каналы, социальные сети, форумы, чаты.

Электронное вмешательство в процессы командования и управления военными объектами и системами, «штабная война», вывод из строя сетей военных коммуникаций.

Достижение прочного превосходства в электромагнитном спектре (EMS — Electromagnetic Spectrum) связано с концепцией ВС США многодоменных операций (MDO, Multi-Domain Operation) и способствует интеграции традиционных и новых операционных сфер. В 2019 году, исходя из доклада американского Центра стратегических и бюджетных оценок следовало, что США понадобится не менее 10 лет, чтобы сократить разрыв с конкурирующей России в электромагнитном спектре. В соответствии с наставлением КНШ ВС США JP 3–85 «Операции объединенных сил в электромагнитном спектре» от 22 мая 2020 г. термин «электронная война» (Electronic Warfare) заменен на термин «электромагнитная война» (Electromagnetic Warfare), который обозначает ведение боевых действий [7]. Основными ее составляющими являются: электромагнитная атака, электромагнитное обеспечение и электромагнитная защита. Надо отметить, что произошла не просто замена терминов, но и реальное изменение организационно-штатных структур основных подразделений, их оснащение современными образцами технических средств.

Примерами такой составляющей могут быть классические радиоигры со стороны вооруженных сил Украины (ВСУ), направленные на введение противника в заблуждение, а также кибервоздействие. Так, по аналитическому отчету компании «Ростелеком-Солар» в первом полугодии 2024 года экспертами зафиксировано 355 тысяч DDoS-атак, совершенных киберпреступниками на российские организации, что на 16% больше, чем за весь 2023 год. Увеличилась мощность таких атак, а продолжительность, наоборот, снизилась, чтобы избежать обнаружения и более эффективно использовать свои ресурсы.

Также можно отметить задержание в Париже основателя мессенджера «Телеграмм» Дурова с целями повлиять на получение ключей шифрования и доступа к контенту пользователей.

1.1. Дезинформация

Дезинформация — это предоставление противнику заведомо ложной информации для более эффективного ведения боевых действий, проверки на утечку информации и направление ее утечки, а также сам процесс манипулирования ею, введение кого-либо в заблуждение путем предоставления неполной или полной, но уже не нужной информации, а также искажения ее части [1]. По данным АНО (автономная не-

коммерческая организация) «Диалог», только за 10 месяцев 2023 года в российском сегменте интернета было зафиксировано три тысячи уникальных фейков и 8.4 миллиона случаев их распространения. По их прогнозам, в этом году число уникальных фейков возрастет до 4.5 тысяч, их копий — до 8 миллионов. При исследовании обычные граждане уверяли, что способны отличить достоверную информацию от недостоверной в 2/3 случаев. Но в реальности, в результате тестирования на предмет наличия базовых компетенций по верификации фейков только 52% экспертов и аналитиков из опрошенных по специальной выборке смогли справиться с заданием, отличив фейк от правдивой информации. Основные потребители фейков — это чаще женщины, чем мужчины (почти 60%) в возрасте от 40 лет. В 55% случаев фейки касаются специальной военной операции, в 17% — политических вопросов, 11% случаев — социальных и криминальных случаев [9].

Меры безопасности (стремление избежать того, чтобы противник узнал о возможностях и намерениях противоборствующей стороны)

В вооруженных силах США обеспечение безопасности предполагает мероприятия по защите информации, информационных систем и другой информационной инфраструктуры от внешних и внутренних угроз. К основным внешним угрозам относится — разведывательная деятельность зарубежных спецслужб, в том числе военной разведки, государственных, общественных, частных и иных организаций и отдельных лиц; воздействия средствами электромагнитных атак, кибератак и других специальных технических средств; диверсионно-подрывная деятельность иностранных спецслужб и сил специальных операций. К основным внутренним угрозам безопасности информации относятся инсайдерские угрозы и разведдеятельность террористических и преступных организаций [2].

Прямые информационные атаки (искажение информации без видимого изменения ее сущности)

Главную опасность представляют не случайные сбои, а целенаправленное воздействие на информационные ресурсы. При этом степень опасности пропорциональна степени централизации и автоматизации процесса управления.

Отметим, что по оценкам зарубежных специалистов восстановление автоматизированных систем раннего предупреждения о воздушно-космическом нападении, систем управления комплексами противоракетной обороны и других систем стратегического назначения практически невозможно. Результаты целенаправленного вмешательства в их работу могут иметь катастрофический характер и, по предполагаемому ущербу, сопоставимы с последствиями применения ядерного оружия [10].

2. Определение контрмер воздействиям на систему и войска связи

Если в XX веке сам процесс донесения информации до целевой аудитории занимал определенное осязаемое время, то с появлением и распространением интернет-технологий эти процессы занимают ровно столько времени, сколько нужно для того, чтобы нажать кнопку «Ввод». Это означает, что у обороняющегося попросту нет времени для принятия решений. Действовать приходится на опережение, а значит, нужно принимать превентивные меры, прикрывая уязвимости и обнаруживая их раньше противника [3].

Проактивными мерами для защиты от информационных войн и атак являются с позиции ведения дезинформации и психологических операций:

- критический анализ источников информации (авторитетность портала, газеты или иного канала);
- кросс-проверка сведений из разных источников;
- использование программного обеспечения (ПО) для анализа текста и изображений (программы «ФотоМАСТЕР», «SUPA», сайты Fakecheck, Snopes);
- развитие критического мышления.
- С точки зрения кибербезопасности необходимо использовать следующие меры:
- защита от несанкционированного доступа (определение перечня данных для служебного пользования, организация учета лиц, получивших доступ к конфиденциальной информации);
- применение программ антивирусной защиты (специальное программное обеспечение для обнаружения вредоносных программ и восстановления поврежденных ими файлов);
- использование межсетевых экранов, как инструмента контролирующего входящий, исходящий и внутрисетевой трафик;
- регулярное резервное копирование и своевременное обновление данных;
- использование средств обнаружения и предотвращения вторжений;
- применение средств анализа и контроля защищенности информации;

- применение криптографической защиты информации (процесс использования криптографических методов и алгоритмов для обеспечения конфиденциальности, целостности, аутентификации и доступности данных).

Таким образом, как следует из предпринимаемых с начала 1990-х гг. усилий по всестороннему развитию концепции информационной войны, американское военно-политическое руководство стремится закрепить за США в XXI в. статус информационной сверхдержавы.

Заключение

Таким образом, результаты анализа сущности и содержания ИВ позволяет сделать вывод, что она имеет ряд отличительных особенностей, основными из которых являются:

1. ИВ любого масштаба может вестись без ее юридического объявления.
2. Затруднены определение времени начала войны, а также распознавание противников, их намерений и возможностей.
3. Отсутствуют традиционные препятствия и границы в связи с интеграцией национальных информационных инфраструктур различных стран в глобальные сети, что обеспечивает возможность ведения ИВ с любой территории в любом районе Земли.
4. Существенно расширяется число гражданских лиц, принимающих непосредственное участие в ИВ.
5. Затруднена классификация происходящих событий (технический сбой, халатность персонала, преступный акт или акт ИВ).
6. Высокая уязвимость информационных систем, обеспечивающих функционирование государства и его отдельных структур, от потенциального воздействия на них средствами ИВ.
7. ИВ может вестись без физического уничтожения людей и объектов.
8. Результаты воздействия в ИВ не пропорциональны числу привлекаемых для ее ведения сил и средств.
9. В ИВ самые развитые государства потенциально являются самыми уязвимыми, что обусловлено значительным превышением темпов разработки и совершенствования информационного оружия над темпами развития технологий защиты.
10. ИВ может вестись без ограничений во времени, что связано с существенной разницей в затратах на ведение информационной и обычной войны.
11. Основные итоги ИВ могут сохраняться в течение длительного периода времени.
12. ИВ обеспечивается специфическими средствами и методами их применения [5].

Главная опасность информационной войны заключается в том, что она не несет видимых признаков разрушения. Поэтому специалистам связи необходимо знать основные составные части информационной войны и своевременно использовать проактивные средства и методы защиты.

Литература

1. Заполев С., Паршин С. Основные составляющие информационных операций вооруженных сил США // Зарубежное военное обозрение, 2021. № 10. С. 3–11.
2. Ласточкин Ю.И., Донсков Ю.Е., Морареску А.Л. Анализ современных концепций по ведению операций в электромагнитном спектре с позиций радиоэлектронной борьбы // Военная мысль. 2021. № 4. С. 29–38.
3. Макаренко С.И. Анализ средств и способов противодействия беспилотным летательным аппаратам. Часть 3 // Системы управления, связи и безопасности. 2020. №2. С. 101–175.
4. Манойло А.В. Информационные войны и психологические операции. Руководство к действию /Горячая линия-Телеком. М.: 2024. – 496с.
5. Маркин А.В. Обобщение боевого опыта южного крыла СВО до апреля 2024 года/Центр специальных программ. М.: Социально-Политическая МЫСЛЬ, 2024. – 220с.
6. Алаудинов А.А. Современные гибридные войны: формы, методы, технологии (на материалах специальной военной операции на Украине) // Горячая линия-Телеком. М.: 2024. – 296с.
7. Новиков В.К. Информационное оружие – оружие современных и будущих войн // Горячая линия-Телеком. М.: 2024. – 288с.
8. Иванов В. Г. Основы построения и оценки эффективности функционирования системы связи специального назначения в международном вооруженном конфликте на основе многосферной и конвергентной структуры ее элементов: Монография. – СПб.: ПОЛИТЕХ, 2023. – 298с.
9. Воронова О.Е, Трушин А.С. Современные информационные войны: стратегии, типы, методы, приемы. – М.: Аспект Пресс, 2020. – 176с.
10. Панарин И.Н. Информационная война и коммуникации // Горячая линия-Телеком, 2023. – 236с.