Проект «Народный перевод»

ОПЕРАЦИИ В КИБЕРПРОСТРАНСТВЕ И РАДИОЭЛЕКТРОННАЯ БОРЬБА

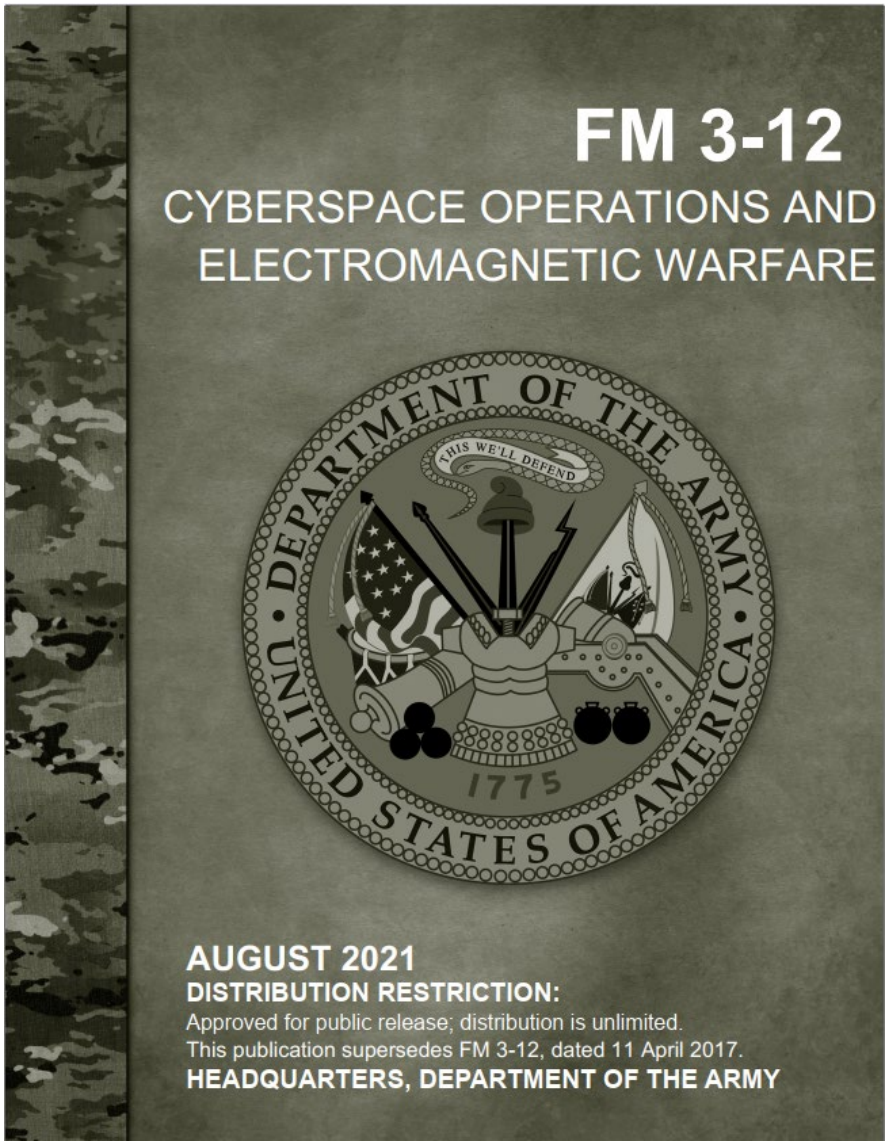
БОЕВОЙ УСТАВ АРМИИ США FM 3-12

Первоначально издано министерством Армии США в августе 2021 года.

Переведено неофициально на русский язык в феврале 2024 года.

Настоящий боевой устав утверждён приказом министра Армии США от 24 августа 2021 г. и заменяет ранее действовавший боевой устав FM 3-12 от 11 апреля 2017 года. Документ доступен на сайте Управления издательской деятельностью США и на сайте Центрального регистра СВ США.

Оригинальная обложка:



Переведено участниками проекта «Народный перевод».

Оглавление

ВСТУПИТЕЛЬНОЕ СЛОВО

За последние два десятилетия незатухающих конфликтов сухопутные войска развернули самые мощные системы связи за всю свою историю. В течение этого времени вооружённые силы США продолжали доминировать в киберпространстве и электромагнитном спектре, проводя операции в Афганистане и Ираке против противника, не способного оспорить технологическое превосходство США. Однако, в последние годы региональные соперники продемонстрировали внушительный потенциал в гибридных войнах. Эти возможности угрожают доминированию сухопутных войск США как в киберпространстве, так и в электромагнитном спектре.

Информационная сеть министерства обороны – сухопутные войска США является неотъемлемой площадкой для ведения боевых действий и критической составляющей системы командования и управления, на которой строится успех операций сухопутных войск. Эффективная эксплуатация, обеспечение безопасности и защита сети для поддержания доверия к её конфиденциальности, целостности и доступности является залогом успеха командиров на всех уровнях. Командир, не имеющий доступа к коммуникационным и информационным системам и данным, рискует потерять жизни подчинённых, утратить критически важные ресурсы или провалить боевую задачу.

В то же самое время противник также все больше полагается на сети и системы вооружения, связанные с сетевыми технологиями. Сухопутные войска, как часть объединённых (межвидовых) сил, должны быть готовы использовать или лишить противника оперативных преимуществ, которые предоставляют эти сети и системы.

По мере того, как сухопутные войска переключают своё внимание на крупномасштабные боевые действия против региональных соперников, мы должны понимать, что противник будет постоянно пытаться получить доступ, найти уязвимости и ухудшить состояние наших сетей и данных.

В будущем, по мере роста возможностей противника, наше продолжающееся господство в киберпространстве и электромагнитном спектре станет менее очевидным, в то же время наша способность получать доступ к киберпространству и зависящим от спектра возможностям станет, как более сложной, так и более важной для борьбы и победы в различных доменах.

Эффективное использование поражающих факторов киберпространства и РЭБ на всех этапах противоборства является ключом к достижению относительных преимуществ в киберпространстве и электромагнитном спектре, при одновременном лишении противника аналогичных возможностей. Для достижения таких относительных преимуществ командиры должны внедрять и согласовывать операции в киберпространстве и ведение РЭБ с прочими силами и средствами вооружённой борьбы путём совместных действий различных родов войск.

Кроме того, для успешного планирования, согласованности и проведения операций в киберпространстве и ведения РЭБ, критически важными являются разведывательная и информационная деятельность, средства связи, а также космический и огневой потенциал. Командиры и штабы осуществляют внедрение и согласование этих возможностей в различных доменах и аспектах боевого обеспечения для достижения максимального взаимодополняющего поражающего воздействия в киберпространстве и электромагнитном спектре.

Боевой устав FM 3-12 определяет и описывает принципы и тактику решения задач в оперативной обстановке, а также даёт представление о боевых действия (операциях) в киберпространстве, ведении РЭБ, их планировании, внедрении и согласовании в рамках оперативного процесса (операций). В нём описываются части и подразделения, проводящие эти операции, и то, как они обеспечивают достижение целей командиров в боевых действиях (операциях) сухопутных войск.

В связи с быстрым развитием своих возможностей, тактики, техники и процедур в киберпространстве и электромагнитном спектре, Головной центр кибероперациий будет пересматривать и обновлять Боевой устав FM 3-12 и вспомогательные публикации, чтобы не отставать от постоянно меняющейся оперативной обстановки.

Нейл С. Херси (NEIL S. HERSEY)

генерал-майор, командование сухопутных войск США

ВВЕДЕНИЕ

Боевой устав FM 3-12 предусматривает реализацию доктрины сухопутных войск по использованию кибер-электромагнитной деятельности для внедрения и согласования боевых действий (операций) в киберпространстве и ведения РЭБ в рамках операций при управлении выделенными участками электромагнитного спектра в интересах совместных наземных операций. Боевой устав FM 3-12 определяет и даёт понимание кибероперации сухопутных войск, ведения РЭБ, уставных и должностных полномочий, ролей, отношений, обязанностей и возможностей для обеспечения боевых действий (операций) сухопутных войск и объединенных операций. В нём раскрываются методы СВ ведения наступательных и оборонительных кибероперации, а также рассматриваются способы внедрения командирами и штабами возможностей киберпространства и РЭБ в рамках всего спектра военных операций.

Боевой устав FM 3-12 охватывает и обосновывает доктрину по объединённым кибероперациям и РЭБ и публикацию ADP 3-0: Доктрина Сухопутных войск – «Операции» (ADP 3-0, Operations) и содержит положения доктрины для рассмотрения взаимосвязи между оперативным процессом сухопутных войск и кибероперациями и РЭБ. Для понимания основ внедрения и согласования кибероперации и РЭБ читатель должен быть знаком с изданиями: ADP 2-0, ADP 3-0, ADP 3-19, ADP 3-37, ADP 3-90, ADP 5-0, ADP 6-0, FM 3-09, FM 3-13, FM 3-55, FM 6-0, ATP 2-01.3, JP 3-12, и JP 3-85.

Боевой устав FM 3-12 раскрывает, как личный состав, участвующий в кибер-электромагнитной деятельности, внедряет и согласовывает функционал и возможности кибероперации и РЭБ в рамках боевого обеспечения, защищает сеть и предоставляет командирам критически важные возможности на всех уровнях в ходе совместных наземных операций.

Боевой устав FM 3-12 содержит четыре главы и семь приложений.

В главе 1 описывается как кибероперации и РЭБ обеспечивают поддержку сухопутных войск при проведении совместных наземных операций. В ней даётся обзор аспектов оперативной обстановки, в которой части и подразделения проводят кибероперации и ведут РЭБ. В данной главе также подробно представлено, как кибероперации и ведение РЭБ оказывают поддержку в боевом обеспечении сухопутных войск.

В главе 2 подробно рассмотрены виды кибероперации и РЭБ, а также связанные с ними задачи и общие поражающие факторы. В ней также рассматривается взаимосвязь кибероперации и РЭБ с другими видами операций сухопутных войск.

В главе 3 представлен обзор организационных структур объединённых сил и сухопутных войск, осуществляющих кибероперации и РЭБ. В ней также описываются роли и обязанности специального отделения кибер-электромагнитной деятельности на различных уровнях. В этой главе рассматривается взаимодействие отделения кибер-электромагнитной деятельности с другими структурными подразделениями штаба и объясняется роль рабочей группы по кибер-электромагнитной деятельности.

В главе 4 рассмотрено, каким образом командиры и штабы осуществляют внедрение и согласование кибероперациий и РЭБ в рамках оперативного процесса. Далее в главе более подробно представлены ключевые исходные и выходные данные, связанные с разведывательной подготовкой района боевых действий, сбором информации, целеуказанием, управлением рисками и информацией.

В Приложении А описаны две наиболее распространённые методики принятия решений в сухопутных войсках (Методика выработки комплексных решений и процесс принятия военных решений) и порядок их применения для планирования, внедрения и согласованности кибероперациий и РЭБ с оперативным и интеграционным процессами.

В Приложении В описаны правила ведения боевых действий и соответствующие разделы Кодекса США, связанные с кибероперациями и РЭБ. Оно включает таблицу, в которой приведены все кибероперации и РЭБ, относящиеся к законодательству США (титульные полномочия). Приложение В содержит таблицу с перечнем федеральных законов, защищающих информацию и права граждан США на неприкосновенность частной жизни.

В Приложении С рассматриваются вопросы, связанные с проведением кибероперациий и РЭБ в составе объединённых сил или с другими участниками совместных действий[1].

В Приложение D рассматриваются национальные силы и средства, силы и средства министерства обороны и резерва СВ США, которые обеспечивают кибероперации. В данном приложении также приводится обзор Киберкомандования США и подчинённых ему объединённых структурных подразделений, обеспечивающих поддержку кибероперациий и РЭБ общевойсковых командиров, использующих силы и средства для выполнения задач в киберпространстве.

В Приложении Е рассматривается, каким образом подразделения сухопутных войск осуществляют запрос на поддержку кибероперациий и РЭБ при совместных действиях. Графические изображения отображают процессы запроса на поддержку как при наступательных, так и при оборонительных кибероперациях.

[1] Участники совместных действий (*англ. unified action partners*) – военные силы, правительственные и неправительственные организации, а также составляющие частного сектора, с которыми вооружённые силы осуществляют планирование, взаимодействие, согласование и внедрение своих действий во время проведения операций – прим. пер.

В Приложении F представлен общий порядок действий для улучшения приёмов и возможностей РЭБ. В нём описаны четыре фазы улучшения приёмов и возможностей РЭБ и их три основные категории и действия.

В Приложении G приводится обзор подготовки военнослужащих и более подробно рассматривается подготовка тех, кто стремится получить профессию в области кибероперациий и ведения РЭБ.

ГЛАВА 1. ОБЩЕЕ ПРЕДСТАВЛЕНИЕ ОБ ОПЕРАТИВНОЙ ОБСТАНОВКЕ

В данной главе описаны аспекты оперативной обстановки, в которой сухопутные войска проводят кибероперации и РЭБ. Рассмотрены их прямые обязанности и изложены фундаментальные принципы ведения кибероперациий и РЭБ. В главе представлены взаимосвязи между кибероперациями, РЭБ и другими аспектами боевого обеспечения.

Общее представление об оперативной обстановке

1-1. Кибероперации и РЭБ играют важную роль в проведении сухопутными войсками совместных наземных операций в составе объединённых сил и во взаимодействии с другими участниками совместных действий.

Кибероперации *(англ. Cyberspace operations, CO)* – это использование средств воздействия на киберпространство, основной целью которых является достижение целей в киберпространстве или с его помощью (JP 3-0).

Радиоэлектронная борьба *(англ. Electromagnetic warfare, EW)* – это военные действия, связанные с использованием электромагнитной и направленной энергии для контроля электромагнитного спектра или для нападения на противника (JP 3-85).

1-2. Киберпространство является одной из пяти сфер, в которых ведутся боевые действия. Операции проводятся в части электромагнитного спектра ((далее – ЭМС) (*англ. electromagnetic spectrum*, *EMS*), например, Bluetooth, Wi-Fi, спутниковый трафик. Поэтому кибероперации и РЭБ требуют распределения радиочастот, управления ими и взаимодействия между операторами средств РЭБ, через которые осуществляются операции по управлению электромагнитным спектром. Операции по управлению спектром состоят из четырёх ключевых функций: управление спектром, распределение частот, взаимодействие со страной пребывания войск и соблюдение правил. Операции по управлению спектром включают предотвращение и уменьшение конфликтов в радиосети и электромагнитных помех (далее – ЭМП) (*англ. electromagnetic interference, EMI*) между своими войсками и войсками страны пребывания во время операций сухопутных войск (см. Наставление ATP 6-02.70).

Киберпространство и электромагнитный спектр

1-3. Киберпространство и ЭМС имеют решающее значение для успеха в современной оперативной обстановке. Как силы США, так и силы противника в значительной степени полагаются на киберпространство и технологии, зависящие от ЭМС, для управления и контроля, сбора информации, понимания ситуации и целеуказания. Достижение относительного превосходства в киберпространстве и ЭМС даёт командирам преимущество перед противником. Проводя кибероперации и РЭБ, командование может ограничить доступные противнику варианты действий, снизить его способность мобилизовывать силы, ослабить его командование и управление, а также снизить его способность эффективно действовать в других доменах.

1-4. Командиры должны использовать возможности киберпространства и РЭБ, применяя силы и средства вооружённой борьбы путём совместных действий различных родов войск овладевать, удерживать и использовать оперативную инициативу.

Эффективное использование кибероперациий и РЭБ требует от командиров и штабов проведения кибер-электромагнитной деятельности (*англ. cyberspace electromagnetic activities, CEMA*).

Кибер-электромагнитная деятельность[2] (далее CEMA) – это процесс планирования, внедрения и согласования кибероперациий и РЭБ для обеспечения совместных наземных операций (ADP 3-0).

Внедряя и согласуя кибероперации и РЭБ, свои войска получают информационное преимущество в различных доменах и направлениях деятельности.

На рис. 1-1 показано, какой вклад вносят кибероперации и РЭБ в операции сухопутных войск.

[2] *Далее в настоящем Боевом уставе вместе с термином «кибер-электромагнитная деятельность» или вместо него используется аббревиатура CEMA (прим. переводчика).*

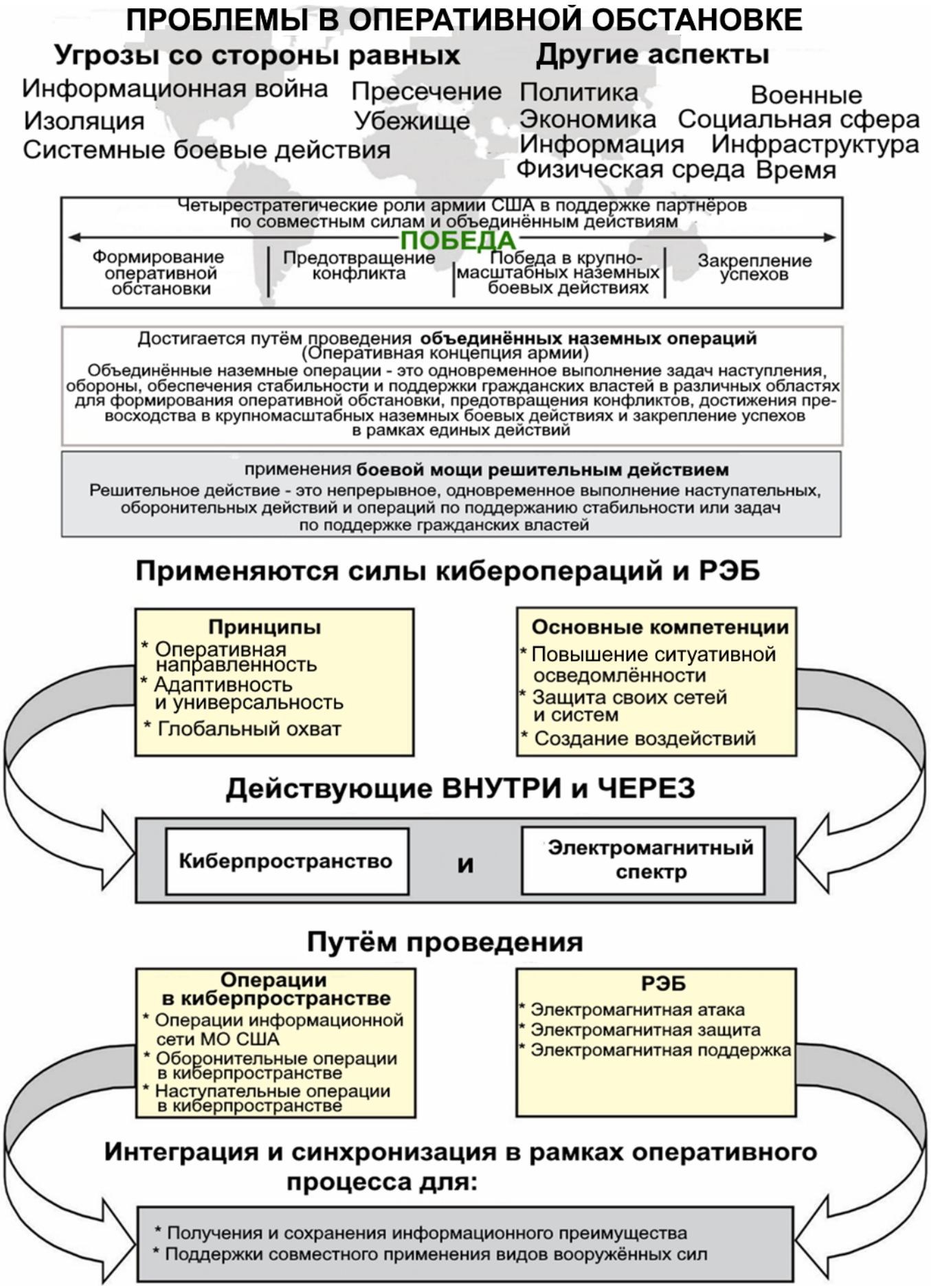


Рис. 1-1. – *Логическая схема кибероперацийи РЭБ*

ПРЕДИСЛОВИЕ

Боевой устав FM 3-12 содержит тактику и порядок взаимодействия, внедрения и согласования боевых действий (операций) сухопутных войск (далее – СВ) в киберпространстве и РЭБ для обеспечения совместных наземных и объединённых операций. Боевой устав FM 3-12 объясняет основы, термины и определения боевых действий (операций) в киберпространстве (далее – кибероперации) и радиоэлектронной борьбы (далее – РЭБ) сухопутных войск. В данном издании описывается, каким образом командиры и штабы осуществляют внедрение кибероперациий и РЭБ в совместные наземные операции. Издание представляет собой всеобъемлющее руководство для командиров и штабов по кибероперациям и РЭБ сухопутных войск на всех уровнях. Издание заменяет Боевой устав FM 3-12 от 11 апреля 2017 года.

Основной целевой аудиторией Боевого устава FM 3-12 являются все представители соответствующего рода войск. Командиры и личный состав штабов сухопутных войск, действующих в качестве объединённой оперативно-тактической группы или многонационального штаба, также должны применять совместную или многонациональную доктрину в отношении всего диапазона военных операций и объединённых или многонациональных сил. Издание также будет полезно инструкторам и преподавателям всех родов сухопутных войск.

Командиры, штабы и их подчинённые обеспечивают соблюдение применимых законов и правил Соединённых Штатов, международных, а также, в некоторых случаях, законов и правил страны пребывания войск. Командиры всех уровней должны следить за тем, чтобы их военнослужащие действовали в соответствии с законами войны и правилами ведения боевых действий (см. Боевой устав FM 6-27). Они также, должны придерживаться военной этики, описанной в Наставлении ADP 1.

В Боевом уставе FM 3-12 в необходимых случаях используются единые термины. Общая и военная терминология и определения приведены как в словаре, так и в тексте. Настоящее издание не является пропагандой каких-либо военных терминов. Термины и определения, для которых Боевой устав FM 3-12 является первоисточником, выделены в тексте жирным шрифтом. Для других определений, приведённых в тексте, термин выделен курсивом, а после определения указан номер публикации его разработчика.

Боевой устав FM 3-12 распространяется на действующий личный состав СВ, Национальной гвардии СВ США, а также на резерв СВ США, если не указано иное.

Разработчиком Боевого устава FM 3-12 является Головной центр кибероперациий СВ США. Подготавливающим органом является Отдел развития доктрин из состава Головного центра кибероперациий СВ США.

Комментарии и предложения предлагается направлять по адресу: ********

1.1. Основные компетенции и фундаментальные принципы

1-5. Зависимость сухопутных войск от сетевых систем и вооружений требует наличия высококвалифицированных специалистов для защиты боевых систем и сетей, зависящих от доступа к киберпространству и электромагнитному спектру. Киберпространство и ЭМС могут быть сильно перегружены из-за использования их противником, нейтральными субъектами и своими войсками, а также постоянных действий противника.

1-6. Противник продолжает разрабатывать современные виды вооружения и сетевые системы, которые проецируют мощь через киберпространство и ЭМС, или зависят от них. Сухопутные войска задействуют возможности киберпространства и РЭБ в рамках сил и средств вооружённой борьбы и путём совместных действий различных родов войск и видов вооружённых сил наносят поражение действиям угрозы (противника) в киберпространстве и ЭМС, защищают свои войска и обеспечивают свободу действий в их интересах на протяжении всего конфликта. Кибервойска и войска РЭБ сухопутных войск отвечают за свои основные компетенции и применяют следующие основополагающие принципы для завоевания и удержания позиций относительного преимущества своими войсками.

1.1.1. Основные компетенции

1-7. Кибервойска и специалисты по РЭБ организованы, обучены и оснащены в целях реализации функционирования областей, которые обеспечивают важные и долговременные возможности сухопутных войск:

- обеспечение понимания ситуации;
- защиту личного состава, сил и средств;
- нанесение поражающих воздействий.

1.1.1.1. Обеспечение понимания ситуации

1-8. Кибервойска осуществляют разведку, наблюдение и рекогносцировку киберпространства в информационной среде и через неё с целью выявления и изучения сетей, систем и процессов противника. Эта информация позволяет командирам лучше понять возможности и уязвимости противника, что повышает их способность определять приоритеты и наносить поражающее воздействие.

1-9. Специалисты РЭБ ведут наблюдение за электромагнитным спектром для сбора боевой информации, используемой для характеристики применения ЭМС противником и понимания особенностей интеграции излучающих систем противника на разных уровнях. Эта информация позволяет определить свои уязвимые места и возможности угроз, а командованию – расставить приоритеты и нанести поражающее воздействие.

1.1.1.2. Защита личного состава, сил и средств

1-10. Кибервойска обеспечивают защиту сетей, боевых платформ, сил и средств, а также данных от текущей или надвигающейся злонамеренной активности в киберпространстве. Защищая критически важные сети и системы, кибервойска помогают поддерживать способность сухопутных войск проводить операции и проецировать силу во всех сферах.

1-11. Войска РЭБ во взаимодействии со структурным подразделением штаба G-6 или S-6 и в поддержку директивы командира осуществляют и усиливают меры по защите своего личного состава, объектов, боевых платформ, сил и средств от неблагоприятных воздействий в ЭМС.

Войска РЭБ предлагают к принятию меры по маскировке или контролю излучения своих сил и средств от обнаружения противником и лишают его возможности обнаруживать и идентифицировать свои подразделения. Войска РЭБ обнаруживают и ослабляют атаки противника в ЭМС в целях обеспечения способности сухопутных войск проводить операции и проецировать силу во всех сферах.

1.1.1.3. Нанесение поражающих воздействий

1-12. Кибервойска оказывают киберпространственные поражающие воздействия на сети, системы и вооружение противника. Эти воздействия повышают способность сухопутных войск вести боевые действия (операции), снижают боевые возможности противника и позволяют проецировать силу во всех сферах.

1-13. Специалисты РЭБ оказывают воздействия на сети, системы и вооружение противника в рамках ЭМС. Эти действия снижают боевые возможности противника, обеспечивают защиту своих войск и усиливают их поражающие способности.

1.1.2. Фундаментальные принципы

1-14. Фундаментальные принципы – это основные правила или предположения, имеющие центральное значение и определяющие подход специалистов по кибероперациям и РЭБ к проведению киберопераций и ведению РЭБ.

Фундаментальными принципами являются:

- оперативная направленность;
- адаптивность и универсальность;
- глобальный охват.

1.1.2.1. Оперативная направленность

1-15. Кибервойска и войска РЭБ выполняют задачи в поддержку основного оперативного замысла командующего. При правильном внедрении и согласовании в рамках сил и средств вооружённой борьбы и путём совместных действий различных родов войск, средства воздействия киберпространства и РЭБ могут создавать многоуровневые проблемы для противника в различных доменах и изменять его относительные боевые возможности. Для достижения этой цели штабы, занимающиеся вопросами кибероперациий и РЭБ, должны уметь осуществлять взаимодействие по всем направлениям боевых действий.

1.1.2.2. Адаптивность и универсальность

1-16. Кибервойска и войска РЭБ ведут боевые действия (операции), используя возможности, адаптируемые к различным требованиям задачи. Возможности сил кибероперациий и войск РЭБ различаются как по численности применяемых сил, так и по величине или масштабу создаваемых ими поражающих факторов. В зависимости от задачи возможности кибероперациий и РЭБ могут использоваться как главные или поддерживающие воздействия для решающих, формирующих или обеспечивающих операций.

1.1.2.3. Глобальный охват

1-17. Характер киберпространственной сферы увеличивает оперативный охват сил кибероперациий и войск РЭБ. Силы, выполняющие боевые задачи, и специалисты по РЭБ обеспечивают стратегическое, оперативное или тактическое воздействие по всему миру с удалённых, совместных или передовых оперативных позиций.

1.2. Оперативная обстановка

1-18. ***Оперативная обстановка*** (*англ. operational environment, OE*) – это совокупность условий, обстоятельств и факторов, которые влияют на применение сил и средств и принятие решения командиром (JP 3-0). Условия в киберпространстве и ЭМС часто быстро меняются и могут как положительно, так и отрицательно влиять на способность командира достичь поставленных целей. Действия своих сил, нейтральных субъектов и противника в киберпространстве и ЭМС могут создавать практически мгновенные последствия на поле боя или в расположении гарнизона. Учитывая глобальный характер киберпространства и ЭМС эти действия могут оказывать влияние на оперативную обстановку командира в зоне ответственности, даже если они могут зарождаться или заканчиваться за пределами этой оперативной обстановки. Воздействия в киберпространстве и РЭБ также пересекаются между собой и оказывают влияние на несколько доменов одновременно.

По этим причинам для захвата, использования и удержания оперативной инициативы командование должно получать и поддерживать глубокое понимание оперативной обстановки, выходящее за пределы наземной сферы и распространяющееся на все сферы и на всю глубину боевых действий.

1-19. ***Оперативная инициатива*** (*англ. operational initiative*) – это определение темпа и условий действий на протяжении всей операции (ADP 3-0). Завоёвывая и удерживая позиции относительного преимущества, включая информационное преимущество в киберпространстве и ЭМС, командование может захватить и удержать оперативную инициативу. Для получения и сохранения информационного преимущества командование должно учитывать временную природу информации и временный характер большинства воздействий в киберпространстве и РЭБ.

В среднем, относительное оперативное преимущество, которое командир может получить от той или иной информации или от поражающих возможностей в киберпространстве или РЭБ, со временем снижается. Это означает, что командир, действующий первым, в среднем получит большее информационное преимущество от аналогичной информации или воздействия, чем командир, действующий позже.

Таким образом, командир, который может ощущать, понимать, принимать решения, действовать и оценивать быстрее, чем противник, как правило, получает наибольшее информационное преимущество.

1-20. Командиры могут использовать возможности киберпространства и РЭБ для повышения уровня ситуативной осведомлённости и понимания противника с помощью разведывательных действий и действий по сканированию пространства. Они могут дополнить и расширить понимание, получаемое командиром в результате сбора информации и разведывательных операций. Командиры также могут использовать возможности киберпространства и РЭБ для быстрого принятия решений и быстрых действий, в отличии от противника.

Защита своих информационных систем и систем связи своих войск от возможного нарушения или использования противником позволяет командиру обеспечить командование и управление и сохранить тактическую и оперативную внезапность. С другой стороны, командир может использовать киберпространство и системы РЭБ для замедления или ослабления процесса принятия решений противником путём нарушения его информационно-разведывательных средств, связи или обработки данных. Чтобы эффективно использовать возможности киберпространства и РЭБ для достижения информационного превосходства, командир должен заблаговременно планировать полную интеграцию операций в киберпространстве и действий в области РЭБ в общий план боевых действий.

1.2.1. Сфера киберпространства

1-21. ***Киберпространство*** является глобальной сферой в информационной среде, состоящей из взаимосвязанных сетей информационно-технологической инфраструктуры и данных, включая Интернет, телефонные сети, компьютерные системы и встроенные процессоры и контроллеры (JP 3-12). Кибероперации требуют использования связей и узлов, расположенных в других физических сферах, для выполнения логических функций, создающих эффекты в киберпространстве, которые затем проникают в физические сферы с помощью проводных сетей и ЭМС.

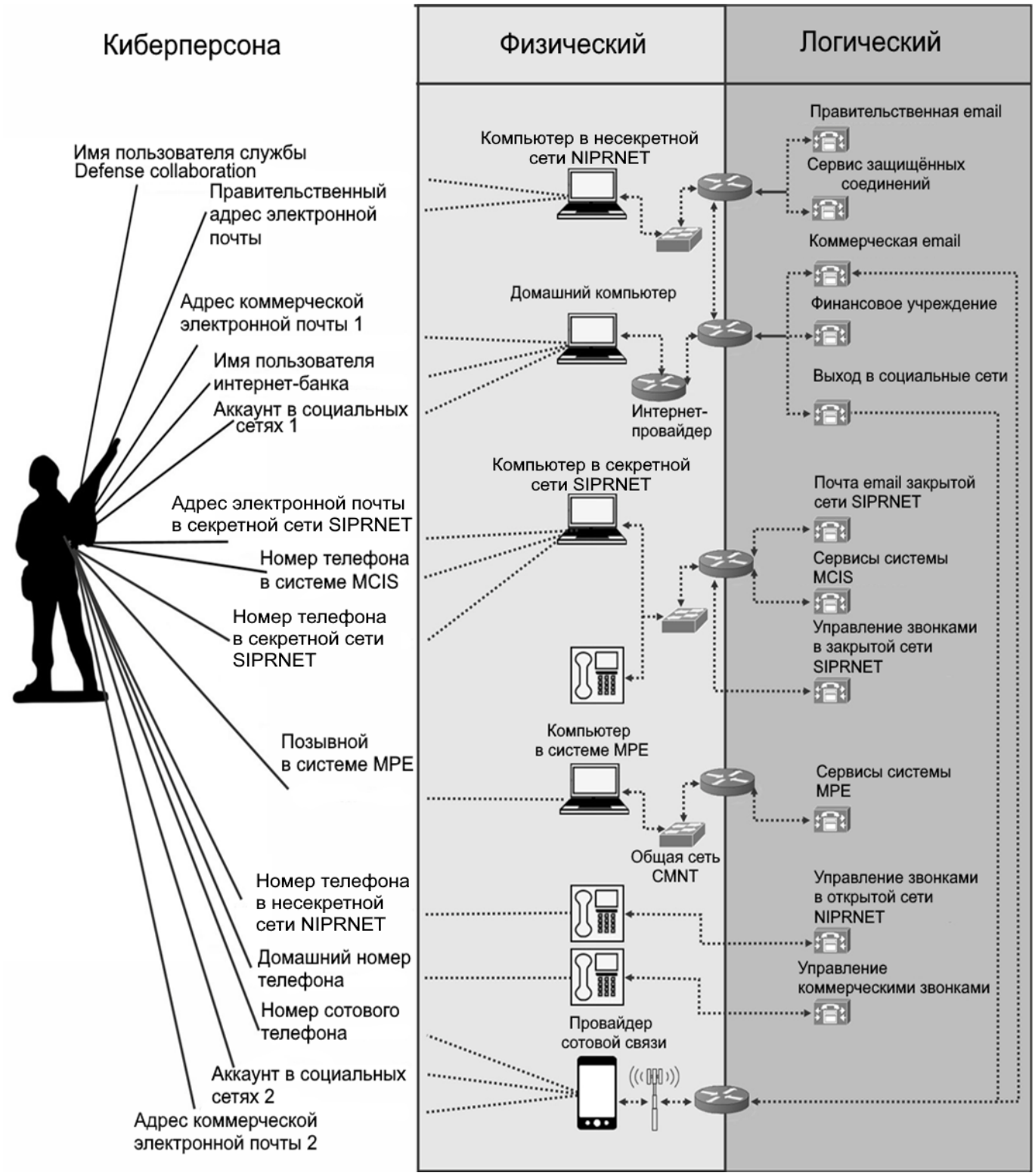
1-22. Использование киберпространства имеет большое значение для проведения операций. Сухопутные войска проводят кибероперации и вспомогательные мероприятия в рамках как самостоятельных, так и объединённых операций. Поскольку киберпространство является глобальной средой связи и обмена данными, оно по своей природе является совместным, межорганизационным, многонациональным и зачастую общим ресурсом, в котором значительное место занимают электромагнитные и разведывательные средства. Сети, системы связи, компьютеры, системы сотовой связи, сайты социальных сетей, технические инфраструктуры – всё это является частью киберпространства как противника, своих войск, так и страны пребывания.

1-23. Для облегчения планирования и проведения кибероперациий иногда используют трёхслойную модель киберпространства. Эти слои взаимозависимые, но каждый из них обладает уникальными характеристиками, влияющими на операции. Кибероперации обычно охватывают все три слоя киберпространства, но могут быть направлены для воздействия на один или несколько конкретных слоёв. Ответственные за планирование должны учитывать вызовы и возможности, предоставляемые каждым слоем киберпространства, а также взаимодействие между ними.

На рис. 1-2 представлена взаимосвязь между тремя слоями киберпространства.

Три слоя киберпространства:

1. Физический сетевой слой.
2. Логический сетевой слой.
3. Персональный кибер слой.



Сокращения:
CMNT (common mission network transport) – общая сеть обмена информацией;
MCIS (mission command information system) – боевая информационная командная система;
MPE (mission partner environment) – операционная среда командования и управления (C2);
NIPRNET (Non-classified Internet Protocol Router Network) – сеть маршрутизаторов несекретного интернет-протокола;
SIPRNET (SECRET Internet Protocol Router Network) – сеть маршрутизаторов секретного интернет-протокола.

Рис. 1-2. – *Взаимосвязь между слоями киберпространственной сети.*

1.2.1.1. Физический сетевой слой

1-24. Физический сетевой слой состоит из устройств и инфраструктуры информационных технологий в физических сферах, которые обеспечивают хранение, транспортировку и обработку информации в киберпространстве, включая хранилища данных и соединения, передающие данные между компонентами сети (JP 3-12). Физические компоненты сети включают аппаратные средства и инфраструктуру, такие как вычислительные устройства, устройства хранения данных, сетевые устройства, а также проводные и беспроводные каналы связи. Компоненты физического слоя сети требуют физических мер безопасности для защиты их от повреждений или несанкционированного доступа. В случае их уязвимости существует угроза получения доступа как к системам, так и к критическим данным.

1-25. Каждый физический компонент киберпространства принадлежит государственной или частной организации. Физический слой часто пересекает геополитические границы, и это одна из причин, по которой кибероперации требуют многоуровневого взаимодействия совместных и объединенных действий союзных ведомств. Ответственные за планирование в киберпространстве используют знание физического расположения как своих, нейтральных субъектов, так и противника: информационных технологий/ресурсов и инфраструктур, чтобы понять соответствующие правовые рамки для кибероперациий и оценить последствия этих операций. Объединённая доктрина относит части киберпространства, в зависимости от того, кто ими владеет или контролирует, к голубому, серому или красному киберпространству (см. JP 3-12). В данном издании эти зоны называются соответственно своим, нейтральным киберпространством или киберпространством противника.

1.2.1.2. Логический сетевой слой

1-26. Логический сетевой слой состоит из элементов сети, связанных друг с другом абстрагированным от физической сети способом, основанным на логическом программировании (коде), управляющим компонентами сети (т.е. связи не обязательно привязаны к конкретной физической линии связи или узлу, а к их способности к логическому обращению и обмену или обработке данных) (JP 3-12). Узлы физического уровня могут логически связываться друг с другом, образуя в киберпространстве сущности, не привязанные к конкретному узлу, пути или человеку. В качестве примера можно привести веб-сайты, размещённые на серверах в нескольких физических местах, доступ к содержимому которых осуществляется через единый унифицированный указатель ресурсов или веб-адрес. Сюда же можно отнести логическое программирование поиска наилучшего коммуникационного маршрута, а не кратчайшего физического пути, для предоставления запрашиваемой информации.

1.2.1.3. Слой кибер-персоны

1-27. Персональный сетевой слой – это представление киберпространства, созданное путём абстрагирования данных логического сетевого уровня с использованием правил, применяемых на логическом сетевом уровне, для разработки описаний цифровых представлений личности субъекта или организации в киберпространстве, называемых кибер-персоной (JP 3-12). Кибер-персоны не ограничиваются одним физическим или логическим местом и могут связываться с несколькими физическими и логическими слоями сети. При планировании и проведении кибероперациий штабы должны понимать, что один субъект или организация (пользователь) может иметь несколько кибер-персон, используя несколько идентификаторов в киберпространстве. Эти различные идентификаторы могут включать различные рабочие и личные электронные адреса, различные идентификаторы на различных веб-форумах, чатах и сайтах социальных сетей.

1-28. Например*:*

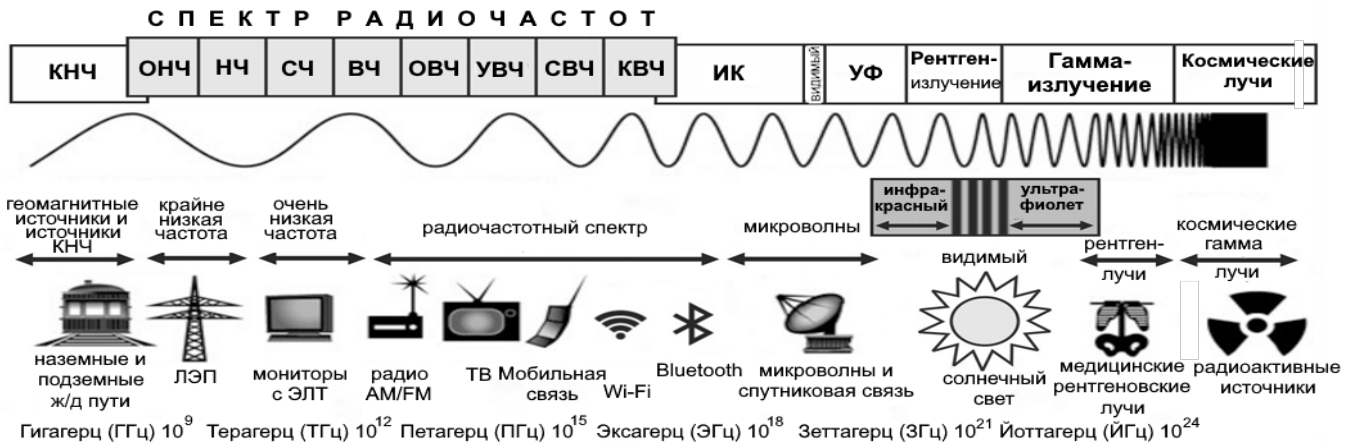
> *Аккаунт* человека на сайте социальной сети, состоящий из имени пользователя и цифровой информации, связанной с этим именем, может быть лишь одной из кибер-персон данного человека. И наоборот, несколько разных пользователей могут разделять одну кибер-персону или набор кибер-персон.

Ответственные за планирование должны понимать, что использование противником кибер-персон может затруднить возложение ответственности за действия в киберпространстве.

1.2.2. Электромагнитный спектр

1-29. Электромагнитный спектр – это пространство для манёвра, необходимое для обеспечения управления в оперативной обстановке и влияющее на все её части и военные операции. Исходя из конкретных физических характеристик, ЭМС организован по частотным диапазонам, включающим радиоволны, микроволны, инфракрасное излучение, видимый свет, ультрафиолетовое излучение, рентгеновское и гамма-излучение.

На рис. 1-3 показан диапазон стандартных частот в ЭМС и некоторые распространённые устройства, работающие в этих частотах.



Сокращения:

АМ	*амплитудная модуляция;*	*ОНЧ*	*очень низкая частота;*
ВЧ	*высокая частота;*	*СВЧ*	*сверхвысокая частота;*
ж/д пути	*железнодорожные пути;*	*СЧ*	*средняя частота;*
ИК	*инфракрасный;*	*УВЧ*	*ультравысокая частота;*
КНЧ	*крайне низкая частота;*	*УФ*	*Ультрафиолетовое излучение;*
ЛЭП	*линия электропередачи;*	*ЭЛТ*	*электронно-лучевая трубка;*
НЧ	*низкая частота;*	*FM*	*частотная модуляция.*

Рис. 1-3. – *Электромагнитный спектр.*

1.2.3. Тенденции и характеристики

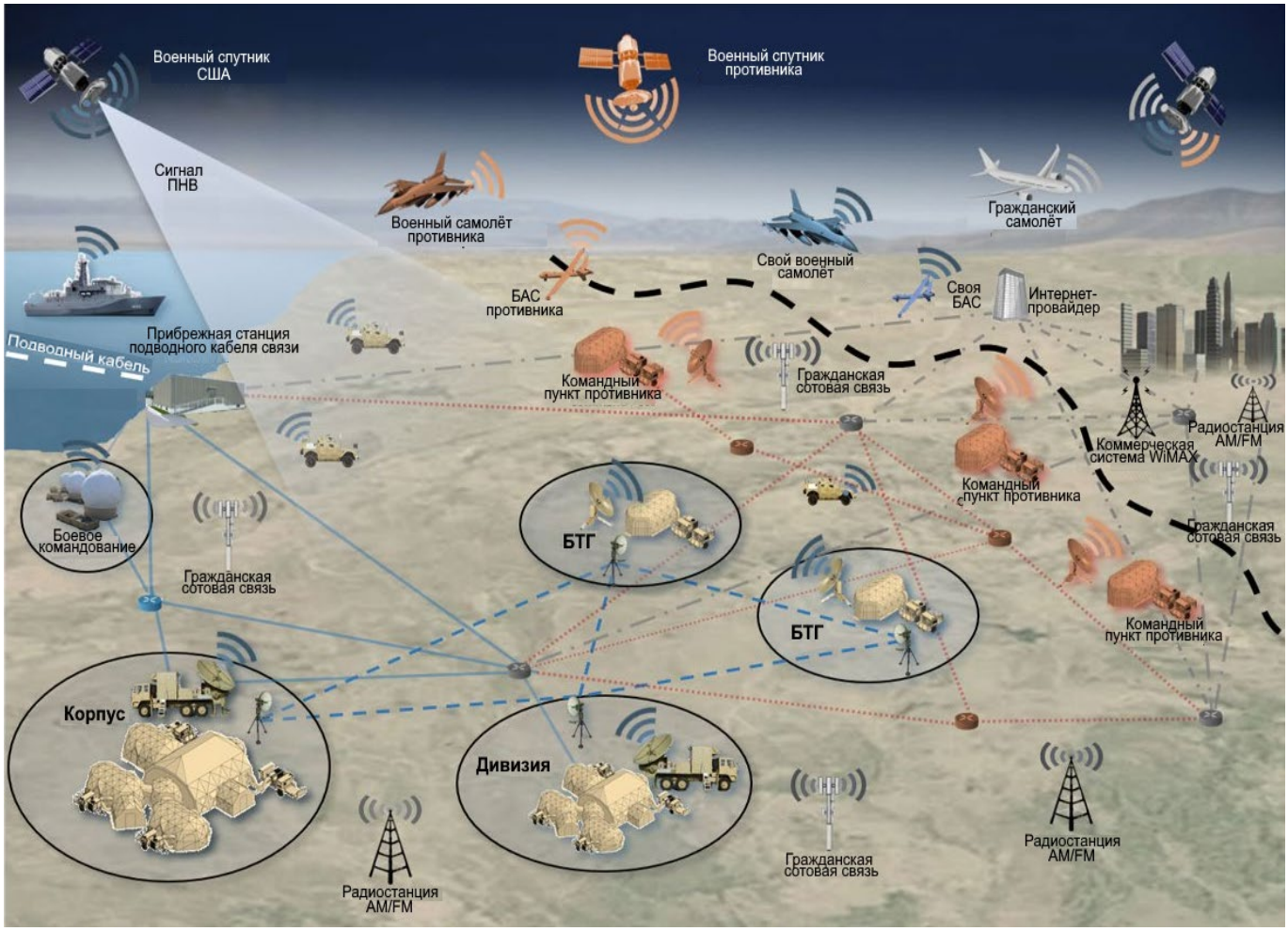
1-30. Стремительное распространение технологий киберпространства и ЭМС еще больше перегрузило и без того сложную оперативную обстановку. Помимо противостояния с угрозами в киберпространстве и ЭМС, ВС США сталкиваются с проблемами, исходящими от нейтральных субъектов. Такие нейтральные системы, как коммерческие самолёты и аэропорты, телекоммуникационная технология для предоставления универсальной беспроводной связи на больших расстояниях для широкого спектра устройств (*англ. Worldwide Interoperability for Microwave Access, WiMAX*) и коммерческая сотовая инфраструктура, способствуют постоянной перегруженности киберпространства и ЭМС. На рис. 1-4 показано киберпространство и ЭМС в перегруженной оперативной обстановке.

1-31. Несколько основных тенденций и характеристик влияют на способность командира использовать киберпространство и ЭМС. К таким тенденциям и характеристикам относятся:

- перегруженная обстановка;
- оспариваемая обстановка;
- угрозы;
- опасности;
- местность/территория.

1.2.3.1. Перегруженная обстановка

1-32. И киберпространство, и ЭМС приобретают статус всё более перегруженной обстановки, которой могут воспользоваться как свои войска, так и нейтральные субъекты и противник для передачи и обработки больших объёмов информации. С 2000 года использование сетевых информационных систем практически во всех аспектах деятельности Сухопутных войск возросло в десять раз. Нейтральные субъекты и противник также расширяют масштабы использования киберпространства и ЭМС в самых разных военных и невоенных целях.



Условные обозначения:

географическая граница	*нейтральная проводная сеть*
своя проводная сеть	*нейтральная беспроводная передача*
своя беспроводная сеть	*проводная связь противника*
своя беспроводная передача	*беспроводная передача противника*

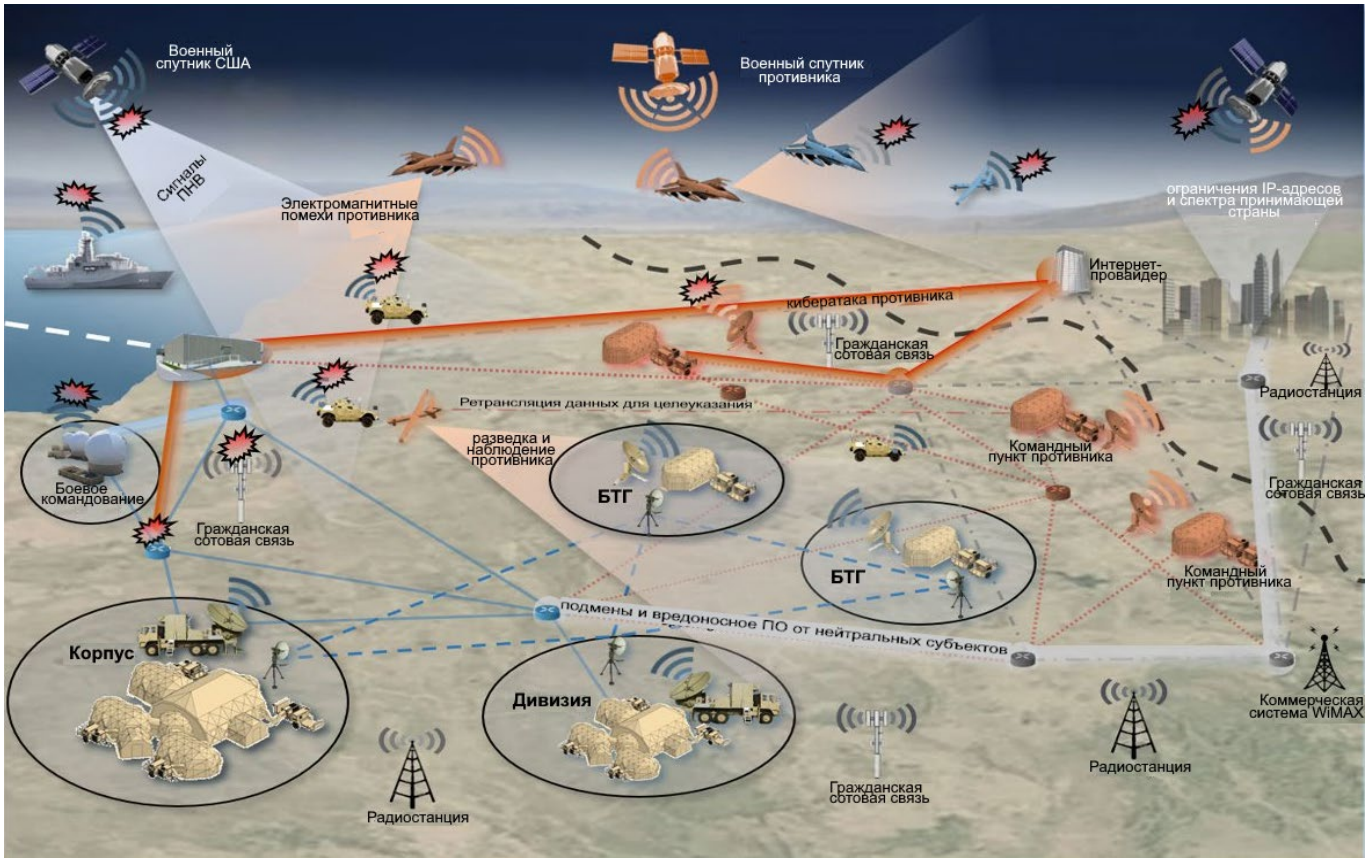
Сокращения:

АМ	*амплитудная модуляция;*	*ПНВ*	*позиционирование, навигация и время;*
БАС	*беспилотная авиационная система;*	*FM*	*частотная модуляция.*
БТГ	*бригадная тактическая группа;*		

Рис. 1-4. – *Перегруженность киберпространства и электромагнитного спектра.*

1.2.3.2. Оспариваемая обстановка

1-33. По мере того, как киберпространство и ЭМС становятся всё более перегруженными, расширяются и возможности государственных и негосударственных субъектов по оспариванию преимуществ США в обеих сферах. Государственные и негосударственные группировки используют широкий спектр передовых технологий, которые могут представлять собой относительно недорогие способы создания значительной угрозы США для небольшого или находящегося в невыгодном материальном положении противника. Применение недорогих средств воздействия на киберпространство может обеспечить преимущество против технологически зависимой страны или организации и асимметричное преимущество для тех, кто иначе не смог бы эффективно противостоять вооружённым силам США (рис. 1-5).



Условные обозначения:

географическая граница
своя проводная сеть
своя беспроводная сеть
своя беспроводная передача
нейтральная проводная сеть
нейтральная беспроводная передача
проводная связь противника
беспроводная передача противника
атакованная система

Сокращения:

БАС	*беспилотная авиационная система;*	*ПНВ*	*позиционирование, навигация и время;*
БТГ	*бригадная тактическая группа;*	*ПО*	*программное обеспечение*
		IP	*Интернет-протокол*

Рис. 1-5. – *Киберпространство и ЭМС в условиях противоборства.*

1.2.3.3. Угрозы

1-34. Для каждой операции угрозы являются неотъемлемой частью оперативной обстановки.

Угроза – это любая комбинация субъектов, организаций или сил, имеющих возможность и намерение нанести ущерб вооружённым силам США, их национальным интересам или родине (ADP 3-0). Угроза – это обобщающий термин, который включает любого субъекта, способного нанести ущерб США или их интересам.

Угрозы:

- противник;
- неприятель;
- равные угрозы;
- гибридные угрозы;
- внутренние угрозы.

1-35. ***Противник*** – это сторона, идентифицированная как враждебная, против которой разрешено применение силы (ADP 3-0). Противник также именуется воюющей стороной или участником боевых действий и рассматривается как таковой в соответствии с законами войны. Противник будет использовать различные передовые технологии для нападения на силы сухопутных войск в киберпространстве и ЭМС, чтобы нарушить или уничтожить возможность проведения операций или сбора информации, которая даст своим войскам стратегическое, оперативное или тактическое преимущество.

1-36. ***Неприятель*** – это сторона, признанная потенциально враждебной по отношению к своим войскам, против которой может быть предусмотрено применение силы (JP 3-0). Хотя неприятель не рассматривается как участник боевых действий, цель по-прежнему заключается в предотвращении и сдерживании конфликта путём удержания его деятельности в рамках желаемого состояния сотрудничества и соперничества.

1-37. ***Равная угроза*** – это противник или неприятель, способный эффективно противостоять вооружённым силам США во всём мире и имеющий относительное преимущество в определённом регионе (ADP 3-0), включая киберпространство и ЭМС. У равных угроз зачастую имеются возможности в киберпространстве и РЭБ, сопоставимые с американскими. Равные угрозы могут использовать эти возможности на всех этапах борьбы для сбора разведывательной информации, задержки развёртывания ВС США, снижения возможностей и срыва операций.

Равные угрозы обладают возможностями электромагнитной атаки (далее – ЭМА) (*англ. electromagnetic attack, EA*), такими как подавление телекоммуникаций и ЭМС, эквивалентными или превосходящими возможности американских сил. Равные угрозы способны осуществлять современные атаки в киберпространстве, включая отказ в обслуживании (полное блокирование программного обеспечения сайта), различные формы фишинга, перехвата и использования вредоносного программного обеспечения (далее – ПО).

1-38. ***Гибридная угроза*** – это разнообразное и динамичное сочетание регулярных сил, нерегулярных сил или преступных элементов, объединённых для достижения взаимовыгодных результатов (ADP 3-0). Командиры и штабы должны понимать, что разнообразие гибридных угроз усложняет проведение операций, поскольку враждебные действия исходят от нескольких субъектов, действующих на различных географических территориях. Гибридная угроза усложняет усилия США по выявлению, определению характеристик, принадлежности и реагированию на угрозы в киберпространстве и ЭМС.

1-39. Организованная преступность или другие негосударственные, нелегальные организации часто распространяют новейшее вредоносное ПО, которое можно купить или получить бесплатно, что позволяет даже субъектам со сравнительно простыми навыками приобретать современные возможности практически без затрат. Из-за низких барьеров для входа и потенциально высокой отдачи США могут ожидать, что всё большее число враждебных субъектов будет использовать средства воздействия на киберпространство для того, чтобы попытаться свести на нет американское преимущество в военном потенциале.

1-40. ***Внутренняя угроза*** – это лицо, обладающее служебным положением и доступом, намеренные действия которого путём шпионажа, оказания поддержки международному терроризму, несанкционированного раскрытия или разглашения информации о планах и намерениях вооружённых сил США приводят к потере или ухудшению ресурсов или возможностей или ставят под угрозу способность организации выполнять свою задачу (AR 381-12).

К внутренним угрозам могут относиться шпионы, находящиеся внутри американских сил или работающие с ними, а также личный состав, который может не осознавать своих действий либо в результате обмана, либо в результате манипуляций третьих лиц.

Внутренние угрозы представляют собой уникальную проблему, поскольку речь идёт о доверенных лицах, имеющих санкционированный доступ к возможностям сухопутных войск и конфиденциальной оперативной информации. К внутренним угрозам могут относиться шпионы, находящиеся внутри американских войск или работающие на них.

Примечание.

> Правоохранительные органы и контрразведка также действуют в киберпространстве, стремясь нейтрализовать преступную деятельность. Противодействие внутренним угрозам относится в основном к компетенции этих организаций и не входит в полномочия кибервойск. Однако информация, обнаруженная в ходе санкционированных кибероперациий, может помочь органам контрразведки и правоохранительным органам.

1.2.3.4. Опасности

1-41. ***Опасность*** – это состояние, которое может привести к травмам, заболеваниям или смерти личного состава, повреждению или потере оборудования или имущества, а также к ухудшению качества выполнения задачи (JP 3-33). Нарушение физической инфраструктуры киберпространства часто происходит из-за ошибок операторов, промышленных аварий и стихийных бедствий. Эти непредсказуемые события могут оказать не менее существенное влияние на ход операций, чем действия противника. Восстановление после аварий и опасных инцидентов может потребовать согласованности действий со стороны министерства обороны или временного использования резервных систем, с которыми операторы могут знакомы не в полном объёме.

1-42. Использование электромагнитной энергии может также влиять на боевые возможности вооруженных сил, техники, систем и платформ. Различные опасности, связанные с электромагнитной энергией, включают электромагнитное воздействие на окружающую среду, проблемы электромагнитной совместимости, электромагнитные помехи, электромагнитный импульс и электромагнитное излучение.

1-43. Опасности электромагнитного излучения включают:

- опасности для личного состава;
- опасности для боеприпасов;
- опасности для топлива;
- воздействие природных явлений, таких как космическая погода, молнии и статические заряды.

1.2.4. Конфликт и соперничество

1-44. Сухопутные войска сталкиваются с постоянным противоборством и конфликтами в киберпространстве и ЭМС, вызванными угрозами, направленными на ослабление их возможностей. Командиры должны искать и использовать возможности для достижения успеха в киберпространстве и ЭМС везде и всегда, где это разрешено.

1.2.4.1. Оспариваемое пространство

1-45. Кибероперации, РЭБ и управление спектром осуществляются в рамках всего диапазона оспариваемого пространства. Под оспариваемым пространством понимается состояние длительной борьбы, осуществляемой посредством сочетания сотрудничества, соперничества, как вне вооружённого конфликта, так и в его рамках. Превосходство в киберпространстве и ЭМС позволяет США проводить операции для достижения целей и выполнения задач, поставленных перед ними президентом и министром обороны. Хотя США могут проводить кибероперации и осуществлять воздействия РЭБ в ходе соперничества вне вооружённого конфликта, они являются важнейшими средствами обеспечения боевых возможностей при проведении крупномасштабных боевых операций в ходе вооружённого конфликта. Соперничество за рамками вооружённого конфликта включает ситуации, в которых объединённые силы предпринимают действия за рамками вооружённого конфликта против стратегического субъекта, преследуя политические цели.

1-46. Операции по управлению спектром выполняют важнейшую функцию в структуре СЕМА. Операции по управлению спектром протекают на всём протяжении противоборства и обеспечивают надлежащее взаимодействие в ЭМС на всем протяжении военных операций.

1.2.4.2. Многосферное расширенное поле боя

1-47. Противник стремится использовать возможности для создания воздействия в различных сферах, чтобы противостоять интересам США и препятствовать операциям американских сил. Угрожающие субъекты будут осуществлять деятельность в информационной среде, космосе и киберпространстве с целью повлиять на американских руководителей и сорвать развёртывание ВС США. Наземные угрозы будут пытаться воспрепятствовать свободе действий объединённых сил в воздушной, наземной, морской, космической и киберпространственной сферах. Они будут нарушать работу в ЭМС, создавать замешательство и оспаривать легитимность действий США. Понимание того, как угрозы могут создавать многочисленные проблемы для сухопутных войск во всех сферах, помогает командирам сухопутных войск выявлять (или создавать), использовать и применять свои возможности. Обеспечение безопасности операций (*англ. operations security*, *OPSEC*) имеет решающее значение для защиты своих важнейших информационных технологических инфраструктур, систем командования и управления, и целеуказания.

Безопасность операций – это возможность идентификации и контроля критической информации, показателей действий своих войск, связанных с военными операциями, и включает контрмеры для уменьшения риска использования противником уязвимостей (JP 3-13.3).

1.2.4.3. Позиции относительного преимущества в киберпространстве и ЭМС

1-48. Сухопутные войска проводят кибероперации и РЭБ для достижения относительного преимущества в киберпространстве и ЭМС, для установления информационного превосходства.

Позиция относительного преимущества *(англ. position of relative advantage)* – это расположение на местности или создание благоприятных условий в районе боевых действий (операций), которые предоставляют командиру временную свободу действий для усиления боевых возможностей или влияния на возможности противника с целью заставить его принять риск и перейти в невыгодную позицию (ADP 3-0).

1.3. Составляющие боевого обеспечения

1-49. В разделе рассматривается, каким образом кибероперации и РЭБ осуществляют боевое обеспечение. В нём представлены типы кибероперации, задачи и действия в области РЭБ, которые способствуют выполнению более обширных задач, связанных с каждой составляющей боевого обеспечения.

1.3.1. Командование и управление

1-50. Командиры в значительной степени полагаются на киберпространство и ЭМС в целях осуществления командования и управления. На уровне корпуса и ниже сеть в системе управления – это информационная сеть министерства обороны – сухопутные войска (далее – информационная сеть МО-СВ) (*англ. Department of Defense information network-Army, DODIN-A*).

Информационная сеть МО-СВ – это управляемый сухопутными войсками анклав информационной сети министерства обороны, который охватывает все информационные возможности сухопутных войск по сбору, обработке, хранению, отображению, распространению и защите информации по всему миру (ATP 6-02.71).

Войска связи обеспечивают создание, управление, безопасность и защиту информационной сети МО-СВ путём проведения операций в информационной сети МО и соблюдения требований кибербезопасности для предотвращения вторжений в информационную сеть МО-СВ.

Более подробную информацию об операциях в информационной сети МО см. в Боевом уставе FM 6-02 и Наставлении ATP 6-02.71. Сети и системы в составе информационной сети МО-СВ позволяют командирам управлять подразделениями, одинаково оценивать оперативную обстановку и взаимодействовать с подчинёнными практически в режиме реального времени.

1-51. РЭБ поддерживает командование и управление посредством электромагнитной защиты (далее – ЭМЗ) (*англ. electromagnetic protection, EP*) для устранения или ослабления негативного воздействия своих, нейтральных, враждебных или природных электромагнитных помех на системы командования и управления. Задачи распределения частот и устранения конфликтов в рамках операций по управлению спектром обеспечивают ЭМЗ (см. ATP 6-02.70). К таким задачам электромагнитной защиты относятся контроль за излучением, снижение воздействия электромагнитной среды, электромагнитная совместимость, электромагнитная маскировка, упреждающие контрмеры и улучшение приёмов и возможностей РЭБ. Эти задачи требуют интеграции с операциями по управлению спектром для управления частотами и устранения помех. В главе 2 данного издания и в Наставлении ATP 3-12.3 подробно рассмотрен вопрос об ЭМЗ.

1.3.2. Движение и манёвр

1-52. Кибероперации и РЭБ повышают эффективность движения и манёвра командиров своих войск, нарушая командование и управление сил противника, снижая уровень ситуативной осведомлённости противника и повышая уровень своей осведомлённости, а также негативно влияя на способность противника принимать обоснованные решения. Благодаря дальности и широте охвата киберпространства Кибервойска зачастую способны поддерживать манёвр своих войск на близких расстояниях, одновременно поддерживая операции в глубине территории. Информацию о боевых действиях (операциях) на переднем крае и в глубине обороны противника см. в Боевом уставе FM 3-0. Средства и методы боевых действий (операций) на переднем крае и в глубине обороны противника приведены в Наставлении ATP 3-94.2.

1-53. Операции в информационной сети МО обеспечивают движение и манёвр путём создания защищённых тактических сетей, обеспечивающих связь со своими войсками, ведущими боевые действия по фронту на переднем крае и в глубине обороны противника, а также связь с вышестоящими штабами в тыловых районах. Информационная сеть МО-СВ выступает в качестве основного средства связи во время движения и манёвра для частей и подразделений.

Спутниковая связь, радиостанции боевых сетей и проводные сети являются элементами информационной сети МО-СВ, используемыми для согласования боевых действий (операций), взаимодействия между подразделениями, понимания обстановки и взаимодействия между огневыми средствами.

Сеть позволяет практически в режиме реального времени обновлять общую оперативную картину. Верхний и нижний уровни информационной сети МО-СВ связывают штабы с подчинёнными, соседними, вышестоящими штабами и с участниками совместных действий.

1-54. Наступательные кибероперации (далее – НКбО) (*англ. offensive cyberspace operations, OCO*) во взаимодействии с другими видами огневых средств также обеспечивают движение и манёвр, создавая предпосылки для рассеивания и вытеснения сил противника. Согласование НКбО с различными средствами поражения создаёт условия, которые позволяют осуществить манёвр с целью завоевания или использования позиций относительного преимущества. Подробно НКбО рассмотрены в главе 2.

1-55. Средства РЭБ обеспечивают движение и манёвр, проводя операции по ослаблению, нейтрализации или уничтожению боевых средств противника в ЭМС. Оборонительная ЭМА защищает свои войска от атак противника во время движения и манёвра, лишая противника возможности использовать ЭМС. Использование своих средств ЭМА для борьбы с радиоуправляемыми устройствами, такими как самодельные взрывные устройства, беспилотники, роботы или радиоуправляемые боеприпасы, является примером оборонительной ЭМА. При оборонительных действиях силы и средства ЭМА РЭБ проводят операции по ослаблению, нейтрализации или уничтожению боевых средств противника в ЭМС. Средства РЭБ осуществляют оборонительную ЭМА, применяя такие возможности, как противодействие радиоуправляемым самодельным взрывным устройствам и устройствам, используемым для обеспечения живучести самолётов. Наступательная ЭМА обеспечивает движение и манёвр путём проецирования силы в рамках времени и темпа замысла манёвра. Электромагнитное подавление, электромагнитное воздействие и электромагнитное зондирование являются примерами наступательных ЭМА. Электромагнитная поддержка (далее – ЭМП) (*англ. electromagnetic support, ES*) обеспечивает движение и манёвр, предоставляя информацию о боевой обстановке для понимания оперативной обстановки.

1-56. Разнообразные задачи ЭМЗ также способствуют движению и манёвру. Специалисты по управлению спектром и специалисты по РЭБ проводят разграничение частот для предотвращения или ослабления частотных помех со стороны своих войск. Согласование частот включает превентивные и смягчающие меры, направленные на то, чтобы радиоэлектронные средства, используемые своими войсками во время выполнения задач по движению и манёвру, не создавали частотных помех радиоэлектронным средствам, используемым другими своими войсками. Электромагнитная маскировка способствует движению и манёвру, скрывая электромагнитные сигналы, излучаемые системами своих войск, использующими различные диапазоны во время боевых действий (операций). Контроль за излучениями во время движения и манёвра снижает уровень электромагнитных помех, создаваемых радиоэлектронными системами связи и навигации своих войск во время движения и манёвра. Войска РЭБ также применяют средства обнаружения перед началом выдвижения в качестве превентивных мер противодействия.

Электромагнитная безопасность обеспечивает движение и манёвр, лишая противника возможности расшифровать информацию, полученную от перехваченной электромагнитной энергии. Более подробно эти задачи рассматриваются в главе 2 данного издания и в Наставлении ATP 3-12.3.

1.3.3. Разведка

1-57. Кибероперации, РЭБ и разведка взаимно выявляют особенности киберпространства и ЭМС в оперативной обстановке, чтобы в процессе принятия военных решений дать рекомендации по действиям своих подразделений. Кибервойска и войска РЭБ обеспечивают сбор информации, которая затем может быть использована специалистами разведки. И наоборот, разведывательные операции предоставляют информацию, которая улучшает понимание оперативной обстановки, обеспечивает целеуказания и поддерживает оборону в киберпространстве и ЭМС. Очень важно, чтобы информация, полученная в ходе кибероперациий и РЭБ, была стандартизирована и передавалась в разведывательное ведомство.

1-58. Разведка обеспечивает кибероперации через организацию процесса разведки, разведывательную подготовку района боевых действий (*англ. intelligence preparation of the battlefield,* IPB) и сбор информации. Разведка на всех уровнях обеспечивает поддержку кибероперациий и планирование РЭБ, а также помогает оценить эффективность и результативность с помощью оценки ущерба от боевых действий.

Ответственные за планирование кибероперациий прибегают к анализу, подготовке докладов и разведывательных данных для понимания оперативной обстановки, разработки планов и целей, а также обеспечения оперативных процессов.

В контексте киберпространства и ЭМС оперативная обстановка включает отображение топологии сети, которая графически показывает, как информация поступает и распределяется внутри оперативной зоны и как данные передаются по сети в район ответственности и из него.

1.3.3.1. Разведывательная подготовка района боевых действий

1-59. В ходе разведывательной подготовки района боевых действий штабы изучают, как противник или неприятель использует киберпространство и ЭМС для достижения своих целей. При определении и анализе района ответственности специалисты по разведке и CEMA в штабе также учитывают государственные и негосударственные субъекты, обладающие возможностями, доступом и намерениями повлиять на свои боевые действия (операции).

1-60. Аналитики разведки при поддержке других структурных подразделений штаба оценивают использование противником киберпространства и ЭМС. Это включает оценку следующих аспектов:

а. Использование киберпространства и возможностей ЭМС неприятелем или противником.

б. Опора на возможности сетевых технологий.

в. Совершенствование потенциала кибератак.

г. Возможности неприятеля по киберзащите.

д. Возможности противника в области РЭБ.

е. Сетевые уязвимости (как противника, так и свои).

ж. Способность согласовывать кибероперации с другими операциями.

з. Использование противником социальных сетей для социальной инженерии.

1-61. При оценке действий противника разведка учитывает, как противник будет использовать киберпространство и ЭМС в своих операциях. При планировании боевых действий командир и штаб должны учитывать направления действий угроз в киберпространстве и ЭМС. См. документ АТР 2-01.3 для получения дополнительной информации о разведывательной подготовке района боевых действий.

1-62. Погода (земная и космическая) также влияет на кибероперации и операции в ЭМС. При оценке метеорологического воздействия штаб рассматривает ключевую обстановку в киберпространстве и ЭМС во взаимосвязи с другими факторами в районе ответственности и зоне проведения операций.

1.3.3.2. Электромагнитная поддержка, радио и радиотехническая разведка

1-63. Электромагнитная поддержка и радио и радиотехническая разведка (далее – РРТР, *англ. signals intelligence*, *SIGINT*) схожи по своим функциям, но для РРТР требуются отдельные разрешения. Специалисты РЭБ осуществляют ЭМП для получения информации в интересах плана действий командира. Личный состав РЭБ имеет полномочия на ведение радио и радиотехнической разведки без ограничений и каких-либо требований.

1-64. Личный состав РЭБ и РРТР выявляют источники излучения в ЭМС и могут передавать друг другу сообщения с данными о цели для цлеуказания, но при этом выполняют разные задачи. Личный состав РЭБ определяет характеристики и идентифицирует источники излучения, анализируя внешние сигналы для немедленного распознавания и предупреждения об угрозе, защиты сил и средств и целеуказания.

Для обеспечения проведения операций ЭМП предоставляет информацию о боевой обстановке, имеющую ограниченную временную ценность. В зависимости от ситуации и полномочий информация электромагнитного обеспечения может быть передана разведывательным подразделениям или соответствующим штабам для дальнейшего анализа радио и радиотехнической разведкой. Личный состав подразделений радио и радиотехнической разведки анализирует параметры внешних сигналов для получения и распространения разведывательной информации, для чего требуются полномочия РРТР.

1.3.4. Огневое обеспечение

1-65. Задачи НКбО и ЭМА являются частью огневого обеспечения. Кибервойска применяют кибератаки для блокирования, ухудшения, подрыва, уничтожения или иного воздействия на киберпространство или информационно-зависимые средства противника. Личный состав РЭБ применяет ЭМА для ослабления и нейтрализации возможностей противника по использованию ЭМС. Воздействия в киберпространстве и операциях РЭБ выходят за пределы киберпространства и ЭМС и могут привести к эффектам второго и третьего порядка, которые могут повлиять на другие физические сферы.

1-66. Поражающие факторы Сухопутных войск в киберпространстве и РЭБ против средств и систем вооружения противника лишают его возможности осуществлять связь, слежение или поражение. Силы и средства РЭБ также обеспечивают огневую поддержку, позволяя вести огонь на поражение за счёт использования электромагнитного обеспечения для поиска, идентификации и определения местоположения или локализации источников излучаемой электромагнитной энергии, используемых противником для целеуказаний. Оборонительные ЭМА могут обеспечить огневую поддержку путём развёртывания ложных целей или помех для маскировки своих сетей управления огнём.

1.3.5. Боевая устойчивость

1-67. Кибероперации способствуют поддержанию боевой устойчивости посредством операций в информационной сети МО и оборонительных киберопераций (далее – ОКбО). К подразделениям, функциям, системам и местам базирования систем обеспечения, которые в значительной степени зависят от операций в информационной сети МО, относятся:

- глобальные цепи поставок;
- логистические сети и информационные системы сухопутных войск;
- мобилизационные платформы и платформы проецирования силы;
- аэропорты выгрузки;
- морские порты выгрузки;

1-68. Операции в информационной сети МО устанавливают необходимые коммуникации для выполнения функций устойчивого обеспечения. При нарушении противником мер по обеспечению кибербезопасности сетей и систем от угроз кибератак Кибервойска обеспечивают защиту систем боевой устойчивости. РЭБ обеспечивает поддержание боевой устойчивости через ЭМЗ и ЭМП, обеспечивая свободу действий для операций в информационной сети МО через ЭМС. Управление, взаимодействие и устранение противоречий между частотами в ЭМС являются функциями операций по управлению спектром. Более подробная информация об оборонительных кибероперациях – внутригосударственных мероприятиях по обороне (далее – ОКбО-ВМО) (*англ. defensive cyberspace operations-internal defensive measures*, *DCO-IDM*) приведена в главе 2.

1.3.6. Защита

1-69. Задачи ОКбО и ЭМЗ в дополнение к задачам по обеспечению кибербезопасности в рамках операций в информационной сети МО являются частью функции защиты. Операции в информационной сети МО, ОКбО-ВМО, ЭМЗ и оборонительные ЭМА поддерживают защиту, обеспечивая безопасность и оборону информационной сети МО-СВ. Кибервойска осуществляют ОКбО-ВМО для обнаружения, определения характеристик, противодействия и ослабления текущих или надвигающихся угроз для информационной сети МО-СВ. Операции в информационной сети МО и ОКбО-ВМО также позволяют решать другие задачи защиты, обеспечивая защищённую связь для:

- безопасности территории;
- полицейских операций;
- восстановления личного состава;
- противовоздушной и противоракетной обороны;
- операций по содержанию под стражей.

1-70. Электромагнитная защита включает действия по защите личного состава, объектов и оборудования от своего, нейтрального или воздействия противника в ЭМС. Электромагнитная защита включает меры по защите своего личного состава и техники в условиях противоборства и перегруженности электромагнитной оперативной обстановки (*англ. electromagnetic operational environment, EMOE*).

Оперативная электромагнитная обстановка – это совокупность фактического и потенциального излучения электромагнитной энергии, условий, обстоятельств и воздействий, которые влияют на решения командира и применение сил и средств. Специалист по управлению спектром СЕМА работает в тесном контакте со специалистом по управлению спектром из подразделения S-6 или G-6 для устранения конфликтов между частотами, используемыми своими подразделениями.

Свои войска могут использовать упреждающие меры, такие как контроль излучений, для уменьшения своей электромагнитной заметности, тем самым повышая уровень безопасности. Оборонительная ЭМА защищает свои войска, отказывая противнику в использовании ЭМС, нарушая его способность обнаруживать цель, наводить или вести огонь из вооружения. Более подробную информацию о контроле излучений см. в главах 2 и 4 настоящего издания.

ГЛАВА 2. ОСНОВЫ КИБЕРОПЕРАЦИЙ И РЭБ

В данной главе рассмотрены типы кибероперации и РЭБ и связанные с ними задачи. В ней подробно представлены общие поражающие факторы, которых командиры могут добиться с помощью кибероперации и РЭБ, а также рассмотрена взаимосвязь между кибероперациями, РЭБ и другими операциями сухопутных войск. В данной главе также обсуждаются вопросы подготовки военнослужащих к выполнению задач по ведению кибероперации и РЭБ.

2.1. Операции в киберпространстве

2-1. Благоприятным условием для кибероперации и РЭБ является согласование своих действий с другими возможностями сухопутных войск с применением сил и средств вооружённой борьбы, которые путём совместных действий различных родов войск позволят достичь целей для нанесения поражения противнику. Кибероперации и РЭБ могут обеспечить командирам относительное преимущество в многосферной борьбе. Воздействия, распространяющиеся из киберпространства в физическую сферу, могут быть сгенерированы и использованы против неприятеля.

Средство воздействия на киберпространство (кибервозможности) – это устройство или компьютерная программа, включая любую комбинацию программного, микропрограммного или аппаратного обеспечения, предназначенная для создания поражающих факторов в киберпространстве или через него (JP 3-12).

Примечание.

> Возможности правоохранительных органов и контрразведки позволяют им создавать необходимое воздействие в киберпространстве в ходе действий по нарушению, уничтожению, блокированию или ослаблению деятельности противника или неприятеля в киберпространстве.

2-2. ***Превосходство в электромагнитном спектре*** – это степень контроля в ЭМС, позволяющая проводить операции в определённое время и в определённом месте без противодействия, при этом оказывая влияние на способность противника делать то же самое (JP 3-85).

РЭБ создаёт воздействия в ЭМС и позволяет командирам добиваться превосходства в ЭМС при проведении операций сухопутными войсками. Возможности РЭБ состоят из систем и вооружений, используемых для выполнения задач радиоэлектронной борьбы по созданию летальных или нелетальных поражающих воздействий в ЭМС и через него.

Применение Россией кибероперациий и РЭБ в ходе российско-украинской войны

В 2013 году пророссийское руководство Украины сделало выбор в пользу более тесных связей с пророссийским Евразийским экономическим союзом вместо подписания договора с Европейским союзом. В ответ на это по всей Украине вспыхнули массовые протесты. Постоянно конкурируя с США и Китаем за увеличение торгового оборота, Россия всегда стремилась получить доступ к расширению торговли в регионе. По мере того, как Украина погружалась в хаос, Владимир Путин и Российская Федерация признали, что сложились оптимальные условия для захвата тёплых черноморских портов Украины в Крыму. Захват этих портов не только обеспечивал выгодный доступ к средиземноморской торговле и коммерции, но и бросал вызов военной мощи США на Чёрном море. Действия России включали также стратегические усилия, направленные на прекращение расширения НАТО и сокращение буферной зоны между Западом и российской экономической экспансией.

Использование Украиной российских средств управления, контроля, связи, компьютерной техники, наблюдения и разведки (C4ISR) сделало их уязвимыми для атак, проводимых Россией. Сформулировав планы кампании на основе тематических мер по воспрещению и дезинформации, российские военные приступили к разработке гибридной кампании, представляющей собой многогранное сочетание регулярных и нерегулярных действий. Российские военные определили, что ключевыми объектами Украины являются их составляющие C4ISR. Россия проникла в украинские телекоммуникационные системы, по мере того как использование Украиной таких средств связи, вероятно, способствовало целенаправленным действиям России. Чтобы внести стратегический, оперативный и тактический хаос в процесс принятия решений на Украине, Россия провела целенаправленные операции в киберпространстве и РЭБ (отказ в обслуживании, манипулирование социальными сетями и т.д.) на критически важных узлах C4ISR. На тактическом уровне применение ВС России направленных действий в киберпространстве и РЭБ обладало высокой поражающей способностью.

Украинские вооружённые силы перебросили несколько механизированных бригад к российской границе с целью пресечения незаконных поставок техники, направляемой сепаратистам на востоке Украины. Утром 11 июля 2014 г. украинские военнослужащие заметили в небе беспилотник. Вскоре после того, как он улетел, одна из украинских бригад подверглась массированному обстрелу из реактивной системы залпового огня 9А52-4 «Торнадо».

В течение четырёх минут на позиции подразделения обрушились ракеты со смесью фугасных, кассетных и термобарических боеприпасов. Вслед за первым ракетным залпом русские применили артиллерийские снаряды с фугасным ВВ, вследствие чего кумулятивное действие снарядов оказалось весьма разрушительным. После анализа результатов операции украинская сторона понесла потери в 37 человек убитыми и 100 ранеными. Один украинский батальон был практически уничтожен, другие из-за больших потерь в личном составе и технике оказались небоеспособными. Позднее было установлено, что возможности Российской Армии по сбору разведывательной информации и геолокации, а также способность обнаруживать украинские узлы связи сыграли значительную роль в том, что русские смогли найти, зафиксировать и уничтожить целую украинскую бригаду. Целенаправленное применение русскими РЭБ и кибератак привело к хаосу в гражданском и военном руководстве Украины и растерянности, что является эффектом второго порядка. Западные лидеры оказались ограничены в своих возможностях реагировать на действия России в регионе. Использование Россией возможностей киберпространства и РЭБ против командования Украины позволило ей захватить Крым и достичь своей стратегической цели – получить торговые и военные порты на Черном море.

2.1.1. Объединённые силы и сухопутные войска

2-3. Объединённые силы и сухопутные войска разделяют кибероперации на три категории в зависимости от той части киберпространства, в которой проводятся операции, и типа кибервойск, осуществляющих эти действия. Каждый из типов кибероперацій имеет различные ограничения по полномочиям, уровням утверждения и взаимодействия. Классификация кибероперацій в сухопутных войсках представлена на рис. 2-1 ниже.

К трём типам кибероперацій относятся.

1. Операции в информационной сети МО (см. АТР 6-02.71).
2. Оборонительные кибероперации (ОКбО).
3. Наступательные кибероперации (НКбО).

2-4. Сухопутные войска проводят операции в информационной сети МО во внутренних сетях и системах сухопутных войск и министерства обороны, задействуя преимущественно войска связи. Сухопутные войска при помощи кибервойск проводят ОКбО, которые включают ещё две подкатегории – оборонительные кибероперации – внутригосударственные мероприятия по обороне и оборонительные кибероперации – меры реагирования (далее – ОКбО-МР) (*англ. defensive cyberspace operations-response actions, DCO-RA*).

Кибервойска проводят ОКбО-ВМО в рамках зоны ответственности информационной сети МО или в других своих сетях, если это разрешено, с целью защиты этих сетей от готовящихся или продолжающихся атак. Иногда кибервойска могут также предпринимать действия против угрожающих субъектов в нейтральных сетях или сетях неприятеля в целях защиты информационной сети МО или своих сетей. Такого рода действия именуются ОКбО-МР и требуют дополнительных полномочий и мер по взаимодействию.

Наконец, кибервойска целенаправленно воздействуют на угрожающие возможности в нейтральных, неприятельских и контролируемых противником частях киберпространства, проводя наступательные операции. Кибервойска могут задействовать объединённые силы из состава сил кибероперций министерства обороны или кибервойска, находящиеся в распоряжении сухопутных войск. Более подробно см. главу 3 настоящего издания.

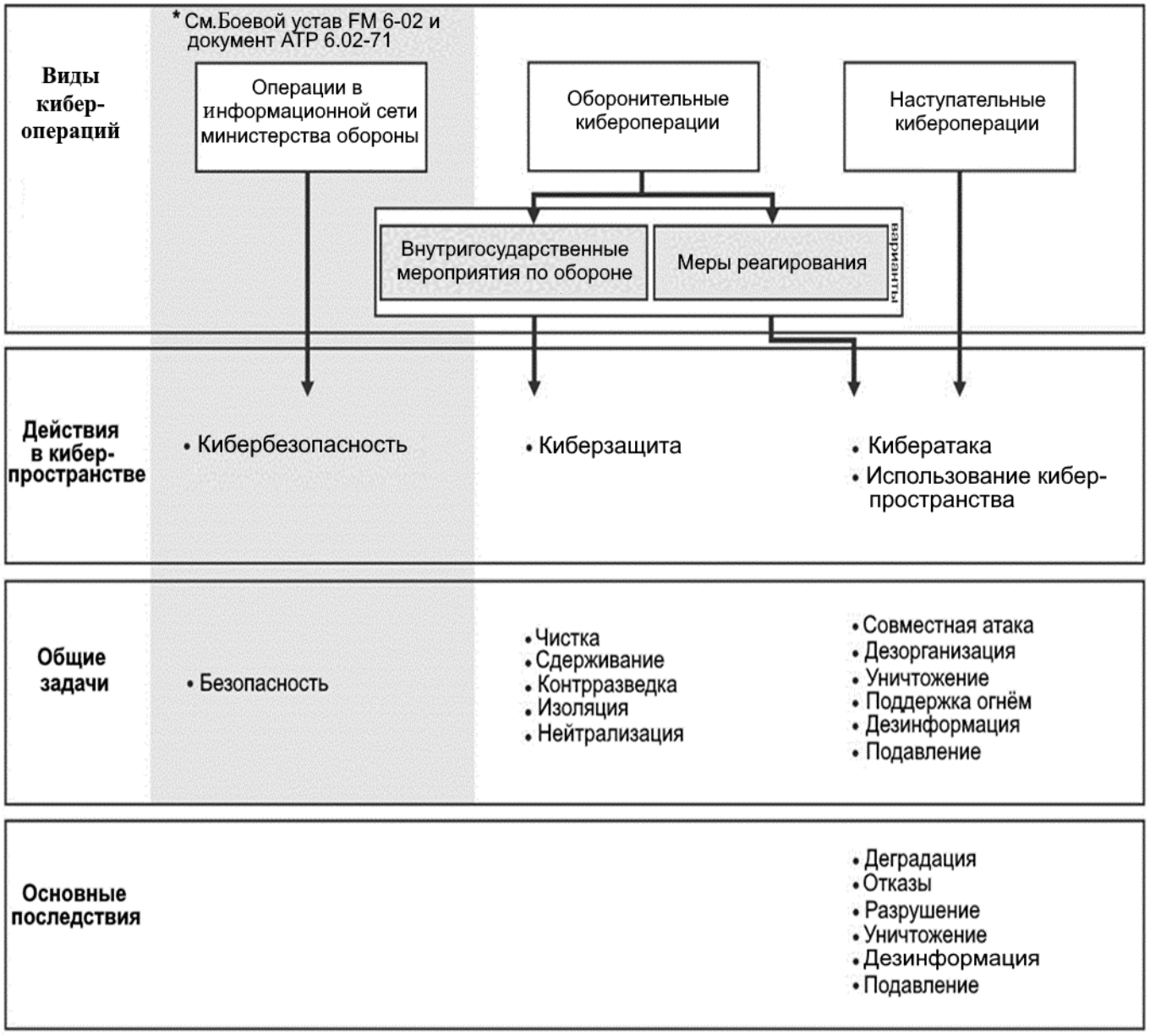


Рис. 2-1. – *Систематизация кибероперций.*

2.1.2. Операции в информационной сети министерства обороны

2-5. ***Информационная сеть министерства обороны (МО)*** – это совокупность информационных возможностей и связанных с ними процессов сбора, обработки, хранения, распространения и управления информацией по запросам военнослужащих, политиков и обеспечивающего персонала, как взаимосвязанных, так и автономных. Сокращённо на английском языке: DODIN (JP 6-0). В неё входят собственные и арендованные коммуникационные и вычислительные системы и сервисы, программное обеспечение (включая приложения), данные, услуги по обеспечению безопасности, другие сопутствующие сервисы, а также системы национальной безопасности.

Операции в информационной сети МО – это операции по обеспечению безопасности, конфигурированию, эксплуатации, расширению, обслуживанию и поддержанию киберпространства министерства обороны для создания и сохранения конфиденциальности, доступности и целостности информационной сети МО. Сокращённо на английском языке: operations DODIN (JP 3-12).

Операции в информационной сети МО обеспечивают авторизованным пользователям на всех уровнях безопасную, надёжную сквозную доступность сетей и информационных систем.

Операции в информационной сети МО позволяют командирам эффективно общаться, взаимодействовать, обмениваться и управлять информацией, а также распространять её с использованием систем информационных технологий.

2-6. Войска связи прокладывают тактические сети, выполняют работы по техническому обслуживанию и поддержанию работоспособности, а также по оценке и тестированию систем безопасности. Войска связи, выполняющие операции в информационной сети МО, могут также проводить ОКбО-ВМО.

Поскольку задачи по обеспечению кибербезопасности и кибероборонe носят постоянный характер действующие приказы по операциям в информационной сети МО и ОКбО-ВМО охватывают большинство задач по обеспечению кибербезопасности и первоначальных задач по кибероборонe.

2-7. В сухопутных войсках для обеспечения безопасности информационной сети МО-СВ используется многоуровневый подход к защите. Многоуровневая защита предполагает использование различных средств физического, политического и технического контроля для защиты от угроз в сети.

Многоуровневая система объединяет людей, технологии и оперативные возможности для создания барьеров безопасности на нескольких уровнях информационной сети МО-СВ.

Различные типы барьеров безопасности включают:

- антивирусное программное обеспечение;
- межсетевые экраны;
- программное обеспечение для защиты от спама;
- обеспечение безопасности средств связи;
- шифрование данных;
- защита паролем;
- физические и технические барьеры;
- непрерывное обучение по вопросам безопасности;
- постоянный мониторинг сети.

2-8. Барьеры безопасности – это защитные меры от действий, которые могут снизить эффективность работы сети, а значит, и системы управления операциями. Кроме того, многоуровневая система включает защиту периметра, защиту корпусов, защиту хоста, физическую безопасность, безопасность личного состава, а также политику и стандарты кибербезопасности. Многоуровневая защита киберпространственной сферы осуществляется на физическом, логическом и административном уровнях управления.

2.1.3. Оборонительные кибероперации

2-9. ***Оборонительные кибероперации*** – это операции по сохранению способности использовать возможности «голубого киберпространства» и защите данных, сетей, устройств, работающих в киберпространстве, и других целевых систем путём отражения текущей или надвигающейся злонамеренной деятельности в киберпространстве (JP 3-12). Термин «голубое киберпространство» обозначает области киберпространства, находящиеся под защитой США, их союзников, а также другие области, приказ на защиту которых может получить министерство обороны США. ОКбО классифицируются по месту совершения действий:

- внутригосударственные мероприятия по обороне (ОКбО-ВМО);
- меры реагирования (ОКбО-МР).

2.1.3.1. Оборонительные кибероперации – внутригосударственные мероприятия по обороне

2-10. ***Оборонительные кибероперации – внутригосударственные мероприятия по обороне*** – это операции, в которых санкционированные оборонительные действия происходят в пределах обороняемой части киберпространства (JP 3-12). Они проводится в пределах киберпространства своих вооружённых сил. ОКбО-ВМО включают действия по обнаружению и устранению киберугроз в сетях своих войск.

Кибервойска применяют оборонительные мероприятия для нейтрализации и устранения угроз, что позволяет восстановить утраченную, скомпрометированную по безопасности или находящуюся под другой угрозой часть информационной сети МО. Кибервойска, осуществляющие ОКбО-ВМО, в первую очередь выполняют задачи по киберзащите, но могут также выполнять некоторые другие задачи, аналогичные задачам по обеспечению кибербезопасности.

2-11. ***Киберзащита*** включает действия, предпринимаемые в защищённом киберпространстве для отражения конкретных угроз, которые нарушили или угрожают нарушить меры кибербезопасности, и действия по обнаружению, определению характеристик, противодействию и ослаблению угроз, включая вредоносное ПО или несанкционированные действия пользователей, а также по восстановлению системы до безопасной конфигурации (JP 3-12). Кибервойска действуют по сообщениям служб кибербезопасности или разведки об активности противника в сетях своих войск. Задачи по киберзащите в ходе ОКбО-ВМО включают поиск угроз в сетях своих войск, применение современных мер противодействия и реагирование для устранения этих угроз и ослабления их последствий.

2.1.3.2. Оборонительные кибероперации – меры реагирования

2-12. ***Оборонительные кибероперации – меры реагирования*** – это операции, являющиеся частью комплекса ОКбО, которые осуществляются вне защищаемой сети или части киберпространства без разрешения собственника затронутой системы (JP 3-12). Такие операции осуществляются за пределами границ информационной сети МО. Некоторые такие операции могут включать действия, которые выходят на уровень применения силы и могут включать физическое повреждение или уничтожение систем противника. ОКбО-МР заключаются в проведении кибератак и использовании киберпространства для задач, присущих НКбО. Однако ОКбО-МР используют эти действия только в оборонительных целях, в отличие от НКбО, которые применяются для демонстрации силы в киберпространстве и через него.

2-13. Принятие решения о проведении ОКбО-МР в значительной степени зависит от более широких стратегических и оперативных условий, таких как наличие или неизбежность начала боевых действий, степень уверенности в определении источника угрозы, ущерба, который нанёс или может нанести противник, а также от соображений национальной политики. ОКбО-МР проводятся национальной оперативной группой (группами) и требуют правильно согласованного военного порядка, взаимодействия с другими участниками совместных действий, а также тщательной проработки масштабов, правил ведения боевых действий и оперативных задач.

2.1.4. Наступательные кибероперации

2-14. ***Наступательные кибероперации*** – это действия, направленные на демонстрацию силы в киберпространстве и через него (JP 3-12). Кибервойска проводят НКбО вне сетей министерства обороны для достижения позиций относительного преимущества путём использования киберпространства и проведения кибератак в поддержку задач командования. Для достижения оптимального эффекта командиры должны интегрировать НКбО в схему манёвра объединённых вооружённых сил на протяжении всего оперативного процесса.

2-15. Сухопутные войска выделяют в состав объединённых сил подразделения кибервойск, подготовленные для выполнения НКбО по всему фронту военных операций. Сухопутные войска, осуществляющие НКбО, действуют под руководством командующего объединёнными силами. Информацию по взаимодействию с другими участниками совместных действий см. в приложении C. Объединённые силы могут предоставлять поддержку НКбО общевойсковым командирам на уровне корпусов и ниже в ответ на запросы в рамках совместного процесса целеуказаний. Более подробную информацию об объединённых силах в киберпространстве см. в приложении D. Нанесение поражающего воздействия на цели в киберпространстве может потребовать длительного планирования, времени на принятие решения и устранения конфликтных ситуаций с организациями, не имеющими отношения к министерству обороны. В главе 4 подробно рассматриваются вопросы целеуказания.

2.1.5. Действия в киберпространстве

2-16. Выполнение этих кибероперациий подразумевает выполнение одной или нескольких конкретных задач, которые в совместной доктрине по киберпространству называются киберпространственными действиями (см. JP 3-12) и применение одного или нескольких киберпространственных средств. На рис. 2-2. показаны взаимосвязи между типами кибероперациий и связанными с ними действиями, местом проведения этих операций в киберпространстве и силами, осуществляющими эти операции. Четыре действия в киберпространстве:

1. Обеспечение кибербезопасности (см. FM 6-02 и ATP 6-02.71).

2. Киберзащита.

3. Использование киберпространства.

4. Кибератака.

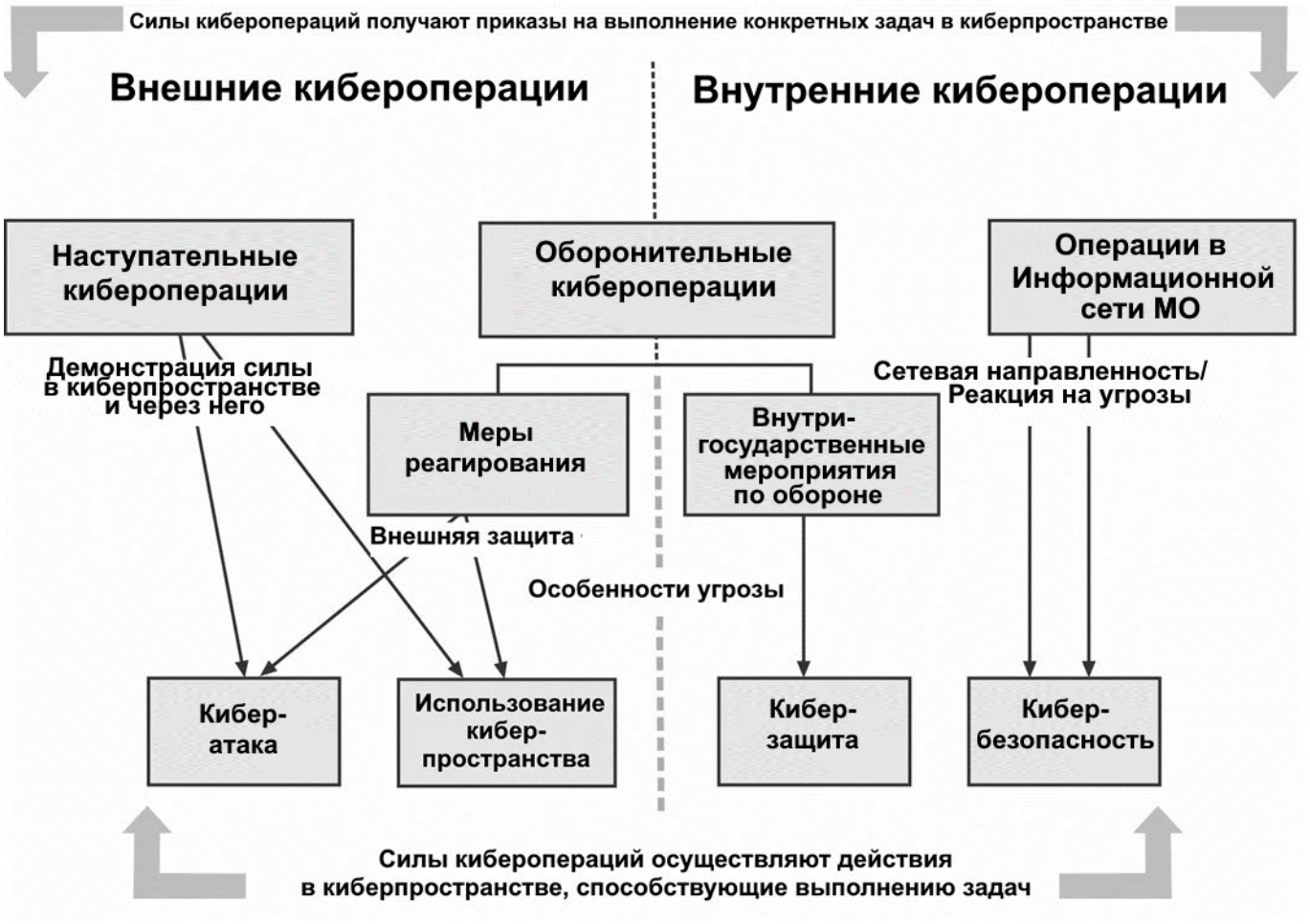


Рис. 2-2. – *Задачи и действия при проведении кибероперации.*

2.1.5.1. Кибербезопасность

2-17. ***Кибербезопасность*** – это действия, предпринимаемые в защищённом киберпространстве для предотвращения несанкционированного доступа, использования или повреждения компьютеров, электронных систем связи и других информационных систем, включая платформенные информационные системы, а также содержащейся в них информации для обеспечения её доступности, целостности, аутентификации, конфиденциальности и безотказности (JP 3-12). Эти превентивные меры безопасности включают защиту информации в информационной сети МО, обеспечение доступности, целостности, подлинности, конфиденциальности и невозможности отказа в доступе к информации. Кибербезопасность, как правило, носит превентивный характер, но также продолжается в рамках ОКбО-ВМО и реагирования на инциденты в случаях, когда киберугроза ставит под угрозу информационную сеть МО. К числу распространённых типов действий по обеспечению кибербезопасности относятся:

- управление паролями;
- исправление ошибок в программном обеспечении;
- шифрование устройств хранения информации;

- обязательное обучение кибербезопасности для всех пользователей;
- ограничение доступа к подозрительным сайтам;
- реализация процедур, определяющих роли, обязанности, политику и административные функции по управлению операциями в Информационной сети МО.

2-18. Тактику проведения операций в информационной сети МО см. в Боевом уставе FM 6-02. Методики проведения операций в информационной сети МО см. в Наставлении ATP 6-02.71.

2.1.5.2. Использование киберпространства

2-19. ***Использование киберпространства*** – это деятельность в киберпространстве, направленная на добывание разведывательных сведений, осуществление манёвра, сбор информации или выполнение других действий, необходимых для подготовки к будущим военным операциям (JP 3-12). Эти операции являются частью действий НКбО или ОКбО-МР в сером или красном киберпространстве, которые не создают воздействий кибератаки и часто предназначены оставаться секретными, и должны быть утверждены оперативными приказами. Использование киберпространства включает мероприятия по оперативной подготовке обстановки для текущих и будущих операций путём получения и сохранения доступа к сетям, системам и узлам, представляющим военную ценность; маневрирования для занятия выгодных позиций в киберпространстве; и размещение средств воздействия на киберпространство для облегчения последующих действий. Действия по использованию киберпространства согласовываются с другими министерствами и ведомствами США в соответствии с национальной политикой.

2.1.5.3. Кибератака

2-20. Действия кибератак, предпринимаемые в киберпространстве, создают заметные эффекты отказа (т.е. ухудшение, нарушение или разрушение) или манипуляции, которые приводят к эффектам отказа в физических доменах (JP 3-12). Кибератака создаёт эффекты в киберпространстве и через него может привести к физическим разрушениям. Модификация или разрушение средств, использующих киберпространство), которые управляют физическими процессами, может привести к последствиям в физических сферах. Некоторые наглядные примеры общих результатов кибератаки включают:

a. Отказ. Предотвращение доступа, работы или доступности определённой функции на определённом уровне в течение определённого времени (JP 3-12). Кибератаки лишают противника возможности доступа к киберпространству, препятствуя функционированию аппаратного и программного обеспечения в течение определённого времени.

б. Ухудшение. Отказ в доступе или работе объекта до уровня, выраженного в виде процента от его пропускной способности. Указан уровень ухудшения. Если требуется конкретное время, его можно указать (JP 3- 12).

в. Нарушение. Полностью, но на некоторое время запретить доступ к объекту или его использование в течение определённого периода времени. Обычно указывается желаемое время начала и окончания работы. Нарушение может рассматриваться как частный случай ухудшения, когда уровень ухудшения составляет 100% (JP 3-12). Командование может использовать кибератаки, которые временно, но полностью лишают противника возможности доступа к киберпространству или каналам связи, чтобы нарушить процесс принятия решений, способность организовать подразделения и осуществлять командование и управление. Эффекты нарушения в киберпространстве обычно ограничены по продолжительности.

г. Уничтожение. Полностью и необратимо лишить цель доступности или работоспособности. Уничтожение максимально увеличивает время и объём отказов. Однако масштабы уничтожения зависят от продолжительности конфликта, поскольку многие цели при наличии достаточного времени и ресурсов могут быть восстановлены (JP 3-12). Командиры могут использовать кибератаки для разрушения аппаратного и программного обеспечения до состояния, не подлежащего ремонту, когда для восстановления работоспособности системы требуется его замена. Уничтожение средств воздействия на киберпространство противника, может включать необратимое повреждение системного программного обеспечения, приводящее к потере данных и информации, или необратимое повреждение аппаратных средств, таких как компьютерный процессор, жёсткий диск или блок питания системы или систем в сети противника.

д. Манипуляция. Манипуляция как форма кибератаки заключается в контроле или изменении информации, информационных систем и/или сетей в сером или красном киберпространстве с целью создания эффекта физического отказа, используя дезинформацию, создание ложных целей и условий, спуфинг, фальсификацию и другие подобные методы. В этом случае используются информационные ресурсы неприятеля в своих целях, чтобы создать эффект отказа, который не сразу проявляется в киберпространстве (JP 3-12). Командиры могут использовать кибератаки для манипулирования информацией или информационными системами противника в поддержку тактических целей дезинформации или в рамках общих действий по дезинформации. Информацию о поддержке действий по дезинформации со стороны сухопутных войск см. в Боевом уставе FM 3-13.4.

Примечание.

> Кибератаки являются видами огневого поражения, осуществляемого в ходе ОКбО-МР и НКбО, и ограничиваются задействованием сил (средств) кибероперацій. Они требуют взаимодействия с другими министерствами и ведомствами США и тщательного согласования с другими летальными и нелетальными поражающими факторами в рамках процесса целеуказаний.

2.2. Радиоэлектронная борьба

2-21. При проведении военных операций современные вооружённые силы полагаются на средства связи, использующие широкую часть ЭМС, что позволяет им вести переговоры, передавать данные, навигационную и хронометрическую информацию, а также осуществлять командование и управление войсками по всему миру. Кроме того, они полагаются на ЭМС для восприятия и осознания оперативной обстановки. Сухопутные войска используют РЭБ для завоевания и удержания позиций относительного преимущества в ЭМС. Вклад сухопутных войск в операции с ЭМС достигается путём внедрения и согласования операций РЭБ и операций по управлению спектром.

Под радиоэлектронной борьбой понимаются военные действия, связанные с использованием электромагнитной и направленной энергии для управления электромагнитным спектром или для атаки на противника.

Войска РЭБ по направлениям деятельности состоят из трёх компонентов: электромагнитная атака, электромагнитная защита и электромагнитная поддержка. Они часто взаимодействуют и поддерживают друг друга в боевых действиях (операциях).

Например:

> Электромагнитная атака с постановкой радиолокационных помех может выполнять функцию защиты своих войск при проникновении в защищаемое воздушное пространство, а также препятствовать получению противником полной оперативной картины.

Рисунок 2-3 иллюстрирует типовую структуру сил и средств РЭБ.

Направления	Электромагнитная атака	Электромагнитная защита	Электромагнитная поддержка
Типы операций	Атака на личный состав, средства, оборудование	Защита своих радиоэлектронных сил и средств	• Перехват • Идентификация • Местонахождение • Оценка
Типы обеспечивающих операций	• Разведка • Атака противника	Упреждающая защита	• Понимание оперативной ситуации • Информация о боевой обстановке • Целеуказание • Разработка разведывательной подготовки района боевых действий
Основные задачи	• Оружие направленной энергии • Электромагнитный импульс • Активные меры противодействия • Меры по дезинформации • Электромагнитное вторжение • Электромагнитные помехи • Электромагнитное зондирование • Перехват и ретрансляция искажённых навигационых сигналов	• Деконфликтизация электромагнитных воздействий • Обеспечение электромагнитной совместимости • Защита от электромагнитного воздействия • Контроль за излучениями • Электромагнитная маскировка • Превентивные меры противодействия • Повышение устойчивости • Резервные режимы применения РЭС в условиях военного времени	• Ведение электромагнитной разведки • Предупреждение об угрозе • Определение направления
Основные последствия	• Нарушение • Деградация • Нейтрализация • Уничтожение • Дезинформация	• Введение в заблуждение • Отказ • Нарушение • Нейтрализация	• Использование • Обнаружение

*Рис. **2-3.** – Систематизация РЭБ*

2.2.1. Электромагнитная атака

2-22. Сухопутные войска ведут как наступательные, так и оборонительные ЭМА для достижения целей командира в интересах выполнения задачи. ЭМА проецируют силу в ЭМС и через него путём проведения активных и пассивных действий по лишению противника возможностей и техники или применением пассивных систем для защиты своих сил и средств.

Электромагнитная атака – это направление РЭБ, связанное с использованием электромагнитной энергии, направленной энергии или противорадиолокационного вооружения для нападения на личный состав, объекты или технику с целью ослабления, нейтрализации или уничтожения боевого потенциала противника и считается одной из форм огневого поражения (JP 3-85). ЭМА требует, чтобы системы или вооружение, излучающие электромагнитную энергию, были активными средствами, а системы, не излучающие и не переизлучающие электромагнитную энергию, были пассивными средствами.

2-23. Наступательная ЭМА предотвращает или снижает эффективность использования противником ЭМС путём применения систем постановки помех и оружия направленной энергии против радиоэлектронных систем и устройств противника.

Наступательные системы и средства ЭМА:

- станции активных помех;
- энергетическое оружие направленного действия;
- самодвижущиеся ложные цели (макеты);
- электромагнитная дезинформация;
- противорадиолокационные ракеты.

2-24. Оборонительная ЭМА обеспечивает защиту от летальных средств поражения, лишая противника возможности использовать ЭМС для целеуказания, наведения и применения вооружения, которое негативно воздействует на системы своих войск. Оборонительная ЭМА обеспечивает проведение мероприятий по защите войск, самозащите и безопасности операций путём ухудшения, нейтрализации или уничтожения возможностей противника по наблюдению за защищаемыми подразделениями.

Оборонительные системы и средства ЭМА:

- расходные материалы (ложные тепловые и активные цели (макеты));
- станции активных помех;
- буксируемые ложные цели (макеты);
- системы инфракрасного противодействия направленной энергии;
- системы радиоуправляемых самодельных взрывных устройств (*англ. Radio controlled improvised explosive device*, *RCIED*);
- противодействие беспилотным авиационным системам (*англ. Counter Unmanned Aerial Systems, C-UAS*).

2-25. Командиру доступны следующие воздействия ЭМА:

a. Уничтожение. Уничтожение приводит к такому состоянию объекта, при котором он не может ни функционировать, ни быть восстановленным до пригодного для использования состояния в сроки, актуальные для текущей операции. В контексте РЭБ уничтожение – это применение ЭМА для ликвидации личного состава, объектов или оборудования противника (JP 3-85).

б. Ухудшение. Ухудшение снижает эффективность или работоспособность системы противника, зависящей от ЭМС. Влияние ухудшения может длиться несколько секунд или сохраняться в течение всей операции (JP 3-85).

в. Нарушение. Вывод из строя, который временно прерывает работу радиоэлектронной системы противника (JP 3-85).

г. Дезинформация. Меры по дезинформации направлены на введение противника в заблуждение путём манипулирования, искажения или фальсификации фактов с целью побудить к реакции, противоречащей его интересам. Дезинформация в контексте РЭБ представляет операторам противника и процессам обработки данных более высокого уровня ошибочные входные данные либо непосредственно через средства обнаружения, либо через сети ЭМС, такие как голосовая связь или каналы передачи данных (JP 3-85).

2.2.1.1. Задачи электромагнитной атаки

2-26. Электромагнитная атака обладает уникальным потенциалом, позволяющим воздействовать на использование противником ЭМС и атаковать противника через ЭМС. Другие наступательные варианты могут повлиять на использование противником ЭМС, но, скорее всего, приведут к сопутствующим потерям за пределами ЭМС, в то время как ЭМА использует ЭМС для оказания своего воздействия. В то же время потенциальные возможности ЭМА стать причиной группового уничтожения в ЭМС требует осторожности и взаимодействия при их использовании.

2-27. Задачи ЭМА:

- применение оружия направленной энергии;
- электромагнитный импульс;
- активные меры противодействия;
- меры по дезинформации;
- электромагнитное вторжение;
- электромагнитные помехи;
- электромагнитное зондирование;
- перехват и ретрансляция искажённых навигационных сигналов.

2.2.1.1.1. Направленная энергия

2-28. ***Направленная энергия*** (*англ. directed energy*) – это общий термин, охватывающий технологии, связанные с созданием пучка концентрированной электромагнитной энергии или атомных или субатомных частиц. (JP 3-85). Направленная энергия становится оружием прямого действия, если используется для проведения ЭМА.

Оружие направленной энергии (*англ. directed-energy weapon*) – это оружие или система, использующие направленную энергию для вывода из строя, повреждения или уничтожения техники, объектов и/или личного состава противника (JP 3- 85). ЭМА с применением оружия направленной энергии называются боевыми действиями с использованием направленной энергии.

Война с применением направленной энергии (*англ. directed-energy warfare*) – это военные действия с использованием вооружения, устройств и контрмер направленной энергии (JP 3-85). Целью боевых действий с использованием направленной энергии является вывод из строя, нанесение прямого ущерба или уничтожение техники, объектов или личного состава противника. Другим применением боевых средств направленной энергии является обнаружение, использование, снижение или предотвращение использования ЭМС противником путем нейтрализации или уничтожения.

2.2.1.1.2. Электромагнитный импульс

2-29. ***Электромагнитный импульс*** (*англ. electromagnetic pulse*) – это мощный всплеск электромагнитного излучения, вызванный ядерным взрывом, энергетическим оружием или природным явлением, который может взаимодействовать с электрическими или электронными системами, вызывая повреждающие скачки тока и напряжения (JP 3-85).

Воздействие электромагнитного импульса может распространяться на сотни километров в зависимости от высоты и мощности импульсного разряда. Высотный электромагнитный импульс может вызвать разрушительное воздействие на территории размером с континент. Наиболее подверженной воздействию ЭМИ или высотного ЭМИ частью ЭМС является радиочастотный спектр. Электромагнитная энергия, создаваемая электромагнитным импульсом, исключает самые высокие частоты оптического (инфракрасное, видимое, ультрафиолетовое) и ионизирующего (X- и гамма-излучение) диапазонов. К косвенным последствиям электромагнитного импульса или высотного электромагнитного импульса относятся электрические возгорания, вызванные перегревом электрических систем и компонентов.

2.2.1.1.3. Активные меры противодействия

2-30. ЭМА включает активные меры противодействия как ответ на атаку противника в рамках ЭМС. Реагирование на атаку противника может включать применение радиочастотных средств противодействия, таких как ложные тепловые цели и дипольные отражатели, для вывода из строя систем и вооружения противника, например, высокоточного или радиоуправляемого вооружения, средств связи и разведывательных систем.

Радиочастотные меры противодействия – это любые устройства или технологии, использующие радиочастотные средства или технологии, которые предназначены для снижения эффективности действий противника, особенно в отношении высокоточных управляемых систем и средств обнаружения (JP 3-85).

Дипольные отражатели – это отражатели для создания радиолокационных помех, состоящие из тонких узких металлических полос различной длины и частотной характеристики, которые используются для отражения эхо-сигналов с целью создания помех (JP 3-85). Активные меры противодействия могут спровоцировать применение оружия направленной энергии или электромагнитного импульса, а также могут включать применение огня на поражение. Сухопутные войска могут выводить из строя системы управления вооружением и разведывательные системы противника путём развёртывания пассивных и активных электро-оптико-инфракрасных средств противодействия, среди которых:

- дым;
- аэрозоли;
- подавители сигнатур;
- ложные цели;
- пиротехника;
- пирофорные вещества;
- лазерные постановщики помех;
- высокоэнергетические лазеры;
- направленная инфракрасная энергия.

2.2.1.1.4. Меры по дезинформации

2-31. Меры по дезинформации направлены на введение противника в заблуждение путём манипулирования, искажения или фальсификации данных с целью побудить его к реакции, противоречащей его интересам. Электромагнитная дезинформация осуществляется путём вброса ложных данных в зависимые от ЭМС сети передачи голоса и данных противника для снижения эффективности разведки, наблюдения и систем обнаружения. РЭБ использует ЭМС для введения противника в заблуждение, что затрудняет принятие решений и определение точного представления о действительном положении Сухопутных войск. Войска РЭБ поддерживают все планы по дезинформации, как объединённые, так и тактические по введению противника в заблуждение применением мер электромагнитной дезинформации и соответствующим образом масштабируя их для достижения желаемого эффекта. Меры электромагнитной дезинформации обеспечивают подачу ложных электромагнитных сигналов, например, путём введения ложных сигналов в системы противника по обнаружению угроз, такие как РЛС.

Полномочия командира по планированию и осуществлению мер дезинформации, интегрированной с мерами электромагнитной дезинформации, могут быть ограничены отдельными полномочиями и правилами ведения боевых действий в области РЭБ (технические средства дезинформации приведены в документах CJCSI 3211.01F и AR 525-21).

2.2.1.1.5. Электромагнитное вторжение

2-32. ***Электромагнитное вторжение*** – это преднамеренное введение электромагнитной энергии в каналы передачи любым способом с целью вызвать замешательство или ввести операторов в заблуждение (JP 3-85). Примером электромагнитного вторжения является вброс ложной или вводящей в заблуждение информации в радиоканалы противника на уровне вышестоящего штаба. Электромагнитное вторжение способно вводить в заблуждение или вызывать замешательство в интеллектуальной системе управления полётом самолёта противника, что ставит под угрозу работу нейронной сети системы управления полётом и способность пилота сохранять управление.

2.2.1.1.6. Электромагнитные помехи

2-33. ***Электромагнитные помехи*** – это преднамеренное излучение, переизлучение или отражение электромагнитной энергии для предотвращения или снижения эффективности использования противником ЭМС с целью ухудшения или нейтрализации его боевого потенциала (JP 3-85). Целями, которые подвержены помехам, могут быть радиостанции, навигационные системы, РЛС и спутники. Электромагнитные помехи могут вывести из строя интеллектуальную систему управления полётом самолёта противника, заглушив его средства обнаружения и связи, что лишает возможности получать навигационные данные или данные о высоте, имеющие решающее значение для выполнения полёта. Электромагнитные помехи могут также помешать или снизить эффективность интегрированной системы ПВО противника, подавляя его средства обнаружения, используемые для вскрытия и идентификации целей.

2.2.1.1.7. Электромагнитное зондирование

2-34. ***Электромагнитное зондирование*** – это преднамеренное излучение, предназначенное для воздействия на устройства или системы противника с целью изучения их функций и эксплуатационных возможностей (JP 3-85). Электромагнитное зондирование предполагает получение доступа к устройствам противника с целью получения информации об их функциях, возможностях и назначении. Электромагнитное зондирование может дать информацию о возможностях противника и его способности влиять на процесс боевых действий (операций). Сухопутные войска могут проводить открытое электромагнитное зондирование с целью вызвать ответную реакцию противника, что позволит раскрыть его местоположение.

2.2.1.1.8. Перехват и ретрансляция искажённых навигационных сигналов

2-35. Выполнение задачи заключается в приёме сигналов радиомаяков и их ретрансляции на той же частоте с целью усложнения навигации. Передача искажённых сигналов приводит к получению неточных пеленгов самолётами или наземными станциями (JP 3-85).

2.2.2. Электромагнитная защита

2-36. ***Электромагнитная защита*** – это направление РЭБ, включающее действия по защите личного состава, объектов и оборудования от любых последствий использования ЭМС своими войсками, нейтральными субъектами или противником, которые ухудшают, нейтрализуют или уничтожают свои боевые возможности (JP 3-85). Меры ЭМЗ устраняют или ослабляют негативное воздействие, возникающее в результате действий своих войск, нейтральных субъектов, противника или естественно возникающих электромагнитных помех.

2-37. Как ЭМЗ, так и оборонительные ЭМА могут оказывать защитное действие. Однако в ЭМЗ особое внимание уделяется защите своих сил и средств, зависящих от ЭМС. Для сравнения, защитные воздействия оборонительной ЭМА направлены на атаку сил и средств противника, которые способствуют его противодействию операциям своих войск. ЭМЗ включает меры по защите своих войск, находящихся вблизи боеприпасов или работающих с ними, путём предотвращения непреднамеренных детонаций под воздействием электромагнитной энергии.

2.2.2.1. Задачи электромагнитной защиты

2-38. Противник в значительной степени заинтересован в снижении эффективности использования ЭМС ВС США. Крайне важно понимать угрозу со стороны противника и уязвимые места своих систем, оборудования и личного состава. Эффективные меры ЭМЗ позволят минимизировать последствия природных явлений и ослабить возможности противника по успешному проведению ЭМП и ЭМА против своих войск.

2-39. Задачи ЭМЗ:

- устранение последствий электромагнитного воздействия;
- электромагнитная совместимость;
- электромагнитная устойчивость;
- контроль за излучениями;
- электромагнитная маскировка;
- превентивные меры противодействия;
- электромагнитная безопасность;
- резервные режимы работы военного времени.

2.2.2.1.1. Устранение последствий электромагнитного воздействия

2-40. ***Электромагнитная уязвимость*** (*англ. electromagnetic vulnerability*) – это характеристики системы, которые способствуют к её определенному ухудшению (неспособности выполнить поставленную задачу) в результате воздействия определённого уровня электромагнитного воздействия (JP 3-85). Любая система, работающая в ЭМС, подвержена электромагнитному воздействию окружающей среды. Любое спектрально-зависимое устройство, подвергающееся воздействию электромагнитного излучения или имеющее проблемы с электромагнитной совместимостью в пределах оперативной электромагнитной обстановки, может привести к увеличению вероятности возникновения таких электромагнитных уязвимостей, как проблемы безопасности, функциональной совместимости и надёжности. Электромагнитная уязвимость проявляется в том случае, если спектрозависимые устройства имеют такой уровень ухудшения своей работы, который делает их неспособными выполнять операции при воздействии электромагнитной среды.

2-41. Электромагнитная совместимость, деконфликтизация ЭМС, ЭМИ и уменьшение электромагнитных помех снижают влияние электромагнитных воздействий. Понимание опасности различных типов электромагнитного излучения позволяет ответственным за планирование принять соответствующие меры по противодействию или ослаблению последствий электромагнитного воздействия. Опасности, связанные с электромагнитным излучением, включают – опасность для личного состава; опасность для боеприпасов; опасность для топлива. Электромагнитное воздействие может возникать и в результате таких природных явлений, как молнии и статические разряды.

2.2.2.1.2. Электромагнитная совместимость

2-42. ***Электромагнитная совместимость*** (*англ. electromagnetic compatibility*) – это способность радиоэлектронных систем, оборудования и устройств работать в предназначенных для них условиях, не вызывая или не подвергаясь неприемлемому или непреднамеренному ухудшению работы из-за электромагнитного излучения или воздействия (JP 3-85). Офицер по управлению спектром СЕМА помогает специалистам G-6 или S-6 в обеспечении электромагнитной совместимости для ослабления электромагнитной уязвимости путём рационального планирования, взаимодействия и управления ЭМС. Оперативные силы имеют минимальные возможности для ослабления проблем электромагнитной совместимости. Вместо этого они должны документировать выявленные проблемы электромагнитной совместимости, чтобы отделы по руководству программами (сил и средств) видов ВС могли согласовать требуемые изменения, необходимые для снижения проблем совместимости.

2.2.2.1.3. Электромагнитная устойчивость

2-43. ***Электромагнитная устойчивость*** (*англ. electromagnetic hardening*) состоит из действий, предпринимаемых для защиты личного состава, объектов и/или оборудования путём подавления, фильтрации, ослабления, заземления, соединения и/или экранирования от нежелательного воздействия электромагнитной энергии (JP 3-85). Электромагнитная устойчивость позволяет защитить свои радиоэлектронные устройства от воздействия электромагнитных помех или таких опасных ЭМА, как лазеры, мощные микроволны или электромагнитные импульсы. В качестве примера электромагнитной устойчивости к электромагнитным излучениям можно привести установку экранирующего канала, состоящего из проводящих или магнитных материалов, для защиты от нежелательного воздействия электромагнитной энергии.

2.2.2.1.4. Контроль за излучениями

2-44. ***Контроль за излучениями*** (*англ. emission control*) – это избирательное и управляемое использование электромагнитных, акустических или других излучателей для оптимизации возможностей командования и управления при минимизации в интересах безопасности операций:

- обнаружения средствами противника;
- взаимных помех между своими системами;
- помех противника при реализации плана военной дезинформации (JP 3-85).

Контроль за излучениями позволяет обеспечить безопасность операций путём:

а. Снижения вероятности обнаружения и противодействия дальности обнаружения средствами противника.

б. Обнаружения и уменьшения электромагнитных помех для своих радиоэлектронных устройств.

в. Обнаружения электромагнитных помех противника, что позволяет выполнить планирование по дезинформации.

2-45. Контроль за излучениями позволяет осуществлять электромагнитную маскировку путём интеграции разведки и РЭБ и для корректировки планов управления спектром и связью. Практический и продуманный план контроля за излучениями в сочетании с другими мерами ЭМЗ является одним из важнейших аспектов обеспечения безопасности операций. В Наставлении ATP 3-13.3 описаны методы обеспечения безопасности операций на уровне дивизии и ниже.

2.2.2.1.5. Электромагнитная маскировка

2-46. ***Электромагнитная маскировка*** (*англ. electromagnetic masking*) – это контролируемое излучение электромагнитной энергии на частотах, используемых своими подразделениями, таким образом, чтобы защитить излучения своих систем связи и электронных систем от средств ЭМП и радиотехнических средств разведки противника без существенного ухудшения работы своих систем (JP 3-85). Электромагнитная маскировка скрывает, искажает или манипулирует электромагнитными излучениями своих войск с целью сокрытия информации о военных операциях или создания ложных представлений у командования противника. Электромагнитная маскировка является важной составляющей военной маскировки, безопасности операций и защиты сигналов.

2.2.2.1.6. Превентивные меры противодействия

2-47. ***Меры противодействия*** – это такая форма военной науки, которая путём применения устройств и/или методов имеет своей целью снижение оперативной эффективности действий противника (JP 3-85). Меры противодействия могут быть пассивными (не излучающими или переизлучающими электромагнитную энергию) или активными (излучающими электромагнитную энергию), и развёртываться заранее или в ответ на действия противника. Упреждающее развёртывание пассивных мер противодействия – это предупредительные процедуры, направленные на срыв атаки противника в ЭМС путём использования пассивных устройств, таких как переизлучающие дипольные отражатели или радиопоглощающий материал, препятствующий отражению радиосигнала.

2.2.2.1.7. Электромагнитная безопасность

2-48. ***Электромагнитная безопасность*** (*англ. electromagnetic security*) – это защита, обусловленная всеми мерами, направленными на лишение неавторизованных лиц ценной информации, которая может быть получена в результате перехвата и изучения ими электромагнитных излучений, не связанных с коммуникациями (например, РЛС) (JP 3-85). Изменение модуляции и характеристик электромагнитных частот, используемых для РЛС, затрудняет перехват и изучение радиолокационных сигналов противником.

2.2.2.1.8. Резервные режимы работы военного времени

2-49. ***Резервные режимы работы военного времени*** (*англ. wartime reserve modes*) – это характеристики и процедуры работы средств обнаружения, связи, навигации, распознавания угроз, оружия и систем противодействия, которые будут способствовать военной эффективности, если до своего использования они для противника неизвестны или неправильно им поняты, однако могут быть использованы или нейтрализованы, если заранее известны (JP 3-85). Резервные режимы работы военного времени намеренно сохраняются в резерве для использования в военное время или в чрезвычайных ситуациях.

2.2.3. Электромагнитная поддержка

2-50. ***Электромагнитная поддержка*** относится к направлению РЭБ, включающему действия по задаче или под непосредственным управлением командира на оперативном уровне с целью поиска, перехвата, идентификации, определения местоположения или локализации источников преднамеренных и непреднамеренных излучений электромагнитной энергии для непосредственного распознавания угрозы, обнаружения и идентификации целей, планирования и проведения будущих боевых действий (операций) (JP 3-85). В многосферных операциях командиры стремятся к доминированию в ЭМС и формированию оперативной обстановки путём обнаружения, перехвата, анализа, идентификации, определения местоположения и воздействия на электромагнитные системы противника (отказ, ухудшение, нарушение, введение в заблуждение, уничтожение и манипулирование), которые поддерживают военные операции. Одновременно они занимаются защитой и обеспечением свободы действий сил США и союзников в ЭМС и через него.

2-51. Целью ЭМП является получение информации о боевой обстановке для поддержки плана действий командира. ***Информация о боевой обстановке*** (*англ. combat information*) – это непроверенные данные, собранные командиром на тактическом уровне или предоставленные ему непосредственно, которые в силу своей ограниченной по времени актуальности или критичности ситуации не могут быть своевременно обработаны и переданы в тактическую (войсковую) разведку, чтобы удовлетворить требования получателя данных тактической разведки (JP 2-01). Информация о боевой обстановке, используемая для планирования или проведения боевых действий (операций), включая операции ЭМА, добывается в соответствии с полномочиями командования, однако при этом необходимо учитывать соображения конфиденциальности стран-партнёров. Дешифрование сообщений является исключительно функцией РРТР и может выполняться только личным составом радио и радиотехнической разведки, действующим под оперативным управлением директора Агентства национальной безопасности и руководителя Службы национальной безопасности (DODI O- 3115.07).

2-52. Электромагнитная поддержка обеспечивает операции путём получения информации о боевой обстановке через ЭМС для проведения воздействий и планирования. Информация о боевой обстановке собирается для немедленного использования в целях распознавания угроз, проведения текущих операций, целеуказаний для ЭМА или летальных ударов, а также для поддержки планирования командиром будущих операций. Данные, собранные с помощью ЭМП, могут способствовать обработке, использованию и распространению данных РРТР для обеспечения требований командира к разведке, целеуказаниям и понимания ситуации. Данные и информация, полученные с помощью ЭМП, зависят от своевременного сбора, обработки и доклада для предупреждения командира и штаба о потенциально важной информации о боевой обстановке.

2.2.3.1. Задачи электромагнитной поддержки

2-53. При оказании ЭМП командиры задействуют взводы РЭБ, входящие в состав рот военной разведки бригадных тактических групп (далее – БТГ), для поддержки усилий по сбору информации, разведки ЭМС, взаимодействия и анализа множества источников путём их отображения и предупреждения, радиопеленгования и геолокации излучений угрозы.

2-54. Задачи ЭМП:

- радиоэлектронная разведка;
- предупреждение об угрозе;
- радиопеленгование.

2.2.3.1.1. Радиоэлектронная разведка

2-55. ***Радиоэлектронная разведка*** (далее – РЭР) (*англ. electromagnetic reconnaissance*) – это обнаружение, определение местоположения, идентификация и оценка посторонних электромагнитных излучений (энергии) (JP 3-85). РЭР – это действие, используемое для поддержки сбора информации и являющееся элементом разведки по выполнению тактических задач (см. главу 4). Информация, полученная в результате РЭР, помогает командиру в понимании ситуации и принятии решений, а также может быть дополнительно обработана для поддержки РРТР. РЭР может привести к изменению ЭМЗ или привести к ЭМА или летальному удару.

2-56. Информация, полученная в результате РЭР, в совокупности с другими источниками информации и разведывательными данными может быть использована для точной геолокации. Точная геолокация включает планирование, взаимодействие и управление своими средствами для определения местоположения радиочастотных систем противника с целью целеуказания. Полученные данные анализируются с целью определения месторасположения источника электромагнитной энергии. Эта информация предоставляет группе огневой поддержки физическое местоположение систем противника, излучающих электромагнитную энергию.

2.2.3.1.2. Предупреждение об угрозе

2-57. Предупреждение об угрозе позволяет командиру и штабу быстро определить непосредственные угрозы для своих войск и реализовать меры противодействия ЭМА или ЭМЗ. Личный состав РЭБ использует средства обнаружения, перехвата, идентификации и определения местоположения электромагнитных сигнатур противника и обеспечивает раннее предупреждение о надвигающейся или потенциальной угрозе. Личный состав РЭБ координирует свои действия со штабными структурами G-2 или S-2 при долгосрочном воздействии обнаруженных излучателей противника.

Предупреждение об угрозе помогает командиру в принятии решений при разработке разведывательной подготовки района боевых действий, актуализации электромагнитного боевого порядка, а также при сопоставлении источников излучения противника с системами связи и вооружения.

2-58. Известные электромагнитные сигнатуры должны быть сопоставлены с электромагнитным боевым порядком, важными целями и списком приоритетных целей, а также предпринимаемыми мерами, предусмотренными текущей политикой или вышестоящим руководством. Неизвестные электромагнитные сигнатуры, обнаруженные в ЭМС, передаются в подразделение штаба G-2 или S-2 для анализа. Специалисты из G-2 или S-2 проверяют известные и неизвестные системы в рамках сбора информации, которая используется в оперативном процессе. Штабы анализируют и докладывают информацию вышестоящим и подчинённым штабам, подразделениям сухопутных войск и объединённых сил, а также другим участникам совместных действий в районе боевых действий (операций).

2.2.3.1.3. Радиопеленгование

2-59. ***Радиопеленгование*** – это процедура получения пеленгов на радиочастотные источники излучения с помощью высоконаправленной антенны и блока индикации на приёмнике перехвата или вспомогательном оборудовании (JP 3-85). Для определения местоположения противника личный состав РЭБ использует различные платформы ЭМП с возможностями пеленгования. Для большей уверенности в определении местоположения противника предпочтительнее использовать несколько систем пеленгования. Платформы электромагнитной поддержки развёртываются в различных формациях для создания базовой линии и увеличения зоны покрытия. Оптимальным считается использование трёх и более пеленгаторов для триангуляции целевого источника излучения.

2.2.3.2. Электромагнитная поддержка и радио и радиотехническая разведка

2-60. ЭМП и РРТР часто используют одни и те же или аналогичные средства и ресурсы, и от личного состава, осуществляющего ЭМП, может потребоваться сбор информации, отвечающей обоим требованиям одновременно. Радио и радиотехническая разведка включает разведку связи, РЭР и разведку внешних технических средств. Общие особенности электромагнитной поддержки и РРТР проявляются на ранних этапах зондирования, сбора, идентификации и определения местоположения иностранных излучений. Различие между ЭМП и РРТР определяется тем, кто осуществляет оперативное управление средствами сбора информации, какие возможности эти средства должны предоставлять и зачем они нужны. Информация и данные становятся объектом радио и радиотехнической разведки, если к сигналу применяются криптографические процессы для определения его релевантности, ценности или значения исключительно для разведки.

Существуют также жёсткие границы между системами, сложностью сигналов и сроками представления информации, которые разделяют ЭМП и РРТР. Хотя и ЭМП, и РРТР предоставляют информацию, соответствующую порогам отчётности, непосредственно поддерживаемому подразделению, радио и радиотехническая разведка обязана дополнительно передавать полученную информацию через систему РРТР США. Дополнительное требование к радио и радиотехнической разведке обеспечивает подотчётность и позволяет получить доступ более широкому числу специалистов разведывательного ведомства к информации для подготовки и распространения дополнительных разведданных, если это необходимо. Более подробная информация о радио и радиотехнической разведке содержится в Наставлении ADP 2-0.

2.2.4. Улучшение приёмов и возможностей РЭБ

2-61. ***Улучшение приёмов и возможностей РЭБ*** (*англ. electromagnetic warfare reprogramming*) – это преднамеренное изменение или модификация систем РЭБ или обнаружения целей, а также тактики и процедур, в которых они используются, в ответ на подтверждённые изменения в оборудовании, тактике или электромагнитной обстановке (JP 3-85). Целью улучшения приёмов и возможностей РЭБ является поддержание или повышение эффективности РЭБ и систем обнаружения и идентификации целей. Улучшение приёмов и возможностей РЭБ включает изменения в программном обеспечении РЭБ и системы целеуказания, таких как системы самообороны, системы наступательного вооружения и системы сбора разведывательных сведений. РЭБ состоит из трёх различных направлений: ЭМА, ЭМЗ и ЭМП, которые обеспечиваются деятельностью по улучшению приёмов и возможностей РЭБ.

2-62. Во время всех учебных занятий и операций сухопутные войска следуют правилам и порядку по улучшению приёмов и возможностей РЭБ, установленным боевым командованием (*англ. combatant command, CCMD*). Части и подразделения разрабатывают программы по улучшению приёмов и возможностей РЭБ, в то время как офицер по кибервойне и РЭБ (*англ. cyber electromagnetic warfare officer*, *CEWO*) следит за тем, чтобы подразделение имело информацию об усилиях, предпринимаемых другими подразделениями для улучшения приёмов и возможностей РЭБ в районе операций, а также соблюдало правила и порядок совместного взаимодействия по улучшению приёмов и возможностей РЭБ. См. приложение F для получения подробной информации об улучшении приёмов и возможностей средств РЭБ.

2.3. Взаимосвязь с другими операциями

2-63. В данном разделе представлена взаимосвязь кибероперацій и РЭБ с другими операциями. В нём рассматривается как кибероперации и РЭБ взаимно поддерживают разведывательные, космические и информационные операции.

2.3.1. Разведывательные операции

2-64. Как операция, ***разведка*** – это: результат сбора, обработки, внедрения, оценки, анализа и объяснения имеющейся информации, касающейся иностранных государств, враждебных или потенциально враждебных сил или элементов, а также районов проведения реальных или потенциальных операций; деятельность, которая приводит к созданию такой информации; организации, занимающиеся такой деятельностью (JP 2-0). Разведка на всех уровнях обеспечивает планирование операций в киберпространстве и РЭБ и помогает определять показатели эффективности и результативности. Разведка также оказывает помощь группе огневой поддержки в разработке списка приоритетных целей (*англ. high payoff target, HPT*) и взаимодействует с отделением CEMA для обеспечения того, чтобы список приоритетных целей включал цели, связанные с РЭБ и киберпространством противника. Разведка также играет решающую роль в оказании помощи группе огневой поддержки в дальнейшей разработке целей, включая передачу целей в объединённую оперативно-тактическую группу (*англ. joint task force, JTF*) для оценки в качестве потенциальных целей для совместного списка целеуказания.

2-65. Сбор информации обеспечивает поддержку кибероперацій и РЭБ путём сбора информации для удовлетворения критических информационных требований командира (*англ. commander's critical information requirement(s), CCIR*) и информационных требований (*англ. information requirements, IR*) штаба о возможностях, деятельности, дислокации и характеристиках киберпространства и ЭМС своих войск, нейтральных субъектов и противника в пределах оперативной обстановки. Сбор информации также способствует наращиванию потенциала. Для понимания целевого пространства, разработки средств и достижения значимых результатов в киберпространстве необходимо иметь надёжный пакет разведывательных данных. В сбор информации входит четыре задачи и направления: разведывательные операции, рекогносцировка, наблюдение и операции безопасности (см. главу 4).

2-66. Информация, полученная в результате сбора информации, определяет процесс разведывательной подготовки района боевых действий. В процессе разведывательной подготовки района боевых действий штабные структуры G-2 или S-2 анализируют параметры оперативной обстановки и задачи в районе ответственности, чтобы определить влияние поражающих возможностей на боевые действия (операции).

Эти параметры влияют на то, каким образом подразделения будут проводить кибероперации и РЭБ в пределах определённого района операции. И наоборот, кибероперации и РЭБ также вносят свой вклад в разведку, обеспечивая сбор информации. Кибероперации и возможности РЭБ обеспечивают сбор информации о боевой обстановке для получения ответов на запросы критических информационных требований командира и информационных требований штаба, а также для ситуативной осведомлённости, целеуказания.

2-67. В ходе операций в ЭМС радио и радиотехническая разведка, кибероперации и РЭБ могут пересекаться. По этой причине эффективная интеграция РРТР, киберопераций, РЭБ и управления спектром выходит далеко за рамки простого взаимодействия. Эффективная интеграция требует как устранения конфликтов, так и выявления окон возможностей для этих операций. Такая интеграция требует тесного взаимодействия штаба, детального процедурного контроля и использования различных технических средств. См. главу 4 для получения дополнительной информации.

2-68. В рамках процесса разведывательной подготовки района боевых действий разведка штаба также определяют ключевые территории неприятеля и противника. В кибероперациях используется концепция ключевой области как модель для определения критических параметров киберпространственного домена. Идентифицированная ключевая область в киберпространстве подвергается воздействию со стороны контролирующей стороны (своей, неприятельской или противника), которое она считает выгодным, например, в обороне, использовании и атаке. Ключевая область в киберпространстве соответствует узлам, связям, процессам или объектам в киберпространстве, будь то часть физического, логического или кибер-персонального слоя. Ключевая область в киберпространстве может включать:

а. Места (участки) в киберпространстве, в которых свои войска могут собирать разведывательные данные.

б. Места (участки) в киберпространстве, поддерживающие сетевое подключение.

в. Точки входа в свои сети, которые требуют приоритетных действий для защиты.

г. Места (участки) в киберпространстве, к которым требуется доступ своих подразделений для выполнения основных функций или задач.

2.3.2. Космические операции

2-69. Киберпространство и космические операции взаимозависимы. Доступ к космической сфере имеет решающее значение для киберопераций, особенно операций в информационной сети МО, обеспечивая глобальную сквозную сетевую связь. В сухопутных войсках доступ к космической сфере возможен только через космические операции.

И наоборот, такие космические возможности, как навигационная борьба, наступательное управление космическим пространством и оборонительное управление космическим пространством, зависят от операций, проводимых в космосе, киберпространстве и в ЭМС. Эта взаимосвязь является критически важной, и управление взаимозависимостью между этими тремя компонентами должно осуществляться на протяжении всего оперативного процесса.

2-70. Как кибероперации, так и РЭБ могут влиять на космические операции. Наземные системы управления спутниками с помощью компьютеров, объединённых в сеть, поддерживают параметры орбиты и управляют бортовой аппаратурой, в частности, поддерживают стабильные орбиты; радиостанции передают компьютерные команды на спутники. Компьютерный код, отправленный непосредственно на спутники на орбите, потенциально может обеспечить дистанционное управление системой, предотвращая доступ других к бортовым информационно-разведывательным средствам или системам связи. Противник также может проникать в наземные системы управления и отдавать спутникам альтернативные команды, чтобы изменить их положение или отключить критически важные системы. Поскольку спутники обычно получают команды с использованием радиочастот, противник может попытаться отключить их аппаратуру или напрямую получить управление над космическим аппаратом, а не пытаться отдавать приказы через наземную систему управления.

2-71. Все космические операции опираются на ЭМС для командования и управления, зондирования и передачи информации. Жизненно важный характер космических операций в мульти-доменных операциях требует тесного взаимодействия с другими видами деятельности в ЭМС, связанными с операциями по управлению спектром, для обеспечения надлежащей расстановки приоритетов, интеграции, согласования и устранения конфликтов. Штабное подразделение G-2 или S-2 использует информацию, полученную в результате космической разведки, наблюдения и обнаружения для оказания помощи командиру и штабу в достижении ситуативной осведомлённости и понимания оперативной обстановки.

2-72. ***Навигационная борьба*** (*англ. navigation warfare*) – это целенаправленные оборонительные и наступательные действия по защите и предотвращению получения информации о позиционировании, навигации и времени путём скоординированного использования операций в космосе, киберпространстве и РЭБ (JP 3-14). Атака с использованием средств навигационной борьбы лишает субъектов угрозы доступа к глобальной навигационной спутниковой системе различными методами, включая наступательные действия в киберпространстве, космические операции и ЭМА. Глобальная навигационная спутниковая система – это общий термин, используемый для описания любой космической системы, предоставляющей информацию о местоположении, навигации и времени (*англ. positioning, navigation, and timing*, *PNT*) по всему миру (например, Глобальная система позиционирования, *англ. Global Positioning System*, *GPS*).

Эффективность навигационной борьбы требует согласования операций в космосе, киберпространстве и РЭБ с летальными и нелетальными поражающими факторами для достижения желаемого результата. РЭБ должна быть согласована с космическими операциями, чтобы получить представление о воздействии операций навигационной борьбы, лишить противника доступа к информации глобальной навигационной спутниковой системы и защитить свои электромагнитные устройства, использующие определённые частоты в рамках ЭМС. См. Боевой устав FM 3-14 для получения дополнительной информации о навигационной борьбе.

2-73. Космическая сфера состоит из трёх сегментов: космического, канала связи и наземного. Космический сегмент представляет собой оперативную область, соответствующую космической сфере, и включает спутники, находящиеся как на геосинхронной, так и на не геосинхронной околоземной орбите. Сегмент канала связи состоит из сигналов, соединяющих наземный и космический сегменты через ЭМС. Наземный сегмент состоит из наземных средств и оборудования, обеспечивающих командование и управление космическими средствами, наземного технологического оборудования, наземных терминалов, пользовательского оборудования, информационно-разведывательных средств для ситуативной осведомлённости в космической обстановке, а также систем связи между этими средствами и оборудованием. К наземным терминалам относятся все наземные, корабельные, подводные и воздушные спутниковые терминалы различных видов ВС, обеспечивающие связь со спутниками космического сегмента. Три сегмента космической сферы в значительной степени опираются на кибероперации для защиты сетевых и информационных технологий и инфраструктур, а также зависят от ЭМС для проведения операций между космическим, каналом связи и наземным сегментами.

2-74. Кибероперации способствуют проведению космических операций путём защиты своих сетей, использующих глобальную навигационную спутниковую систему, и нацеливанием на аналогичные возможности противника и неприятеля. Кроме того, в ходе киберопераций обеспечивается сетевое взаимодействие между наземными средствами и оборудованием в наземном сегменте космического домена. Войска РЭБ обеспечивают ведение навигационной борьбы, лишая противника доступа к информации глобальной навигационной спутниковой системы и одновременно защищая свои космические средства, работающие в ЭМС.

2-75. Интеграция операций в киберпространстве, РЭБ и космосе позволяет командирам и штабам на каждом уровне согласовать потенциал и воздействия. Возможности космического базирования (космический сегмент) позволяют проводить распределённые и глобальные кибероперации. Возможности киберпространства и космического базирования обеспечивают оперативную и своевременную поддержку, позволяющую командирам проецировать боевые возможности с высших уровней на тактический уровень.

Согласование с операциями по управлению спектром необходимо для обеспечения доступности ресурсов в ЭМС и предотвращения конфликтов в спектре. См. Боевой устав FM 3-14 для получения дополнительной информации о космических операциях.

2.3.3. Информационные операции

2-76. ***Информационные операции*** (англ. *Information operations, IO*) – это комплексное использование в ходе военных действий средств, связанных с информацией, в сочетании с другими направлениями операций для оказания влияния, подрыва, искажения или подмены принятия решений противником и потенциальным противником при одновременной защите своих средств (JP 3-13). Информационные операции осуществляют внедрение и согласование информационных возможностей для создания воздействия в информационной среде и через нее для обеспечения оперативного преимущества командира. Информационные операции выполняют оптимизацию информационного компонента боевых возможностей, обеспечивают и усиливают все остальные элементы для получения оперативного преимущества над угрозой (противником). Информационные операции состоят из трёх взаимосвязанных действий, которые работают в тандеме и перекрывают друг друга:

а. Планирование и согласование действий штаба под руководством командира.

б. Подготовительная и оперативная работа подразделений, связанных с информационными возможностями, подразделениями информационных операций или штабными структурами совместно с рабочей группой информационных операций.

в. Действия по оценке, которые выполняются всеми участниками процесса.

2-77. При использовании командирами возможностей киберпространства и РЭБ для создания желаемых условий в оперативной обстановке они согласовывают эти действия через информационные операции. Командиры используют кибероперации и РЭБ для получения стратегического преимущества в киберпространстве и ЭМС. Возможности киберпространства и РЭБ обеспечивают поддержку операций, позволяя обмениваться информацией между своими войсками или оказывая влияние на способность противника использовать киберпространство и РЭБ.

2-78. Кибероперации и воздействия РЭБ оказывают влияние, нарушают, искажают или манипулируют циклом принятия решений противником. Кибероперации поддерживают операции в рамках НКбО или ОКбО-МР путём создания воздействия типа «отказ» или «манипуляция» с целью ухудшения, нарушения работы или уничтожения средств воздействия на киберпространство противника или изменения информации, информационных систем или сетей противника.

РЭБ поддерживает операции через ЭМА, ухудшая, нейтрализуя или уничтожая способность противника использовать ЭМС. РЭБ также поддерживает операции посредством ЭМЗ, скрывая или манипулируя сигнатурами в ЭМС своих войск для ухудшения или введения в заблуждение информационно-разведывательных средств противника или систем обнаружения и идентификации целей. При интеграции и согласовании с другими возможностями кибероперации и РЭБ могут оказать поддержку командирам в создании благоприятных условий для информационного преимущества, будь то в киберпространстве, ЭМС или в других доменах.

2-79. Кибероперации и РЭБ также могут создавать когнитивные эффекты, воздействуя на физические объекты противника. Например, воздействие на огневой потенциал противника с помощью кибератаки или ЭМА может лишить его возможности эффективно использовать артиллерию или создать сомнения в её надежности.

Аналогичным образом, ограничение возможностей противника по использованию киберпространства или ЭМС в критических точках может повлиять на его решения при осуществлении командования и управления. Согласование оборонительных операций в РЭБ и киберпространстве с другими возможностями также может нарушить способность противника принимать решения, обеспечивая при этом свободу действий своих войск.

2-80. Кибероперации и РЭБ, согласованные в рамках оперативного процесса и процесса целеуказаний, могут предоставить командирам дополнительные пути и средства для:

а. Воздействия на возможности противника, которые обеспечивают информационную поддержку или влияют на принятие решений.

б. Воздействия на возможности угроз в области командования и управления, передвижения и манёвра, огневого поражения, разведки, связи и информационной войны.

в. Воздействия на возможности угроз, направленных на атаку систем командования и управления и связанных с ними систем поддержки принятия решений.

г. Воздействия на возможности угроз, связанных с распространением, публикацией или передачей информации, направленной на убеждение соответствующих субъектов в необходимости противодействия операциям сухопутных войск.

д. Обеспечения появления у противника дезинформации, направленной против средств принятия решений, сбора разведывательных сведений и информации, связи, распространения информации, а также командования и управления.

е. Обеспечения безопасности своих операций для защиты критически важной информации.

ж. Обеспечения проведения своих действий по оказанию влияния, таких как операции по информационной поддержке, для улучшения или поддержания позитивных отношений с иностранными субъектами в операционной зоне и вокруг неё, а также для ослабления влияния угроз на эти субъекты.

з. Защиты своей информации, технических сетей и возможностей принятия решений от использования противником и неприятелем средств информационной войны.

ГЛАВА 3. СТРУКТУРНЫЕ ПОДРАЗДЕЛЕНИЯ, КОМАНДОВАНИЕ И УПРАВЛЕНИЕ

Глава охватывает аспекты обеспечения действий в киберпространстве и при ведении радиоэлектронной борьбы, доступные командирам сухопутных войск. В ней описаны роли, обязанности и возможности Киберкомандования сухопутных войск США и подчинённых ему частей и подразделений. Подробно представлена организация и действия отделения кибер-электромагнитной деятельности, его роли и обязанности. Рассматриваются аспекты взаимодействия отделения кибер-электромагнитной деятельности с другими структурными подразделениями штаба и объясняется роль рабочей группы кибер-электромагнитной деятельности.

3.1. Организационная структура киберподразделений сухопутных войск

3-1. Кибероперации и РЭБ позволяют командирам сухопутных войск понимать и владеть оперативной обстановкой, обеспечивать принятие решений и воздействовать на противника. Командиры на уровне бригадной тактической группы и выше полагаются на подчинённые им отделения СЕМА для эффективного использования возможностей сухопутных войск и совместных кибервозможностей и возможностей РЭБ.

Во время совместных боевых действий (операций) корпус или дивизия, определённая как межвидовая оперативно-тактическая группа или как штаб объединённых сил выстраивает взаимодействие между подчинённым начальником группы управления в ЭМС и отделением СЕМА в целях создания группы управления операциями в ЭМС (*англ. electromagnetic spectrum operations,* E*MSO*) для обеспечения группы управления объединёнными операциями в ЭМС (*англ. joint electromagnetic spectrum operations cell, JEMSOC*).

Многочисленные по составу сухопутные войска и объединённые части и подразделения выделяют силы и средства для использования в кибероперациях и ведения РЭБ. Командиры на уровне корпусов и ниже должны иметь общее представление о роли и обязанностях этих частей и подразделений, каким образом они взаимодействуют с отделениями СЕМА.

3-2. В данном разделе представлен обзор структурных подразделений сухопутных войск, обеспечивающих кибероперации и ведение РЭБ в интересах командиров сухопутных войск. Раздел описывает командование силами и средствами кибероперациий сухопутных войск – Киберкомандование сухопутных войск США (*United States Army Cyber Command, ARCYBER*) и подчинённые ему части и подразделения.

3.1.1. Киберкомандование сухопутных войск

3-3. Киберкомандование сухопутных войск использует и защищает военные сети и воздействует на киберпространство противника в целях защиты государства. Киберкомандование сухопутных войск быстро разрабатывает и внедряет средства воздействия на киберпространство в интересах своих войск для будущей борьбы со стойким и адаптивным противником. Киберкомандование сухопутных войск также объединяет разведывательные действия, огневое обеспечение, космические, психологические операции, стратегические коммуникации, работу с общественностью, специальные технические операции, кибероперации, РЭБ и информационные операции, что позволяет командирам сухопутных войск обладать преимуществом в принятии решений во время учений и боевых действий.

3-4. Киберкомандование сухопутных войск защищает информационную сеть министерства обороны-СВ через проведение ОКбО-ВМО и операций в информационной сети министерства обороны. Командующий Киберкомандованием сухопутных войск также является начальником штаба объединённых сил в киберпространстве (*англ. joint force headquarters-cyber, JFHQ-C [Army]*). В этой роли он обладает возможностью проводить НКбО для атаки и развития успеха против противника с разрешения Киберкомандования США (*англ. Unites States Cyber Command, USCYBERCOM*). Киберкомандование СВ – это связующее звено сухопутных войск, куда поступают доклады и оценки киберинцидентов и событий, связанных с предполагаемой деятельностью противника. Командование сетевых технологий СВ (*англ. United States Army Network Enterprise Technology Command, NETCOM*) и региональный киберцентр действуют как главные оперативные рода войск, получив от Киберкомандования СВ полномочия по оперативному управлению силами и средствами и руководству кибероперациями в рамках операций информационной сети МО над всеми сетями сухопутных войск. Киберкомандование СВ выступает в качестве основной службы по кибербезопасности сухопутных войск и обеспечивает надзор за реализацией программы, в то время как Командование сетевых технологий и региональные киберцентры выступают в качестве основных исполнителей программы. Части и подразделения, подчиняющиеся Киберкомандованию сухопутных войск:

- Командование сетевых технологий СВ;
- 1-е управление информационных операций (наземное);

- 780-я бригада военной разведки;
- бригада киберзащиты;
- 915-й батальон кибероперaций.

3.1.2. Центр информационных операций сухопутных войск

3-5. Центр информационных операций сухопутных войск (*англ. Army Information Warfare Operations Center*, *AIWOC*) служит ключевым хабом Киберкомандования СВ для взаимодействия, интеграции, согласования и отслеживания кибероперaций, РЭБ, информационных операций и ответов на запросы разведки в поддержку национальных, региональных указаний и указаний сухопутных войск. Центр информационных операций сухопутных войск обеспечивает глобальную и региональную ситуативную осведомлённость, осуществляя управление выполнением задачи всеми подчинёнными и приданными силами кибер- и информационных операций сухопутных войск.

3-6. Центр информационных операций сухопутных войск состоит из личного состава, обладающего знаниями в области информационного обеспечения (информационные операции, кибероперации, РЭБ, психологические операции, работа с общественностью и гражданскими организациями, дезинформация, л/с Космического командования США и подразделений специальных технических операций), включая представителей всех штабных структурных подразделений и командированных из смежных учреждений и организаций. Центр информационных операций сухопутных войск отвечает за интеграцию информационных возможностей штаба в процессы текущих боевых задач и планов командования. Кроме того, Центр информационных операций сухопутных войск:

- получает доклады от подчинённых органов управления;
- готовит доклады для вышестоящих штабов;
- обрабатывает запросы на поддержку (*англ. requests for support, RFS*);
- издаёт боевые приказы (*англ. operation order, OPORD*) и приказы о задачах в киберпространстве (*англ. cyber tasking order, CTO*);
- консолидирует потребности командующего в критической информации;
- отвечает на запросы о предоставлении информации из вышестоящих штабов, боевых командований, других видов (служб) вооружённых сил и ведомств;
- оценивает общий ход текущих операций.

3.1.1.1. Командование сетевых технологий сухопутных войск

3-7. Командование сетевых технологий СВ осуществляет руководство глобальными операциями в интересах части информационной сети МО, находящейся под управлением сухопутных войск, обеспечивая свободу действий в киберпространстве и препятствуя в этом противнику.

Командование сетевых технологий СВ обеспечивает безопасность, снабжение и работу, формирует, расширяет и использует информационную сеть министерства обороны – сухопутные войска. Командование сетевых технологий СВ всецело развивает ОКбО-ВМО, создавая и сохраняя их конфиденциальность, доступность и целостность. Ключевая задача Командования сетевых технологий СВ охватывает все аспекты несекретной и секретной сетевой передачи, обмена и хранения данных. Оперативный центр информационной сети МО Командования сетевых технологий СВ осуществляет командование и управление, контролирует оперативную согласованность, обеспечивает непрерывный мониторинг в режиме реального времени и отчётность о глобальных операциях информационной сети МО в интересах видов (служб) вооружённых сил и объединённых сил в целях обеспечения их возможностями влиять на ход боевых действий (операций), а также обеспечивает обнаружение и решение проблем во всей глобальной сети.

3-8. Региональные киберцентры постоянно проводят операции в информационной сети МО и обеспечивают ОКбО-ВМО по информационной сети МО-СВ, обеспечивая свободу действий сухопутных войск и объединённых сил в киберпространстве и лишая противника такой возможности. Региональные киберцентры размещены в континентальной части США, Европе, Республике Корея, Тихоокеанском регионе и Юго-Западной Азии для обеспечения непрерывного и бесперебойного обслуживания на каждом театре военных действий. Региональные киберцентры являются контактным пунктом для частей и подразделений сухопутных войск, куда можно сообщить о киберинцидентах. Региональные киберцентры несут полную ответственность за обеспечение безопасности информационной сети МО-СВ.

3.1.1.2. Бригада киберзащиты

3-9. Бригада киберзащиты обеспечивает оборону ключевых областей в киберпространстве, сдерживая угрозы и оказывая воздействие, обеспечивающее свободу действий своих войск и лишающее её противника. Бригада киберзащиты отвечает за организацию, подготовку, оснащение, постановку задач и развёртывание групп киберзащиты (*англ. cyber protection team*, *CPT*) по всему миру для усиления подразделений поддержки (обеспечения), по штату входящих в подразделения защиты информационных сетей в ходе боевых действий (операций) и учений, а также для оценки готовности частей и подразделений к киберзащите и оказания им помощи. Командир бригады киберзащиты имеет право в соответствии с инструкцией выполнять задачи ОКбО-ВМО, включая действия по защите киберпространства, для возобновления и восстановления безопасности утраченного, скомпрометированного в отношении безопасности или находящегося под другой угрозой «голубого киберпространства».

3.1.1.3. 915-й батальон кибероперaций

3-10. 915-й батальон кибероперaций – это гибкий по структуре экспедиционный батальон сухопутных войск, состоящий из экспедиционных групп СЕМА (*англ. expeditionary CEMA team*, *ECT*). Экспедиционные группы СЕМА включают кибервойска, операторов СЕМА РЭБ, офицеров по информационным операциям, группу целеуказания и личный состав разведки. Личный состав разведки 915-го батальона кибероперaций собирает информацию для своих групп СЕМА и проводит анализ разведданных для поддержки и проведения операций экспедиционными группами СЕМА.

Киберкомандование СВ развёртывает экспедиционные группы СЕМА для обеспечения поддержки НКбО, ОКбО, информационных операций и РЭБ в интересах командований сухопутных войск. Экспедиционные группы СЕМА обладают возможностями проведения НКбО, ОКбО, РЭБ и информационных операций при поддержке боевых действий (операций) сухопутных войск. Некоторые операции СЕМА требуют разрешения и полномочий, делегированных Киберкомандованием США, командующими географическими боевыми командованиями или командирами с полномочиями по управлению радиоэлектронной борьбой.

915-й батальон кибероперaций относится только к сухопутным войскам и не входит в состав сил кибероперaций министерства обороны; однако все задачи по НКбО, проводимые 915-м батальоном, должны быть сначала утверждены и санкционированы Киберкомандованием США.

3.1.1.4. 1-е управление информационных операций

3-11. 1-е управление информационных операций – это формирование сухопутных войск в составе действующей структуры информационных операций. Это многосоставное соединение бригадного уровня, состоящее из штаба, штабного подразделения и двух батальонов.

Задача 1-го управления информационных операций заключается в обеспечении поддержки информационных операций и кибероперaций в интересах сухопутных войск и других видов вооружённых сил путём развёртывания групп, планирования и анализа, а также специальной подготовки.

3.1.1.5. 780-я бригада военной разведки (кибер)

3-12. 780-я бригада военной разведки (кибер) проводит кибероперации для нанесения поражающих воздействий противнику в интересах сухопутных войск и объединённых сил. Основной задачей 780-й бригады военной разведки является обеспечение и проведение кибероперaций.

Подразделения бригады пользуются полномочиями по постановке оперативных задач радио и радиотехнической разведки, делегированными командующим Киберкомандованием СВ, полномочиями разведки по сбору информации из открытых источников, делегированными командующим Командованием разведки и безопасности СВ, и многочисленными полномочиями по сбору информации в киберпространстве, делегированными командующим Киберкомандованием США для наблюдения и разведки в целях осуществления кибероперациий. Штаб предоставляет силы и средства для Киберкомандования СВ и национальных сил кибероперациий (*англ. cyber national mission force, CNMF*).

3.2. Структурные подразделения РЭБ

3-13. В данном разделе описаны структурные подразделения объединённых сил и сухопутных войск, находящиеся в распоряжении корпусов и ниже при ведении боевых действий (операций) объединённых сил и сухопутных войск. В нём представлены и рассмотрены взводы РЭБ из состава бригадных тактических групп. Раздел также включает обзор сводного подразделения разведки, информационных операций, кибероперациий, РЭБ и космических операций (*англ. Intelligence, Information, Cyber, EW, and Space, I2CEWS*), выделенного в многосферную оперативно-тактическую группу.

3.2.1. Взвод РЭБ (бригадная тактическая группа)

3-14. Взводы РЭБ входят в состав роты военной разведки инженерного батальона БТГ. Взвод РЭБ состоит из трёх отделений РЭБ, способных обеспечить поддержку РЭБ в ходе боевых действий. Хотя отделение CEMA согласовывает РЭБ и кибероперации с оперативным процессом оно должно взаимодействовать с отделом S-2 штаба БТГ для постановки задачи роте военной разведки на развёртывание средств взвода РЭБ для выполнения боевых задач РЭБ.

3-15. Взвод РЭБ ведёт РЭР с целью обнаружения и местоопределения источников излучений и радиоэлектронных средств противника в заданном районе операций с использованием средств обнаружения. Данные и информация, полученные в результате РЭР, обеспечивают командира информацией о боевой обстановке. Эти данные и информация также поддерживают управление боевыми действиями в ЭМС, обеспечивая непрерывной ситуативной осведомлённостью специалиста отделения CEMA для разработки и обновления общей картины оперативной электромагнитной обстановки. Взвод РЭБ также может проводить ЭМА для уничтожения и нейтрализации радиоэлектронных средств противника.

3-16. Получив полномочия на управление радиоэлектронным поражением (воздействием) от объединённой оперативно-тактической группы, командующий наземным компонентом объединённых сил (*англ. – Joint Force Land Component*

Commander, JFLCC) может далее передать полномочия на управление радиоэлектронным поражением (воздействием) подчинённым командирам сухопутных войск. Полномочия по управлению радиоэлектронным поражением (воздействием) – это более широкое развитие полномочий по постановке помех, позволяющее подчинённым командирам передавать или прекращать передачу электромагнитной энергии.

Полномочия по управлению радиоэлектронным поражением (воздействием) позволяют командирам контролировать боевые задачи ЭМА, проводимых в их районах операций, в рамках ограничений, накладываемых вышестоящими штабами. Перед получением полномочий на воздействие в ЭМС командиры должны убедиться в полноте владения ситуативной осведомлённостью об оперативной электромагнитной обстановке, оперативным контролем возможностей РЭБ и способностью контролировать и оценивать степень воздействия РЭБ внутри своего района операции для определения корректирующих действий в случае необходимости. Командиры также должны убедиться, что задачи, выполняемые в рамках ведения РЭБ не нанесут поражения радиоэлектронным средствам своих войск. За управление спектром отвечает руководитель по управлению спектром G-6 или специалист по управлению спектром G-6 или S-6.

3-17. Взводы РЭБ улучшают приёмы и возможности имеющегося оборудования РЭБ в соответствии с сообщениями о воздействии на систему, полученными по каналам обеспечения технической поддержки военного оборудования, которые включают рекомендации по реагированию на выявленные угрозы. Командиры могут потребовать от взвода РЭБ немедленно внести изменения в свою тактику для восстановления или улучшения производительности оборудования РЭБ (см. приложение F для получения дополнительной информации об улучшении приёмов и возможностей РЭБ).

3.2.2. Подразделение разведки, информационных операций, кибероперации, РЭБ и космических операций

3-18. Подразделение разведки, информационных операций, кибероперации, РЭБ и космических операций представляет подразделение в размере батальона в составе многосферной оперативно-тактической группы и включающее усиленное отделение СЕМА. Оно обеспечивает поддержку кибероперации и РЭБ в интересах командования силами и средствами сухопутных войск, группировки сухопутных войск на ТВД или объединённой оперативно-тактической группы, осуществляющей совместные высокоточные удары большой дальности в ходе многосферных операций. В состав подразделения входят четыре роты, состоящие из кибервойск, способных осуществлять ОКбО-ВМО на уровне вида ВС, и операторов РЭБ, способных оказывать воздействия через ЭМА на всей территории назначенного района операции для многосферной оперативно-тактической группы.

3-19. Подразделение разведки, информационных операций, кибероперaций, РЭБ и космических операций имеет штатные средства зондирования и разведки, информации и космических операций, которые при интеграции и согласовании с ОКбО-ВМО и РЭБ позволяют сухопутным войскам одновременно защищать свою назначенную часть информационной сети МО-СВ, нарушая, воспрещая и ухудшая возможности противника в ЭМС. Структура подразделения разработана с учётом постоянно меняющейся оперативной обстановки, когда объединённые операции проводятся совместно и одновременно в нескольких сферах.

3.3. Кибер-электромагнитная деятельность на уровне корпуса и ниже

3-20. Отделения CEMA на уровне армейских корпусов, дивизий, бригадных тактических групп и бригад армейской авиации подчиняются структуре G-3 или S-3 штаба. Командиры несут ответственность за внедрение отделениями CEMA кибероперaций и РЭБ в их замысел операции. Отделение CEMA привлекает основный личный состав штаба к деятельности в рабочей группе CEMA для оказания помощи в планировании, разработке, интеграции и согласовании кибероперaций и РЭБ.

Примечание:

> Структура отделения CEMA одинаковая во всех армейских корпусах и нижестоящих звеньях. Тем не менее, 1-е управление информационных операций может усилить отделение CEMA на уровне армейского корпуса, чтобы обеспечить расширенные возможности для согласования и интеграции кибероперaций и РЭБ с информационными операциями (см. главу 4).

3.3.1. Роль командира

3-21. Командиры руководят непрерывной интеграцией кибероперaций и РЭБ в оперативном процессе как в боевой обстановке, так и в пункте постоянной дислокации. Максимально используя кибероперации и РЭБ в рамках совместных действий всех родов войск, командиры способны ощущать, понимать, принимать решения, действовать и оценивать быстрее, чем это делает противник, и добиваться преимущества в принятии решений в многообразии существующих сфер в ходе ведения боевых действий.

3-22. Командир обязан:

- включать кибероперации и РЭБ в оперативный процесс.
- постоянно внедрять стандарты кибербезопасности, техническое и административное управление.
- понимать, предвидеть и учитывать поражающие возможности, трудности и ограничения киберпространства и РЭБ, поражающие возможности второго и третьего порядка.

- понимать правовые и оперативные полномочия для воздействия на части киберпространства или ЭМС, представляющих угрозу.
- понимать влияние кибероперациий и ведения РЭБ на боевую задачу и схему манёвра.
- понимать, как выбранный вариант действий (англ. *course of action, COA*) влияет на приоритезацию ресурсов в их части информационной сети МО-СВ.
- использовать инструменты воздействия в киберпространстве и в ЭМС для обеспечения замысла операции.
- разрабатывать и обеспечивать замысел и руководство действиями и поражающими факторами внутри и вне информационной сети МО-СВ.
- поэтапно определять критически важные задачи, чтобы обеспечить возможность определения ключевой области в киберпространстве.
- обеспечивать активное взаимодействие между штабами, подчинёнными частями и подразделениями, вышестоящими штабами и другими участниками совместных действий, что обеспечит общее понимание места каждого в киберпространстве и ЭМС.
- утверждать приоритетные цели, их обозначение, очерёдность сбора и меры по снижению рисков.
- обеспечивать согласованность операций в киберпространстве и действий РЭБ с другими подразделениями, обладающими большой огневой мощью и нелетальными средствами для обеспечения замысла операции.
- контролировать развитие кибероперациий и подготовку подразделений РЭБ в пункте постоянной дислокации.

3.3.2. Отделение кибер-электромагнитной деятельности

3-23. Отделение кибер-энергетической деятельности (далее – отделение CEMA) осуществляет планирование, взаимодействие и интеграцию НКбО, ОКбО и действий РЭБ в интересах замысла командира. Отделение CEMA взаимодействует с различными структурными подразделениями штаба для обеспечения единства действий по достижению общих оперативных целей командира, например, с G-2 или S-2 для достижения ситуативной осведомлённости об окружающей обстановке и понимания места войск противника, своих войск и положения нейтральных субъектов, действующих в районе операций. Отделение CEMA отвечает за регулярное представление командиру и штабу обновлённой информации о НКбО и других операциях, проводимых в районе операций. Отделение CEMA отвечает за согласование и интеграцию кибероперациий и РЭБ с оперативным процессом и другими интеграционными процессами.

В состав отделения СЕМА входят:

- офицер по кибервойне и РЭБ;
- офицер по кибервойне;
- специалист РЭБ;
- сержант-майор РЭБ (в корпусе) или первый сержант РЭБ (в дивизии);
- сержант РЭБ;
- специалист по управлению спектром СЕМА.

3.3.2.1. Офицер по кибервойне и РЭБ

3-24. Офицер по кибервойне и РЭБ (*англ. – cyber electromagnetic warfare officer*, *CEWO*) – это назначенный командиром офицер штаба, ответственный за интеграцию, взаимодействие и согласованность действий в киберпространстве и ЭМС. Он отвечает за понимание всех задействованных засекреченных и несекретных принципов в отношении киберпространства и спектра, и оказывает командиру поддержку в планировании, взаимодействии и согласовании кибероперaций, РЭБ и СЕМА. Командир, которому были переданы полномочия по управлению РЭБ из вышестоящего штаба, может дополнительно передать их офицеру по кибервойне и РЭБ. Конкретные роли и обязанности офицера по кибервойне и РЭБ см. в ATP 3-12.3.

Задачи офицера по кибервойне и РЭБ:

- выдача рекомендаций командиру по вопросам поражающих факторов в киберпространстве (включая связанные с этим правила ведения боевых действий, поражающие факторы и ограничения) во взаимодействии с военным юристом штаба;
- выдача рекомендаций командиру в отношении рисков боевой задачи, связанными с возможными уязвимостями в киберпространстве и РЭБ, а также возможностей противника;
- анализ оперативной обстановки для понимания того, как она повлияет на операции в киберпространстве и ЭМС;
- разработка и поддержание сводной матрицы синхронизации целей в киберпространстве и РЭБ, и рекомендация целей для размещения в матрице синхронизации целей подразделений;
- оказание помощи g-2 или s-2 в разработке и управлении боевым порядком в ЭМС;
- выполнение функций органа управления ЭМА при выполнении задач РЭБ по указанию командира;

- выдача рекомендаций командиру по вопросам поражающих факторов киберпространства и РЭБ, и каким образом они могут повлиять на оперативную обстановку;
- приём и интеграция войск РЭБ и кибервойск и связанных с ними возможностей в операции;
- взаимодействие с вышестоящим штабом для поддержки НКбО и РЭБ по утверждённым целям;
- выдача рекомендаций по проведению кибероперации и представление критических информационных требований командира по РЭБ;
- подготовка и обработка всех запросов на поддержку в киберпространстве и РЭБ;
- контроль за ходом и выполнением кибероперации и подготовкой личного состава РЭБ в пункте постоянной дислокации;
- предоставление инструкции и руководства для применения штатных и приданных средств кибероперации и РЭБ;
- постановка задач для всех назначенных средств РЭБ.

3.3.2.2. Офицер по кибервойне (корпус и бригада) или офицер по кибероперациям (дивизия)

3-25. Офицер по кибервойне (корпус и бригада) или офицер по кибероперациям (дивизия) оказывает помощь офицеру по кибервойне и РЭБ во внедрении и согласовании кибероперации в оперативном процессе и обеспечивает правильное понимание возможностей киберпространства. Офицер по кибервойне или офицер по кибероперациям в целях поражающего воздействия при проведении наступательных кибероперации осуществляет взаимодействие с офицером по кибервойне и РЭБ в рамках предварительного анализа и обработки потенциальных целей, полученных от подчинённых подразделений.

Офицер по кибервойне или офицер по кибероперациям:

- помогает офицеру по кибервойне и РЭБ по вопросам внедрения, взаимодействия и согласования кибероперации и РЭБ с боевыми действиями;
- представляет информацию в интересах офицера по кибервойне и РЭБ о последствиях кибероперации, включая соответствующие правила ведения боевых действий, поражающие факторы и ограничения, используемые для помощи командиру;
- помогает офицеру по кибервойне и РЭБ в разработке и ведении матрицы синхронизации целей в киберпространстве и назначении целей для наступательных кибероперации для утверждения командиром;

- помогает офицеру по кибервойне и РЭБ в мониторинге и оценке показателей эффективности и результативности при обновлении результатов воздействий кибероперациий на оперативную обстановку;
- помогает офицеру по кибервойне и РЭБ в запросе и взаимодействии для поддержки наступательных кибероперациий наряду со внедрением полученных сил кибероперациий в боевые действия;
- координирует с другими участниками совместных действий возможности в киберпространстве, которые дополняют или расширяют положение кибероперациий подразделения;
- взаимодействует со структурными подразделениями штаба G-2 или S-2 и с G-6 или S-6 в рамках кибероперациий;
- разрабатывает и внедряет подготовку по кибероперациям и РЭБ в ППД.

3.3.2.3. Специалист РЭБ

3-26. Специалист РЭБ (*англ. Electromagnetic Warfare Technician*, *EWT*) является критически важным элементом для отделения СЕМА и взвода РЭБ, поскольку они выступают в качестве постоянных технических и тактических экспертов на всех уровнях. Специалист РЭБ оказывает поддержку в достижении целей выполняемой боевой задачи, осуществляя взаимодействие, интеграцию и согласование поражающих факторов СЕМА для получения и использования преимущества над противниками как в киберпространстве, так и в ЭМС, одновременно препятствуя и ухудшая использование тех же возможностей неприятелем и противником. По особым функциональным обязанностям специалиста РЭБ см. документ АТР 3-12.3.

Специалист РЭБ:

- исполняет обязанности офицера по кибервойне и РЭБ или командира взвода РЭБ, в случае вакантной должности;
- исполняет обязанности проверяющего при подготовке по РЭБ в подразделении;
- обеспечивает и участвует в разработке штабом текущей оценки СЕМА;
- оказывает помощь в разработке электромагнитного боевого порядка противника и управлении им. Внедряет электронные технические данные об угрозах, идентифицированные в электромагнитном боевом порядке, в рамках процесса разведывательной подготовки района боевых действий;
- консультирует по техническому и тактическому применению систем РЭБ объединённых сил и сухопутных войск и внедряет РЭБ в процесс целеуказания;

- помогает офицеру по кибервойне и РЭБ с рекомендуемыми средствами РЭБ в соответствии с вариантом действий, которые соответствуют задаче каждого подразделения РЭБ;
- координирует информацию целеуказания и согласовывает действия ЭМА и ЭМП со специалистами разведки (G-2 или S-2);
- помогает специалисту по управлению спектром (G-6 или S-6) с техническими данными ЭМЗ для улучшения контроля излучений для подразделения;
- проводит, поддерживает и обновляет данные об электромагнитной обстановке;
- определяет поражающие электромагнитные факторы противника и своих войск;
- помогает офицеру по защите сил в разработке мер по смягчению последствий для беспилотных авиационных систем при использовании средств РЭБ;
- помогает в разработке и распространении стандартных операционных процедур (*англ. standard operating procedures*, *SOPs*) и боевых учений во всём подразделении.
- консультирует и контролирует приобретение средств РЭБ, включая непрограммное записывающее оборудование;
- контролирует обслуживание штатных средств РЭБ;
- помогает офицеру по кибервойне и РЭБ в подготовке и обновлении приложения по РЭБ к оперативным распоряжениям;
- помогает в разработке и применении стандартов выбора целей для РЭБ;
- разрабатывает и реализует концепции и процедуры РЭБ для поддерживаемых подразделений;
- планирует, организует, внедряет, контролирует и оценивает операции и среду угроз в интересах офицера кибервойск и РЭБ;
- запрашивает и проводит оценку боевого ущерба в результате воздействия РЭБ.

3.3.2.4. Сержант-майор РЭБ (корпус) или первый сержант РЭБ (дивизия)

3-27. Сержант-майор РЭБ или первый сержант РЭБ является старшим военным помощником офицера по кибервойне и РЭБ по вопросам радиоэлектронной борьбы. Он помогает офицеру по кибервойне и РЭБ и офицеру по кибероперациям в вопросах внедрения, взаимодействия и проведения кибероперациий, а также РЭБ. Сержант-майор РЭБ или первый сержант РЭБ представляет офицеру по кибервойне и РЭБ исходные данные о действиях РЭБ и связанных с ними последствиями в районе операций. Он помогает специалисту РЭБ в обновлении и управлении электромагнитным боевым порядком.

3-28. Сержант-майор РЭБ или первый сержант РЭБ помогает офицеру по кибервойне и РЭБ и офицеру по кибероперациям в разработке и обновлении матрицы синхронизации целей в киберпространстве, в частности, целей, связанных с РЭБ, и помогает назначать цели ЭМА для утверждения командиром. Сержант-майор РЭБ или первый сержант РЭБ представляет информацию офицеру по кибервойне и РЭБ о том, как поражающие факторы РЭБ могут повлиять на оперативную электромагнитную обстановку. Конкретные роли и обязанности сержанта-майора РЭБ и первого сержанта РЭБ см. в Наставлении ATP 3-12.3.

3-29. Сержант-майор РЭБ и первый сержант РЭБ взаимодействует со специалистом РЭБ в вопросах разработки и реализации подготовки РЭБ в ППД. Разработка обучения ведения РЭБ является основной обязанностью сержанта-майора РЭБ. Он оценивает все аспекты подготовки по РЭБ и проводит аттестацию инструкторов в подчинённых подразделениях. Сержант-майор РЭБ следит за тем, чтобы обучение по РЭБ было организовано надлежащим образом, отражало современную методологию и соответствовало требованиям сухопутных войск.

3.3.2.5. Сержант РЭБ

3-30. Сержант РЭБ (*англ. EW noncommissioned officer*, *EW NCO*) управляет наличием и использованием средств РЭБ, закреплённых за подразделением. Сержант РЭБ является старшим разработчиком методики подготовки подразделения для ведения РЭБ. Он собирает и хранит данные для исследований электромагнитной энергии, а также эксплуатирует и обслуживает средства РЭБ. Сержант РЭБ оказывает поддержку специалисту по управлению спектром СЕМА в организации работы по оптимальному использованию радиочастотного спектра. Сержант РЭБ координирует с G-2 или S-2 разработку и проведение интегрированных тренировок по РРТР и ЭМП для личного состава РЭБ. Когда командир или офицер по кибервойне и РЭБ обладают полномочиями по управления ЭМА сержант РЭБ оказывает поддержку в управлении средствами РЭБ во время боевых действий (операций). Сержант РЭБ помогает сержанту-майору РЭБ или первому сержанту РЭБ в проведении подготовки по РЭБ в ППД.

3.3.2.6. Специалист по управлению спектром СЕМА

3-31. Специалист по управлению спектром СЕМА оказывает поддержку отделению СЕМА в планировании, взаимодействии, оценке и внедрении РЭБ посредством организации работы с радиочастотами. Он определяет оперативную электромагнитную обстановку для отделения СЕМА. Специалист по управлению спектром СЕМА:

- докладывает об электромагнитных помехах, обнаруженных операторами РЭБ, руководителю или специалисту по управлению спектром подразделения G-6 или S-6. Загружает доклады в онлайн сеть объединённых докладов о вмешательстве в спектр.

- совместно со специалистом по управлению спектром G-6 или S-6 обеспечивает использование радиочастотного спектра во время боевых действий (операций) с помощью РЭБ.
- помогает специалисту РЭБ в разработке и управлении электромагнитным боевым порядком.
- согласовывает частоты, используемые в РЭБ и кибероперациях для защиты радиочастот, используемых своими войсками во взаимодействии со специалистом по управлению спектром G-6 или S-6.
- докладывает руководителю или специалисту по управлению спектром G-6 или S-6 об электромагнитных помехах от систем РЭБ для снижения негативных последствий.
- определяет способность средств РЭБ обслуживать спектр и обеспечивать частотно-технологическую поддержку.
- ведет частотные карты, диаграммы и доклады об инцидентах электромагнитных помех, обнаруженных при выполнении задач РЭБ.
- оказывает поддержку офицеру по кибервойне и РЭБ в вопросах отдачи руководящих указаний в подразделении для устранения конфликтов и урегулирования электромагнитных помех между системами РЭБ и другими системами своих войск.

3.3.3. Рабочая группа CEMA

3-32. Отделение CEMA возглавляет рабочую группу CEMA. Рабочая группа CEMA не является официальной рабочей группой, для которой требуются специально обученный личный состав из других подразделений. При необходимости, для реализации замысла операции рабочая группа CEMA оказывает поддержку офицеру по кибервойне и РЭБ в плане взаимодействия и внедрения кибероперациий и РЭБ. Отделение CEMA обычно взаимодействует с ключевыми командирами во время штабных совещаний, проводимых в рамках режима боевой работы подразделения, и на протяжении всего оперативного процесса. Участие в рабочей группе CEMA варьируется в зависимости от требований к боевой задаче.

3-33. Рабочая группа CEMA должна быть интегрирована в режим боевой работы штаба, при необходимости. Она отвечает за взаимодействие по горизонтали и вертикали для поддержки боевых действий и оказания помощи группе огневого обеспечения на всём протяжении выполнения задачи. Как правило, рабочая группа CEMA состоит из представителей подразделений штаба и обычно включает:

- представителя G-2 или S-2;
- представителя G-6 или S-6;
- офицера по информационным операциям или представителя;

- специалиста по управлению спектром G-6 или S-6;
- офицера управления огневой поддержкой или представителя группы огневой поддержки;
- юриста штаба;
- офицера охраны.

3.3.4. Штаб и обеспечение на уровне корпуса и ниже

3-34. В ходе оперативного процесса и связанных с ним интеграционных процессов кибероперации и РЭБ требуют совместных и согласованных усилий с другими ключевыми специалистами. Структурное подразделение G-6 или S-6 контролирует операции в информационной сети МО, специалист по управлению спектром G-6 или S-6 осуществляет взаимодействие со специалистом по управлению спектром отделения СЕМА для согласования операций управления спектром с РЭБ. Структурное подразделение G-2 или S-2 руководит внедрением и согласованием процесса разведывательной подготовки района боевых действий и сбора информации. Офицер по информационным операциям контролирует внедрение и согласование информационных возможностей, связанных с информационными операциями. Юрист штаба консультирует командира по вопросам законности операций.

3.3.4.1. Помощник начальника штаба по разведке

3-35. Структурное подразделение G-2 или S-2 представляет разведданные для поддержки СЕМА. G-2 или S-2 способствует пониманию сложившейся обстановки с противником и других параметров операции и задачи. Личный состав G-2 или S-2 оказывают прямую или косвенную поддержку кибероперациям и РЭБ через сбор информации, обеспечения понимания ситуации и поддержки целеуказания и информационных операций.

Дополнительно G-2 или S-2 осуществляет обеспечение СЕМА путём:

- оценки разведывательных данных и планов СЕМА, контроля за сбором и анализом информации для поддержки разведывательной подготовки района боевых действий, разработки целей, оценки варианта действий противника и ситуативной осведомлённости;
- постоянного мониторинга разведывательных операций и взаимодействия разведки с вышестоящими, нижестоящими и подчинёнными уровнями;
- координации радио и радиотехническая разведки;
- координации разведки и местных правоохранительных органов для укрепления безопасности киберпространства;

- руководства разведывательной подготовкой района боевых действий и развития её результатов;
- контроля за развитием и управлением электромагнитным боевым порядком;
- предоставления для СЕМА разведывательной информации из всех источников;
- координации с G-3 или S-3 и группой огневого обеспечения для определения важных целей из списка приоритетных целей в соответствии с вариантом действий для каждого подразделения;
- взаимодействия с разведывательным ведомством для подтверждения кибератак или ЭМА противника в оперативной обстановке;
- запроса разведывательного обеспечения и взаимодействия с разведывательной ведомством и местными правоохранительными органами для сбора оперативной информации по угрожающим кибероперациям и РЭБ в оперативной обстановке;
- предоставления информации и разведданных об угрозах в киберпространстве и характеристиках РЭБ, которые облегчают понимание ситуации и способствуют принятию решений;
- взаимодействия с военными метеорологами ВВС для уточнения обстановки на местности и погодных условий с целью уточнения ситуативной осведомлённости;
- обеспечения планов и операций по сбору информации для поддержки разработки целей СЕМА, требований по обновлению целей и оценки боевых действий;
- подготовки запросов на получение информации и её сбор для удовлетворения потребностей, превышающих возможности штатной разведки подразделения;
- сбора, обработки, хранения, отображения и распространения информации о кибероперациях и РЭБ на протяжении всего оперативного процесса и через системы командования и управления;
- объединения всех важных целей в списке приоритетных целей;
- предоставления информации (исходных данных) о защищаемых частотах от разведывательной службы;
- предоставления отделению СЕМА и G-6 или S-6 приоритетных требований по использованию ЭМС для разведывательных операций;
- участия в качестве члена рабочей группы СЕМА;
- оказания помощи специалисту по управлению спектром СЕМА в снижении электромагнитных помех и устранения конфликтных ситуаций в ЭМС, а также определении источника недопустимых электромагнитных помех.

3.3.4.2. Помощник начальника штаба по связи

3-36. Во взаимодействии с объединёнными силами и другими участниками совместных действий (в зависимости от обстоятельств) личный состав G-6 или S-6 прямо или косвенно обеспечивает кибероперации, проводя операции в информационной сети МО. G-6 или S-6 является основным представителем штаба, отвечающим за операции по управлению спектром.

Подразделение G-6 или S-6 осуществляет обеспечение СЕМА путём:

- создания тактической части информационной сети МО-СВ, известной как тактическая сеть, на уровне ТВД и ниже;
- проведения операций в информационной сети МО, включая обеспечение кибербезопасности, для удовлетворения потребностей частей и подразделений в средствах связи;
- оказания помощи в определении характеристик киберугроз, характерных для действий противника, и связанных с ними возможностей в рамках своих сетей, а также консультирования по выбранному варианту действий для кибероперациий;
- проведения оценок рисков кибербезопасности на основе тактики, методов и процедур противника или неприятеля, выявления уязвимостей в критически важной инфраструктуре, которые могут потребовать мер защиты, превышающих возможности подразделения и требующих поддержки ОКбО-ВМО;
- участия в деятельности рабочей группы СЕМА;
- обеспечения общей оперативной картины информационной сети МО для планирования и ситуативной осведомлённости;
- предоставления предметной экспертизы в отношении проводных и беспроводных сетей;
- обеспечения конфигурации, реализации и мониторинга мер безопасности в информационной сети МО-СВ на основе докладов об угрозах;
- надзора за операциями по управлению спектром;
- реализации многоуровневой безопасности путём использования инструментов для обеспечения многоуровневой кибербезопасности и контроля подготовки по вопросам безопасности в части или подразделении;
- взаимодействия с региональным киберцентром для понимания и соблюдения всех положений и процедур кибероперациий в регионе;
- запроса доступа к спутникам и шлюзам через региональный центр спутниковой связи;
- взаимодействия с региональным сетевым концентратором для установления сетевого подключения и услуг доступа.

3.3.4.3. Офицер (корпус и дивизия) по информационным операциям или представитель (бригада и ниже)

3-37. Офицер по информационным операциям или представитель возглавляет отделение информационных операций в части или подразделении. Он вносит свой вклад в разведывательную подготовку района боевых действий, выявляя и оценивая противника в районе операций. Офицер по информационным операциям или представитель разбирается в вопросах взаимосвязи командования с подразделениями, имеющими информационные возможности, и строит взаимодействие с ними соответствующим образом. Он взаимодействует с этими подразделениями по информационным вопросам, чтобы определить пути оптимизации воздействия информационных средств на другие информационные средства путём их согласования. Офицер по информационным операциям или представитель руководит планированием, согласованием и использованием сил и средств, связанных с информацией, которые не управляются владельцем или представителем этих сил и средств. Офицер по информационным операциям или представитель осуществляет взаимодействие с отделением СЕМА в рамках внедрения кибероперациий и РЭБ в информационные операции.

Офицер по информационным операциям или представитель:

- возглавляет рабочую группу по информационным операциям;
- определяет наиболее эффективные информационные силы и средства для достижения целей командира;
- согласовывает кибероперации и РЭБ с другими информационными ресурсами для достижения целей командира в информационной среде;
- оценивает риск задачи и риск для войск в рамках кибероперациий, РЭБ и задействования других информационных возможностей во взаимодействии с отделением СЕМА;
- выявляет недостатки в информационных ресурсах, не устранимые на уровне части или подразделения;
- осуществляет взаимодействие с сухопутными войсками, видами ВС или объединёнными силами по вопросам информационного обеспечения для восполнения недостающих возможностей частей и подразделений;
- обеспечивает информацией, по мере необходимости, в интересах безопасности операции на уровне части или подразделения;
- осуществляет взаимодействие с отделением СЕМА по выполнению задач управлением киберпространством и задач дезинформации по ЭМА для введения в заблуждение;

- оценивает эффективность и вносит изменения в план использования информационных возможностей;
- разрабатывает материалы, описывающие все военные и гражданские инфраструктуры связи и каналы связи в районе операций во взаимодействии с G-2 или S-2;
- определяет местоположение и описывает все системы в ЭМС и излучатели в оперативной электромагнитной обстановке во взаимодействии с G-2 или S-2, отделением CEMA и другими владельцами информационных ресурсов;
- выявляет сетевые уязвимости своих войск, нейтральных субъектов и противника во взаимодействии с G-2 или S-2, отделением CEMA и другими владельцами информационных ресурсов;
- обеспечивает понимание информационных условий в оперативной обстановке во взаимодействии с G- 2 или S-2;
- участвует в процессе принятия военных решений и разработке информационных требований, связанных с информационными операциями;
- принимает участие в деятельности рабочей группы CEMA;
- внедряет информационные операции в процесс целеуказаний подразделения;
- внедряет внештатные информационные силы и средства в операции;
- обеспечивает актуализацию информации в общей оперативной картине;
- осуществляет взаимодействие с координатором огневой поддержки по вопросам применения летальных и нелетальных поражающих средств.

3.3.4.4. Специалист по управлению спектром G-6 или S-6

3-38. Специалист по управлению спектром G-6 или S-6 согласовывает использование ЭМС для различных коммуникационных и электронных систем и ресурсов. Он осуществляет обеспечение CEMA путём:

- согласования ресурсов спектра в интересах подразделения;
- согласования использования спектра с вышестоящими штабами, странами пребывания и международными агентствами, по мере необходимости;
- согласования распределения, присвоения и использования частот;
- согласования ресурсов спектра для средств связи, используемых в целях проведения операций по дезинформации;
- взаимодействия со специалистом по управлению спектром вышестоящего штаба для ослабления электромагнитных помех, обнаруженных в части оперативной электромагнитной обстановки подразделения;

- обращения за помощью к вышестоящим штабным специалистам по управлению спектром для решения проблемы неустранимых внутрисетевых электромагнитных помех;
- участия в деятельности рабочей группы СЕМА.
- оказания помощи специалисту по управлению спектром СЕМА в устранении противоречий между требованиями для своего ЭМС с планируемыми операциями РЭБ, кибероперациями и сбором информации.
- взаимодействия со специалистом по управлению спектром СЕМА для внедрения и согласования операций по управлению спектром с РЭБ.

3.3.4.5. Группа огневой поддержки

3-39. Группа огневой поддержки планирует, взаимодействует, внедряет, согласовывает и организует текущее и последующее огневое обеспечение для достижения целей командира. Согласование огневой поддержки может включать взаимодействие с объединёнными силами и другими участниками совместных действий. Группа огневой поддержки координирует свои действия с отделением СЕМА для согласования, планирования и проведения кибератак и ЭМА в рамках процесса целеуказаний. Группа огневой поддержки обеспечивает действия СЕМА посредством:

- руководства рабочей группой целеуказаний и участия в процессе целеуказаний под руководством командира.
- оказания помощи G-2 или S-2 в согласовании плана сбора информации с кибероперациями, РЭБ и другими огневыми средствами.
- согласование объединённых, межорганизационных и многонациональных сил и средств, огневой поддержки и управления средствами обнаружения противорадиолокационных средств.
- представления командиру и штабу информации о состоянии развёрнутых РЛС подразделения, в том числе о зонах наблюдения каждой РЛС.
- внедрения и согласования кибероперaций и РЭБ с другими средствами огневой поддержки.
- взаимодействия с отделением СЕМА и подразделением G-2 или S-2 в разработке и управлении списком приоритетных целей, стандартами выбора целей, матрицей наведения и матрицей целеуказаний, которые включают цели кибератаки и ЭМА.
- планирования, обучения, выполнения и оценки всех аспектов огневой поддержки с учётом кибервоздействий и РЭБ, а также их отработки в ходе тренировок.

- разработки схемы ведения огня с командиром и G-3 или S-3, включающей кибероперации и РЭБ.
- рассмотрения целей из совместного списка целей, добавленных в список целей подразделения, для поражения которых требуются нештатные ресурсы.
- выработки рекомендаций по определению важных целей для включения их в список приоритетных целей.
- направления списка приоритетных целей подразделений в вышестоящие штабы для включения в совместный процесс целеуказания.
- предоставления исходных данных в план сбора информации.
- взаимодействия с G-2 или S-2 в рамках рекомендаций по целевой области (областей), представляющую интерес.
- участия в рабочей группе СЕМА.
- добавления кибератаки и ЭМА в матрицу синхронизации огневого поражения.
- предоставления требований к информации в качестве исходных данных для сбора информации.
- согласования средств разведки и наблюдения через процесс целеуказания в интересах определения предполагаемых целей для поддержки выполнения задач по приоритетным целям.
- взаимодействия с отделением СЕМА для разработки планов перемещения всех радиоэлектронных средств в рамках ЭМЗ, обеспечивая при этом постоянное перемещение РЛС подразделения для избежания обнаружения противником.

3.3.4.6. Юрист штаба

3-40. Юрист штаба является представителем начальника военно-юридической службы на местах и основным юридическим советником командира. Он также консультирует рабочую группу СЕМА по действующим нормам права и законности в отношении кибероперациий и РЭБ, особенно таких задач в киберпространстве и РЭБ, которые могут затрагивать интересы некомбатантов. Юрист штаба является экспертом подразделения по вопросам военного права, правил ведения боевых действий, защиты некомбатантов, обращения с задержанными, а также фискального и контрактного права, предоставляя командирам и личному составу важные материалы для разработки планов, директив и решений, связанных с применением летальных и нелетальных средств поражения целей. Юрист штаба поддерживает СЕМА посредством:

- контроля соблюдения норм и законов в киберпространстве и РЭБ.

- анализа потенциальных кибероперацій и РЭБ на основе соответствующих правовых норм и полномочий, предоставленных на национальном уровне и на уровне боевого командования.
- участия в деятельности рабочей группы CEMA для предоставления юридических консультаций по кибероперациям и РЭБ.
- участия в деятельности рабочей группы целеуказаний для обсуждения предлагаемых целей и во взаимодействии с другими участниками – обеспечения уверенности в действительности и значимости целей и законности способа атаки.

ГЛАВА 4. ВНЕДРЕНИЕ В ОПЕРАТИВНОМ ПРОЦЕССЕ

В данной главе рассматривается, каким образом отделение CEMA внедряет кибероперации и РЭБ в рамках оперативного процесса. В ней описываются четыре вида оперативного процесса и то, какой вклад вносит рабочая группа в каждый из них. В главе подробно описано, каким образом отделение CEMA и члены рабочей группы согласовывают кибероперации и РЭБ с процессами разведывательной подготовки района боевых действий, сбора информации, целеуказаний, управления рисками и управления знаниями.

4.1. Оперативный процесс

4-1. В армейскому корпусе и ниже планирование, согласование и внедрение кибероперацій и РЭБ осуществляются отделением CEMA во взаимодействии с основным личным составом штаба, которые формируют рабочую группу CEMA. Отделение CEMA является подразделением G-3 или S-3 и тесно взаимодействует с участниками рабочей группы CEMA для обеспечения единства усилий по выполнению задач командира. Внедрение и согласование кибероперацій и РЭБ:

- объединяет усилия сухопутных войск и объединённых сил по разработке, управлению, обеспечению безопасности и защите информационной сети МО.
- обеспечивает передачу информации, собранную в киберпространстве и ЭМС, соответствующим специалистам для обеспечения командира и штаб ситуативной осведомлённостью об оперативной обстановке, целеуказаниями и в качестве возможных разведданных.
- обеспечивает эффективное использование средств кибероперацій и РЭБ для сбора информации и целеуказания.
- обеспечивает надлежащее взаимодействие между сухопутными войсками, объединёнными силами, другими участниками совместных действий и принимающими странами перед началом кибероперацій и РЭБ.

4-2. ***Оперативный процесс*** включает основные действия по командованию и управлению, выполняемые во время операций: планирование, подготовка, выполнение и постоянная оценка операции (ADP 5-0). Оперативный процесс – это принятая в сухопутных войсках система организации и осуществления командования и управления. Рабочая группа CEMA даёт возможность командиру получить представление о киберпространстве и оперативной электромагнитной обстановке. Благодаря такому пониманию командир может лучше представить и описать конечное состояние операции и оперативный подход; это, в свою очередь, позволяет ему принимать и формулировать решения, направлять, руководить и оценивать операции. При проведении крупномасштабных боевых операций командир и штаб корпуса или дивизии должны согласовывать замысел операции с соседними корпусами и дивизиями, объединёнными силами, другими участниками совместных действий для обеспечения единства усилий.

4-3. Командиры, штабы и подчинённые штабы используют оперативный процесс для организации усилий, внедрения функций боевых действий в различных доменах и согласования сил для выполнения задач. Сухопутные войска планируют, готовят, осуществляют и оценивают кибероперации и РЭБ во взаимодействии с объединёнными силами и другими участниками совместных действий, при необходимости. Командиры и штабы сухопутных войск, вероятно, будут координировать или взаимодействовать с объединёнными силами для содействия проведению кибероперaций и РЭБ. По этой причине командиры и штабы должны быть хорошо осведомлены о системах и процессах совместного планирования, которые позволяют проводить кибероперации и РЭБ. Некоторые из этих систем и процессов включают:

- процесс объединённого (межвидового) планирования (см. Наставление JP 5-0);
- адаптивное планирование (см. Наставление JP 5-0);
- процесс рассмотрения и утверждения кибероперaций (см. приложения A и C);
- процесс планирования объединённых операций в ЭМС (см. JP 3-85).

4.1.1. Планирование

4-4. ***Планирование*** – это искусство и наука понимания ситуации, представления желаемого будущего и определения эффективных путей его достижения (ADP 5-0). Командиры используют искусство командования и науку управления для обеспечения поддержки замысла кибероперации и РЭБ в соответствии со стратегией операций. Независимо от того, планируются ли кибероперации и РЭБ и направляются ли они вышестоящим штабом или запрашиваются тактическими подразделениями, своевременные действия штаба и участие командиров в сочетании с постоянной ситуативной осведомлённостью о киберпространстве и ЭМС имеют решающее значение для успешного решения задачи.

4-5. Методика выработки и принятия комплексных решений сухопутных войск и процесс принятия военных решений – две методики планирования, используемые штабами сухопутных войск. Члены рабочей группы CEMA должны полностью понимать эти два метода. Подробное рассмотрение, как CEMA интегрирует кибероперации и РЭБ в методику выработки и принятия комплексных решений сухопутных войск и в процесс принятия военных решений представлено в приложении А.

4-6. Методика выработки и принятия комплексных решений сухопутных войск заключается в более продуктивном и системном подходе к решению сложных, плохо сформированных проблем. Процесс принятия военных решений состоит из более дедуктивного и аналитического подхода к планированию, и командиры на уровне корпуса и ниже, скорее всего, будут чаще использовать процесс принятия военных решений, нежели методику выработки и принятия комплексных решений сухопутных войск. Однако командиры могут использовать другой подход к планированию или комбинировать подходы. Независимо от подхода к планированию, командиры и штабы должны интегрировать кибероперации и РЭБ на протяжении всей работы по планированию. Командиры и штабы в процессе планирования должны:

а. Понимать ситуации и разрабатывать решения проблем. Командир и штаб формируют представление о домене киберпространства, информационных аспектах оперативной и электромагнитной обстановки в пределах назначенного района операций. Командиры и штабы формируют ситуативное понимание влияния кибероперациий и воздействия РЭБ на различные домены и разрабатывают решения для устранения проблем, которые могут негативно повлиять на нейтральных субъектов и свои войска.

б. Организовать силы и расставить приоритеты. Командир и штаб организуют выполнение задач в киберпространстве и РЭБ и реализуют мероприятия по очерёдности оказания поддержки. ***Приоритет поддержки*** – это очерёдность, устанавливаемая командиром для поддержки подчинённого подразделения в соответствии с его значимостью для выполнения задачи (документ ADP 5-0).

в. Направлять, координировать и согласовывать действия. Командир и штаб используют эту функцию планирования для руководства, координации и согласования кибероперациий, РЭБ и операций по управлению спектром с задачами, выполняемыми с помощью разведывательных операций, информационных операций и процесса целеуказания.

г. Предвидеть события и адаптироваться к меняющимся обстоятельствам. Командир и штаб предвидят возможные атаки со стороны угроз в киберпространстве и ЭМС и адаптируют их к неопределённому характеру операций путём реализации активных и пассивных мер противодействия, связанных с обеспечением кибербезопасности и ЭМЗ.

Для адаптации к изменяющимся условиям командир и штаб прибегают к таким инструментам, как точки принятия решений[3], ответвления[4] и продолжения[5] (см. Наставление ADP 5-0).

4-7. Процесс разведывательной подготовки района боевых действий начинается и согласуется с оперативным процессом во время планирования и продолжается на всём его протяжении. В процессе разведывательной подготовки района боевых действий G-2 или S-2 поддерживает кибероперации и РЭБ, предоставляя командиру и штабу проанализированную разведывательную информацию об оперативных изменениях и изменениях задачи в районе ответственности для определения условий, имеющих отношение к этим операциям. Такая информация помогает командиру и штабу в понимании оперативной обстановки, определении возможностей для кибероперациий и РЭБ, а также выработки соответствующих вариантов действий.

4-8. В процессе планирования группа огневой поддержки использует замысел командира и замысел операции для разработки плана огневой поддержки. План огневой поддержки – это план, в котором рассматриваются все доступные средства огневой поддержки. В нём описывается, как в сухопутных войсках огонь с закрытых огневых позиций, совместный огонь и обнаружение целей интегрируются с манёвром для обеспечения оперативного успеха (см. Боевой устав FM 3-09). Координатор или руководитель огневой поддержки взаимодействует с офицером по кибероперациям и РЭБ для внедрения кибератак и ЭМА в план огневой поддержки.

4-9. Конечным результатом планирования является оперативный план (*англ. operation plan*, *OPLAN*) или боевой приказ (*англ. – operation order, OPORD*). Оперативный план разрабатывается командиром и штабом заблаговременно до начала выполнения и превращается в боевой приказ после получения указания на его реализацию в определённое время или в связи с определённым событием. Офицер по кибервойне и РЭБ отвечает за заполнение Приложения C, дополнение 12, и по запросу оказывает помощь G-6 или S-6 в заполнении Приложения H, дополнения 1 и 6 к оперативному плану или боевому приказу. Офицер по кибервойне и РЭБ также отвечает за внесение дополнений, изменений и уточнений в Приложение C, дополнение 12, и оказание помощи в уточнении Приложения H, дополнения 1 и 6, по мере необходимости, для частных приказов (*англ. – fragmentary order, FRAGORD*) (см. Приложение A, где описаны методика выработки и принятия комплексных решений сухопутных войск, процесс принятия военных решений и документы CEMA для приказов).

---

[3] Точки принятия решений – расчёт сил и средств для ввода в бой в случае изменения обстановки – прим. пер.

[4] Ответвления – заранее предусмотренные варианты развития событий в ходе боя – прим. пер.

[5] Продолжения – варианты развития событий следующей операции, исходя из итогов текущей – прим. пер.

4.1.2. Подготовка

4-10. ***Подготовка*** состоит из мероприятий, выполняемых подразделениями и военнослужащими для улучшения их способности к выполнению операции (ADP 5.0). Подготовительные мероприятия включают начало сбора информации, подготовку операций в информационной сети МО, тренировки, обучение и инспекции. Подготовка требует активного участия командира, штаба подразделения и военнослужащих в обеспечении готовности сил к выполнению операций.

4-11. Подготовительные мероприятия обычно начинаются во время планирования и продолжаются в ходе выполнения. В корпусе и ниже подчинённые подразделения, которым поставлена задача использования возможностей кибероперациий и РЭБ (определённых в оперативном плане или боевом приказе), проводят подготовительные мероприятия для повышения эффективности действий сил и средств в ходе операции. Командиры управляют процессом подготовки, осуществляя руководство и давая оценку. Используя следующие функции подготовки, командиры и штабы могут:

а. Улучшить понимание ситуации. Командиры, штабы и подчинённые подразделения продолжают совершенствовать знания о киберпространстве и оперативной электромагнитной обстановке в назначенном районе операций, в том числе улучшать понимание того, как использование киберпространства и ЭМС может повлиять на операции в различных доменах.

б. Выработать общее понимание плана. Командиры, штабы и подчинённые подразделения, которым поставлена задача, вырабатывают общее понимание плана (описанного в оперативном плане или оперативном приказе) путём проведения тренировок в пунктах постоянной дислокации и центрах боевой подготовки. Эти учебные мероприятия предоставляют отличную возможность подчинённым командирам, начальникам и рядовому составу выполнить разработанный план в условиях контролируемой обстановки и выявить проблемы в разрабатываемом плане, требующие внесения изменений.

в. Обучить и повысить квалификацию в решении критических задач. В ходе учений и тренировок подчинённые подразделения приобретают и оттачивают навыки выполнения индивидуальных и коллективных задач, необходимых для успешного проведения кибероперациий и РЭБ. Командиры также предусматривают время на подготовку с учётом ожидаемых и непредвиденных событий и обстоятельств.

г. Ввести новые войска. Командиры выделяют время на подготовку к вводу в действие новых войск, сформированных в соответствии с поставленными задачами. Ввод войск включает выделение подразделений, перемещение средств кибероперациий и РЭБ, а также приём и интеграцию новых подразделений и военнослужащих в состав сил. Организованным для выполнения задачи войскам требуется время на подготовку, чтобы ознакомиться с требованиями и стандартами прибывающего подразделения и понять свою роль в общем плане.

Получающему подразделению требуется время для оценки возможностей и ограничений сил и средств кибероперaций и РЭБ, входящих в состав оперативной группы, и интеграции новых возможностей.

д. Обеспечить размещение сил и средств. Организация размещения и постановка задач происходят одновременно. Командиры обеспечивают наличие в составе средств кибероперaций и ЭМА необходимого личного состава и оборудования с проведением предоперационных проверок, а также следят за тем, чтобы эти средства и силы находились в нужном месте и в нужное время.

4.1.3. Выполнение

4-12. ***Выполнение*** – это приведение плана в действие путём применения боевых возможностей для выполнения поставленной задачи (ADP 5-0). Командир, штаб и подчинённые командиры сосредотачивают своё внимание на воплощении решений, принятых в ходе планирования и подготовки, в действия. Командиры проводят наступательные кибероперации и ЭМА для проецирования боевой мощи через киберпространство и ЭМС, проводят ОКбО и ЭМЗ для защиты своих войск и систем, а также ведут разведку в киберпространстве и ЭМС для сбора информации о боевой обстановке с целью непрерывного обновления ситуативной осведомлённости.

4-13. Командиры должны понимать, что подробное планирование обеспечивает разумный прогноз выполнения, но также должны знать, что ситуации в киберпространстве и в оперативной электромагнитной обстановке могут быстро меняться. В ходе выполнения командиры предпринимают согласованные действия по захвату, удержанию и использованию оперативной инициативы, принимая на себя риск.

4-14. ***Оперативная инициатива*** – это установление темпа и условий действий на протяжении всей операции (ADP 3-0). Создавая перед противником многочисленные междоменные проблемы, включая киберпространство и ЭМС, командиры заставляют его постоянно реагировать, что ставит его в невыгодное положение. Командиры могут использовать кибератаки и ЭМА для того, чтобы заставить командиров противника отказаться от предпочтительных вариантов действий и совершить опасные ошибки. Командиры сохраняют инициативу, согласуя кибератаки и ЭМА как огневые средства в сочетании с другими элементами боевых возможностей для оказания жёсткого давления на противника с использованием постоянно меняющихся комбинаций боевых возможностей в темпе, которому противник не может эффективно противостоять.

4-15. Командиры и штабы продолжают использовать средства сбора информации и РЭР для выявления попыток противника вернуть инициативу. Собранная информация может быть использована для корректировки приоритетности целеуказания и планов огневой поддержки, включая кибератаки и ЭМА, чтобы держать противника в напряжении.

4-16. Как только свои войска захватывают инициативу, они немедленно используют её в своих интересах, проводя непрерывные операции для ускорения разгрома противника. ***Поражение*** – это лишение войск возможности достичь своей цели (ADP 3-0). Командование может использовать кибератаки и ЭМА для срыва попыток противника восстановить силы и усугубить дезорганизацию противника путём нанесения ударов по его узлам управления и разведывательным центрам.

4.1.4. Оценка

4-17. ***Оценка*** – это определение прогресса в выполнении задачи, создании эффекта или достижении цели (JP 3-0). Командир и штаб постоянно оценивают кибероперации и РЭБ, чтобы определить, привели ли они к желаемому эффекту. Оценочные мероприятия способствуют принятию решений, позволяя выяснить ход операции для разработки и уточнения планов.

4-18. Оценка как предшествует, так и направляет другие виды деятельности в рамках оперативного процесса, и не существует единого способа её проведения. Командиры разрабатывают эффективный план оценки с учётом уникальных задач, стоящих перед ними. Командир разрабатывает план оценки посредством:

- разработкой подхода к оценке (планирование);
- разработкой плана оценки (планирование);
- сбора информации и разведданных (выполнение);
- анализа информации и разведданных (выполнение);
- обменом обратной связью и рекомендациями (выполнение);
- адаптацией планов или операций (планирование и выполнение).

Примечание:

> Более подробная информация об оперативном процессе приведена в Наставлении ADP 5-0.

4.2. Процессы внедрения

4-19. Командиры и штабы внедряют боевое обеспечение и согласовывают силы для адаптации к меняющимся условиям на протяжении всего оперативного процесса. Отделение СЕМА согласовывает кибероперации и РЭБ с оперативным процессом и связанными с ним процессами внедрения для выявления угроз в киберпространстве и ЭМС, для нацеливания и атаки на системы противника в киберпространстве и ЭМС, а также для поддержки боевого обеспечения. Рис. 4-1 иллюстрирует интегрирование и согласование СЕМА на протяжении всего оперативного процесса с использованием различных интеграционных процессов.

4-20. Оперативный процесс – это основной вид деятельности, осуществляемый командиром и штабом. Командир и штаб интегрируют и согласовывают задачи СЕМА с пятью ключевыми процессами внедрения на протяжении всего оперативного процесса (см. рис. 4-1). Процессы внедрения:

1. Разведывательная подготовка района боевых действий.
2. Сбор информации.
3. Целеуказание.
4. Управление рисками.
5. Управление знаниями.

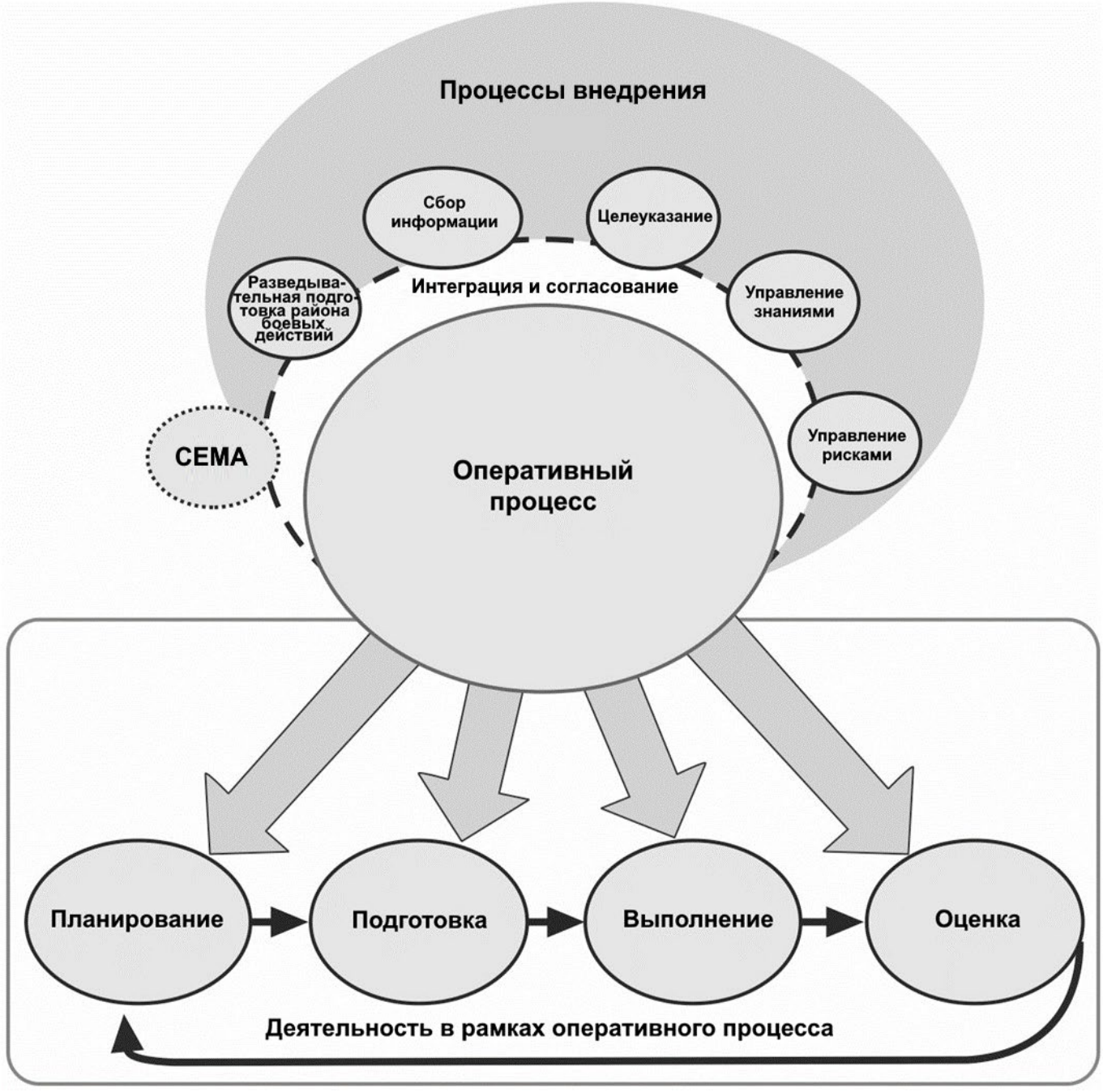


Рис. 4-1. – *Оперативный процесс и процессы внедрения*

4.2.1. Разведывательная подготовка района боевых действий

4-21. В целях интеграции и согласования задач и операций по сбору информации подразделение G-2 или S-2 руководит работой личного состава в рамках процесса разведывательной подготовки района боевых действий. ***Разведывательная подготовка района боевых действий*** – это систематический процесс анализа переменных параметров задачи, таких как противник, рельеф, погода и гражданские условия в районе ответственности, с целью определения их воздействия на ход операции (ATP 2-01.3). Разведывательная подготовка района боевых действий помогает в разработке глубокого понимания соответствующих аспектов оперативной обстановки, включая угрозы.

4-22. Внедрение процесса разведывательной подготовки района боевых действий в оперативный процесс очень важно для поддержки способности командира понимать оперативную обстановку и наглядно представлять себе операции на протяжении всего оперативного процесса. Внедрение процесса разведывательной подготовки района боевых действий в оперативный процесс является инструментом, позволяющим командирам разрабатывать и проводить операции непрерывно. Внедрение процесса разведывательной подготовки района боевых действий в оперативный процесс обеспечивает получение информации и разведданных, необходимых для планирования, подготовки, выполнения и оценки операций. Четыре этапа в процессе разведывательной подготовки района боевых действий:

1. Определение оперативной обстановки.
2. Описание влияния окружающей среды на операции.
3. Оценка угрозы.
4. Определение варианта действий по устранению угрозы.

4-23. Процесс разведывательной подготовки района боевых действий начинается в ходе планирования и продолжается в течение всего оперативного процесса. Результатом процесса являются документы, используемые для разработки вариантов действий для своих войск и точек принятия решения для командира в ходе планирования. Результаты разведывательной подготовки района боевых действий имеют решающее значение для планирования кибероперациий и РЭБ.

4.2.1.1. Определение оперативной обстановки

4-24. Подразделение штаба G-2 или S-2 использует процесс разведывательной подготовки района боевых действий для определения параметров киберпространства и оперативной электромагнитной обстановки в текущей оперативной обстановке. Определение параметров киберпространства и оперативной электромагнитной обстановки позволяет командиру и штабу визуализировать средства киберпространства и РЭБ как своих войск, так и противника через три слоя киберпространства и в ЭМС.

Отделение CEMA поддерживает процесс разведывательной подготовки района боевых действий, помогая G-2 или S-2 в разработке и управлении электромагнитным боевым порядком.

4-25. Подразделение штаба G-2 или S-2 отвечает за согласование доступных ресурсов радио и радиотехнической разведки. Информация о боевой обстановке, полученная в ходе кибероперациий и РЭБ, помогает G-2 или S-2 в определении оперативной обстановки. Кроме того, G-2 или S-2 могут объединить разведывательные дисциплины с оперативно-розыскной деятельностью для сбора информации, связанной с киберпространством и РЭБ, чтобы определить полную оперативную обстановку.

4-26. Подразделение штаба G-2 или S-2 использует сведения, полученные в ходе сбора информации, для создания электронных рабочих слоёв района операций, включающих аспекты местности, связанные с кибероперациям и электромагнитным спектром, в назначенном районе операций. Электронный рабочий слой киберпространства района операций может отображать физический слой киберпространства гораздо легче, чем логический или киберперсональный слои. Получение информации о средствах, которые используются угрозой для воздействия на киберпространство на логическом и киберперсональном уровнях, осуществляется с помощью радио и радиотехнической разведки, оперативно-розыскной деятельности или использования киберпространства.

4-27. Подразделение штаба G3 должно обеспечить официальное распространение и доступность для разведывательного сообщества информации, собранной оперативными системами, платформами и средствами обнаружения, например, используемыми для мониторинга своих сетей во время проведения операций в информационной сети МО. Это критически важный компонент, необходимый для определения оперативной обстановки в поддержку кибероперациий, а также для того, чтобы G2 или S2 могли оценить угрозу.

4.2.1.2. Описание влияния окружающей среды на операции

4-28. В результате ответов на информационные требования, полученных от отделения CEMA, G-2 или S-2 определяют типы угроз и возможности киберпространства и РЭБ, а также определяют последствия для окружающей среды. Важно учитывать, как воздействие внешней среды скажется на операциях своих войск и войск противника, включая те, которые могут повлиять на киберпространство и ЭМС. К таким соображениям относятся рельеф местности, погода, данные об освещённости, а также гражданские факторы. Анализ местности позволяет командиру понять её влияние на кибероперации и РЭБ.

Рабочая группа CEMA проводит анализ киберпространства и местности, связанной с ЭМС, используя традиционные методы и изучая пять военных аспектов местности при определении направлений действий противника:

1. Наблюдение и сектора обстрела.
2. Пути подхода.
3. Основной рельеф.
4. Препятствия.
5. Укрытие и маскировка.

4-29. Гражданские аспекты применяются путём взаимного пересечения с оперативными параметрами. G-2 или S-2 включает такие гражданские аспекты, как покрытие сотовой связью, Интернет-провайдеры, распределение электроэнергии для промышленных, коммерческих и жилых районов.

4-30. Угрозы в киберпространстве и ЭМС, а также все собранные и проанализированные на предмет воздействия на окружающую среду разведывательные сведения включаются в такие продукты разведывательной подготовки района боевых действий, как электронные рабочие слои угроз, таблицы описания угроз, матрицы воздействия на местность, анализ местности или модифицированный комбинированный электронный рабочий слой препятствий и оценки.

4.2.1.3. Оценка угрозы

4-31. Во взаимодействии с отделением CEMA подразделение G-2 или S-2 определяет киберпространство угроз и возможности РЭБ, доктринальные принципы, а также тактику, методы и процедуры, используемые противником в назначенном районе операций. Использование противником киберпространства и ЭМС для достижения или поддержки своих целей различается. Используя исходные данные различных видов разведки, G-2 или S-2 и отделение CEMA оценивают угрозу, создают модели угроз, разрабатывают общие варианты действий против угрозы и определяют важные цели противника (*англ. high value target, HVT*). При создании модели угрозы G-2 или S-2 учитывает киберпространство и особенности ЭМС, чтобы определить, как противник внедряет и использует возможности кибероперации и РЭБ.

4-32. Противник, скорее всего, будет располагать средствами воздействия на киберпространство и РЭБ, которые действуют в рамках всего боевого обеспечения. Для повышения ситуативной осведомлённости G-2 или S-2 должны выявлять средства киберпространства и ЭМС противника, задействованные для поддержки каждой боевой операции. G-2 или S-2 также оценивает нейтральных субъектов и противника, проводящих кибероперации и в ЭМС во всём районе операций, и направляет информацию правоохранительным органам местных властей и сухопутных войск или контрразведке.

Нейтральные субъекты и неприятель:

- национально-государственные субъекты;
- транснациональные негосударственные субъекты или террористы;
- преступные организации или многонациональные киберсиндикаты;
- отдельные субъекты, хактивисты или небольшие группы;
- внутренние угрозы;
- автономные системы, программное обеспечение и вредоносный код.

4-33. Данные, собранные путём оценки угрозы, помогают разработать модели угроз, показывающие, каким образом противник проводит операции, включая характеристики угроз об использовании ими киберпространства и ЭМС. Модель угроз также описывает, как противник исторически реагировал на различные типы кибератак и ЭМА в аналогичных обстоятельствах по отношению к оперативной обстановке и всей операции.

4-34. В дополнение к модели угрозы G-2 или S-2 создаёт описания возможностей угрозы, которые согласуются с моделью угрозы и включают варианты или другие вспомогательные операции, которые противник может применить для воздействия на выполнение задач американскими войсками. Модели угроз определяют порядок разработки вариантов действий по устранению угроз.

4.2.1.4. Определение плана действий по устранению угрозы

4-35. Подразделение G-2 или S-2 использует данные, полученные в ходе оценки угрозы, для определения и разработки всех вариантов действий, возможных для противника. G-2 или S-2 взаимодействует с отделением CEMA для разработки вариантов действий по устранению угроз, касающихся возможностей противника в киберпространстве и ЭМС. G-2 или S-2 предоставляет G-3 или S-3 информацию и разведданные, необходимые для разработки вариантов действий для своих войск, противодействия этим имеющимся угрозам и влияния этих вариантов на операции своих войск. G-2 или S-2 также сотрудничает с отделением CEMA для разработки контрмер в соответствии с вариантом противодействия угрозам в киберпространстве и электромагнитном спектре. Каждый вариант действий по устранению угрозы включает идентифицированные кибератаки и важные цели, связанные с ЭМА, такие как узлы, центры командования и управления, вышки связи, спутники, поставщики интернет-услуг, волоконно-оптические линии и местные электроподстанции.

4-36. При разработке вариантов действий для своих войск, связанных с противодействием возможностям противника в киберпространстве и в ЭМС, G-2 или S-2 совместно с отделением CEMA учитывает такие соображения, как использование противником киберпространства и в ЭМС в прошлом и типы операций, связанных с киберпространством и электромагнитным спектром, которые он проводил.

Подразделение G-2 или S-2 оказывает помощь отделению CEMA в определении конкретных сил и средств киберпространства и РЭБ подразделения, которые могут дать желаемый эффект при борьбе с важными целями.

4-37. Структурное подразделения G-2 или S-2 должно понимать, что киберугроза может действовать за пределами назначенного района операций подразделения. Противник может использовать доверенных лиц по всему миру за пределами зоны интересов подразделения. Разработка варианта действий по устранению угроз осуществляется на основании предварительного определения важных и приоритетных целей. Варианты действий по устранению угроз включают шаблоны и схемы событий, в которых определяются потенциальные цели, указанный район потенциальной угрозы и район объектов потенциальной угрозы. ***Указанный район потенциальной угрозы*** – это геопространственная область, узел или звено системы, по которым может быть собрана информация, удовлетворяющая определенному информационному требованию (JP 2-01.3). ***Район объектов потенциальной угрозы*** – это географический район, в котором своими войсками могут быть захвачены и поражены важные цели (JP 2-01.3).

4-38. Отделение CEMA проводит анализ особенностей среды для изучения аспектов характера среды в киберпространстве и в ЭМС для определения препятствий, таких как брандмауэры, блоки портов, средства обнаружения угроз и возможности подавления помех, которые требуют немедленного устранения для продолжения операций. В отделении CEMA также определяются различные пути подхода кибератаки и ЭМА на киберпространство и возможности ЭМС противника. В ходе анализа киберсреды CEMA выявляет потенциальные слабые места на позициях своих войск в киберпространстве и в ЭМС, которые требуют дополнительного прикрытия и маскировки с помощью таких методов, как защита от электромагнитного излучения, защита паролем, контроль излучений или использование методов скрытия Интернет-протокола.

4-39. При анализе киберсреды важно определить ключевые места в киберпространстве и в ЭМС, которые могут стать точками доступа. Эти точки доступа обеспечивают пути подхода или могут служить секторами наблюдения и обстрела, где возможно отслеживать, перехватывать или записывать сетевой трафик путём радио и радиотехнической разведки, использования киберпространства или ЭМП. Определив препятствия, связанные с киберпространством и РЭБ, пути подхода, укрытия и маскировку, а также сектора наблюдения и обстрела отделение CEMA может определить места на этих участках местности, которые следует рассматривать как ключевые. К ключевым участкам относятся важнейшие точки доступа для наблюдения за надвигающимися угрозами и подступами для нанесения кибератак и ЭМА. В качестве ключевых зон рассматриваются зоны в киберпространстве и зоны ЭМС, связанные с критическими объектами в информационной сети МО.

Примечание:

> Для получения дополнительной информации о процессе разведывательной подготовки района боевых действий см. в Наставлении ATP 2-01.3.

4.2.2. Сбор информации

4-40. ***Сбор информации*** – это деятельность, которая синхронизирует и интегрирует планирование и использование средств обнаружения и наблюдения, а также систем обработки, использования и распространения информации для непосредственной поддержки текущих и будущих операций (FM 3-55). Эти средства обнаружения и наблюдения могут включать киберсредства и средства РЭБ, осуществляющие кибероперации, электромагнитное зондирование и РЭР для сбора информации.

4-41. Сбор информации – это получение информации и представление её на обработку. Сбор информации объединяет функции разведки и оперативного штаба с упором на ответы на запросы критических информационных требований командира и информационных требований штаба, которые помогают командиру и штабу в формировании оперативной обстановки и проведении операций. Командир управляет сбором информации, который координируется штабом и возглавляется G-2 или S-2.

Этапы сбора информации:

1. **1.** Планирование требований и оценка объёма собираемой информации.
2. **2.** Постановка задачи и управление сбором.
3. **3.** Осуществление сбора информации.

4-42. Сбор информации позволяет командиру понять и наглядно представить себе ход операции. Он позволяет выявить пробелы в информации, что требует привлечения разведывательных средств к использованию киберпространства, РЭР и электромагнитному зондированию для получения данных об этих пробелах. Этапы целеуказания «принятие решения» и «обнаружение» также в значительной степени зависят от сбора информации. Кибервозможности противника, выявленные путём сбора информации, помогают рабочей группе CEMA обнаруживать потенциальные цели и ключевые зоны в киберпространстве.

4.2.2.1. Планирование требований и оценка сбора информации

4-43. Структурное подразделение G-2 или S-2 взаимодействует с другими специалистами штаба для получения и утверждения информационных запросов для сбора. Отделение CEMA предоставляет G-2 или S-2 информационные запросы, связанные с киберпространством и ЭМС, запрашивая информацию о своих войсках, противнике и нейтральных субъектах, действующих в районе операций.

Офицер по кибервойне и РЭБ определяет все информационные запросы, связанные с киберпространством и ЭМС, чтобы представить их командиру в качестве потенциальных критических информационных требований. G-2 или S-2 готовит инструменты планирования требований и рекомендует G-3 или S-3 ресурсы киберпространства и РЭБ для сбора информации.

4.2.2.2. Постановка задачи и управление сбором информации

4-44. В дополнение к тому, что G-2 или S-2 использует радио и радиотехническую разведку для сбора информации, G-3 или S-3 может поставить задачу силам и средствам киберпространства и РЭБ на обеспечение действий по сбору информации. В этом случае отделение CEMA будет помогать G-2 или S-2, выделяя штатные средства РЭБ и запрашивая дополнительные средства РЭБ и киберпространства по мере необходимости. G-2 или S-2 отвечает за поддержание согласования всех средств и сил, используемых для сбора информации.

4.2.2.3. Осуществление сбора информации

4-45. При сборе информации основное внимание уделяется сбору данных, которые отвечают критическим информационным требованиям командира и информационным требованиям для анализа в процессе разведки района ведения боевых действий требованиям. Эта информация помогает в формировании оперативной обстановки и получении информации о противнике. Деятельность по сбору информации позволяет получить сведения о противнике, в том числе о его возможностях и средствах, зависящих от киберпространства и ЭМС. Деятельность по сбору информации начинается сразу после получения информации о задачах оперативного процесса и продолжается в течение всего периода подготовки и выполнения.

4-46. Структурное подразделение G-2 или S-2 осуществляет сбор информации путём ведения:

- разведывательных операций;
- рекогносцировки;
- наблюдения.
- операций по безопасности.

4.2.2.3.1. Разведывательные операции

4-47. ***Разведывательные операции*** – это задачи, решаемые подразделениями разных видов военной разведки, с целью получения информации для выполнения подтверждённых требований (ADP 2-0). Благодаря разведывательным операциям G-2 или S-2 получает информацию о возможностях, действиях, расположении и характеристиках угрозы.

В разведывательных операциях для сбора информации о киберпространстве и ЭМС используются различные виды разведки для удовлетворения требований критических информационных требований командира и информационных требований штаба. Однако знания, полученные от других видов разведки, также могут дать представление о киберпространстве и в ЭМС. В дополнение к сбору информации о равноправных и почти равноправных угрозах силами и средствами РРТР в ходе оперативно-розыскной деятельности собирается информация о незаконной деятельности в киберпространстве и ЭМС, проводимой во всём назначенном районе операций. Для получения дополнительной информации об оперативно-розыскной деятельности см. AR 195-2.

4.2.2.3.2. Рекогносцировка

4-48. ***Рекогносцировка*** является боевой задачей получения информации о деятельности и ресурсах противника или неприятеля, а также данных о метеорологических, гидрографических или географических характеристиках конкретного района путём визуального наблюдения или других методов обнаружения (JP 2-0).

Рекогносцировка позволяет получить информацию о назначенном районе операций. С помощью рекогносцировки G-2 или S-2 могут собирать информацию о таких оперативных параметрах задачи, как характеристики области, препятствия для передвижения противника и союзников, а также расположение сил противника и гражданских лиц. Комбинированное применение трёх методов разведки (пешей, на транспортных средствах и воздушной) позволяет определить местоположение и тип (типы) своих, гражданских и угрожающих киберпространственных средств и средств РЭБ, действующих в назначенном районе боевых действий (операций). По запросу отделение CEMA поддерживает рекогносцировочные действия G-2 или S-2, используя средства РЭБ для проведения РЭР с целью сбора сведений в ЭМС и запрашивая поддержку НКбО для проведения киберразведки в киберпространстве.

4.2.2.3.3. Наблюдение

4-49. ***Наблюдение*** – это систематическое изучение воздушно-космических, киберпространственных, наземных или подземных районов, мест, личного состава или предметов с помощью визуальных, слуховых, электронных, фотографических или других средств (JP 3-0).

Наблюдение включает наблюдение за территорией с целью сбора информации и мониторинга гражданского населения и угроз в указанном районе потенциальной угрозы и районе объектов потенциальной угрозы. Наблюдение может быть самостоятельным или являться частью разведывательной операции. Сбор сведений в киберпространстве и ЭМС в рамках задачи наблюдения также называется наблюдением за сетью.

Наблюдение за сетью – это наблюдение за организационными, социальными, коммуникационными, киберпространственными или инфраструктурными связями и отношениями (FM 2-0). Наблюдение за сетью может также включать подробную информацию о связях и отношениях между людьми, группами и организациями, а также о роли и значении тех или иных компонентов физической или виртуальной инфраструктуры.

4-50. Информация, собранная с помощью наблюдения за сетью и других видов наблюдения, является вспомогательным средством для процесса разведывательной подготовки района боевых действий. Собранная информация позволяет получить представление о возможностях и средствах киберпространства и РЭБ противника. По запросу отделение СЕМА обеспечивает усилия G-2 или S-2 по наблюдению, запрашивая поддержку наступательных кибероперации для применения средств, использующих киберпространство, или использования средств РЭБ для ведения РЭР с целью наблюдения в киберпространстве противника и нейтральной стороны, а также в ЭМС. Информация, собранная в ходе разведки с использованием киберпространства и РЭР, включает такие параметры задачи и оперативной обстановки, как характеристики местности, препятствия противника и своих войск, дислокация сил противника и гражданского населения.

4.2.2.3.4. Операции по безопасности

4-51. ***Операции по безопасности*** – это операции, проводимые командирами с целью раннего и точного предупреждения о действиях противника, предоставления защищаемым силам времени и пространства для манёвра с целью реагирования на действия противника и развития ситуации, позволяющей командирам эффективно использовать свои защищённые войска (ADP 3-90). Раннее и точное предупреждение предоставляет своим войскам время и возможность манёвра для реагирования, а командиру – возможность применить меры защиты. Киберзащита, кибербезопасность и ЭМЗ включают действия, позволяющие заблаговременно обнаруживать и нейтрализовать угрозы в киберпространстве и ЭМС. Кроме того, силы и средства ЭМП ведут РЭР для получения информации о дислокации угроз противника в ЭМС и корректировки усилий по обеспечению безопасности.

4-52. Конечной целью операций по безопасности является сбор информации о варианте действий противника, обеспечивающей раннее предупреждение и постоянный срыв атак противника. В ходе операций по безопасности собранная информация о варианте действий противника в киберпространстве и в ЭМС позволяет подразделениям принимать упреждающие меры, не позволяющие средствам разведки, наблюдения и обнаружения противника определять местоположение, сильные и слабые стороны своих войск. Операции по обеспечению безопасности также предоставляют возможности для выявления важных целей для будущих кибератак или ЭМА.

Примечание:

> Дополнительные сведения о разведке см. Боевой устав FM 2-0. Для получения более подробных сведений о сборе информации см. Боевой устав FM 3-55.

4.2.2.4. Аспекты местности

4-53. Ключевая местность – это любой населённый пункт или район, захват или удержание которого даёт заметное преимущество одной из сторон (JP 2-01.3). Ключевая область в киберпространстве и в ЭМС сопоставима с территориями в других сферах в том смысле, что доминирование в ней позволяет любому участнику боевых действий занять выгодную позицию. Поддержание безопасного доминирования в киберпространстве и ЭМС является выполнимой задачей при проведении кибероперациий и РЭБ. Захват и удержание всего киберпространства и ЭМС для изоляции всех противника и неприятелей – недостижимая цель. Кроме того, как свои войска, так и силы противника могут занимать одну и ту же область в киберпространстве и в ЭМС или использовать одни и те же способы ведения кибероперациий и действий в ЭМС, не подозревая о присутствии друг друга. Другой особенностью областей в киберпространстве является то, что в нём присутствуют виртуальные компоненты, идентифицируемые на логическом сетевом уровне или на уровне кибер-персоны. По этой причине определение ключевых областей киберпространства является важнейшей составляющей планирования кибероперациий. Как и в случае с физической сферой, командиры и штабы должны учитывать все военные аспекты местности. Однако, в отличие от физической сферы, командиры и штабы должны помнить, что область в киберпространстве может измениться в любой момент.

Например:

> Злоумышленник, манипулирующий межсетевым экраном для создания путей подхода, или противник, удаляющий узел из сети, могут быть ключевой областью.

4-54. Препятствиями в киберпространстве могут быть межсетевые экраны и блокировка портов. Пути подхода в киберпространство могут быть проанализированы с целью выявления узлов и связей, соединяющих конечные точки с конкретными объектами. Скрытие и маскировка могут включать сокрытие IP-адресов или организацию защищённого паролем доступа к сетям и сетевым системам. Сектора наблюдения и обстрела киберпространства включают районы, в которых можно отслеживать, перехватывать или записывать сетевой трафик. Ключевые области киберпространства обеспечивают точки доступа к основным линиям связи, ключевые маршрутные точки для наблюдения за входящими угрозами, точки запуска кибератак и важные для целей боевой задачи участки киберпространства, связанные с критическими объектами, подключёнными к информационной сети МО.

4-55. Препятствия в ЭМС могут включать электромагнитное воздействие окружающей среды, развёртывание противником средств (датчиков и РЛС) для обнаружения использования ЭМС, а также применение противником мер защиты от электромагнитного излучения, маскировки и безопасности. Пути подхода в электромагнитном спектре могут быть проанализированы для выявления зависимых от спектра систем, устройств и связанных с ними инфраструктур, которые связывают конечные точки с конкретными местами (точная геолокация). Укрытие и маскировка могут включать контроль излучения или реализацию таких методов электромагнитной маскировки, как низкая заметность, низкая вероятность перехвата и низкая вероятность обнаружения. К зоне досягаемости относятся те области ЭМС, где электромагнитная энергия противника может быть обнаружена, идентифицирована и оценена с помощью РЭР.

4-56. Ключевая область в ЭМС включает частоты, используемые в качестве точек доступа и точек запуска радиоэлектронных систем, устройств и связанных с ними инфраструктур противника. Ключевая область также включает частоты, используемые для упреждающих контрмер, наблюдения за входящими угрозами и критическими объектами, зависящими от ЭМС. Ключевая физическая территория также имеет огромное значение для успеха операций РЭБ. Ключевая территория, обеспечивающая превосходство прямой видимости над позициями противника, поможет своим войскам сохранить заметное преимущество над противником.

4-57. Участники рабочей группы СЕМА должны соотнести задачи и цели с анализом области в процессе планирования, чтобы определить ключевые области в киберпространстве своём киберпространстве, нейтральном и киберпространстве противника (см. приложение А). Соотнесение целей с ключевыми областями обеспечивает выявление зависимостей задач в киберпространстве и ЭМС и установление приоритетов для их защиты. Результаты деятельности взаимозависимых систем, сетей и инфраструктуры, обеспечивающих выполнение поставленной задачи, могут потребовать углублённого анализа для разработки индивидуального управления рисками.

4.2.3. Целеуказание

4-58. ***Целеуказание*** – это процесс выбора и определения приоритетности целей, а также подбор соответствующих мер реагирования на них с учётом оперативных требований и возможностей (JP 3-0). *Цель* – это субъект или объект, расцениваемый как неприятель и рассматриваемый для возможного поражения или других действий (JP 3-60).

4-59. При целеуказании для воздействия в киберпространстве физический сетевой уровень является средой, через которую проходят все цифровые данные. Физический сетевой уровень включает проводные (наземный и подводный кабель) и беспроводные (радио, радиорелейные, сотовые, спутниковые) средства передачи.

Физический сетевой уровень является опорной точкой, используемой при целеуказании, для определения географического расположения сил и средств противника в киберпространстве и ЭМС.

4-60. При целеуказании ответственные за планирование могут знать о логическом местоположении некоторых целей, не зная их физического местоположения. То же самое справедливо и для защиты от угроз в киберпространстве. Специалисты по защите могут знать логическую точку возникновения угрозы, не обязательно зная её физическое местоположение. Поражение целей логического сетевого уровня возможно только с использованием средств киберпространства.

4-61. Логический сетевой уровень предоставляет специалистам по разработке целей альтернативное представление о цели, отличное от физического сетевого уровня. Положение цели на логическом уровне определяется её IP-адресами. Цели, расположенные по их IP-адресам, показывают, как узлы физического уровня соотносятся между собой, образуя сети в киберпространстве. Для обнаружения и идентификации целей на логическом уровне требуется IP-адрес и доступ к логической сети для оказания кибервоздействия. Способность противника изменять конфигурацию сети логического уровня может усложнить ведение огневого удара и воздействие на цели как логического, так и киберперсонального уровня, однако оперативная выгода от воздействия на эти цели часто перевешивает проблемы с целеуказанием.

4-62. Невозможность выделить киберперсону в отдельную область или форму на физическом и логическом уровнях сети создаёт уникальные сложности. В силу этих сложностей для определения целей на уровне киберперсон часто требуется использование нескольких методов сбора разведывательной информации и проведение обширного анализа, чтобы выработать понимание ситуации и выявить реальные цели. Как и логический уровень сети, киберперсоны могут быстро изменятся по сравнению с изменениями на физическом уровне сети.

4-63. Электромагнитная атака наиболее эффективна против спектрально-зависимых целей, которые трудно обнаружить физически, невозможно точно нанести огневое поражение или требуется лишь временно вывести из строя. Группа огневой поддержки планирует, готовит, выполняет и оценивает огневую поддержку текущих и будущих операций, внедряя согласованное летальное и нелетальное поражающее воздействие в процессе целеуказания. Летальное и нелетальное поражающее воздействие включает непрямой удар, противовоздушную и противоракетную оборону, совместный огонь, кибер- и электромагнитные атаки.

4-64. Целеуказание – это многопрофильная работа, требующая согласованного взаимодействия между командиром, группой огневой поддержки и несколькими отделами штаба, которые образуют рабочую группу по целеуказаниям.

Командир определяет приоритетность огневых средств для рабочей группы по целеуказаниям и предоставляет чёткие и краткие указания по воздействию, ожидаемому от всех огневых средств, включая кибератаки и ЭМА. ***Приоритетность огневого поражения*** – это указание командира штабу, подчинённым командирам, специалистам по планированию огневого поражения и вспомогательным службам применять огневые средства в соответствии с относительной важностью задачи подразделения (FM 3-09). Рабочая группа по целеуказаниям решает, какие цели, как, где и когда поражать, исходя из указаний и приоритетов командира.

4-65. Рабочая группа по целеуказаниям определяет летальные и нелетальные средства, включая средства кибератаки и ЭМА, для достижения желаемого воздействия по каждой цели, обеспечивая соблюдение правил ведения боевых действий. Отделение CEMA участвует в рабочей группе по целеуказаниям и предоставляет рекомендации по применению киберпространства и действий, связанных с ЭМС, против целей для выполнения замысла командира и включения в схему огня. ***Схема огня*** – это подробная логическая последовательность целей и мероприятий огневой поддержки для поиска и поражения целей для выполнения задач, поставленных командиром (JP 3-09).

4-66. Отделение CEMA работает в тесном контакте с группой огневой поддержки для координации и управления средствами киберпространства и РЭБ в рамках плана огневой поддержки. Этот процесс называется координацией огневой поддержки и представляет собой планирование и ведение огня таким образом, чтобы с достаточной точностью поразить цели подходящим вооружением или группой оружия (JP 3- 09).

4.2.3.1. Функции целеуказания

4-67. Подразделение штаба G-2 или S-2 во взаимодействии с отделением CEMA и группой огневой поддержки обнаруживает, идентифицирует и определяет местоположение целей посредством поиска целей. Для эффективного применения вооружения, включая ЭМА и кибератаки, необходимы достаточные разведывательные сведения, полученные в результате обнаружения целей. G-2 или S-2 осуществляет сбор информации для предоставление разведывательных сведений группе огневой поддержки, участникам рабочей группы по целеуказаниям и участникам органа управления по целеуказаниям. Эта информация включает угрозы для киберпространства и возможностей ЭМС, которые требуют индивидуального или комбинированных поражающих возможностей при летальных или нелетальных ударах.

4-68. Процесс целеуказания происходит непрерывно в ходе всей операции. Принятая в сухопутных войсках методика целеуказания, состоит из четырёх функций: принятие решения, обнаружение, нанесение удара и оценка (*англ. – decide, detect, deliver, and assess, D3A*). Эти функции выполняются в течение всего оперативного процесса.

Командиры и штабы также должны знать объединённую методологию целеуказания и понимать, как связаны между собой все эти процессы и методики, поскольку кибероперации и РЭБ обычно координируются командующим объединёнными силами. В табл. 4-1 показана взаимосвязь между оперативным процессом, объединённым циклом целеуказания, D3A и процессом принятия военных решений.

Таблица 4-1

Процесс целеуказаний

Оперативный процесс		Объединённый цикл целеуказания	D3A	Процесс принятия военных решений	Задачи целеуказания
Непрерывная оценка	План	**1. Задачи командира, указания по целеуказаниям и намерения**	**Принятие решения**	**Анализ задачи**	• Проанализировать значимость целей для разработки огневой поддержки (включая возможности сил и средств кибероперацій, РЭБ и информационных) важных целей. • Обеспечить огневую поддержку, информационные возможности, в киберпространстве и РЭБ, связанные с процессом целеуказания, и по указанию командира желаемые воздействия.
		2. Выявление целей и определение приоритетов.		**Разработка варианта действий**	• Выявить потенциальные приоритетные цели. • Устранить конфликты и координировать выявление потенциальных приоритетных целей. • Разработать список приоритетных целей. • Установить стандарты отбора целей. • Разработать матрицу наведения атаки. • Разработать задачи для огневой поддержки, РЭБ и сил кибероперацій. • Разработать соответствующие показатели результативности и эффективности.
		3. Анализ возможностей.		**Анализ варианта действий**	• Уточнить список приоритетных целей. • Уточнить стандарт выбора цели. • Уточнить матрицу наведения атаки. • Уточнить задачи огневой поддержки. • Уточнить соответствующие показатели результативности и эффективности.

Оперативный процесс		**Объединённый цикл целеуказания**	**D3A**	Пр**оцесс принятия военных решений**	**Задачи** целеуказания
Непрерывная оценка	**План**	**4. Решение командира и расстановка сил**	**Принятие решения**	**Разработка распоряжений**	• Завершить составление списка приоритетных целей. • Завершить разработку стандартов отбора целей. • Завершить разработку матрицы наведения атаки. • Завершить формирование матрицы согласования целеуказаний • Завершить разработку задач огневой поддержки. • Завершить разработку показателей результативности и эффективности. • Представить требования к информации в G-2/S-2 батальона или бригады.
	Подготовка	**5. Планирование операций и их выполнение**	**Обнаружение**		• Выполнить план сбора информации. • Уточнить требования к информации по мере получения ответов. • Уточнить список приоритетных целей, матрицу наведения атаки и матрицу согласования целеуказания. • Уточнить задачи, связанные с огневой поддержкой, киберпространством и РЭБ. • Уточнить соответствующие показатели результативности и эффективности.
	Выполнение	**6. Оценка**	**Нанесение поражения**		• Нанести огневое поражение, кибер- и электромагнитные атаки в соответствии с матрицей наведения атаки и матрицей согласования целеуказаний.
	Оценка		**Оценка**		• Оценить выполнение задачи (по показателям эффективности). • Оценить результаты (по показателям эффективности). • Уточнить задачи огневой поддержки и соответствующие действия и при необходимости повторно поразить цель.

4.2.3.1.1. Принятие решения

4-69. Функция принятия решения является первым этапом процесса целеуказания. Она начинается с процесса принятия военных решений и продолжается на протяжении всей операции. Отделение CEMA выполняет следующие действия при принятии решения в процессе целеуказаний:

а. Угроза средствам и возможностям, связанным с киберпространством и РЭБ, при анализе ценности целей для выявления важных целей. ***Важная цель*** – это цель, которая необходима командиру противника для успешного выполнения задачи (JP 3-60).

б. Выявление потенциальных приоритетных целей, связанных с киберпространством и РЭБ. ***Приоритетная цель*** – это цель, поражение которой значительно повлияет на успех варианта действий своих войск (JP 3-60). Приоритетная цель – это важная цель, которую необходимо захватить и успешно поразить для успешного выполнения задачи командира.

в. Конкретные цели, которые должны быть обнаружены и поражены с использованием средств кибератаки или ЭМА с учётом установленных стандартов выбора целей.

г. Место и время, когда цели могут быть обнаружены в ходе разведывательных действий, и как долго цель будет оставаться неподвижной.

д. Задачи по рекогносцировке, разведке и захвату целей, на которые направлены кибератаки или ЭМА, а также определение наличия у подразделения необходимых сил и средств кибератаки или ЭМА для нанесения соответствующих ударов.

е. Информационные требования штаба, связанные с киберпространством и ЭМС, необходимые для целеуказаний.

ж. Когда, где и с каким приоритетом должны быть поражены цели и какие средства кибератаки или ЭМА должны быть задействованы для достижения результата.

з. Уровень эффективности, характеризующий успешную кибератаку или ЭМА и достижение цели командира.

и. Если кибератака или ЭМА может воздействовать на цель и каким образом, то какой тип кибератаки или ЭМА может обеспечить желаемый эффект.

к. Как получить информацию, необходимую для оценки кибератаки или ЭМА с целью определения успеха или неудачи, и кто будет её собирать и обрабатывать.

л. Кто будет принимать решения, определяющие успех или неудачу кибератаки или ЭМА?

м. Какие действия будут предприняты в случае неудачи кибератаки или ЭМА, и кто имеет право руководить этими действиями?

н. Определить имеющиеся в подразделении средства РЭБ для постановки задач и приступить к разработке частного приказа.

о. Составление запросов для поддержки НКбО для удовлетворения требований целеуказаний.

п. Взаимодействие с подразделениями вышестоящего, нижестоящего и соседнего уровней для поддержки РЭБ с целью устранения выявленных недостатков в возможностях РЭБ.

р. Составление запроса для объединённой тактической авиации на воздушную ЭМА и, при необходимости, других необходимых форм запроса по РЭБ.

с. Установить связь с вышестоящим командованием для получения информации о том, были ли подтверждены предполагаемые цели кибератаки и ЭМА, и внесены ли они в совместный список целей штаба, или объединённой оперативно-тактической группы.

т. Обсуждение рисков, связанных с киберпространством и РЭБ, которые командир будет использовать для определения рисков.

у. Определение уровня полномочий для поражения целей с использованием кибератак и ЭМА.

4-70. В ходе принятия решения рабочая группа по целеуказаниям определяет ограничения по целям, которые запрещают или ограничивают кибератаки или ЭМА на определённые цели без согласования с вышестоящими органами. Источники этих ограничений могут включать военные риски, законы войны, правила ведения боевых действий или другие факторы. Объединённая оперативно-тактическая группа вносит объекты, находящиеся в районе операций, запрещённые для атаки, в список запрещённых к нанесению ударов, а цели с ограничениями – в список ограниченных целей.

4.2.3.1.2. Обнаружение

4-71. Функция обнаружения является вторым этапом в процессе целеуказания; на этом этапе средства ЭМП или другие средства захвата цели обнаруживают и отслеживают заданную цель с требуемым уровнем точности во времени и пространстве. При выполнении функции обнаружения G-2 или S-2 координирует с рабочей группой по целеуказаниям разработку плана сбора информации. Перед нанесением удара группа по целеуказаниям должна установить показатели результативности и эффективности для кибер- и электромагнитных атак, чтобы обеспечить их соответствие целям командира.

4-72. Рабочая группа по целеуказаниям фокусирует внимание на усилиях по наблюдению путём определения указанных районов потенциальной угрозы и районов объектов потенциальной угрозы, внедрённых в план сбора информации. Указанные районы потенциальной угрозы обычно выбираются для получения указаний на варианты действий противника, но могут быть связаны и с условиями оперативной обстановки.

4-73. Рабочая группа по целеуказаниям выявляет приоритетные цели в процессе планирования и проведения командно-штабных учений. Целевые районы интересов, требующие специфического взаимодействия с использованием средств кибер- или ЭМА, отличаются от районов поражения. Район поражения – это район сосредоточения, в котором командир применяет всё имеющееся вооружение для поражения цели. В отличие от этого для поражения цели в районе потенциальной угрозы используется особая система вооружений. При выполнении функции обнаружения отделение СЕМА выполняет следующие действия:

а. Предоставляет информационные требования штаба, связанные с киберпространством и РЭБ, для определения приоритетных целей, которые после утверждения командиром добавляются к приоритетным требованиям разведки.

б. Ставит задачи средствам РЭБ, при необходимости, вести РЭР для сбора информации.

в. Уточняет важные и приоритетные цели для кибер- и электромагнитных атак.

г. Определяет, можно ли воздействовать на выявленные цели с помощью наступательной кибероперации или ЭМА (или и того, и другого), и какой тип возможностей ЭМА может создать желаемый эффект

Примечание.

> Отделение СЕМА само по себе не может определить тип средств кибератаки на объекты. Отделение СЕМА должно согласовывать свои действия со специалистами СЕМА вышестоящих штабов и соответствующими объединёнными структурами по киберпространству, чтобы получить представление о наличии, целесообразности и пригодности конкретных возможностей киберпространства.

д. Обеспечивает включение целей для кибер- и электромагнитных атак в совместный интегрированный список приоритетных целей объединённой оперативно-тактической группы и в объединённый цикл целеуказаний.

е. Разрабатывает запросы для поддержки наступательной кибероперации.

4.2.3.1.3. Нанесение поражения

4-74. Функция нанесения поражения в процессе целеуказания выполняет указания на поражение цели и обеспечивает решение командира на бой после подтверждения местоположения и идентификации приоритетных целей.

Тесное взаимодействие между отделением CEMA, разведкой и группой огневой поддержки является критически важной при обнаружении целей и проведение кибератак и ЭМА. Координатор или офицер огневой поддержки подробно описывает координацию огня в оперативном плане или в боевом приказе или матрице согласования целей.

4.2.3.1.4. Оценка

4-75. Функция оценки выполняется в течение всего оперативного процесса. В ходе выполнения задачи оценки цели постоянно уточняются и корректируются командиром и штабом в ответ на новые или непредвиденные ситуации, возникающие в ходе операций. При оценке боевых действий оценивается эффективность воздействия на цель средств кибератаки и ЭМА и даются рекомендации по повторной атаке, продолжению атаки или её прекращению. Рекомендации по повторному удару, продолжению атаки и прекращению ЭМА даются совместно G-3 или S-3 и разведкой, утверждаются командиром. Более подробная информация о цикле целеуказания и процессе разработки целей приведена в документе ATP 3-60.

4.2.3.2. Факторы при целеуказании

4-76. Группа огневой поддержки во взаимодействии с G-3 или S-3 и G-2 или S-2 использует цикл целеуказания и процессы выявления целей для выбора, установления приоритетов, определения типа воздействия и продолжительности воздействия на цели. Планирование, внедрение, согласование и оценка кибероперацийи РЭБ со стороны CEMA проявляются в процессе целеуказания. Три важных аспекта кибероперацийи РЭБ, которые необходимо учитывать в процессе целеуказания:

1. Характеристика возможностей кибероперацийи РЭБ.
2. Каскадные, комбинированные и побочные поражающие факторы.
3. Обратимость поражающих факторов:
    - вопросы, связанные с запросом поддержки НКбО для целеуказания.

4.2.3.3. Характеристика возможностей кибероперацийи РЭБ

4-77. Средства воздействия на киберпространство определяются на основании собранных разведывательных данных, а также на основании оперативных данных и параметров задачи, полученных в отношении оперативной обстановки. При проведении кибероперацийкибервойска, прежде чем начать воздействие на цель, учитывают такие условия, как тип компьютерной операционной системы противника или неприятеля, марка и модель аппаратного обеспечения, версия программного обеспечения, установленного на компьютере противника или неприятеля, а также доступность ресурсов для проведения кибератаки.

4-78. Возможности РЭБ также формируются на основе собранной разведывательной информации об оперативных параметрах и параметрах задачи, достигнутых в отношении оперативной электромагнитной обстановки. В РЭБ при целеуказании ответственные за планирование сравнивают типы и возможности известных спектрозависимых устройств, используемых противником, с доступностью ресурсов РЭБ, прежде чем приступить к созданию поражающих воздействий РЭБ на цели. Цели включают радиоэлектронные устройства противника, переносимые личным составом, и радиоэлектронные устройства, используемые с или в системах вооружения, системах обнаружения, средствах кибервоздействия, которым для работы требуется использование ЭМС.

4.2.3.4. Каскадные, комбинированные и побочные поражающие факторы

4-79. Отделение СЕМА должно понимать, что в киберпространстве пересекаются интересы военных, других государственных структур, корпораций и частного сектора. Эти пересечения особенно важны для оценки возможных каскадных, комбинированных или побочных поражающих факторов при обнаружении и идентификации целей противника и его кибервозможностей. Такой же уровень рассмотрения вопросов требуется и при целеуказании радиоэлектронных устройств противника и неприятеля в ЭМС.

4-80. Кибервозможности могут создавать поражающие факторы, выходящие за пределы географических границ районов операций и районов предназначения командира. Использование средств кибервоздействия в целях нападения или манипуляции в районе предназначения требует дополнительных полномочий, помимо тех, которыми наделены командующие корпусами и ниже. Последствия, возникающие в результате кибератак, могут вызвать каскадные поражающие факторы, выходящие за пределы системы, подвергшейся нападению, которые не были очевидны для ответственных за планирование целеуказаний. Иногда каскадные поражающие факторы могут проходить через подчинённые системы для получения доступа к нацеливаемой системе. Каскадные поражающие факторы также могут распространяться через побочные или высокоуровневые системы для получения доступа к нацеливаемой системе.

Комбинированные поражающие факторы – это совокупность различных кибервоздействий, которые взаимодействовали между собой как преднамеренно, так и непреднамеренно. Эффекты, возникающие в результате ЭМА, могут вызвать каскадные поражающие факторы в ЭМС за пределами радиоэлектронных устройств противника или неприятеля, нарушая или лишая свои войска доступа к электромагнитному спектру на всей территории оперативной электромагнитной обстановки.

4-81. Побочные поражающие факторы, включая сопутствующие потери – это случайное воздействие военных кибероперациий или РЭБ на некомбатантов и гражданские кибервозможности или средства РЭБ, которые не являлись целями при осуществлении огневого поражения.

Примечание:

> Правилами ведения боевых действий или боевым приказом можно ограничить кибероперации или РЭБ только теми задачами, которые могут привести к отсутствию или минимальным побочным поражающим факторам. Специалист по управлению спектром СЕМА должен провести деконфликтизацию объединённого списка частот ограничения для ослабления электромагнитных помех перед всеми боевыми задачами РЭБ.

4.2.3.5. Обратимость поражающих факторов

4-82. Ответственным за планирование целеуказаний необходимо учитывать уровень управления, который может быть обеспечен в ходе каждой кибер- и электромагнитной атаки.

Категоризация обратимости поражающих факторов:

а. Обратимые поражающие факторы оператора. Эти воздействия могут быть отменены, восстановлены или прекращены своими войсками. Обратимые поражающие факторы оператора, как правило, несут в себе меньший риск нежелательных последствий, включая раскрытие или ответные действия.

б. Обратимые поражающие факторы, не связанные с оператором. Это воздействия, которые ответственные за планирование целеуказаний не могут отменить, восстановить или прекратить после выполнения. Обратимые поражающие факторы, не связанные с оператором, обычно несут в себе более высокий риск ответной реакции на угрозу или других нежелательных воздействий и могут потребовать более тщательного согласования.

4.2.3.5.1. Вопросы, связанные с запросом поддержки наступательной кибероперации для целеуказаний

4-83. Внедрение НКбО в процесс целеуказаний требует как долгосрочной подготовки, так и планирования задачи в режиме реального времени в ходе оперативного процесса. В связи с разработкой целей и доступом к возможностям НКбО и противника в киберпространстве необходимо подчеркнуть важность долгосрочной подготовки и планирования НКбО для целенаправленных целей и воздействий.

4-84. При планировании поддержки НКбО для атаки выбранных целей рабочая группа СЕМА должна:

а. Определить, является ли цель пригодной для поражения с помощью НКбО. Как правило, единственными потенциальными целями, получающими воздействие от кибератаки, являются активно функционирующие в той или иной части информационной среды (генерация, обработка, хранение, передача данных, а также потребление или уничтожение цифровых данных).

б. Убедиться, что объект не был уже выбран или не включён в существующий список целеуказаний. Если он ещё не выбран или не внесён в текущий список целеуказаний, то он должен быть предложен для дальнейшего целеуказания.

в. Консолидировать все получившие ответы критические информационные требования командира и информационные требования штаба. Они могут включать такие угрожающие киберпространству разведданные, как каналы или узлы; связанное аппаратное или программное обеспечение; конкретные версии и конфигурации программного обеспечения, протокол связи; физические или логические зависимости; конкретные идентификаторы (IP-адрес, адрес контроля доступа к машине, идентификатор международного абонента мобильной связи или номера телефонов).

г. Определить, включают ли разведданные, полученные с помощью разведывательной подготовки района боевых действий, информацию, необходимую для того, чтобы при целеуказании формировались способы получения доступа к кибервозможностям противника. К числу способов получения доступа к кибервозможностям противника относятся телефония, Интернет-протокол, встроенные системы и радиочастоты.

д. Отделение СЕМА отвечает за регулярное предоставление уточнённой информации о способности боевой оперативной группы проводить НКбО, а также за предоставление уточнённой информации о поддерживаемой операции.

Примечание:

> Доступ к кибервозможностям противника не гарантирует успеха применяемой кибератаки. Боевая оперативная группа должна адаптировать силы и средства для создания необходимых поражающих факторов на кибервозможности противника.

4.2.4. Управление рисками

4-85. ***Управление рисками*** – это процесс выявления, оценки и контроля рисков и принятия решений, которые уравновешивают затраты на риск с преимуществами при выполнении задачи (JP 3-0) и являются элементом командования и управления. Риск – это подверженность кого-либо или чего-либо ценного опасности, вреду или потерям, присущая всем видам деятельности.

Командир и штаб осуществляют управление рисками на протяжении всего оперативного процесса с целью выявления и снижения рисков, связанных с опасностями, которые могут привести к потерям среди личного состава и гражданских лиц, повреждению или уничтожению техники, а также иным образом повлиять на эффективность выполнения задачи. Аспекты операций по киберзащите и кибербезопасности и боевых задач ЭМЗ включают меры по снижению рисков в рамках управления рисками.

4-86. Управление рисками внедрено в деятельность по планированию и продолжается в течение всего оперативного процесса. Управление рисками состоит из следующих этапов:

а. Определение опасных факторов.

б. Оценка степени опасности.

в. Формирование управления и принятия решений о рисках.

г. Внедрение элементов контроля.

д. Контроль и оценка.

4-87. Отделение CEMA, как и все штабные подразделения, включает управление рисками в расчёты кибероперации и связанных с РЭБ текущих оценок и рекомендации по снижению рисков. Подразделение G-3/S-3 координирует управление рисками между всеми штабными звеньями в оперативном процессе. Более подробная информация о процессе управления рисками приведена в Наставлении ATP 5-19.

4.2.4.1. Риски в киберпространстве и ЭМС

4-88. Риск присущ для всех военных операций. Когда командиры принимают на себя риски они создают возможности для захвата, удержания и использования инициативы и достижения решающих результатов. Готовность идти на риск часто является ключевым фактором для выявления слабых мест противника, которые он считает недосягаемыми для противника. Командиры оценивают и уменьшают риски на протяжении всего оперативного процесса. Многие риски для информационной сети МО-СВ исходят от противника, неприятеля и инсайдеров. Некоторые угрозы хорошо оснащены и обучены, другие – новички, использующие легкодоступное и относительно недорогое оборудование и программное обеспечение. Пользователи информационной сети МО-СВ проходят обучение основам кибербезопасности, уделяя особое внимание безопасному использованию информационных технологий и пониманию общих угроз в киберпространстве.

4-89. Управление рисками – это основной процесс принятия решений в Сухопутных войсках по выявлению опасностей и контролю рисков. Этот процесс применяется ко всем типам операций, задач и мероприятий, включая кибероперации.

Факторы боевой задачи, противник, местность и погода, имеющиеся войска и поддержка, доступное время, а также гражданские вопросы обеспечивают стандартизированную методику для рассмотрения рисков, основанных как на угрозах, так и на опасностях. Риски, связанные с кибероперациями, подразделяются на четыре основные категории:

1. Оперативные риски.

2. Технические риски

3. Политические риски.

4. Риски безопасности операций.

4.2.4.1.1. Оперативные риски

4-90. Оперативные риски связаны с последствиями, которые угрозы в киберпространства и ЭМС создают для результативности выполнения задачи. Оперативные последствия являются мерилом эффективности кибератаки и ЭМА. Кибервторжение или кибератака, как и в ЭМС, может поставить под угрозу сети, системы и данные, что может привести к таким оперативным последствиям, как ранение или смерть личного состава, повреждение или потеря оборудования или имущества, ухудшение состояния сил и средств, ухудшение качества выполнения задачи или даже ее провал. Утечка данных из сетей сухопутных войск может нарушить элемент внезапности и привести к потере инициативы. Силы противника или неприятеля могут проводить кибератаки и в ЭМС на незащищённые сети и средства сухопутных войск, ставя под угрозу будущие кибератаки и кибероперации.

4-91. Свои войска, проводящие кибероперации и РЭБ, сталкиваются с многочисленными оперативными рисками. Командир и штаб оценивают эффект цепной реакции от применения кибер- и электромагнитных атак. Отделение СЕМА объясняет командирам и штабу особенности различных проявлений кибер- и электромагнитных атак и связанных с ними поражающих факторов. Отделение СЕМА помогает командиру и штабу понять обратимы ли последствия кибер- и электромагнитных атак для осознания, что некоторые последствия бесповоротные. Осознание особенностей атак, эффекта цепной реакции и необратимости результата обеспечивает командира ситуативной осведомлённостью для оценки приемлемых рисков при проведении киберопераций и РЭБ.

4-92. При проведении НКбО и ЭМА необходимо учитывать риск, который может преждевременно раскрыть противнику местоположение и намерения своих войск. Некоторые типы НКбО и ЭМА, применённые лишь однажды – не смогут быть эффективно использованы снова. Поражающие факторы каскадной реакции от применения НКбО и ЭМА способны создать сложности другим операциям.

4-93. Персональные электронные устройства, такие как умные часы, смартфоны, планшеты, ноутбуки и игровые системы, могут стать брешью для безопасности киберпространства и возможностей РЭБ своих войск. Офицер по кибервойне и РЭБ собирает информацию о рисках, связанных с применением переносных электронных устройств, от G2 или S2 и обеспечения безопасности операций и даёт рекомендации командиру по их использованию в подразделении.

4.2.4.1.2. Технические риски

4-94. Технические риски возникают в системах информационной сети МО-СВ при наличии подтверждённых уязвимостей и угрозе использования неприятелем этих уязвимостей. Почти каждая техническая система в сухопутных войсках объединена в сеть, в результате уязвимость в одной системе компрометирует другие подключённые системы, создавая общую уязвимость. Эти потенциально уязвимые сетевые системы и компоненты снижают способность сухопутных войск проводить операции. ОКбО снижают риски, защищая от определённых кибератак, не позволяя противнику воспользоваться техническими уязвимостями, которые способны подорвать процесс проведения операции.

4-95. При разработке защищённых устойчивых информационных систем принимают во внимание накладывающиеся риски, безопасность, действия разведки и контрразведки, особенности аппаратного и программного обеспечения, чтобы помочь специалистам снизить технические риски. Свои войска принимают во внимание технические риски при проведении кибератак, чтобы не допустить уязвимости используемых ими сетей для ответных кибератак противника. Сухопутные войска используют многоуровневый подход, используя:

- противовирусные и противовредоносные программы;
- системы защиты сетей;
- обновление системного программного обеспечения и патчи для устранения конкретных уязвимостей;
- средства обнаружения и мониторинга несанкционированного доступа к сети
- внедрение мер кибербезопасности и физической безопасности для снижения технических рисков.

4-96. Элементы, перечисленные в пункте 4-95, весьма важны для защиты при их эффективном внедрении и регулярном обновлении.

4.2.4.1.3. Политические риски

4-97. Политический риск относится к органам власти, юридической поддержке и международному праву. Политики затрагивают границы киберпространства, полномочия и обязанности в нём.

Командиры и лица, принимающие решения, должны оценивать риски и учитывать вероятные развивающиеся и сопутствующие результаты пересечения интересов военной, гражданской, правительственной, частной и корпоративной деятельности в общих сетях киберпространства. Законы, Кодекс США, единый кодекс военной юстиции, правила, публикации, оперативные приказы и стандартные операционные процедуры – вместе определяют решения, касающиеся деятельности в киберпространстве.

4-98. Политический риск включает рассмотрение международных норм и практики, последствия отклонения от этих норм и потенциальные изменения в международной репутации из-за последствий, возникающих в результате кибероперации. Кибератаки могут осуществляться через сети, принадлежащие, управляемые и географически расположенные в пределах суверенитета нескольких правительств. ЭМА также может оказывать влияние на частоты в спектре, принадлежащем и эксплуатируемом коммерческими, государственными и другими нейтральными пользователями. Поэтому крайне важно учитывать правовые, культурные и политические издержки, связанные с использованием киберпространства и ЭМС, как пути подхода.

4-99. Политические риски возникают, когда политика не принимает во внимание оперативную необходимость. Например, установленные правила, ограничивающие кибероперации для снижения побочных поражающих факторов, могут привести к тому, что работа подразделения будет сведена к кибератакам, не приводящим к результатам, необходимым для успеха выполнения задачи. Анализ побочных поражающих факторов для соблюдения норм и правил отличен от анализа пропорциональности и необходимости, требуемого законом войны. Даже если предлагаемая кибероперация является приемлемой после анализа побочных последствий, предлагаемая кибероперация или задача РЭБ должны быть легитимными и допустимыми в соответствии с законами войны.

4-100. Политические риски применяются к управлению рисками в соответствии с гражданскими или правовыми соображениями. Выполнение задач наступательной кибероперации или ЭМА могут представлять риск для гражданского населения и некомбатантов принимающей страны в оперативной обстановке, где постоянной целью является минимизация сопутствующих потерь. Во время боевой задачи в интересах сухопутных войск представить возможность населению принимающей страны продолжать выполнять повседневные действия. Перебои в работе общественных сетей могут представлять опасность для сухопутных войск из-за возможных социальных последствий, приводящих к беспорядкам, преступности и появлению повстанческих сил, стремящихся использовать гражданские беспорядки.

4.2.4.1.4. Риски безопасности операций

4-101. В киберпространстве и ЭМС существуют риски безопасности операций. Сухопутным войскам нужны программы кибербезопасности и обучения личного состава для исключения или снижения рисков безопасности операций. Командиры создают и настаивают на исполнении программ безопасности операций для снижения рисков. Меры безопасности операций включают деятельность и информацию в информационной сети МО и вне информационной сети МО системах и сетях. Защита конфиденциальной и критически важной информации – это забота всего личного состава. ЭМЗ предотвращает несанкционированный доступ к информации, которую противник перехватывает в ЭМС с помощью операций электромагнитной разведки. Для получения дополнительной информации о безопасности операций см. AR 530-1 и ATP 3-13.3.

4.2.5. Управление знаниями

4-102*. Управление знаниями* – это процесс использования потока знаний для совершенствования общего понимания, обучения и принятия решений (ADP 6-0). Четыре составляющие управления знаниями – это люди, процессы, инструменты и организации. Управление знаниями облегчает обмен опытом, информацией между командиром, штабом и войсками для создания и поддержания ситуативной осведомлённости и повышения эффективности. Через управление знаниями информация попадает к нужному лицу в нужное время, содействуя принятию решения.

4-103. При управлении знаниями необходимая информация о кибероперациях и РЭБ, их инструментах своевременно предоставляется из вышестоящего штаба рабочей группе CEMA для принятия решений при анализе задачи и разработке варианта действий. В рамках процесса управления знаниями разведывательные сведения от кибероперации и РЭБ, полученные в ходе сбора информации и информационных операций, распространяются для принятия решений рабочей группой CEMA. Этапы управления знаниями:

1. Оценка.
2. Проработка.
3. Развитие.
4. Проверка.
5. Применение.

4-104. Офицер по кибервойне и РЭБ отвечает за установление и контроль потоков информации о всех кибероперациях и РЭБ через личный состав штаба, включая вышестоящие и нижестоящие уровни. Он также несёт ответственность за предоставление информационных требований G-2 или S-2 для получения важной информации, необходимой для понимания киберпространства и ЭМС в рамках оперативной обстановки.

Информация, полученная от информационных требований, также имеет решающее значение для способности отделения CEMA осуществлять надлежащую интеграцию и согласование кибероперациий и РЭБ с оперативным процессом.

4-105. Отделение CEMA и взаимодействующие с ним подразделения штаба придают операциям смысл, обмениваясь как неявными, так и явными знаниями. ***Неявные знания*** – это то, что собрал конкретный человек; уникальный, личный запас знаний, полученных из жизненного опыта, обучения и сети друзей, знакомых и профессиональных коллег (ATP 6-01.1). Все члены рабочей группы CEMA обладают знаниями, полученными в результате многолетнего оперативного и стратегического опыта, включая изученные особенности, тонкости и обходные пути предыдущих операций. ***Явные знания*** – это систематизированные или формально документированные знания, организованные и переданные другим лицам с помощью цифровых или нецифровых средств (ATP 6-01.1). Явное знание – это авторитетное знание, содержащее оценки и суждения, не подразумеваемые, а содержащиеся в теориях, правилах, доктринах. Для получения дополнительной информации о процессе управления знаниями см. ATP 6-01.1.

Приложение А

Приложение А. Методики сухопутных войск, используемые для планирования

Кибероперации и РЭБ требуют детального планирования и согласования с мероприятиями по планированию в рамках оперативного процесса. При планировании операций подразделения обычно полагаются на две наиболее распространённые методики сухопутных войск: методика выработки комплексных военных решений сухопутных войск (*англ. Army design methodology, ADM*) и процесс принятия военных решений (*англ. military decision-making process, MDMP*). В данном приложении обсуждается, как кибероперации и РЭБ внедряются и согласовываются в оперативном процессе и процессах внедрения с использованием методики выработки и принятия комплексных решений сухопутных войск и процесса принятия военных решений.

А-1. Методики планирования

А-1. Планирование – это непрерывная познавательная деятельность, и, хотя с него может начинаться оперативный процесс, оно не ограничивается составлением плана или приказа. Планирование может быть хорошо структурировано с участием командира, штаба, подчинённых командиров и других лиц, которые разрабатывают полностью согласованный план или приказ. Планирование также может быть менее строгим, в нём могут участвовать только командир и отдельные специалисты и подчинённые.

А-2. Приёмы и методы планирования меняются в зависимости от обстоятельств. Ответственные за планирование могут планировать вперёд, начиная с текущего момента, располагая потенциальные решения и действия в последовательном порядке, пока не достигнут желаемого конечного результата. Иногда ответственные за планирование разрабатывают планы в обратном порядке, начиная с предполагаемого конечного состояния и двигаясь в обратном направлении. Методы планирования могут быть аналитическими, как в процессе принятия военных решений, или более системными, как в методике выработки и принятия комплексных решений. Методика выработки и принятия комплексных решений и процесс принятия военных решений – две наиболее часто применяемые в сухопутных войсках методологии планирования. Результатом планирования является оперативный план или боевой приказ.

Примечание:

> Далее описывается только внедрение и согласование киберопераций и РЭБ в рамках оперативного процесса с использованием процессов внедрения. В данном приложении не рассматривается вопрос о том, как процессы внедрения или другие задачи включаются в оперативный процесс. Более подробную информацию о том, как процессы внедрения и другие задачи интегрируются в оперативный процесс, можно найти в документах разработчиков по каждому процессу.

А-1.1. Методика выработки и принятия комплексных решений

А-3. ***Методика выработки и принятия комплексных решений*** – это методика применения критического и творческого мышления для понимания, визуализации и описания проблем и подходов к их решению (ADP 5-0). Когда проблемы сложно выявить, конечное состояние операции не ясное или вариант действий не является самоочевидным; командиры используют методику выработки и принятия комплексных решений. Она особенно полезна в качестве вспомогательного средства при концептуальном планировании и должна быть интегрирована с детальным планированием, обычно связанным с процессом принятия военных решений, для создания исполняемых оперативных планов и боевых приказов.

Отделение CEMA участвует в составе группы по разработке методики, когда это необходимо, для понимания сложностей кибероперацій и проблем РЭБ. Методика выработки и принятия комплексных решений помогает в концептуальном планировании интеграции и согласования кибероперацій и РЭБ с основным замыслом операции.

Методика выработки и принятия комплексных решений имеет системный характер (фокусируется только на отдельных частях полного плана) и требует интеграции с более детальной и аналитической методикой планирования, такой как процесс принятия военных решений, для создания исполняемых оперативных планов и боевых приказов. В отличие от процесса принятия военных решений методика выработки и принятия комплексных решений не содержит заранее предписанных шагов. Тем не менее, с ней связаны несколько видов деятельности, которые включают:

1. Формулирование оперативной обстановки.
2. Формулирование проблем.
3. Разработка оперативного подхода.
4. Переформулирование при необходимости.

А-4. При изучении оперативной обстановки рабочая группа CEMA фокусируется на предоставлении группе по разработке методики полного понимания текущих условий в киберпространстве и ЭМС, в которых будет решаться предстоящая задача. Изучая оперативную обстановку, командир и штаб могут определить желаемое конечное состояние для оперативной обстановки, включая желаемые условия в киберпространстве и ЭМС, необходимые для проведения операций.

А-5. После того, как командир и штаб определяют желаемое конечное состояние для оперативной обстановки, рабочая группа CEMA начинает формулировать проблемы, связанные с выявленными препятствиями в киберпространстве и ЭМС, мешающие продвижению к желаемому конечному результату.

После того, как будет сформулирована каждая проблема и будут выработаны общие меры по предотвращению или уменьшению каждой проблемы, рабочая группа CEMA помогает командиру в разработке оперативного подхода к решению всех выявленных проблем. После выработки оперативного подхода к решению проблем командир и штаб переходят к более детальному процессу планирования – такому, как процесс принятия военных решений.

A-1.2. Процесс принятия военных решений

A-6. Процесс принятия военных решений является наиболее распространённой итеративной методикой планирования, используемой для понимания ситуации и задачи, разработки варианта действий и создания оперативного плана или боевого приказа. Командир, группа CEMA и штаб внедряют кибероперации и РЭБ в процесс принятия военных решений. Отделения CEMA в значительной степени опирается на взаимодействие со штабом, как участником рабочих групп CEMA, и его поддержку в планировании, интеграции и согласовании киберопераций и РЭБ в рамках процесса принятия военных решений

A-7. Процесс принятия военных решений состоит из семи этапов:

1. Этап 1: Получение задачи.
2. Этап 2: Анализ задачи.
3. Этап 3: Разработка варианта действий.
4. Этап 4: Анализ варианта действий.
5. Этап 5: Сравнение вариантов действий.
6. Этап 6: Утверждение варианта действий.
7. Этап 7: Издание, рассылка и передача приказов.

A-1.2.1. Этап 1: Получение задачи

A-8. Командиры инициируют процесс принятия военных решений после получения или в процессе ожидания задачи. На этом этапе отделение CEMA создаёт рабочую группу CEMA, состоящую из специалистов, участвующих во внедрении и согласовании киберопераций и РЭБ в рамках общей операции. Раннее оповещение позволяет рабочей группе CEMA определить количество времени, отведённое на планирование, внедрение и согласование киберопераций и РЭБ с общей операцией, и принять решение о подходе к планированию для выполнения этой задачи. Рабочая группа CEMA собирает необходимые материалы для подготовки к этапу 2: Анализ задачи. Эти материалы включают:

a. Текущие оценки киберопераций и РЭБ, в том числе:

- факты, касающиеся киберпространства и электромагнитной оперативной обстановки в назначенном районе операций;

- предположения относительно киберпространства и электромагнитной оперативной обстановки в назначенном районе операций;
- имеющиеся возможности для действий в киберпространстве и РЭБ своих войск и союзных сил в назначенном районе, включая имеющиеся технические данные;
- рекомендации по списку приоритетных целей для сменяемых подразделений;
- подробный список частот сменяемого подразделения;
- действия противника и его возможности в киберпространстве и РЭБ, включая имеющиеся технические данные;
- выводы и рекомендации для достижения целей командира в кибероперациях и РЭБ.

б. Соответствующие публикации, включая нормативные акты и доктрину СВ и объединённых сил по кибероперациям и РЭБ.

в. Все документы, связанные с задачей и районом операций, включая оперативный план или боевой приказ вышестоящего штаба, карты и рельеф местности, известные возможности своего, нейтрального киберпространства и РЭБ, а также киберпространства и РЭБ противника, используемые в районе операций, оперативные схемы.

г. Результаты разведки и оценки вышестоящего штаба и других организаций касающиеся действий своих войск, нейтральных субъектов, угроз в киберпространстве и РЭБ, а также военных аспектов местности в зоне ответственности, связанных с киберпространством и с РЭБ.

А-9. При развёртывании кибероперацийи ЭМА рабочая группа СЕМА обновляет данные о кибероперациях и выполняет оценку РЭБ, особенно по вопросам состояния своих войск, кибервозможностей и возможностей РЭБ, а также ключевых гражданских факторов. ***Текущая оценка*** (*англ. running estimate*) – это непрерывная оценка текущей ситуации, используемая для определения того, проводится ли текущая операция в соответствии с замыслом командира и осуществимы ли запланированные на будущее действия (ADP 5-0).

А-10. Рабочая группа СЕМА проводит первичную оценку времени и ресурсов, доступных для планирования, подготовки и начала кибероперацийи РЭБ, которые могут потенциально обеспечить замысел командира. Таблица А-1 иллюстрирует действия и ключевые результаты рабочей группы СЕМА на этапе 1: Получение задачи.

Таблица А-1

Этап 1: Получение задачи

Основные исходные данные	Процесс	Основные выходные данные
• Объявление тревоги командиром и первичные указания.	• Сбор инструментов, относящихся к кибероперациям и РЭБ.	• Обновление текущей оценки киберопераций и РЭБ.
• Планы операций или боевые приказы вышестоящих штабов.	• Уточнение текущих оценок киберопераций и РЭБ.	• Консолидация других необходимых инструментов киберопераций и РЭБ.
• Вышестоящие штабы предоставляют соответствующие инструменты киберопераций и РЭБ, включая текущие оценки.	• Предоставление данных по кибероперациям и РЭБ для первичных указаний и боевого приказа.	

А-1.2.2. Этап 2: Анализ задачи

А-11. Процесс принятия военных решений продолжается оценкой ситуации, называемой анализом задачи. Командир и штаб, информируемые подчинёнными и соседними командирами, а также союзниками, собирают, анализируют и объединяют информацию для понимания текущих условий оперативной обстановки. Благодаря анализу задачи командир и штаб могут получить ситуативную осведомлённость в данной оперативной обстановке. Затем они могут определить, *что* командование должно выполнить, ***когда*** и ***где*** должны быть проведены операции и ***почему*** операция необходима.

А-12. Отделение CEMA анализирует и объединяет материалы киберопераций и РЭБ, собранные на этапе 1: Получение задачи, для достижения ситуативной осведомлённости в киберпространстве, ЭМС и информационной среде в районе операций, в котором будет проводиться операция. Рабочая группа CEMA анализирует оперативный план или боевой приказ вышестоящего штаба, уделяя особое внимание Приложению C, Дополнение 12. Подразделение штаба G-6 или S-6 фокусируется на Приложении H. Анализируя оперативный план или боевой приказ вышестоящего штаба, отделение CEMA может добиться понимания задач и целей подразделения в киберпространстве и РЭБ, и о том, как они способствуют выполнению задачи, замыслу командира и концепции операций. Во время анализа задачи рабочая группа CEMA использует оперативный план или боевой приказ вышестоящего штаба для получения информации об имеющихся ресурсах киберпространства и РЭБ, сроках операции, а также задач в киберпространстве и РЭБ, выполняемых другими видами ВС и участниками совместных действий.

A-13. Во время анализа задачи G-2 или S-2 руководит разведывательной подготовкой района боевых действий, анализируя такие параметры задачи, как противник, местность, погода и гражданские факторы в районе операций. Отделение CEMA взаимодействует с G-2 или S-2 на протяжении всей разведывательной подготовки района боевых действий, чтобы помочь проанализировать влияние этих изменяющихся факторов на кибероперации и РЭБ. Это взаимодействие включает использование материалов и данных, полученных от вышестоящего штаба, для первичного анализа местности.

A-14. Процесс разведывательной подготовки района боевых действий выявляет критические пробелы в знаниях командира об оперативной обстановке, включая пробелы в одном или нескольких военных аспектах местности и общей информационной среды, связанных с киберпространством и ЭМС. Командир и штаб используют эти пробелы в качестве руководства для выработки своих информационных требований или результатов разведывательной подготовки района боевых действий. Рабочая группа CEMA устанавливает исходные информационные требования для получения информации о пробелах, выявленных в ходе анализа местности, для оценки киберпространства и оперативной электромагнитной обстановки. Результаты разведывательной подготовки района боевых действий, предоставляемые отделением CEMA, в совокупности с результатами разведывательной подготовки района боевых действий, выработанными другими штабами во время анализа задачи для других операций, включают:

а. Составление первичного списка приоритетных разведывательных задач.

б. Разработка полного уточнённого комбинированного электронного рабочего слоя препятствий с учётом киберпространства и РЭБ в назначенном районе операций.

в. Разработка электронных рабочих слоёв угроз, включая киберпространство и РЭБ в назначенном районе операций.

г. Список важных целей кибероперации и РЭБ.

д. Выявление военных аспектов местности, связанных с киберпространством и РЭБ.

е. Предварительные шаблоны и матрицы событий, включающие вопросы кибероперации и РЭБ.

A-15. Рабочая группа CEMA анализирует оперативный план или боевой приказ вышестоящего штаба и указания вышестоящего командира, чтобы определить свои назначенные и взаимосвязанные задачи, связанные с операциями в киберпространстве и РЭБ. ***Назначенная задача*** (*англ. specified task*) – это задача, специально поставленная подразделению его вышестоящим штабом (FM 6-0). ***Взаимосвязанная задача*** (*англ. implied task*) – это задача, которая должна быть выполнена для осуществления назначенной задачи или операции, но не указанная в приказе вышестоящего штаба (FM 6-0).

Графа «***что***» из формулировки операции в оперативном плане или боевом приказе вышестоящего штаба всегда является задачей. Отделение CEMA определяет важные задачи из назначенных и взаимосвязанных киберзадач и задач РЭБ, включённых в рекомендованную формулировку операции подразделения. ***Важная задача*** (*англ. essential task*) – это назначенная или взаимосвязанная задача, которая должна быть выполнена для достижения цели операции (FM 6-0).

A-16. Отделение CEMA рассматривает текущий список задач подразделения по использованию средств киберпространства и РЭБ, взаимодействие с командованием и подразделениями поддержки, приданными для усиления, а также состояние текущих средств и возможностей для кибероперации и РЭБ и их ограничения. Отделение CEMA также анализирует возможности в киберпространстве и РЭБ соседних, объединённых, союзных сил и гражданских организаций, действующих в районе операций подразделения. В результате анализа отделение CEMA определяет наличие в данных подразделениях и организациях ресурсов, необходимых для выполнения всех назначенных, взаимосвязанных и важных задач, а также для определения других кибересурсов и ресурсов РЭБ, необходимых для успеха выполнения задачи. Офицер по кибервойне и РЭБ докладывает командиру обо всех выявленных недостатках ресурсов для кибероперации и РЭБ, информацию о которых необходимо направить в вышестоящий штаб. Отделение CEMA докладывает командиру о любых отклонениях от стандартной организации задач, которые следует учитывать при разработке указаний по планированию.

A-17. Рабочая группа CEMA определяет любые ограничения, налагаемые на подразделение в отношении кибероперации и РЭБ. ***Ограничение*** (*англ. constraint*) – это ограничивающее условие, наложенное вышестоящим командованием (FM 6-0). Ограничение диктует действие или бездействие, тем самым ограничивая свободу действий подчинённого командования. Ограничения указаны в пункте 3 оперативного плана или боевого приказа. Отделение CEMA должно хорошо знать ограничения в киберпространстве и РЭБ, включая используемый спектр, типы разрешённых средств кибероперации и РЭБ, а также полномочия на кибероперации и РЭБ, делегированные и не делегированные командиру подразделения.

A-18. Рабочая группа CEMA собирает критически важные факты, основываясь на анализе задачи и оперативных данных, предоставленных в рамках процесса разведывательной подготовки района боевых действий, а также от соседних, вышестоящих, объединённых и союзных подразделений. Эта информация помогает в разработке предположений об обстановке в киберпространстве и оперативной электромагнитной обстановке в назначенном районе операций. Факт – это истинное утверждение или утверждение, считающееся истинным в данный момент. Предположение – это допущение о текущей ситуации или о будущем ходе событий, одно из которых или оба считаются верными в отсутствие достоверных доказательств, необходимых для того, чтобы командир в процессе планирования смог выполнить оценку ситуации и принять решение о выборе варианта действий.

При отсутствии фактов рабочая группа CEMA выдвигает предположения о ситуации в киберпространстве и ЭМС в назначенном районе операций. Эти предположения включают потенциальные угрозы в киберпространстве и РЭБ, действующие в назначенном районе операций.

A-19. Отделение CEMA использует управление рисками для определения приоритетов в области кибербезопасности. Оно взаимодействует со специалистом по управлению спектром G-6 или S-6 для анализа совместного списка разрешённых частот и устранения явных и потенциальных конфликтов частот и сетей. Отделение CEMA использует защиту от электромагнитного излучения для ослабления электромагнитного воздействия на окружающую среду, решения проблем электромагнитной совместимости, реализации электромагнитной защищённости и электромагнитной маскировки.

A-20. В ходе анализа операции рабочая группа CEMA выявляет пробелы (в киберпространстве и РЭБ) в информации, полученной от вышестоящих штабов, соседних и объединённых подразделений, других участников выполнения задачи. Информация об этих пробелах предоставляется командиру и добавляется к критическим информационным требованиям командира, которые подразделяются на две категории: приоритетные требования к разведывательным данным и требования к информации о своих войсках. ***Приоритетное требование к разведывательным данным*** (*англ. priority intelligence requirement*) – это требование к разведывательным данным, заявленное в качестве приоритета для разведывательного обеспечения, которое необходимо командиру и штабу для понимания противника или других аспектов боевой обстановки (FM 6-0). ***Требование к информации о своих войсках*** (*англ. friendly force information requirement*) – это информация, необходимая командиру и штабу для понимания состояния своих войск и возможностей обеспечения (FM 6-0).

A-21. Отделение CEMA тесно взаимодействует с G-3 (или S-3) и G-2 (или S-2) при разработке плана первичного сбора информации. Оно также взаимодействует с этими подразделениями штаба для уточнения усилий по сбору информации с целью получения ответов на вопросы, необходимые для разработки эффективного плана. Отделение CEMA предоставляет командиру приоритетные требования к разведывательным данным и требования к информации о своих войсках по кибероперациям и РЭБ в качестве вклада в план сбора информации.

A-22. Первичный план сбора информации позволяет начать операции по рекогносцировке, наблюдению и разведке. Подразделение G-2 или S-2 несёт общую ответственность за план сбора информации и тесно взаимодействует с G-3 или S-3, а также получает информацию для обеспечения процесса разведывательной подготовки района боевых действий путём согласования доступных данных PPTP для удовлетворения критически важных информационных требований командира и

информационных требований штаба, а также предоставления командиру разведывательных данных по всей оперативной обстановке для непрерывного владения ситуативной осведомлённостью.

A-23. По мере поступления информации отделение CEMA обновляет текущие оценки кибероперациий и РЭБ, что позволяет вносить необходимые коррективы в общий план операции. Отделение CEMA оценивает использование имеющегося времени, сравнивая время, необходимое для выполнения задач кибероперациий и РЭБ, с графиком вышестоящего штаба, и определяет возможность выполнения задачи в отведённое время. Отделение CEMA вносит необходимые уточнения в план операций, стараясь не выходить за временные рамки, и информирует командира о любых задачах, которые не могут быть выполнены в отведённое время, особенно о тех, которые считаются критическими или важными. Командир использует эту информацию для определения допустимых рисков и информирования вышестоящих штабов о недостатках, выявленных в связи с временными ограничениями.

A-24. Отделение CEMA участвует в разработке критериев оценки варианта действий, устанавливая стандарты для измерения эффективности и результативности кибероперациий и РЭБ, рассматриваемых в рамках одного варианта действий, по сравнению с другими вариантами. Разработка этих критериев в ходе анализа задачи помогает устранить предвзятость перед анализом и сравнением вариантов действий. Таблица A-2 иллюстрирует действия и ключевые результаты рабочей группы CEMA на этапе 2: Анализ задачи.

Таблица A-2

Этап 2: Анализ задачи

Основные исходные данные	Процесс	Основные выходные данные
• Первичные указания командира. • Материалы вышестоящих штабов, включая оперативный план/боевой приказ, а также данные разведки и другие интеллектуальные продукты. • Интеллектуальные материалы из других организаций.	• Анализ информации по кибероперациям и РЭБ из материалов вышестоящих штабов. • Участие в брифинге по анализу задач. • Участие в процессе разведывательной подготовки района боевых действий. • Анализ оперативного плана/боевого приказа вышестоящего штаба на наличие назначенных и взаимосвязанных, важных задач кибероперациий и РЭБ	• Понимание задач, целей и вклада подразделения в выполнение задач кибероперациий и РЭБ. • Понимание имеемых средств кибероперациий и РЭБ и хронологических рамок их использования. • Понимание задач кибероперациий и РЭБ смежных, поддерживающих и поддерживаемых подразделений в назначенном районе операций.

Основные исходные данные	Процесс	Основные выходные данные
• Материалы методики выработки комплексных решений (если только командир не решит сразу перейти к процессу принятия военных решений).	• Изучение текущей системы организации задач подразделения по работе со средствами киберпространства и РЭБ. • Изучение средств воздействия на киберпространство и РЭБ смежных, объединённых сил и других участников выполнения задач и гражданских организаций в назначенном районе операций. • Сбор критически важных фактов для разработки предположений. • Начало работы над процессом управления рисками, связанными с кибероперациями и РЭБ. • Продолжение анализа информации о кибероперациях и РЭБ из вышестоящих штабов, соседних и объединённых подразделений, других участников совместных действий.	• Получение полной информации о назначенном районе операций, включая всех участников выполнения задачи. • Выявление критических проблем в киберпространстве, ЭМС и информационной среде в назначенном районе операций. • Перечисление исходных требований к разведке, связанных с кибероперациями и РЭБ, используемых для определения первоочередных требований к разведке, уточнённых электронных рабочих слоёв препятствий, угроз, обнаружения важных целей, особенностей местности, шаблонов не уточнённых событий и матриц. • Выявление назначенных, взаимосвязанных и важных задач, используемых для рекомендуемой формулировки задачи. • Определение средств, необходимых для выполнения назначенных, взаимосвязанных и важных задач. • Определение потребности в дополнительных средствах для кибероперациий и РЭБ (с передачей в вышестоящие штабы). • Знание ограничений в кибероперациях и РЭБ, налагаемых вышестоящим командованием.

Основные исходные данные	Процесс	Основные выходные данные
		• Упреждение отклонений от стандартной организации задач для штаба, чтобы помочь командиру в подготовке рекомендаций по планированию для выработки плана действий. • Разработка предположений по кибероперациями и РЭБ, включая киберугрозы и угрозы РЭБ, существующие в районе проведения операций, необходимых для планирования. • Определение особых факторов кибероперациий и РЭБ, требующих снижения рисков. • Выявление пробелов в информации по кибероперациям и РЭБ для удовлетворения критических информационных требований командира, и разработка плана сбора такой информации. • Уточнение текущих оценок кибероперациий и РЭБ. • Согласование и внедрение средств кибервоздействия и РЭБ для проведения информационных операций. • Установление стандартов оценки эффективности и результативности кибероперациий и РЭБ при разработке критериев оценки плана действий.

A-1.2.3. Этап 3: Разработка варианта действий

A-25. При разработке варианта действий для последующего анализа и сравнения создаются варианты, отвечающие замыслу командира и указаниям по планированию.

Вариант действий – это широкое потенциальное решение выявленной проблемы. При разработке варианта действий рабочая группа CEMA использует инструменты, полученные и проанализированные из вышестоящего штаба, соседних и объединённых подразделений, а также от других участников совместных действий в сочетании с намерением командира, собранным руководством по планированию. Отделение CEMA участвует в разработке варианта действий, осуществляя внедрение и согласование кибероперaций и РЭБ в вариант действий с использованием оперативного и тактического искусства. При выработке различных вариантов рабочая группа CEMA разрабатывает различные методы внедрения, согласования и проведения кибероперaций и РЭБ, которые находятся в рамках замысла командира и руководства по планированию.

A-26. Отделение CEMA оказывает помощь другим специалистам штаба в изучении каждого предполагаемого варианта на предмет обоснованности с использованием критериев оценки, установленных на этапе 2: «Анализ задачи». При рассмотрении обоснованности каждого предполагаемого варианта критерии отбора должны включать:

а. Обоснованность. Внедрённые и согласованные кибероперации и РЭБ в вариант действий, которые обеспечивают выполнение боевой задачи в рамках установленных ограничений по времени, району, ресурсам киберпространства и РЭБ.

б. Приемлемость. Внедрение и согласование кибероперaций и РЭБ в вариант действий позволяет сбалансировать затраты и риски с получаемыми преимуществами.

в. Целесообразность. Кибероперации и РЭБ поддерживают вариант действий, который выполняет задачу в соответствии с замыслом командира и указаниями по планированию.

г. Различимость. Внедрение, согласование, а также порядок проведения кибероперaций и РЭБ должны быть различными для каждого разрабатываемого варианта действий. Эти различия должны включать организацию задач, имеющиеся возможности киберпространства и РЭБ, а также возможность использования ресурсов киберпространства и РЭБ соседних, объединенных подразделений и других участников совместных действий.

д. Полнота. Кибероперации и РЭБ, внедрённые и согласованные в вариант действий, должны включать:

- Каким образом кибероперации и РЭБ будут поддерживать оперативный процесс.
- Каким образом кибероперации и РЭБ обеспечивают операции по формированию, созданию и сохранению необходимых условий для успеха в решающих операциях или действиях.

- Каким образом действия в киберпространстве и РЭБ поддерживают операции по формированию необходимых условий, создавая и сохраняя условия для успеха во время решающих операций или действий.
- Каким образом кибероперации и РЭБ поддерживают вариант действий, учитывая наступательные, оборонительные действия, а также поддержку устойчивости или защиту гражданских властей.
- Каким образом осуществлять кибероперации и РЭБ, выполняя назначенные, взаимосвязанные и важные задачи для достижения желаемых результатов в киберпространстве и ЭМС.
- Каким образом использовать средства и возможности киберпространства и РЭБ для ослабления препятствий, получения доступа к различным путям подхода (включая наблюдение и секторы огня) и защиты ключевой области в киберпространстве и ЭМС.

A-27. При разработке варианта командиры и штаб должны понимать и ценить непредсказуемый и неопределённый характер оперативной обстановки. Отделение CEMA должно демонстрировать такое же понимание и осознание непредсказуемости и неопределённости при поддержке разработки схем кибероперациий и РЭБ для каждого варианта.

A-28. Рабочая группа CEMA оценивает кибероперации и РЭБ как средства для боевой мощи (оценка относительной боевой мощи).

Боевая мощь (*англ. combat power*) – это совокупность разрушительных, конструктивных и информационных возможностей, которые воинская часть или подразделение может применить в данный момент времени (ADP 3-0). Боевая мощь включает боевое обеспечение, командование и информацию.

A-29. Рабочая группа CEMA проводит оценку как штатных, так и нештатных кибервозможностей и возможностей РЭБ, доступных для операции. Эта оценка помогает отделению CEMA произвести грубый подсчёт соотношения своих кибервозможностей и возможностей РЭБ с известными кибервозможностями и возможностями РЭБ противника.

A-30. Отделение CEMA сравнивает сильные стороны совместных (штатных и не штатных) своих возможностей воздействий на киберпространство и РЭБ со слабыми сторонами воздействия на киберпространство и РЭБ противника, и наоборот.

Отделение CEMA использует это сравнение для выявления уязвимостей в киберпространстве и ЭМС своих войск и для получения понимания об эффективном проведении кибероперациий и РЭБ в назначенном районе операций.

A-31. На основании указаний командира и первичных результатов оценки относительной боевой мощи рабочая группа CEMA разрабатывает различные схемы кибероперaций и РЭБ для выработки вариантов действий. Схема для каждого варианта должна отражать противодействие для каждого вероятного варианта действий противника с учётом основных задач по обеспечению стабильности (обеспечение определенного уровня гражданской безопасности, гражданского управления и некоторых важных служб). Рабочая группа CEMA использует «мозговой штурм» для выработки вариантов с целью получения максимально широкого набора вариантов при создании схем кибероперaций и РЭБ для вариантов действий. В ходе «мозгового штурма» все участники рабочей группы должны сохранять непредвзятость при разработке предлагаемых вариантов.

A-32. Рабочая группа CEMA определяет необходимые доктринальные требования СВ и объединённых сил к кибероперациям, РЭБ, а также к поддерживающим и обеспечивающим операциям. Далее рабочая группа CEMA рассматривает потенциальные кибервозможности и возможности РЭБ для нештатных подразделений и других невоенных организаций и ведомств.

A-33. При выработке замысла операции командир и штаб разрабатывают оперативную схему, позволяющую визуализировать и описать применение боевой мощи во времени, пространстве, целях и ресурсах. Оперативная схема состоит из четырех компонентов:

1. Командирам назначается район боевых действий для проведения операций.
2. Командиры могут назначать глубокие, ближние, тыловые районы и районы взаимодействия для описания физического расположения сил во времени и пространстве.
3. В районах глубокого, близкого, тылового обеспечения и сосредоточения командиры разрабатывают решающие, формирующие и поддерживающие операции, чтобы чётко определить цель операции.
4. Командиры определяют основные и вспомогательные действия для установления приоритетов в распределении ресурсов.

A-34. Рабочая группа CEMA проводит «мозговой штурм» для выработки вариантов обеспечения необходимых возможности в киберпространстве и РЭБ для поддержки четырёх компонентов оперативной структуры. После того как рабочая группа CEMA изучила возможности поддержки кибероперaций и РЭБ для каждого варианта действий, она изучает каждый вариант для определения – удовлетворяет ли он критериям отбора, указанным в пункте A-28, изменяя, добавляя и исключая варианты действий по мере необходимости. Во время проверки рабочая группа CEMA уделяет особое внимание разработанной схеме кибероперaций и РЭБ для каждого варианта действий. Рабочая группа CEMA должна избегать создания одного хорошего варианта на основе нескольких несовершенных при выработке вариантов.

A-35. Рабочая группа CEMA определяет необходимые возможности воздействия на киберпространство и РЭБ для использования в качестве средств обеспечения боевых возможностей, необходимых для выполнения соответствующих задач и целей решающих операций, операций по формированию необходимых условий и поддерживающих операции (третий компонент оперативной схемы). Рабочая группа CEMA использует исторические нормативы планирования в качестве отправной точки для определения необходимого соотношения сил и средств в киберпространстве и РЭБ к силам и средствам в киберпространстве и РЭБ противника, которое приведёт к желаемому результату.

A-36. Рабочая группа CEMA также рассматривает соотношение возможностей воздействия в киберпространстве и РЭБ, необходимых для формирования оперативной обстановки, в результате чего формируется первичный перечень общего количества средств воздействия в киберпространстве и РЭБ, необходимых для выполнения задачи. Рабочая группа CEMA добавляет эту информацию в общий состав сил подразделения, используемых в общем замысле операции командира. В общей концепции операции командир описывает, как объединённые силы выполнят задачу в рамках замысла командира.

A-37. Отделение CEMA участвует в брифинге по варианту действий, на котором штаб доводит до сведения командира каждый разработанный вариант. Офицер по кибервойне и РЭБ информирует командира о действиях и возможностях в области киберпространства и РЭБ, включённых в каждый вариант, в том числе о последствиях, обусловленных условиями оперативной обстановки и задачи. Он также объясняет, как каждая стратегия кибероперaций и РЭБ может привести к желаемому результату. После брифинга по варианту действий командир выбирает или изменяет выбранные варианты действий для дальнейшего анализа и отдаёт указание по планированию.

A-38. В процессе разработки варианта действий рабочая группа CEMA продолжает уточнять оценки киберпространства и РЭБ, а также данные разведывательной подготовки района боевых действий (такие как электронные рабочие слои, важные цели и аспекты территории). Таблица A-3 иллюстрирует действия и ключевые результаты рабочей группы CEMA на этапе 3: «Разработка варианта действий».

A-39. Используя информацию, полученную в результате совместных действий рабочей группы CEMA, отделение CEMA разрабатывает пояснительные записки и схемы по кибероперациям и РЭБ для G-3 или S-3, которые включаются в итоговые пояснительные записки и вспомогательные схемы по каждому варианту действий. В такой пояснительной записке описывается, как кибероперации и РЭБ поддерживают выполнение варианта с учётом реализации концепции совместных действий различных видов ВС и родов войск. На схеме наглядно демонстрируется, как кибероперации и РЭБ будут поддерживать войска, осуществляющие движение и манёвр, включая развёртывание войск.

Таблица А-3

Этап 3: Разработка варианта действий

Основные исходные данные	Процесс	Основные выходные данные

• Формулировка задачи командира, указания по планированию и замысел.
• Требования командира к критически важной информации.
• Обновлённая разведывательная подготовка материалов по району боевых действий.
• Актуальные материалы по кибероперациям и РЭБ вышестоящих штабов, включая обновлённые текущие оценки.
	• Выработка различных вариантов кибероперацій и РЭБ для каждого варианта действий.
	• Оказание помощи в изучении каждого разрабатываемого варианта действий на предмет его эффективности.
	• Оценка кибероперацій и РЭБ как задач оценки боевой мощи.
	• Оценка имеющихся средств и возможностей в киберпространстве и РЭБ (штатных и нештатных) для проведения операции.
	• Сравнение объединённых возможностей своих войск в киберпространстве и РЭБ с возможностями противника и наоборот.
	• Определение необходимых требований доктрин СВ и объединённых сил.
	• Разработка документов и проектов, связанных с киберпространством и РЭБ.
	• Участие в разработке оперативного процесса.
	• Участие в брифинге о ходе работы.
		• Внедрение и проверка эффективной схемы кибероперацій и РЭБ для каждого предлагаемого варианта действий.
		• Примерное сопоставление возможностей действий в киберпространстве и РЭБ противника.
		• Определение известных уязвимостей в своих возможностях в киберпространстве и РЭБ.
		• Определение видов средств воздействия в киберпространстве и РЭБ, необходимых для поддержки соответствующих задач и целей решающих, формирующих и поддерживающих операций.
		• Уточнение текущих оценок кибероперацій и РЭБ, связанных с разведкой, и материалов по подготовке поля боя.
		• Документы и проекты плана действий, связанные с киберпространством и РЭБ.:
		  • Обеспечение организации выполнения задач силами кибероперацій и средствами РЭБ.
		  • Описание – как кибероперации и РЭБ поддерживают общую концепцию операций.

Примечание:

> Командир может отклонить все варианты действий, принять один или несколько вариантов или создать новый, включив в него отдельные элементы из одного или из нескольких вариантов действий, представленных на брифинге. Если командир отклоняет все варианты действий, штаб начинает заново разрабатывать новые варианты. Принятые или изменённые варианты действий переходят к этапу 4: «Анализ варианта действий и командно-штабные учения».

A-1.2.4. Этап 4: Анализ варианта действий и командно-штабные учения

A-40. Анализ вариантов действий позволяет командиру и штабу выявить сложности, проблемы взаимодействия или вероятные результаты планируемых действий для каждого варианта (принятого или изменённого на этапе 3: «Разработка варианта действий»). На этом этапе рабочая группа CEMA может определить наличие уязвимостей в каждой схеме кибероперациий и РЭБ, внедрённой в каждый принятый или изменённый вариант действий. Эти уязвимости могут включать:

а. Вероятные нежелательные воздействия в киберпространстве и РЭБ на оперативные параметры и параметры боевой задачи и наоборот.

б. Потенциальные проблемы взаимодействия с внешними (нештатными) подразделениями при проведении кибероперациий и ведения РЭБ.

в. Отсутствие необходимых возможностей в киберпространстве и РЭБ для достижения желаемого результата.

A-41. Рабочая группа CEMA использует эту новую информацию для пересмотра и уточнения частей варианта действий, связанных с киберпространством и РЭБ, по мере появления расхождений. Анализ варианта действий может также выявить потенциальные проблемы исполнения, решений и непредвиденных обстоятельств, что может потребовать повторного планирования.

A-42. Процесс, используемый для анализа варианта действий, называется командно-штабные учения (далее – КШУ). Командно-штабные учения состоят из правил и этапов, позволяющих визуализировать ход операции с учётом сил и средств и возможностей противника для каждого возможного варианта действий. КШУ включают в сценарий переменные параметры задачи, в том числе последствия и требования к гражданскому населению в районе операций.

A-43. С помощью КШУ рабочая группа CEMA может визуализировать необходимые возможности киберпространства и РЭБ для соответствующих целей в районе операций. Рабочая группа CEMA может также определить потенциальные уязвимости, требующие защиты в киберпространстве и РЭБ.

Во время КШУ группа CEMA оказывает помощь G-3 или S-3 в выполнении своих обязанностей командования в ходе КШУ, проводя оценку кибероперaций и РЭБ в рамках замысла манёвра своих войск. Отделение CEMA также оказывает помощь G-3 или S-3, внося материалы, связанные с киберпространством и РЭБ, в формулировки плана действий и вспомогательный документ по каждому варианту действий. Результатом проведения КШУ являются уточнённые варианты действий с уточнёнными схемами кибероперaций и РЭБ, с заполненной синхронизирующей матрицей, а также уточнёнными шаблонами и схемами обеспечения принятия решений для каждого варианта действий.

Примечание:

> Подразделение G-6 или S-6 оценивает операции в информационной сети МО, операции по управлению спектром и их осуществимость по каждому разыгрываемому варианту действий в ходе командно-штабных учений.

A-44. В синхронизирующей матрице фиксируются результаты командно-штабных учений и отображается порядок согласования действий своих подразделений по каждому варианту действий во времени, пространстве и целям по отношению к действиям противника. Она включает согласование и интеграцию кибероперaций и РЭБ в интересах боевого обеспечения по каждому варианту действий. Шаблон и матица поддержки принятия решений иллюстрируют ключевые решения и потенциальные действия, которые могут возникнуть в ходе выполнения каждого варианта действий.

A-45. Отделение CEMA участвует в брифинге по командно-штабным учениям, доводя информацию до подчинённых подразделений кибероперaций и РЭБ, чтобы убедиться, что все понимают результаты КШУ. Отделение CEMA регистрирует все моменты командно-штабных учений, связанные с киберпространством и РЭБ, прежде чем провести брифинг для командира. Отделение CEMA разрабатывает и подаёт заявку на дополнительные средства воздействия в киберпространстве и РЭБ для уменьшения уязвимостей, выявленных в ходе КШУ. Таблица A-4 иллюстрирует действия и ключевые результаты рабочей группы CEMA на этапе 4: «Анализ варианта действий и командно-штабные учения».

Таблица А-4.

Этап 4: Анализ вариантов действий и КШУ

Основные исходные данные	Процесс	Основные выходные данные
• Пересмотренное указание командира по планированию • Предлагаемые варианты действий, включая решения по кибероперациям и РЭБ • Уточнённые материалы разведывательной подготовки района боевых действий. • Актуальные материалы по кибероперациям и РЭБ вышестоящих штабов, включая уточнённые текущие оценки. • Допущения, сделанные на предыдущих этапах.	• Участие в командно-штабных учениях. • Определение уязвимых мест в плане кибероперацийи РЭБ для каждого варианта действий в КШУ. • Разработка проектов документов для запроса поддержки дополнительных средств киберпространства и РЭБ. • Представление материалов по кибероперациям и РЭБ для включения в синхронизирующую матрицу.	• Уточнённая схема кибероперацийи РЭБ для каждого варианта действий • Уточнённые данные разведки района боевых действий, используемые для целеуказания и электронных рабочих слоёв. • Дополнительная информация, необходимая командиру для выполнения основных требований командира к критической информации. • Подача запросов на дополнительные средства воздействия в киберпространстве и средства РЭБ. • Уточнённая текущая оценка кибероперацийи РЭБ. • Уточнённые предположения.

А-1.2.5. Этап 5: Сравнение вариантов действий

А-46. Командир и штаб объективно и независимо оценивают разработанные в ходе КШУ варианты действий на основе критериев оценки, установленных на этапе 2: «Анализ задач» и уточнённых на этапе 3: «Разработка варианта действий». Цель состоит в определении сильных и слабых стороны для каждого варианта действий и выборе варианта с наибольшей вероятностью успеха, а также разработке оперативного плана или боевого приказа.

А-47. Отделение CEMA проводит анализ преимуществ и недостатков с использованием схемы принятия решений для оценки каждого варианта по заданным критериям оценки. В отделении CEMA выделяются преимущества и недостатки кибероперацийи РЭБ для каждого варианта, относящегося к общей задаче. Отделение CEMA представляет эти выводы командиру и другому личному составу штаба. Отзывы, полученные в ответ на запросы о поддержке рабочей группы CEMA, вносят свой вклад в многочисленные определяющие факторы при анализе преимуществ и недостатков.

A-48. Результаты анализа преимуществ и недостатков, проведённого всеми специалистами, заносятся в матрицу принятия решений, позволяющую командиру тщательно и логично сравнить и оценить варианты действий. Матрица решений помогает командиру принять оптимальное решение.

A-49. После анализа и сравнения штаб определяет предпочтительный вариант действий и даёт рекомендации. Если штаб не в состоянии прийти к единому мнению, начальник штаба (ответственный офицер) решает, какой вариант действий рекомендовать. Затем штаб проводит брифинг по принятию решения для командира, в котором начальник штаба отмечает изменения, внесённые в каждый вариант действий в результате командно-штабных учений. Таблица A-5 иллюстрирует действия и ключевые результаты рабочей группы CEMA на этапе 5: «Сравнение вариантов действий».

Таблица A-5

Этап 5: Сравнение вариантов действий

Основные исходные данные	Процесс	Основные выходные данные
• Уточнённые материалы разведывательной подготовки района боевых действий. • Уточнённые варианты действий с уточнёнными схемами кибероперaций и РЭБ. • Актуальные материалы по кибероперациям и РЭБ вышестоящих штабов, включая уточнённые текущие оценки. • Обратная связь по поданным запросам на поддержку в киберпространстве и РЭБ.	• Проведение анализа преимуществ и недостатков для каждого варианта действий. • Сравнение и оценка вариантов действий с отделением CEMA с акцентом на схему киберпространства и РЭБ. • Проведение брифинга по решению о порядке для рекомендации предпочтительного варианта действий штаба.	• Рекомендуемый штабом вариант действий. • Уточнённая текущая оценка киберпространства и РЭБ.

A-1.2.6. Этап 6: Утверждение варианта действий

A-50. После брифинга по принятию решения командир выбирает вариант, который наилучшим образом позволяет выполнить поставленную задачу. Если командир отклоняет все варианты, штаб возобновляет процесс разработки нового варианта. Если командир изменяет предложенный вариант или даёт штабу совершенно другой вариант, штаб проводит командно-штабные учения с новым вариантом действий и представляет результаты командиру со своими рекомендациями.

A-51. После утверждения варианта действий командир издаёт окончательное руководящее указание по планированию, включающее уточнённый замысел командира и новые критические требования командира к информации для обеспечения выполнения варианта. Окончательное указание по планированию также содержит любые дополнительные положения по очерёдности боевого обеспечения, подготовке приказов, репетициям и подготовке. Он также включает приоритеты, необходимые для сохранения свободы действий и обеспечения непрерывной устойчивости.

A-52. Командир определяет приемлемые риски в окончательных указаниях по планированию, чтобы получить согласование от вышестоящего командира для принятия рисков, которые могут повлиять на выполнение задачи вышестоящего командира. На основании решения командира и окончательного руководства по планированию штаб преобразует утверждённый вариант действий в замысел операций и отдаёт предварительное распоряжение подчинённым командирам. Отделение CEMA продолжает доработку Дополнения 12 к Приложению C к оперативному плану или к боевому приказу и оказывает помощь подразделению G-6 или S-6 в работе с Дополнениями 1 и 6 к Приложению H, если это необходимо. Таблица A-6 иллюстрирует действия и ключевые результаты рабочей группы CEMA на этапе 5: «Утверждение варианта действий».

Таблица A-6

Этап 6: Утверждение варианта действий

Основные исходные данные	Процесс	Основные выходные данные
• Уточнённая текущая оценка кибероперациий и операций в ЭМС. • Оценка вариантов действий. • Предлагаемый штабом вариант действий • Актуальные материалы по кибероперациям и РЭБ вышестоящих штабов, включая уточнённые текущие оценки. • Обратная связь по поданным запросам на поддержку в киберпространстве и РЭБ.	• Обзор окончательных указаний командира по планированию. • Обзор допустимого для командира риска. • Предоставление информации о кибероперациях и РЭБ в соответствии с предварительным распоряжением.	• Окончательные указания командира по планированию. • Утверждённый вариант действий. • Допустимые риски командира. • Проект Приложения C, Дополнения 12 к предварительному распоряжению. • Оказание помощи G-6/S-6 в подготовке проекта Приложения H, Дополнений 1 и 6, в зависимости от ситуации, для предварительного распоряжения.

Основные исходные данные	Процесс	Основные выходные данные
		• Уточнение замысла командира, критических требований командира к информации о своих войсках. • Уточнённые предположения. • Передача предварительного распоряжения подчинённым штабам.

A-1.2.7. Этап 7: Издание, распространение и передача приказов

A-53. Штаб преобразует утверждённый вариант действий в оперативный план или в боевой приказ с чётким, лаконичным замыслом операции и вспомогательной информацией. Изложение варианта действий становится замыслом операций для оперативного плана или боевого приказа. Отделение CEMA отвечает за отработку окончательного варианта Дополнения 12 к Приложению C к оперативному плану или боевому приказу. Отделение CEMA оказывает помощь G-6 или S-6 в работе с Дополнениями 1 и 6 к Приложению H, в зависимости от ситуации.

A-54. Прежде чем командир утвердит оперативный план или боевой приказ, штаб обеспечивает его согласованность и соответствие замыслу вышестоящего командира путем сверки и перекрёстной передачи планов и приказов. Штаб проводит сверку плана и приказов, детально анализируя весь оперативный план или боевой приказ и все приложения к нему, добиваясь полного согласия всего штаба. В процессе согласования штаб в явном виде сопоставляет замысел, задачу и критические информационные требования командира с замыслом операций и различными схемами обеспечения, включая схему кибероперациий и РЭБ. По всем несоответствиям и пробелам в планировании принимаются корректирующие решения.

A-55. Штаб проводит сверку планов и приказов, сравнивая оперативный план или боевой приказ с планами вышестоящих и соседних командиров для достижения единства действий и обеспечения соответствия плана замыслу вышестоящего командира. Как и при сверке, так и при перекрёстном анализе также выявляются несоответствия или пробелы в планировании, требующие корректирующих мер. На этапе 7 осуществляется переход от планирования к подготовительной деятельности в рамках оперативного процесса. Последней процедурой этапа 7 является утверждение оперативного плана или боевого приказа командиром.

Командир подписывает оперативный план или боевой приказ, G-3 или S-3 передают утверждённый оперативный план или боевой приказ в подчинённые штабы, а командир и штаб начинают переход к подготовительным мероприятиям оперативного процесса. Ниже в таблице A-7 показаны действия и основные результаты деятельности рабочей группы CEMA на этапе 7: «Издание, рассылка и передача приказов и распоряжений».

Таблица A-7

Этап 7: Издание, рассылка и передача приказов

Основные исходные данные	Процесс	Основные выходные данные
• Утверждённый командиром план действий. • Актуальные материалы по кибероперациям и РЭБ вышестоящих штабов, включая уточнённые текущие оценки. • Обратная связь по поданным запросам на поддержку в киберпространстве и РЭБ. • Проект Приложения C, Дополнения 12 к оперативному плану или приказу.	• Участие в согласовании планов и приказов. • Участие в перекрёстной сверке планов и приказов. • Рассмотрение командиром проекта оперативного плана или боевого приказа.	• Утверждённый оперативный план или боевой приказ с доработанными приложениями, включая Приложение C, Дополнение 12 и Приложение H (G6/S6). • Передача утверждённого оперативного плана или боевого приказа подчинённым штабам. • Переход к подготовительным мероприятиям оперативного процесса.

A-2. Приложение C и Приложение H к оперативному плану или приказу

A-2.1. Приложения C и H

A-56. В оперативных планах, боевых приказах, частных приказах и предварительных распоряжения информация о кибероперациях и РЭБ содержится в различных пунктах, а также в Приложении C и Приложении H. В оперативных планах, боевых приказах, частных приказах схема CEMA рассматривается в пункте 3.g. (Кибер-электромагнитная деятельность) и пункте 5.g. (Связь). В предварительных распоряжениях информация о кибероперациях и РЭБ приведена в пункте 5.g. (Связь).

Примечание:

> Пункт 5.g. (Связь) содержит информацию об операциях в информационной сети МО и операциях по управлению спектром.

A-57. Пункт 3.g. (Кибер-электромагнитная деятельность) описывает, как СЕМА поддерживает замысел операций, и отсылает читателя к Дополнению 12 (Кибер-электромагнитная деятельность) к Приложению С (Операции) и Приложению Н (Связь), если это необходимо. Ниже приведены подразделы Дополнения 12 к Приложению С и Приложению Н с информацией о кибероперациях и РЭБ:

а. Приложение С (Операции), Дополнение 12 (Кибер-электромагнитная деятельность) – Офицер по кибервойне и РЭБ

- Вкладка А – Наступательные кибероперации.
- Вкладка В – Оборонительные кибероперации.
- Вкладка С – Электромагнитная атака.
- Вкладка D – Электромагнитная защита.
- Вкладка Е – Электромагнитная поддержка.

б. Приложение Н (Связь) – структурное подразделение штаба G-6 или S-6

- Дополнение 1 – Операции в информационной сети МО.
- Дополнение 2 – Схема организации голосовой, видеосвязи и передачи данных.
- Дополнение 3 – Спутниковая связь.
- Дополнение 4 – Зарубежный обмен данными.
- Дополнение 5 – Операции по управлению спектром (при содействии СЕМА).
- Дополнение 6 – Информационные сервисы.

Примечание.

> Для получения дополнительной информации об оперативных планах, боевых приказах, частных приказах и предварительных распоряжениях см. боевой устав FM 6-0.

A-2.2. Дополнение 12 (Кибер-электромагнитная деятельность) к Приложению С (Операции) к оперативным планам и боевым приказам

A-58. В Дополнении 12 к Приложению С к оперативному плану или боевому приказу описываются кибероперации и направления РЭБ (ЭМА, ЭМЗ и ЭМП), обеспечивающие замысел операций командира. Офицер по кибервойне и РЭБ несёт общую ответственность за издание Дополнения 12 к Приложению С и контролирует работу отделения СЕМА по оказанию помощи G-6 или S-2 в разработке Дополнений 1 и 6 к Приложению Н. В Дополнении 12 к Приложению С описывается схема процессов интеграции и согласования кибероперций, РЭБ и СЕМА. Оно также включает ограничения для кибероперций и РЭБ, поступающие из вышестоящих штабов. Рисунок А-1 иллюстрирует Дополнение 12 к Приложению С и связанные с ним вкладки.

[ГРИФ ОГРАНИЧЕНИЯ ДОСТУПА]

Разместить гриф ограничения доступа в верхней и нижней частях каждой страницы оперативного плана или боевого приказа. Разместить обозначение грифа ограничения доступа перед каждым пунктом и подпунктом в круглых скобках. Инструкции по обозначению грифа и маркировке релизов см. в AR 380-5.

Копия ## из ## копий
Штаб, издавший приказ
Место издания
Группа «Дата-время» подписи
Номер сообщения

Включает полный заголовок, если приложение распространяется отдельно от основного приказа или приложение более высокого уровня.

ДОПОЛНЕНИЕ 12 (КИБЕР-ЭЛЕКТРОМАГНИТНАЯ ДЕЯТЕЛЬНОСТЬ) К ПРИЛОЖЕНИЮ С (ОПЕРАЦИИ) К ОПЕРАТИВНОМУ ПЛАНУ/ПРИКАЗУ [номер] [(кодовое название операции)] – [(штаб, издавший приказ)] [(гриф ограничения доступа)]

(НС) **Ссылки**: *Добавить любые конкретные ссылки на кибер-электромагнитную деятельность, при необходимости.*

1. (НС) Обстановка. *Включить информацию, касающуюся киберопераций и РЭБ, которая не указана в пункте 1 Приложения С (Операции) или которая требует расширения.*

а. (НС) Район интересов. *Включить информацию, влияющую на киберпространство и ЭМС; киберпространство может расширить район локальных интересов до глобальных интересов*.

б. (НС) Район операций. *Включить информацию, влияющую на киберпространство и ЭМС; киберпространство может расширить район операций за пределы физического пространства манёвра.*

в. (НС) Противник. *Перечислить известные и возможные места дислокации и действия киберподразделений и подразделений РЭБ на один уровень выше и на два уровня ниже, издающего приказ. Указать уязвимые места информационных систем, киберсистем и систем РЭБ противника. Перечислить кибероперации и РЭБ противника, которые окажут влияние на операции своих (американских) войск. Разместить возможные планы действий противника и применение им средств кибероопераций и РЭБ. При необходимости см. Приложение В (Разведка).*

г. (НС) Свои силы. *Изложить план кибер-электромагнитной деятельности вышестоящего штаба. Перечислить плановые обозначения, местоположения и схему расположения вышестоящих, соседних и других средств кибероопераций и РЭБ, которые поддерживают или влияют на штаб, издавший приказ, или требуют координации и дополнительной поддержки. Определить свои средства и ресурсы кибероопераций и РЭБ, влияющие на подчинённого командира. Выявить уязвимые места киберпространства и ЭМС своих войск. Определить союзные иностранные силы, с которыми подчинённые командиры могут взаимодействовать. Выявить потенциальные конфликты в ЭМС, особенно для объединённых или многонациональных операций. Устранить конфликты и определить приоритеты распределения спектра.*

[№ страницы]
[ГРИФ ОГРАНИЧЕНИЯ ДОСТУПА]

Рис. А-1. – *Приложение С, Дополнение 12.*

[ГРИФ ОГРАНИЧЕНИЯ ДОСТУПА]

д. (НС) Межведомственные, межправительственные и неправительственные организации. Определить и описать другие организации в районе операций, которые могут повлиять на кибероперации и РЭБ или на применение специального оборудования и тактики кибероперациий и РЭБ. При необходимости см. Приложение V (Межведомственное).

е. (НС) Третья сторона. *Выявить и описать другие организации, как местные, так и внешние по отношению к району операций, способные оказать влияние на кибероперации и РЭБ или на применение специфического оборудования и тактики для кибероперациий и РЭБ. В эту категорию входят криминальные и маргинальные группировки.*

ж. (НС) Гражданские вопросы. *Описать аспекты гражданской обстановки, влияющие на кибероперации и РЭБ. См. вкладку С (Гражданские вопросы) к Дополнению 1 (Оценка разведки) к Приложению В (Разведка) и Приложению К (Военно-гражданское сотрудничество) по мере необходимости.*

з. (НС) Приданные и отданные подразделения. *Перечислить приданные или откомандированные подразделения только в том случае, если это необходимо для уточнения структуры задачи. Перечислить все приданные или откомандированные средства кибероперациий и РЭБ, а также ресурсы, имеющиеся в распоряжении вышестоящих штабов. См. Приложение А (Состав сил и средств) при необходимости.*

и. (НС) Допущения. *Перечислить все специфические допущения для кибер-электромагнитной деятельности.*

2. (НС) Боевая задача. *Изложить задачу командира и описать кибероперации и РЭБ для поддержки основного плана или приказа.*

3. (НС) Выполнение.

а. Схема кибер-электромагнитной деятельности. *Описать, как кибероперации и РЭБ поддерживают замысел командира и замысел операций. Установить очерёдность оказания поддержки подразделениям на каждом этапе операции. Указать, каким образом воздействие через киберпространство и РЭБ приведёт к ухудшению, разрушению, уничтожению и введению в заблуждение противника. Назвать оборонительные и наступательные меры в киберпространстве и РЭБ. Определить целевые группы и воздействия по приоритетам. Описать общую концепцию внедрения кибероперациий и РЭБ. Перечислить отделения штаба, подразделения и рабочие группы, отвечающие за те или иные аспекты кибер-электромагнитной деятельности. Включить методы сбора информации о киберпространстве и РЭБ, разработанные в отделениях штаба, подразделениях и рабочих группах за пределами отделения СЕМА и рабочей группы. Описать план интеграции совместных действий и неправительственных участников и организаций. См. Приложение С (Операции) при необходимости. Этот раздел призван дать представление и понимание компонентов киберпространства и РЭБ, а также, как эти виды деятельности внедряются в оперативный план. Рекомендуется включить в это дополнение описание технических требований.*

В данном дополнении основное внимание уделяется требованиям к интеграции кибероперациий и РЭБ, а при необходимости для уменьшения дублирования даются ссылки на соответствующие дополнения и приложения.

[№ страницы]
[ГРИФ ОГРАНИЧЕНИЯ ДОСТУПА]

Рис. А-1. – *Приложение С, Дополнение 12 (продолжение).*

[ГРИФ ОГРАНИЧЕНИЯ ДОСТУПА]

(1) (НС) Организация боевых действий. Дать указания по правильной организации боевых действий, включая назначение подразделения, номенклатуру и тактическую задачу.

(2) (НС) Прочие условия. Привести любую другую информацию, необходимую для планирования, которая ранее не упоминалась.

б. (НС) Схема кибероперaций. *Описать, как кибероперации поддерживают замысел командира и концепцию операций. Описать общую концепцию реализации запланированных мероприятий по кибероперациям. Описать процесс интеграции других участников совместных действий и неправительственных организаций в операции, включая требования и ограничения в киберпространстве. Определить риски, связанные с кибероперациями. Включить сопутствующие потери, обнаружение, присвоение, «дружественный огонь» (нанесение поражения силам США или союзников или многонациональным сетям или информации), а также возможные конфликты. Описать действия, позволяющие предотвратить действия противника и неприятеля, направленные на критическое снижение возможностей объединённого командования по эффективному ведению военных операций в районе операций. Определить меры противодействия и ответственное за них подразделение. Перечислить предупреждения и способы их контроля. Указать, каким образом в рамках задач кибероперaций будут уничтожаться, разрушаться, выводиться из строя и блокироваться компьютерные сети противника. Определить и установить приоритетность наборов целей и воздействий в киберпространстве. Если необходимо, указать, как кибероперации способствуют выполнению операции. Определить планы по обнаружению или присвоению идентификации действий противника и неприятеля в физических доменах и киберпространстве. Убедиться, что подчинённые подразделения проводят оборонительные кибероперации. Согласовать работу отделения СЕМА с офицером по информационным операциям. Передавать запросы на проведение наступательных кибероперaций в вышестоящие штабы для утверждения и реализации. Описать, как работа операции в информационной сети МО поддерживает замысел командира и концепцию операций. Согласовать операции в информационной сети МО с G-6 (S-6). Определить приоритетность использования приложений, работающих в киберпространстве. Обеспечить использование средств кибервоздействия в тех случаях, когда основной целью является достижение целей в киберпространстве или с его помощью. Следует учитывать ухудшение работы сети. (При необходимости, для избежания дублирования, указать соответствующие приложения и дополнения).*

(1) (НС) Операции в информационной сети МО. *Описать, как осуществляется взаимодействие, согласование и обеспечение информационных операций, интегрированных с G-6 (S-6) для разработки, создания, конфигурирования, защиты, эксплуатации, обслуживания и поддержания сетей. См. Приложение H (Связь) при необходимости.*

(2) (НС) Оборонительные кибероперации. *Описать, как осуществляется выполнение, взаимодействие, интеграция, согласование и обеспечение операций по защите информационной сети МО-СВ и сохранение способности использовать свои кибервозможности.*

[№ страницы]
[ГРИФ ОГРАНИЧЕНИЯ ДОСТУПА]

Рис. А-1. – *Приложение С, Дополнение 12 (продолжение).*

[ГРИФ ОГРАНИЧЕНИЯ ДОСТУПА]

(3) (НС) Наступательные кибероперации. *Описать, как осуществляется взаимодействие, интеграция, согласование и обеспечение наступательных кибероперацийдля достижения осведомлённости в реальном времени и направления динамических действий и мер реагирования. Включает идентификацию целей и информацию об оперативной схеме, операции по захвату и нападению, а также обеспечение разведывательной информацией. Описать полномочия, необходимые для проведения наступательных кибероперацийй.*

в. (НС) Схема радиоэлектронной борьбы. *Описать, как РЭБ поддерживает замысел командира и концепцию операций. Установить очерёдность оказания поддержки подразделениям на каждом этапе операции. Указать, каким образом задачи РЭБ будут направлены на ослабление, разрушение, отказ и введение в заблуждение противника. Описать процесс интеграции и взаимодействия возможностей РЭБ государственных и негосударственных структур в поддержку замысла командира и концепции операции. Указать мероприятия ЭМА, ЭМЗ и ЭМП, и план их внедрения. Определить наборы целей и воздействия по приоритетам для операций РЭБ. Согласовать с офицером по информационным операциям. При необходимости см. следующие приложения: Вкладки C, D, E (РЭБ) к Дополнению 12 (Кибер-электромагнитная деятельность); к Дополнению 15 (Информационные операции) к Приложению C.*

(1) (НС) Электромагнитная атака. *Описать, как наступательная деятельность электромагнитных атак скоординирована, внедрена, согласована и поддерживает операции. См. Вкладку C (Электромагнитная атака) к Дополнению 12 (Кибер-электромагнитная деятельность).*

(2) (НС) Электромагнитная защита. *Описать, как оборонительная деятельность ЭМЗ скоординирована, внедрена, согласована и поддерживает операции. См. Вкладку D (Электромагнитная защита) к Дополнению 12 (Кибер-электромагнитная деятельность).*

(3) (НС) Электромагнитная поддержка. *Описать, как деятельность электромагнитной поддержки скоординирована, согласована и поддерживает операции. См. Вкладку E (Электромагнитная поддержка) к Дополнению 12 (Кибер-электромагнитная деятельность).*

г. (НС) Схема операций по управлению спектром. *Описать, как операции по управлению спектром поддерживают замысел командира и концепцию операций. Изложить результаты, которых хочет добиться командир, определяя приоритетность задач по управлению спектром. Перечислить цели и основные задачи для достижения этих целей. Изложить план по управлению спектром, распределение частот, взаимодействие с принимающей стороной и план реализации соответствующей политики. Описать план внедрения оперативных возможностей других участников для совместных действий по управлению спектром. См. Приложение H (Связь), при необходимости.*

д. (НС) Задачи подчинённым подразделениям. *Указать задачи кибероперацийй и РЭБ, не входящие в основной приказ, для каждого подчинённого подразделения.*

[№ страницы]

[ГРИФ ОГРАНИЧЕНИЯ ДОСТУПА]

Рис. А-1. – *Приложение C, Дополнение 12 (продолжение).*

[ГРИФ ОГРАНИЧЕНИЯ ДОСТУПА]

е. (НС) Инструкции по координации. *Указать инструкции по работе в киберпространстве и РЭБ, не указанные в основном приказе, применимые к двум или более подчинённым подразделениям. Определить и выделить все специфические для кибероперaций и РЭБ правила применения оружия, меры по снижению риска, вопросы экологии, требования по взаимодействию между подразделениями, критические информационные требования командира и информационные требования штаба, относящиеся к кибер-электромагнитной деятельности.*

4. (НС) Обеспечение. *Определить приоритеты по обеспечению выполнения ключевых задач и специальных дополнительных инструкций для кибероперaций и РЭБ, при необходимости. При необходимости см. Приложение F (Обеспечение).*

а. (НС) Тыловое обеспечение. *Использовать подпункты для определения приоритетов и конкретных указаний по тыловому обеспечению кибероперaций и РЭБ. См. Дополнение 1 (Тыловое обеспечение) к Приложению F (Обеспечение) и Приложению P (Обеспечение принимающей страной) по мере необходимости.*

б. (НС) Личный состав. *Использовать подпункты для определения приоритетов и конкретных инструкций по кадровому обеспечению кибероперaций и РЭБ. См. Дополнение 2 (Поддержка кадровых служб) к Приложению F (Обеспечение), при необходимости.*

в. (НС) Медицинское обеспечение. *См. Дополнение 3 (Медицинское обеспечение в Сухопутных войсках) к Приложению F (Обеспечение), при необходимости.*

5. (НС) Управление и связь.

а. (НС) Управление.

(1) (НС) Место командира. *Указать местонахождение ключевых руководителей кибероперaций и РЭБ.*

(2) (НС) Требования по связи. *Указать требования по связи и взаимодействию в киберпространстве и РЭБ, не предусмотренные стандартными операционными процедурами подразделения.*

б. (НС) Контроль.

(1) (НС) Командные пункты. *Описать работу командных пунктов (далее – КП) кибероперaций и РЭБ, включая месторасположение каждого КП, время открытия и закрытия.*

(2) (НС) Доклады. *Указать доклады по кибероперациям и РЭБ, не включенные в стандартные операционные процедуры. См. Приложение R (Доклады), при необходимости.*

в. (НС) Связь. *Учесть все требования по связи для кибероперaций и РЭБ. См. Приложение H (Связь), при необходимости.*

ПОДТВЕРЖДЕНИЕ: *Включать только в случае, если приложение распространяется отдельно от основного приказа.*

[Фамилия командира]
[Воинское звание командира]

*Командир или уполномоченный представитель подписывает оригинал приложения. Если представитель подписывает оригинал, добавить фразу «**За Командира**». Подписанный экземпляр является историческим экземпляром и остается в архиве штаба.*

[№ страницы]
[ГРИФ ОГРАНИЧЕНИЯ ДОСТУПА]

Рис. А-1. – *Приложение C, Дополнение 12 (продолжение).*

[ГРИФ ОГРАНИЧЕНИЯ ДОСТУПА]

ОФИЦИАЛЬНОЕ ДОЛЖНОСТНОЕ ЛИЦО:

[Фамилия официального должностного лица]
[Воинское звание официального должностного лица]

Используется только в случае, если командир не подписывает оригинал приложения. Если командир подписывает оригинал, дальнейшая аутентификация не требуется. Если командир не подписывает, то подпись готовившего его офицера штаба требует заверения, а в блоке подписи указываются только фамилия и звание командира.

ПРИЛОЖЕНИЯ: Перечислить вложения нижнего уровня (вкладки и приложения). Если конкретное вложение не используется, указать рядом с номером вложения **«не используется»**. Стандартные операционные процедуры подразделения определяют порядок разработки и формат вложений. Общие приложения включают следующие:

ДОПОЛНЕНИЕ 12 (КИБЕР-ЭЛЕКТРОМАГНИТНАЯ ДЕЯТЕЛЬНОСТЬ) К ПРИЛОЖЕНИЮ С (ОПЕРАЦИИ) К ОПЕРАТИВНОМУ ПЛАНУ/ПРИКАЗУ [номер] [кодовое наименование] - [издающий штаб] [гриф заголовка]

ПРИЛОЖЕНИЯ: Перечислить приложения (вкладки и приложения)

Вкладка A – Наступательные кибероперации

Вкладка B – Оборонительные кибероперации

Вкладка C – Электромагнитная атака

Вкладка D – Электромагнитная защита

Вкладка E – Электромагнитная поддержка

РАССЫЛКА: Указывать только в случае, если распространяется отдельно от основного приказа или приложений более высокого уровня.

[№ страницы]
[ГРИФ ОГРАНИЧЕНИЯ ДОСТУПА]

Рис. A-1. – *Приложение C, Дополнение 12 (продолжение).*

Приложение B. Правила ведения боевых действий и Кодекс США

В данном приложении рассматриваются основные принципы и законы (правила ведения боевых действий), которые регулируют (или разрешают) действия командиров, руководителей и личного состава при проведении кибероперациий и РЭБ. Конституция США устанавливает полномочия президента как верховного главнокомандующего вооружёнными силами и наделяет Конгресс полномочиями финансировать и контролировать вооружённые силы. Президент, как верховный главнокомандующий, управляет действиями вооружённых сил и, в соответствии с законами, принятыми Конгрессом, осуществляет руководство вооружёнными силами.

Введение

B-1. Командиры сухопутных войск проводят кибероперации и РЭБ по указаниям президента США, министра обороны и командующего(их) боевым(и) командования(ми), назначенного(ых) для проведения операций от имени президента. Эти указания относятся к полномочиям президента, вытекающим из статьи II Конституции США, Билля о правах, других исполнительных распоряжений, политики президента, нормативных актов министерства обороны и министерства армии, договорных обязательств США и других законов (включая ассигнования на финансирование), принятых Конгрессом.

B-2. В рамках этого правового поля сухопутные войска проводят кибероперации и РЭБ в соответствии с распоряжениями, боевыми приказами, правилами ведения боевых действий и политикой, реализуемой министром обороны и командующими боевыми командованиями. Сухопутные войска выполняют кибероперации и РЭБ в составе объединённых сил. Киберкомандование США несёт общую ответственность за надзор за кибероперациями министерства обороны.

B-1. Правила ведения боевых действий

B-3. Командиры, начальники и личный состав должны понимать и применять основные принципы права вооружённых конфликтов, правила ведения боевых действий, общие ограничения, меры предосторожности при нападении, разделение военных действий, специальную защиту, национальный суверенитет и экологические вопросы в их взаимосвязи с международным правом. Право вооружённых конфликтов – это часть международного права, регулирующая вооружённые столкновения и опирающаяся на фундаментальные принципы военной необходимости, гуманности, соразмерности, различия и чести, которые применимы к ведению Сухопутными войсками кибероперациий и РЭБ.

B-4. Правила ведения боевых действий – это директивы, изданные компетентным военным органом, которые определяют обстоятельства и ограничения, при которых американские войска будут начинать или продолжать боевые действия с другими противостоящими силами. Правила ведения боевых действий – это то, как оперативные командиры регулируют действия вооружённых сил в контексте применимой политической и военной политики, внутреннего и международного права. Правила применения вооружённой силы представляют собой основу, которая охватывает цели национальной политики, требования задач и верховенство закона. Все решения, связанные с кибероперациями и РЭБ, оперативное командование принимает с учётом действующих правил ведения боевых действий.

B-5. В целом нанесение ударов по ограниченным районам, гражданскому населению, гражданским или защищённым объектам, как правило, не является преднамеренным, если только они не становятся субъектами угрозы, непосредственно участвующими в боевых действиях самостоятельно или в составе группы. В таких случаях эти субъекты теряют защиту от непосредственного поражения. Если противник использует гражданское население в качестве «живого щита», то, при условии непринятия непосредственного участия в боевых действиях, оно всё равно является нейтральным участником. Командиры должны учитывать гражданское население, используемое в качестве «живого щита», при определении уровня чрезмерности применяемой силы в ходе планируемого наступления. Командир обеспечивает принятие возможных мер предосторожности для снижения риска нанесения ущерба гражданскому населению. Как правило, нанесение ударов по гражданским субъектам не допускается; однако офицеры по информационным операциям будут проводить анализ целей и направлять применение информационного потенциала, включая воздействие кибероперации и РЭБ в поддержку противодействия дезинформации, а также для информирования и влияния на гражданские структуры как неприятеля, так и свои.

B-6. Гражданские объекты – это такие объекты или места, которые не являются законными военными объектами. Командиры преднамеренно не могут наносить удары исключительно по гражданским объектам или районам. Кроме того, если такие объекты или места находятся рядом с целями противника или в непосредственной близости от них, ответственный командир должен провести анализ сопутствующих потерь. Если будет затронут защищённый объект или объект, включённый в список запрещённых для нанесения ударов, командиры должны принять соответствующие меры для ослабления последствий или запросить исключение объекта из списка запрещённых для нанесения ударов, прежде чем законно санкционировать нанесение удара по этому объекту. Использование противником гражданского и защищённого объекта или места в военных или боевых целях может привести к потере защищённого статуса, в результате чего он становится объектом для атаки.

B-7. Командиры должны предпринимать активные шаги и меры предосторожности, чтобы избежать чрезмерных случайных жертв среди гражданского населения и повреждений гражданского имущества. Участники группы по целеуказаниям при разработке целей должны обеспечить использование надёжных разведывательных данных и проверку целей для выбора целей противника, а не гражданских объектов для поражения. Удары по объектам, содержащим сооружения, влияющие на природные ресурсы, включая плотины, дамбы и объекты атомной энергетики, должны тщательно рассматриваться как создающие потенциально катастрофический сопутствующий ущерб.

B-2. Кодекс США

B-8. Сухопутные войска проводят операции по указанию президента в соответствии с ассигнованиями, разрешениями и положениями Кодекса США, установленными Конгрессом. Эти положения охватывают широкие области права, включая внутреннюю безопасность, регулирование вооружённых сил, федеральные преступления, Национальную гвардию, приобретение и обслуживание информационных технологий, управление спектром и разведку.

B-9. Раздел 6 «Внутренняя безопасность» устанавливает ответственность за анализ информации и защиту инфраструктуры, главных специалистов по информации и надзор за безопасностью киберпространства. В Раздел 6 входит комплексная оценка ключевых ресурсов, уязвимостей критической инфраструктуры и определение приоритетов для принятия защитных и вспомогательных мер в отношении угроз.

B-10. Раздел 10 «Вооружённые силы» позволяет сухопутным войскам организовывать, обучать, оснащать и обеспечивать подразделения и штабы сухопутных войск, кибероперациий и РЭБ. Полномочия и ограничения в Разделе 10 обеспечивают контекст и основу того, каким образом министр обороны руководит военными кибероперациями, РЭБ и военной разведкой.

B-11. Раздел 18 «Преступления и уголовное судопроизводство». Сухопутные войска проводят кибероперации и РЭБ в соответствии с федеральным законодательством и принимают меры по обеспечению соблюдения прав граждан на проведение незаконных обысков и изъятий в соответствии с 4-й поправкой. Координация действий с Управлением уголовного розыска сухопутных войск США обеспечивает надлежащее расследование преступной деятельности в информационной сети МО в соответствии с положениями Раздела 18. Командование уголовного розыска сухопутных войск США несёт непосредственную ответственность за обеспечение соблюдения закона о преступлениях, предусмотренных Разделом 18 Кодекса США, если они затрагивают интересы министерства обороны или военнослужащих сухопутных войск. В Раздел 18 включены преступления, совершаемые в киберпространстве.

B-12. Раздел 32 «Национальная гвардия» определяет подразделения Национальной гвардии как воинские части штата, которые оснащены и обучены в соответствии с федеральным законодательством. Национальная гвардия может проводить операции в интересах своего штата, но оплачиваемые федеральным правительством в соответствии с Разделом 32 Кодекса США, если министр обороны США сочтёт, что такая задача отвечает интересам министерства обороны.

B-13. Раздел 40 глава 113 «Приобретение информационных технологий» распространяется на сухопутные войска и все федеральные агентства. Раздел 40 устанавливает обязанности руководителей агентств и главных информационных директоров агентств, а также руководство по приобретению информационных технологий.

B-14. Раздел 44 «Печать, полиграфия и документооборот» устанавливает ответственность руководителей агентств по выполнению законодательных требований и полномочий по обеспечению информационной безопасности и управлению информационными ресурсами. В обязанности и требования входит обеспечение информационной безопасности в киберпространстве.

B-15. Раздел 47 «Телекоммуникации» устанавливает законодательные требования и полномочия для доступа и использования ЭМС в США и ведении федеральных агентств. Главный специалист по информационным технологиям/G-6, как указано в документе AR 5-12, реализует национальные, международные, внутриминистерские, объединённые, принимающей страны пребывания и министерства армии США вопросы политики управления спектром и руководит в сухопутных войсках. В этом качестве главный специалист по информационным технологиям/G-6 обеспечивает соблюдение положений раздела 47 Кодекса США, а также других применимых федеральных законов, законов МО и политики управления ЭМС военных ведомств для минимизации радиочастотных помех на полигонах и объектах МО и видов ВС при проведении таких мероприятий, как тестирование Глобальной системы позиционирования и выдача разрешений на ЭМА на обучение, тестирование и оценку.

B-16. Раздел 50 «Война и национальная оборона» содержит полномочия правительства США по ведению как военной, так и разведывательной деятельности. Разведывательная деятельность, осуществляемая правительством США, должна быть надлежащим образом санкционирована, соответствовать Конституции и проводиться в соответствии с указаниями президента. Исполнительный приказ № 12333 устанавливает структуру и организацию разведывательного ведомства в соответствии с указаниями президента США. Например, в приказе Агентство национальной безопасности определено в качестве головной организации по радио и радиотехнической разведке. Политические документы министерства обороны, в том числе Руководство министерства обороны № 5240.01 (DODM 5240.01), устанавливают требования МО США к проведению разведывательных операций.

B-17. Сухопутные войска строго ограничивают и контролируют сбор информации о гражданских лицах США на территории Соединенных Штатов Америки. Документ AR 381-10 определяет виды, средства и ограничения, касающиеся сбора, хранения и распространения информации в США и о гражданских лицах США. Данное положение распространяется на киберпространство в пределах границ США и на гражданское население США за рубежом. В таблице B-1 приведены разделы Кодекса США по вопросам киберпространства. Раздел 18 Кодекса США освобождает оперативно-розыскную деятельность от некоторых ограничений, касающихся сбора и хранения информации о гражданских лицах США.

Таблица В-1

Положения Кодекса США по вопросам киберпространства

Кодекс США	Наименование	Основное положение	Главная организация	Роль в киберпространстве
Раздел 6	Внутренняя безопасность	Национальная безопасность	Министерство внутренней безопасности	Безопасность киберпространства США
Раздел 10	Вооружённые силы	Национальная оборона	Министерство обороны	Обеспечение, обучение и оснащение ВС США для проведения военных кибероперация
Раздел 18 Раздел 28	Преступления и уголовное судопроизводство Судебная власть и судопроизводство	Правоприменение	Министерство юстиции	Предупреждение преступлений, задержание и преследование преступников, действующих в киберпространстве
Раздел 32	Национальная гвардия	Подготовка и проведение операций по национальной обороне и гражданской поддержке в США.	Национальная гвардия СВ штата, Национальная гвардия ВВС штата	Ликвидация последствий стихийных бедствий в стране (в случае привлечения к федеральной службе Национальная гвардия включается в Раздел 10, Вооружённые силы
Раздел 40	Публичные здания, собственность и общественные работы	Роли и обязанности начальника по информационным технологиям	Все федеральные министерства и ведомства	Разработка и применение стандартов в области закупки информационных технологий и их безопасности
Раздел 44	Печать, полиграфия и документооборот	Определяет основные обязанности и полномочия агентства в области политики информационной безопасности	Все федеральные министерства и ведомства	Основа деятельности по кибербезопасности, изложенная в Инструкции министерства обороны 8330.01 «Поддержка деятельности по кибербезопасности операций в информационной сети МО»
Раздел 50	Война и национальная оборона	Широкий спектр военной, внешнеполитической, разведывательной и контрразведывательной деятельности	Командования, виды ВС и агентства, входящие в состав министерства обороны, а также разведывательные ведомства, подчинённые Директору национальной разведки	Обеспечение интересов США путем проведения военных и разведывательных операций в киберпространстве

B-3. Законы и политика, защищающие граждан США

B-18. В США нет единого федерального закона или политики, регулирующей безопасность киберпространства, информационную безопасность или неприкосновенность частной жизни американских граждан. Помимо федеральных законов и политики, во многих штатах США законы о безопасности киберпространства и уведомлении о нарушениях данных регулируются отраслевыми федеральными нормативными актами и законодательством штатов, имеющими различную сферу действия и юрисдикцию. В таблице B-2 описаны многие федеральные законы и политики, обеспечивающие защиту граждан США в киберпространстве и ЭМС. Эти законы и политика защищают граждан США только на национальном уровне. На граждан США, находящихся за пределами США, распространяются правила той международной страны или штата, в которой они проживают или которую посещают.

Таблица B-2

Федеральные законы и политика в области безопасности киберпространства, защищающие граждан США

Наименование	Описание
Закон Сарбейнза-Оксли (Кодекс США 15, глава 98)	Требует, чтобы организации в США подтвердили свои учётные данные в области кибербезопасности*. Это относится только к публичным компаниям.
Регламент Комиссии по ценным бумагам и биржам (Свод федеральных правил 17, часть 248, Подраздел A)	Конфиденциальность финансовой информации потребителей и защита персональных данных. Регулирование безопасности, требующее соответствующих мер кибербезопасности*. Применяется ко всем американским и иностранным брокерам, дилерам, инвестиционным компаниям и инвестиционным консультантам, которые зарегистрированы в Комиссии по ценным бумагам и биржам.
Закон Грэмма-Лича-Блайли (Кодекс США 15, Подраздел I)	Является законом об информационной безопасности и конфиденциальности, применяется к финансовым учреждениям и включает в себя банки, страховые компании, охранные фирмы, небанковских ипотечных кредиторов, автодилеров и специалистов по подготовке налоговых деклараций.
Закон о мобильности и подотчётности медицинского страхования (Свод федеральных правил 45, часть 160 и 164	Содержит правила безопасности, конфиденциальности и уведомлений о нарушениях. Применяется к поставщикам медицинских услуг, планам медицинского страхования, информационным центрам здравоохранения и, в некоторых случаях, деловым партнёрам этих типов предприятий, называемых застрахованными организациями. В результате этот Закон может охватывать такие разнообразные организации, как медицинские страховые компании и фармацевтические компании.

Наименование	Описание
Закон о Федеральной торговой комиссии, раздел 5 (Кодекс США 15, Раздел 45.	Оба закона - о защите информации, требующий принятия соответствующих мер кибербезопасности, и о защите персональных данных. Применяется почти к каждой организации в США, за исключением банков и обычных перевозчиков.
Федеральное положение о закупках для нужд обороны (Свод федеральных правил 48, 252.204-7012)	Регулирование кибербезопасности*, применимое к подрядчикам министерства обороны США. Требует от подрядчиков и субподрядчиков, которые обрабатывают, хранят или передают оборонную информацию, предоставлять адекватную безопасность для защиты данных в несекретных информационных системах.
Закон о защите конфиденциальности детей в Интернете (Кодекс США 15, глава 91, и Кодекс федеральных правил 16, часть 312)	Это закон о конфиденциальности и кибербезопасности, который применяется к веб-сайтам и онлайн-сервисам, предназначенным для детей в возрасте до 13 лет. Также применяется, если оператор сайта знает, что дети в возрасте до 13 лет используют веб-сайт. Регулирует вопросы, каким образом такие веб-сайты собирают, используют и/или раскрывают личную информацию от детей и о детях.
Федеральный закон о защите 1974 года (Кодекс США 5, глава 5, раздел 552a)	Применяется только к агентствам федерального правительства США и регулирует сбор, хранение, использование и распространение личной информации о лицах, которая хранится в системах или записях федеральных агентств. Он запрещает раскрытие информации из системы записей, контролируемой федеральным агентством, без письменного согласия субъекта, за исключением случаев, когда раскрытие разрешено в соответствии с одним из 12 предусмотренных законом исключений. Это относится ко всем лицам, которые являются резидентами США (как законно, так и незаконно)
Закон о защите конфиденциальности потребителей 2017 года (Билль Палаты представителей США 4081)	Обеспечивает конфиденциальность и безопасность конфиденциальной личной информации, предотвращает и снижает кражу личных данных и уведомляет о нарушениях безопасности, связанных с конфиденциальной личной информацией. Это также повышает эффективность помощи правоохранительным органам и других мер защиты от нарушений безопасности, мошеннического доступа и неправомерного использования личной информации. Он применяется к организациям, которые собирают, используют, получают доступ, передают, хранят или утилизируют конфиденциальную личную информацию в количестве 10 000 или больше граждан США в течение любого 12-месячного периода.

Наименование	Описание
Управление по санитарному надзору за качеством пищевых продуктов и медикаментов (Свод федеральных правил 21, часть II)	Регламент использования электронных записей в клинических исследованиях. Это закон о кибербезопасности, который применяется к организациям, участвующим в клинических исследованиях медицинских изделий, включая спонсоров, клинических исследователей, институциональные наблюдательные советы и контрактные исследовательские организации. Многие из этих операций также подпадают под действие Закона о переносимости и подотчётности медицинского страхования. Это касается использования информационно-технологических систем этих организаций, включая любые электронные системы, используемые для создания, изменения, обслуживания, архивирования, извлечения, или передаче записей, используемых в клинических исследованиях.
Положение о деривативных клиринговых организациях Комиссии по торговле товарными фьючерсами (Свод федеральных правил 17, часть 39, подраздел B и 39.18-Системные гарантии)	Применяется к производным клиринговым организациям (организациям, выступающим в качестве посредника для клиринговых операций с товарами для будущих поставок или операций с товарными опционами).
Закон о конфиденциальности электронных коммуникаций и Закон о хранимых коммуникациях (Кодекс США 18, главы 119 и 121	Вместе они также известны как Закон о прослушивании телефонных разговоров и являются законами о конфиденциальности. Изначально созданные для ограничения слежки без ордера они, однако, также запрещают преднамеренное использование, разглашение или доступ к любым проводным, устным или электронным коммуникациям без авторизации.
Европейско-Американская программа «Щит конфиденциальности»	Защищает данные жителей Европы, хранящиеся и обрабатываемые организациями в США

Приложение С. Интеграция с другими участниками совместных действий

Сухопутные войска проводят операции в составе объединённых сил и регулярно взаимодействуют с участниками совместных действий в рамках совместных операций. Таким образом, командиры сухопутных войск должны работать с другими участниками совместных действий на протяжении всего оперативного процесса. В данном приложении обсуждается, как командиры и штабы на объединённом уровне интегрируют кибероперации и РЭБ с другими участниками совместных действий.

С-1. Особенности объединённых операций

С-1. Операции сухопутных войск, связанные с использованием киберпространства и ЭМС, могут иметь общие последствия. Каждый род и вид вооруженных сил имеет свои задачи по проведению кибероперацій, требования к ЭМС и возможности РЭБ, которые составляют единое целое, согласование которого осуществляется в штабе объединённой оперативно-тактической группы.

Отделение CEMA обеспечивает, чтобы кибероперации и РЭБ были согласованы с объединёнными информационными операциями, операциями по управлению спектром и доктриной.

С-2. Армейский корпус, функционирующий как штаб объединённой оперативно-тактической группы, объединяет отделение CEMA, офицера по информационным операциям и руководителя по управлению спектром для создания группы управления объединёнными операциями в ЭМС.

Каждый компонент вида вооружённых сил, подчинённый штабу объединённой оперативно-тактической группы, создаёт свою группу управления операциями в ЭМС, входящую в группу управления объединёнными операциями в ЭМС. Корпус или дивизия, назначенные в качестве штаба объединённых сил, также обязаны создать группу управления операциями в ЭМС, объединив в ней отделение CEMA, офицера по информационным операциям и руководителя по управлению спектром.

С-3. План операций в районе боевых действий определяет планирование использования возможностей киберпространства и РЭБ. Сухопутные войска предоставляют объединённый план действий в киберпространстве и РЭБ в интересах обеспечения объединённых операций.

Примечание:

> Для получения дополнительной информации об информационных операциях см. JP 3-13. Для получения дополнительной информации об объединённых операциях по управлению спектром см. JP 3-85.

C-2. Межведомственные и межправительственные аспекты

C-4. Командиры сухопутных войск должны учитывать уникальные возможности, структуру и приоритеты участников межведомственного и межгосударственного взаимодействия перед проведением кибероперациий и РЭБ. Успешные операции с привлечением других участников совместных действий требуют единого понимания операции и общего видения её цели.

C-5. Межведомственные и межправительственные участники часто имеют командные отношения, порядок подчинения и процессы планирования, которые значительно отличаются от таких же процессов в сухопутных войсках. Чтобы понять эти различия полномочий и процессов необходимо установление тесных связей до начала операций, т.к. вероятно, заниматься этим задним числом будет поздно и не эффективно. Участники для решения задач часто создают комитеты, фокусные группы и межведомственные рабочие группы, организованные по функциональному признаку. Командир несет ответственность за разработку требований по координации работы межведомственных и межправительственных организаций, а также за создание группы связи. Такая группа аналогична группам, которые используются и при проведении международных операций.

C-6. Правила, требования, стандарты межведомственных и межправительственных структур могут оказываться более строгими, чем в сухопутных войсках. Могут присутствовать различия в юридических полномочиях, ролях, обязанностях, процедурах и процессах принятия решений. Командиры добиваются единого видения межведомственными и межправительственными планировщиками военных возможностей, требований, оперативных ограничений, связей и правовых вопросов. Штабы, интегрирующие этих участников в операции, должны понимать характер этих отношений и виды поддержки, которую они могут оказать. При отсутствии формального руководства, командирам, вероятно, потребуется консенсус для достижения поставленных задач с участием этих организаций.

C-7. Командиры принимают во внимание менее жёсткие полномочия и политику, которых придерживаются межведомственные и межправительственные участники. Некоторые из их полномочий и политик могут включать методы, которые позволяют достичь желаемого результата более экономично, эффективно или с меньшим риском возникновения каскадных эффектов. Командиры должны быть готовы использовать их, когда это целесообразно.

C-3. Особенности многонациональных операций

C-8. Подразделения сухопутных войск, проводящие кибероперации и РЭБ в рамках международных операций, нуждаются в активном взаимодействии с другими участниками. Эффективное взаимодействие и связь позволяют снизить сложности, вызванные различиями в политике, и облегчить системную интеграцию и обмен информацией.

C-9. Различия в национальных стандартах и законах о суверенитете в киберпространстве и ЭМС могут повлиять на легальность или готовность страны участвовать в кибероперациях и РЭБ. Некоторые участники могут отказаться от участия в операции, в то время как другие предоставят свои возможности или будут проводить свои операции отдельно от операции командования Сухопутными войсками.

C-10. Обеспечение связи играет важную роль в ситуации, когда многонациональные силы взаимодействуют во время боевых операций. На связь оказывают влияние проблемы совместимости. Несовместимость оборудования и программного обеспечения, а также различия в стандартах, политике информационной безопасности и безопасности в киберпространстве могут вызвать пробелы в защите или функциональных возможностях, требующие дополнительных усилий для устранения. Такие проблемы, скорее всего, замедлят сбор, распространение и обмен информацией между участниками. Командиры и штабы должны предусмотреть несовместимость и различия в системе связи до начала многонациональной операции.

C-11. Обмен информацией и разведданными с союзниками и международными участниками является жизненно важным в многонациональных операциях. Особое внимание и осторожность необходимы при обмене информацией в связи с различающимися политиками по использованию и классификации информации. При координации кибероперациий и РЭБ с иностранными участниками подразделения Сухопутных войск должны обеспечить строгое соблюдение процедур раскрытия информации иностранным партнёрам и процедур безопасности киберпространства. Соображения безопасности могут препятствовать полному раскрытию некоторых возможностей в киберпространстве и РЭБ или планирования, ограничивая усилия по их согласованию. Эффективное согласование подразумевает доступ к системам и информации на низшем возможном уровне секретности. Командиры несут ответственность за установление процедур раскрытия разведывательной информации иностранным участникам. Для получения дополнительной информации об обмене данными с иностранными партнёрами см. AR 380-10.

C-4. Особенности взаимодействия с неправительственными организациями

C-12. Командиры обеспечивают соблюдение процедур безопасности в киберпространстве при проведении кибероперациий с неправительственными организациями. Планирование с участием неправительственных организаций может потребоваться для иностранной гуманитарной помощи, миротворческих миссий и военно-гражданских операций. Привлечение этих организаций к участию в операции требует от командира соблюдения баланса между потребностью неправительственной организации в информации и безопасностью операции.

Многие неправительственные организации могут проявлять нежелание связываться с военными, чтобы не подвергать риску свой статус независимых субъектов. Многие стремятся сохранить этот статус, чтобы не потерять свободу манёвра или не подвергать сотрудников риску во враждебной среде. Планирование на стратегическом уровне по включению негосударственных организаций в операции по делам гражданского населения, скорее всего, будет согласовываться с кибероперациями.

C-5. Особенности страны пребывания

C-13. Каждое государство обладает суверенитетом над своим киберпространством и ЭМС в пределах своей географической территории. Использование киберпространства страны и её ЭМС требует координации и согласования с помощью официальных разрешений и сертификатов. Взаимодействие со страной пребывания по использованию ЭМС зависит от операций по управлению спектром. Координация использования частотного спектра основывается в основном на потенциальных возможностях электромагнитных помех для местных приёмных устройств. Эта координация гарантирует начальную доступность спектра и возможность поддержки операций и обеспечивает доступность киберпространства, например, распределение рабочего диапазона. Цель взаимодействия – расширить возможности совместной защиты киберпространства. Важно учитывать наличие соседних со страной пребывания государств, особенно если войска размещены, обучаются или действуют на их территориях. Также критически важно обеспечение совместимости защитных мер, таких как системы противодействия, для предотвращения «дружественного огня» по своим системам.

C-6. Особенности развёртывания

C-14. Системы кибероперацій и РЭБ сложные и постоянно развиваются. Боевая готовность военнослужащих и их способность приступить к выполнению задач сразу по прибытии являются ключевыми факторами для обеспечения полной боеспособности и готовности войск. Проведение кибероперацій и РЭБ в местах постоянной дислокации уникально по ряду причин. Командный состав, физически не находящиеся в одном месте, должен использовать телефонную или виртуальную связь для совместной работы и взаимодействия. В дополнение к вышесказанному ограничения, обусловленные законодательством, политикой и нормативными актами, могут ограничивать использование кибероперацій и РЭБ на военном объекте. Специализированные задачи для различных объектов (испытания, обучение и техническое обслуживание) могут иметь особые требования. Также важно установить рабочие отношения с гарнизонными организациями, такими как Сетевой корпоративный центр (*англ. Network Enterprise Center, NEC*). Офицер по кибервойне и РЭБ работает с группами обеспечения развёртывания и службами страны пребывания по включению подготовки по кибероперациям и РЭБ в план учёбы их организаций.

C-7. Особенности частного сектора

C-15. Частный сектор играет важную роль в киберпространстве и ЭМС. Сухопутные войска полагаются на связи со своими военно-промышленными структурами и частным сектором для многих не связанных с боевыми действиями повседневных функций обеспечения и обслуживания. Например, электронные базы данных и интерфейсы для медицинских сервисов, бухгалтерские и финансовые услуги, ведение кадровых записей, техобслуживание оборудования и логистические функции. Глобальный транспорт и логистика нуждаются в обмене данными между военными и частными сетями. Сухопутные войска полагаются на судоходные компании, поставщиков транспортных услуг и оборудования как участников глобальной транспортной системы.

C-16. Сетевая безопасность и надёжность сетей частного сектора оказывают прямое влияние на операции министерства обороны. Личный состав МО не управляет этими сетями, однако они необходимы для эффективных операций сухопутных войск. Ответственность за эти сети лежит на их владельцах.

C-17. Частный сектор внёс основной вклад в развитие информационных технологий, в результате чего министерство обороны США всё больше полагается на готовые коммерческие технологии. Многие из этих продуктов разработаны, изготовлены или используют компоненты, произведённые за границей. Эти производители, продавцы, поставщики услуг и разработчики могут попасть под влияние противника или невольно использоваться им для выпуска поддельных продуктов или продуктов со встроенными уязвимостями. Форма МО США DD 1494 (Заявка на распределение частот оборудования) определяет совместимость и унификацию производимых радиоэлектронных систем для нужд национальных потребителей. Министерство обороны США следует процедурам и оценивает риски для обеспечения надлежащего управления цепочкой поставок с тем, чтобы приобретение программного и аппаратного обеспечения не оказывало негативного влияния на безопасность информационной сети МО.

C-18. Информационная сеть МО использует коммерческие сети, такие как подводные кабели, оптоволоконные сети, телекоммуникационные сервисы, спутниковые и микроволновые антенны местных телефонных компаний и арендованные каналы спутников. Многие из этих коммерческих сетей принадлежат иностранцам или находятся под иностранным управлением и влиянием. Зависимость от коммерческих систем делает проведение кибероперации и РЭБ уязвимыми для отказа в доступе, прерывания обслуживания, перехвата и мониторинга связи, проникновения и компрометации данных. Командиры сухопутными войсками стремятся к снижению рисков путём соблюдения правил безопасности работы и кибербезопасности, проверок оборудования поставщиков, шифрования и ужесточения требований к обучению кибербезопасности.

Приложение D. Национальные организации, министерство обороны, резерв сухопутных войск и объединённые организации по кибероперациям и РЭБ

В приложении D рассматриваются национальные подразделения, подразделения министерства обороны и резерв сухопутных войск, которые поддерживают кибероперации. В данном приложении также приводится обзор Киберкомандования США и подчинённых ему объединённых подразделений, обеспечивающих кибероперации и РЭБ и поддержку сил кибероперацій в интересах командования сухопутных войск.

D-1. Национальные организации и учреждения

D-1. Конституция США устанавливает полномочия президента как Верховного главнокомандующего вооружёнными силами и предоставляет Конгрессу полномочия по финансированию и регулированию вооружённых сил. Президент, как Верховный главнокомандующий, осуществляет командование вооружёнными силами и, согласно законам, утверждённым Конгрессом, несёт ответственность за управление вооружёнными силами.

D-2. Министерство юстиции и министерство внутренней безопасности также играют ключевую роль в обеспечении национальной безопасности в киберпространстве в сотрудничестве с министерством обороны. Министерство юстиции возглавляет национальные мероприятия по расследованию кибертерроризма, шпионажа, компьютерных вторжений и крупных кибермошенничеств, а также отвечает за защиту коммерческих доменов .com, .net и .org.

Министерство внутренней безопасности отвечает за надзор защиты домена .gov, и предоставление помощи и экспертных знаний владельцам и операторам частного сектора.

Министерство обороны США защищает домен .mil.

D-3. Федеральное бюро расследований, входящее в состав министерства юстиции, проводит внутренние операции по обеспечению национальной безопасности, расследует и пресекает преступления в киберпространстве, а также собирает, проводит анализ и обеспечивает внутреннюю киберразведку. Отдел национальной кибербезопасности министерства внутренней безопасности взаимодействует с правительством, промышленностью, научными кругами и международным сообществом, чтобы сделать кибербезопасность национальным приоритетом и общей ответственностью. Для получения дополнительной информации об обязанностях министерства внутренней безопасности см. Объединённую доктрину кибероперацій.

D-4. Каждый из родов вооружённых сил имеет органы военной полиции и контрразведки, которые выполняют множество функций Федерального бюро расследований и министерства внутренней безопасности США, специфичных для соответствующего рода вооружённых сил. К ним относятся Управление специальных расследований ВВС, Служба уголовных расследований ВМС, Командование уголовных расследований сухопутных войск США и Командование разведки и безопасности сухопутных войск США.

D-5. Во взаимодействии с министерством внутренней безопасности и ответственными должностными лицами штатов и местных органов власти Бюро Национальной гвардии координирует усилия Национальной гвардии по обеспечению безопасности страны, защите важнейших объектов государственной инфраструктуры и реагированию на чрезвычайные ситуации в киберпространстве штатов. Во многих штатах созданы группы быстрого реагирования на события в киберпространстве, способные реагировать на чрезвычайные ситуации в киберпространстве страны.

D-2. Подразделения министерства обороны

D-6. Министерство обороны использует средства воздействия на киберпространство для подготовки и проведения кибероперaций в целях защиты США в соответствии с полномочиями министра обороны. Полномочия на кибероперации, осуществляемые вооружёнными силами США, вытекают из Конституции США и федерального закона.

D-7. Ключевые разделы Кодекса США, применимые к министерству обороны, включают Раздел 10 «Вооружённые силы»; Раздел 50 «Война и национальная оборона»; и Раздел 32 «Национальная гвардия». В приложении D, таблице D-1 рассматриваются все применимые разделы Кодекса США, которые применяются к кибероперациям. Следующие агентства оказывают прямую или косвенную поддержку кибероперациям:

- Агентство национальной безопасности и Центральная служба безопасности.
- Агентство оборонных информационных систем
- Разведывательное управление МО.
- Национальное агентство геопространственной разведки.
- Национальное разведывательное управление.

D-2.1. Агентство национальной безопасности и Центральная служба безопасности

D-8. Агентство национальной безопасности является головной организацией правительства США в области криптологии, и его задачи охватывают как задачи радио- и радиотехническая разведки, так и деятельность по обеспечению безопасности киберпространства.

Центральная служба безопасности осуществляет сбор, обработку, анализ, создание, распространение данных радио- и радиотехнической разведки и другие криптологические операции, назначаемые директором Агентства национальной безопасности и начальником Центральной службы безопасности.

D-9. Агентство национальной безопасности и Центральная служба безопасности обеспечивают руководство и помощь в области разведки и киберпространства подразделениям министерства обороны, занимающимся сбором, обработкой, анализом, добыванием и распространением данных и информации радио- и радиотехнической разведки в интересах внешней разведки и контрразведки. Они обеспечивают национальные и ведомственные задачи и осуществляют поддержку PPTP в ходе военных операций по заданию министра обороны.

D-2.2. Агентство оборонных информационных систем

D-10. Агентство оборонных информационных систем является ведомством министерства обороны, состоящим из военнослужащих, гражданского персонала и подрядчиков, привлекаемых для проведения кибероперациий и выполнения задач, схожих с задачами кибервойск, находящихся в распоряжении Киберкомандования США, однако действующих на уровне министерства обороны. Агентство по оборонным информационным системам проводит операции в информационной сети МО и выполняет задачи ОКбО-ВМО на глобальном и корпоративном уровнях в рамках своей части информационной сети МО, соблюдая директиву командующего Киберкомандования США через начальника штаба объединённых сил – информационная сеть МО.

D-11. Агентство оборонных информационных систем предоставляет инженерную, архитектурную и организационную поддержку для интегрированных операций в информационной сети МО, включая управление предприятием, управление контентом и цифровую свободу манёвра. Агентство оборонных информационных систем решает задачи ОКбО-ВМО в своей части информационной сети МО для ослабления последствий, выполнения восстановления работоспособности на глобальном и корпоративном уровнях по указанию командира, штаба объединённых сил – информационная сеть МО.

D-12. Агентство оборонных информационных систем приобретает и поддерживает контроль над всеми ресурсами коммерческой спутниковой связи *(англ. satellite communications, SATCOM*) (если только министерство обороны не предоставит отказ запрашивающей организации), поддерживая командующего Стратегическим командованием США в качестве эксперта системы спутниковой связи SATCOM для коммерческих шлюзов SATCOM и министерства обороны. Через коммерческую спутниковую связь SATCOM Агентство оборонных информационных систем обеспечивает дальнюю связь для всего МО и видов ВС.

D-2.3. Разведывательное управление министерства обороны

D-13. Разведывательное управление министерства обороны удовлетворяет потребности в военной разведке министра и заместителя министра обороны, председателя Объединённого комитета начальников штабов и директора национальной разведки. Оно обеспечивает вклад военной разведки в национальную внешнюю разведку и контрразведку.

D-14. Разведывательное управление министерства обороны планирует, управляет и проводит разведывательные операции в мирное время, в условиях кризиса и в военное время. Разведывательное управление министерства обороны выступает в качестве ведущего органа министерства обороны по координации разведывательного обеспечения для удовлетворения требований боевого командования, возглавляет усилия по анализу и сбору информации со всеми операциями, а также объединяет и согласовывает возможности военной обороны и национальной разведки.

D-2.4. Национальное агентство геопространственной разведки

D-15. Национальное агентство геопространственной разведки является агентством боевого обеспечения и организацией-членом разведывательного сообщества, подчинённой министру обороны, заместителю министра по разведке и директору национальной разведки. Национальное агентство геопространственной разведки производит своевременную, актуальную и точную геопространственную разведку для объединённых сил и является основным источником анализа, продуктов, данных и услуг геопространственной разведки на национальном уровне.

Национальное агентство геопространственной разведки представляет рекомендации по постановке задач для используемых службой платформ и информационно-разведывательных средств сбора данных геопространственной разведки воздушного и наземного базирования.

D-16. Национальное агентство геопространственной разведки предоставляет группу поддержки Национального агентства геопространственной разведки для непосредственной поддержки центра разведывательных операций командующего объединёнными силами и включает группы поддержки Национального агентства геопространственной разведки для каждой из служб, агентств министерства обороны и нескольких агентств, не входящих в состав министерства обороны.

В соответствии с концепцией приоритетов национальной разведки Национальное агентство геопространственной разведки управляет требованиями к сбору данных со спутников и разрабатывает протоколы распространения данных для Национальной системы геопространственной разведки.

D-2.5. Национальное разведывательное управление

D-17. Национальное разведывательное управление является ведомством министерства обороны и входит в состав разведывательного сообщества. Национальное разведывательное управление отвечает за исследования и разработки, приобретение, запуск, развертывание и эксплуатацию наземных систем и соответствующих средств обработки данных, обеспечивающих сбор разведывательных данных и информации для выполнения национальных и ведомственных задач и других потребностей правительства США.

D-3. Резервные формирования

D-18. Национальная гвардия и резерв сухопутных войск США опираются на свои гражданские, академические, промышленные и межведомственные сообщества, чтобы подготовить военнослужащих, обладающих специальными навыками, способностями и опытом ведения операций в киберпространстве. Сухопутные войска эффективно используют возможности резервных подразделений и их средства воздействия на киберпространство, предоставляя расширенные возможности в тех областях, которые зачастую слишком дороги и требуют слишком много времени для резервных формирований, чтобы справиться с ними самостоятельно.

D-3.1. Бюро Национальной гвардии

D-19. Руководитель Бюро Национальной гвардии является советником командующего Киберкомандования США. Он помогает планировать и координировать кибероперации и выполнение задач РЭБ, запрашиваемых командующими войсками или председателем Объединённого комитета начальников штабов. Бюро Национальной гвардии обеспечивает связь между Киберкомандованием США и 50 штатами, Содружеством Пуэрто-Рико, округом Колумбия, Гуамом и Виргинскими островами по всем вопросам деятельности Национальной гвардии.

D-3.2. Национальная гвардия сухопутных войск

D-20. Национальная гвардия СВ является важнейшей составляющей общего потенциала сухопутных войск по проведению кибероперацій. Она проводит кибероперации в 54 штабах объединённых сил, поддерживая как сухопутные войска, так и штаты в соответствии с положениями Разделов 10 и 32 Кодекса США. Их приоритетной задачей является создание и обеспечение безопасной киберсреды США посредством проведения кибероперацій путём защиты критически важных узлов киберпространства, развития ситуативной осведомлённости о кибероперациях, а также оказания поддержки гражданским властям в реагировании на инциденты и защите критической инфраструктуры.

Национальная гвардия является экспертным звеном СВ по защите критической инфраструктуры и важнейших ресурсов. Национальная гвардия обеспечивает поддержку сухопутным войскам и Киберкомандования США в проведении операций в киберсетях, киберподдержке и ведении кибервойны.

D-3.3. Резерв сухопутных войск США

D-21. Резерв сухопутных войск США предоставляет обученный и готовый личный состав для выполнения кибероперациий для обеспечения требований задач объединённых сил, сухопутных войск и боевого командования. Военнослужащие резерва сухопутных войск США обладают зрелостью и глубоким опытом, обеспечивая готовность к проведению текущих и будущих операций. Уникально то, что резерв сухопутных войск США будет напрямую связан с планами Киберкомандования США на случай чрезвычайных ситуаций, что позволит ему мобилизовать личный состав для обеспечения планов и операций резерва Сухопутных войск, поддерживающих кибероперации. Резерв Сухопутных войск США имеет экспедиционный (мобилизационный) характер и оказывает поддержку резерву Сухопутных войск и Киберкомандованию США в области киберпространства.

D-4. Киберкомандование США

D-22. План единого командования и различные приказы министра обороны США наделяют Киберкомандование США полномочиями по координации всех операций министерства обороны в киберпространстве, включая операции по эксплуатации, обеспечению безопасности и защите информационной сети МО. Киберкомандование США выполняет свои задачи в рамках трёх основных направлений деятельности: обеспечение безопасности, эксплуатации и защиты информационной сети МО; защита страны от нападения в киберпространстве; обеспечение поддержки киберпространства по требованию боевого командования. Киберкомандование США руководит операциями по обеспечению безопасности и обороне информационной сети МО, используя директивные полномочия для кибероперациий. В случае необходимости Киберкомандование США также проводит военные кибероперации за пределами информационной сети МО в поддержку национальных целей. Более подробную информацию о функциях и обязанностях Киберкомандования США см. в JP 3-12.

D-23. Кибероперации проводятся кибервойсками, состоящими как из действующих военнослужащих, так и гражданского персонала. Кибервойска МО включают силы, подчиняющиеся Киберкомандованию США в рамках глобального процесса управления силами, войска, находящиеся в распоряжении видов ВС, и резервные формирования. В состав кибервойск также входит личный состав, выполняющий функции поставщиков услуг кибербезопасности, установленные службами и ведомствами МО для защиты сегментов информационной сети МО.

Поставщики услуг в области кибербезопасности – это, как правило, сертифицированные гражданские сотрудники и подрядчики министерства обороны, выполняющие такие услуги по защите информационной сети МО, как аналитика, поддержка инфраструктуры, реагирование на инциденты, аудит и управление поставщиками услуг.

D-4.1. Силы кибероперaций

D-24. Командующий Киберкомандованием США осуществляет боевое командование силами кибероперaций. Командующий Киберкомандованием США использует подразделения сил кибероперaций для выполнения национальных стратегических задач или выделяет подразделения для поддержки задач боевого командования через штаб объединённых сил в киберпространстве. Силы кибероперaций – это часть общих сил министерства обороны для проведения кибероперaций. Силы кибероперaций состоят из подразделений трёх типов:

- Силы кибероперaций боевого применения.
- Силы киберзащиты.
- Национальные силы кибероперaций (*англ. Cyber national mission force, CNMF*).

D-4.1.1. Силы кибероперaций боевого применения

D-25. Силы кибероперaций боевого применения осуществляют наступательные кибероперации и соответствующую техническую и аналитическую деятельность для поддержки операций географических или функциональных боевых командования. При наличии соответствующих полномочий и распоряжений силы кибероперaций боевого применения осуществляют кибератаки в нейтральном киберпространстве и киберпространстве противника с целью создания воздействия, направленного против потенциала угрозы. В состав сил кибероперaций боевого применения входят боевые оперативные группы и группа (группы) боевого обеспечения.

D-26. Боевые оперативные группы – это тактические группы, осуществляющие киберразведку и кибератаки в нейтральном киберпространстве и киберпространстве противника. Группы боевого обеспечения – это технические группы, которые оказывают поддержку боевым оперативным группам посредством анализа разведданных, использованием средств воздействия на киберпространство, лингвистического обеспечения и планирования.

D-4.1.2. Силы киберзащиты

D-27. Силы киберзащиты проводят оборонительные кибероперации-внутригосударственные мероприятия по обороне в пределах информационной сети МО или, при наличии соответствующих полномочий и указаний, в киберпространстве, используемом своими войсками за пределами информационной сети МО.

Силы киберзащиты состоят из группы (групп) киберзащиты, организованной, обученной и оснащённой для защиты назначенного киберпространства во взаимодействии и при поддержке владельцев сегментов, поставщиков услуг кибербезопасности и пользователей. Типы групп киберзащиты:

- **Национальные группы киберзащиты**. Назначение и руководство осуществляется штабом Национальных сил кибероперацій (*англ. Cyber National Mission Force-Headquarters, CNMF-HQ*).
- **Группы киберзащиты информационной сети МО**. Назначение и руководство осуществляется штабом объединённых сил – информационная сеть МО.
- **Группы киберзащиты боевых командований**. Назначение и руководство осуществляется боевыми командованиями.
- **Группы киберзащиты видов ВС**. Назначение и руководство осуществляется компонентом вида ВС, отвечающего за киберпространство.

D-4.1.3. Национальные силы кибероперацій

D-28. Национальные силы кибероперацій проводят ОКбО против киберугроз на основе приоритетов Киберкомандования США и национальных приоритетов. Национальные силы кибероперацій могут проводить ОКбО в информационной сети МО или, когда это разрешено, за пределами информационной сети МО в киберпространстве, используемом своими войсками. Когда это разрешено и согласовано национальные силы кибероперацій проводят ОКбО-МР в нейтральном киберпространстве и киберпространстве противника. Национальные силы кибероперацій состоят из национальных оперативных групп, национальной группы (групп) обеспечения и национальных групп киберзащиты.

D-29. Национальные оперативные группы – это тактические группы, которые проводят ОКбО-МР. Национальные группы обеспечения оказывают поддержку национальным оперативным группам в проведении разведывательного анализа, использовании средств воздействия на киберпространство, лингвистическом обеспечении и планировании. Национальные группы киберзащиты проводят ОКбО-ВМО на национальном уровне, который может распространяться на защиту союзных структур, не относящихся к министерству обороны, или сетей критической инфраструктуры по приказу министра обороны. Национальные силы кибероперацій находится в подчинении и управляется штабом Национальных сил кибероперацій. В таблице D-1 ниже представлена взаимосвязь между подразделениями сил кибероперацій, связанными с ними задачами и действиями в киберпространстве и типичными оперативными местами в киберпространстве, используемом своими войсками, нейтральными субъектами и противником.

Таблица D-1

Подразделения сил кибероперaций и связанные с ними группы

Тип кибероперации	Кибервойска, проводящие операцию	Место в киберпространстве	Тип кибердействий
Операции в информационной сети МО	Силы кибероперaций, находящиеся в распоряжении вида ВС	Информационная сеть МО	Кибербезопасность
Наступательные кибероперации	Силы кибероперaций боевого применения, состоящие из боевых оперативных групп, поддерживаемых группами боевого обеспечения	Нейтральное киберпространство и киберпространство противника	Кибератака и использование киберпространства
Оборонительные кибероперации-внутригосударственные мероприятия по обороне (в пределах информационной сети МО)	Силы киберзащиты, состоящие из вида ВС, информационной сети МО, групп киберзащиты боевых командований	Своё киберпространство	Защита киберпространства
Оборонительные кибероперации-внутригосударственные мероприятия по обороне (за пределами информационной сети МО)	Силы киберзащиты, состоящие из национальных групп киберзащиты	Киберпространство за пределами информационной сети МО, используемое своими войсками	Защита киберпространства
Оборонительные кибероперации-меры реагирования	Национальные силы кибероперaций, в состав которых входят национальные оперативные группы, поддерживаемые национальными группами обеспечения	Нейтральное киберпространство и киберпространство противника	Кибератаки и использование киберпространства

D-4.2. Подразделения, подчинённых Киберкомандованию США

D-30. На рис. D-1 представлено распределение групп из состава сил кибероперaций между Киберкомандованием США и подчинёнными подразделениями и боевыми командованиями.

Подчинёнными подразделения Киберкомандования США:

- штаб национальных сил кибероперaций;
- штаб объединённых сил - информационная сеть МО;
- кибер-штаб объединённых сил (всего четыре);
- кибер-командования компонентов видов вооруженных сил.

Примечание.

> Командование Береговой охраны – единственное из видов ВС, которое сохраняет оперативный контроль над всеми своими кибервойсками в соответствии с меморандумом о соглашении между министерством обороны и министерством внутренней безопасности. Командующий Киберкомандованием Береговой охраны не имеет двойного статуса в качестве командующего кибер-штаба объединённых сил.

D-4.2.1. Штаб национальных сил кибероперaций

D-31. Штаб национальных сил кибероперaций осуществляет защиту киберпространства страны путём планирования, координации, выполнения и контроля задач оборонительных кибероперaций против угроз в киберпространстве. Штаб национальных сил кибероперaций использует национальные группы киберзащиты для борьбы с внутренними угрозами для критически важных объектов в киберпространстве, не принадлежащими министерству обороны. Командующий национальными силами кибероперaций осуществляет оперативное управление национальными оперативными группами, национальными группами обеспечения и национальными группами киберзащиты.

D-4.2.2. Штаб объединённых сил – информационная сеть МО

D-32. Во взаимодействии со всеми боевыми командованиями штаб объединённых сил – информационная сеть МО руководит и проводит глобальные операции в информационной сети МО и ОКбО-ВМО. Штаб объединённых сил – информационная сеть МО является координационным центром для межведомственного согласования глобальных мероприятий штаба объединённых сил – информационная сеть МО и ОКбО-ВМО, которые могут затрагивать более одного подразделения министерства обороны. Киберкомандование США делегировало оперативный контроль кибер-компонентов видов вооружённых сил штабу объединённых сил – информационная сеть МО по защите информационной сети МО. Кроме того, Киберкомандование США делегировало полномочия по руководству операциями в киберпространстве боевых командований штабу объединённых сил – информационная сеть МО, что позволяет ему ставить задачи видам ВС и другим подразделениям МО принимать меры по обеспечению безопасности и защите киберпространства во всей информационной сети МО.

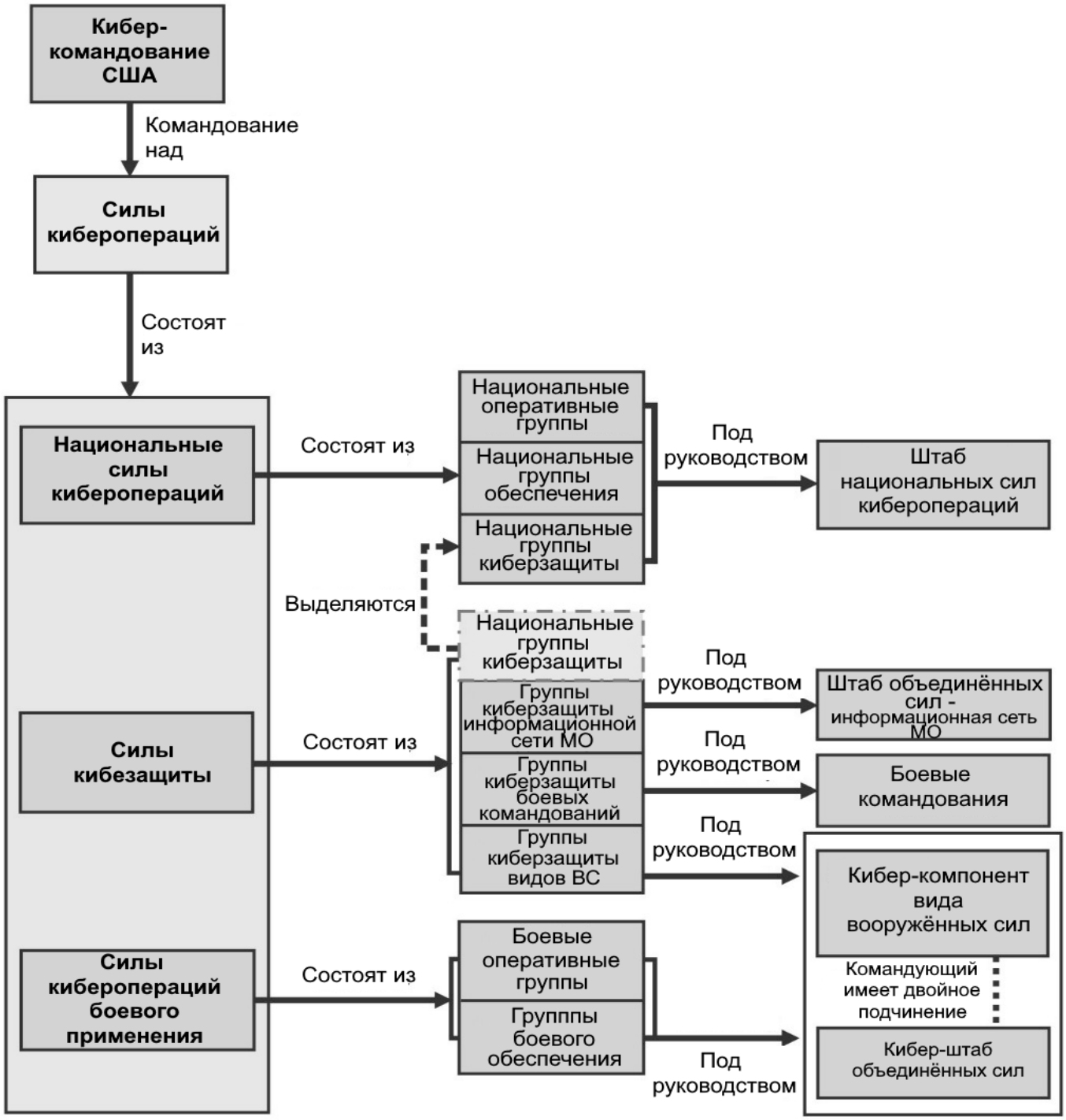


Рис. D-1. – *Распределение сил кибероперацій*

D-4.2.3. Киберкомандования вида вооружённых сил

D-33. Киберкомандование США и штаб объединённых сил – информационная сеть МО проводят операции в информационной сети МО и ОКбО-ВМО через подчинённые кибер-компоненты видов вооружённых сил. Во взаимодействии или под руководством командующего штаб объединённых сил - информационная сеть МО, кибер-компоненты видов вооружённых сил проводят операции в информационной сети МО и ОКбО-ВМО в пределах своей соответствующей части информационной сети МО.

Штаб объединённых сил делегирует кибер-компонентам видов ВС директивные полномочия по кибероперациям для действий в пределах обслуживаемой ими части информационной сети МО. В сухопутных войсках командующий Киберкомандованием СВ руководит операциями в информационной сети МО и ОКбО-ВМО в пределах информационной сети МО-СВ. Каждый командующий кибер-компонентом вида вооружённых сил, за исключением командующего Киберкомандованием Береговой охраны, имеет двойное подчинение от командующего, Киберкомандования США для командования одним из четырёх кибер-штабов объединённых сил

D-4.2.4. Кибер-штаб объединённых сил

D-34. Кибер-штаб объединённых сил анализирует, планирует и проводит наступательные кибероперации в общей поддержке одного или нескольких боевых командований. Кибер-штабы объединённых сил уточняют требования к разведке в киберпространстве, обеспечивают оперативное командование и управление боевыми группами и группами боевого обеспечения, а также поддерживают внедрение наступательных кибероперацийв планы и приказы боевых командований.

D-35. Командиры сухопутных войск должны понимать, что кибер-штаб объединённых сил, поддерживающий их операцию, не обязательно будет штабом кибер-штабом объединённых сил (сухопутные войска). Поскольку кибер-штабы объединённых сил связаны отношениями поддержки с конкретными боевыми командованиями, кибер-штаб объединённых сил, поддерживающий подразделение сухопутных войск, будет зависеть от того, какому боевому командованию подчиняется или придано это подразделение для выполнения задачи.

Например:

> Операции в рамках поддержки Индо-Тихоокеанского командования ВС США будут проводиться через кибер-штаб-объединённых сил (ВМС), а операции в рамках обеспечения Центрального командования ВС США будут проводиться через Киберкомандование сухопутных войск, выполняющего функции кибер-штаба объединённых сил (СВ).

D-5. Боевые командования

D-36. Киберкомандование США назначает группы киберзащиты боевых командований в географические и функциональные боевые командования для проведения ОКбО-ВМО в пределах их зоны ответственности. Боевые командования имеют штатные объединённые киберцентры и получают прямую поддержку подразделений комплексного планирования кибероперацийй, выделенных Киберкомандованием США.

D-37. Боевые командования применяют выделенные им группы киберзащиты для проведения оборонительных кибероперацийвнутригосударственных мероприятий по обороне в сетях и системах, которые используют и обслуживают боевые командования. Однако войска под командованием боевых командований часто действуют в сетях и системах, обслуживаемых видами вооружённых сил, где командующие боевыми командованиями не имеют технического управления. Боевые командования полагаются на штаб объединённых сил - информационная сеть МО для руководства операциями в информационной сети МО и ОКбО-ВМО в этих сетях, обслуживаемых видами вооружённых сил, или в других сетях, которые технически не управляются боевым командующим.

D-5.1. Объединённый киберцентр

D-38. Многие боевые командования объединяют действия штаба по планированию, интеграции, синхронизации, мониторингу и оценке кибероперации в рамках объединённого киберцентра. Личный состав, назначенный в объединённый киберцентр, обычно является профильными специалистами по тактике, методам и процедурам наступательных и оборонительных кибероперации и выступает в качестве советников боевых командующих. Каждый объединённый киберцентр поддерживается назначенным подразделением совместного планирования кибероперации.

D-39. Штаб армейского корпуса может взаимодействовать с объединённым киберцентром, или структурами совместного планирования кибероперации, являясь штабом объединённой оперативно-тактической группы. В большинстве других ситуаций, штаб армейского корпуса взаимодействует в первую очередь со штабом кибероперации в объединённой оперативно-тактической группе или штабом по ведению РЭБ и кибероперации (СЕМА) в группировке СВ на ТВД. Командиры сухопутных войск и штаб на уровнях ниже корпуса редко взаимодействуют с объединённым киберцентром или структурами совместного планирования кибероперации.

D-5.2. Подразделение совместного планирования кибероперации

D-40. Подразделение совместного планирования кибероперации является подчинённой структурой Киберкомандования США, которое совместно с объединённым киберцентром боевого командования и штабом осуществляет консультативное обеспечение в интересах боевого командования и служит как резервная поддержка Киберкомандования США. Подразделения совместного планирования кибероперации включают личный состав Киберкомандования США, штаба объединённых сил - информационная сеть МО и кибер-штаба объединённых сил, находятся в оперативном подчинении кибер-штаба объединённых сил, которое поддерживает конкретного командующего боевым командованием, и

располагаются на одной базе с каждым боевым командованием для полной интеграции в объединённый киберцентр или в кибер-штаб.

Подразделения совместного планирования кибероперациий включают специалистов по оперативному планированию кибероперациий и других профильных специалистов, необходимых для поддержки разработки требований к кибероперациям в зоне ответственности и для оказания помощи специалистам планирования боевого командования в координации, интеграции и предотвращения конфликтов в ходе кибероперациий.

D-41. Подразделение совместного планирования кибероперациий оказывает поддержку объединённому киберцентру в понимании ситуативной осведомлённости и делится своевременной информацией о киберугрозах в зоне ответственности. Подразделение совместного планирования кибероперациий оказывает поддержку объединённой разведывательной подготовки (осуществляемой несколькими видами вооружённых сил) оперативной обстановки в киберпространстве, ведет анализ системы целей, представляет описание целей боевому командованию для включения в перечень целей.

D-5.3. Группа управления объединёнными операциями в ЭМС

D-42. Группа управления объединёнными операциями в ЭМС включает специалистов РЭБ и управления спектром, рекомендующих боевому командованию тактику, технику и порядок объединённых кибероперациий в зоне ответственности. Полномочия по руководству и взаимодействию группы, как правило, делегируется командиру группы от боевого командования, что позволяет обеспечить единство командования ЭМС в объединённой оперативно-тактической группе в зоне ответственности. Координация управления ЭМС позволяет объединённому командованию планировать, координировать, контролировать, управлять, оценивать и расставлять приоритеты при выполнении совместных операций РЭБ. В целях РЭБ группа управления объединёнными операциями в ЭМС разрабатывает и ставит текущие задачи в ЭМС компонентам видов вооружённых сил в их зоне ответственности. Задачи операций ЭМС содержат директивы ЭМС и включаются в план объединённых операций в ЭМС.

D-43. Группа управления объединёнными операциями в ЭМС боевого командования отвечает за всё оперативное планирование, выполнение и оценку объединённых операций в ЭМС, если только не были создана группа управления объединёнными операциями в ЭМС оперативно-тактической группы и ей не были делегированы эти полномочия. В таком случае группа управления боевого командования осуществляет планирование, координацию и руководство на уровне театра военных действий, но делегирует полномочия по координации действий в ЭМС группе управления объединённой оперативно-тактической группы для выполнения поставленных задач в назначенном районе объединённых операций. Армейский корпус, назначенный

штабом объединённой оперативно-тактической группы, совмещает руководство ЭМС с отделением CEMA для формирования компонента сухопутных войск в своей группе управления объединёнными операциями в ЭМС.

Другие компоненты видов вооружённых сил также формируют группы управления операциями в ЭМС для поддержки штаба объединённой оперативно-тактической группы.

D-44. Группа управления объединёнными операциями в ЭМС боевого командования может ограничить права группы управления объединённой оперативно-тактической группы координировать электромагнитный спектр, оставив общую координацию и командование. При делегировании полномочий по координации использования электромагнитного спектра, объединённая оперативно-тактическая группа выполняют задачи РЭБ через выделенные им подразделения видов вооружённых сил. Каждый вид вооружённых сил создает подчинённые группы операций в ЭМС, создавая управленческие, штабные или технические каналы между группой управления объединёнными операциями в ЭМС объединённой оперативно-тактической группы и подчинёнными подразделениями. На рис. D-2 показана условная национальная организационная структура операций в ЭМС для командного, штабного и технического каналов. Каналы управления – это прямые пути подчинённости (ADP 6-0). Командиры и уполномоченные штабные офицеры используют каналы управления для осуществления командной деятельности. Штабные офицеры используют каналы управления для осуществления командной деятельности. Штабные каналы представляют собой пути передачи данных между штабами и используются для управления (ADP 6-0). Штабные каналы передают информацию по планированию, доклады, управляющие инструкции и другую информацию для командования операцией. Технические каналы – пути передачи данных между двумя технически схожими подразделениями, офисами или отделами штаба, выполняющими техническую функцию, требующую специальных знаний, или управляют выполнением технических функций (ADP 6-0). Технические каналы обычно используются для управления выполнением технических функций.

D-45. Армейский корпус или дивизия, назначенные для командования сухопутными войсками и морской пехотой в районе объединённых операций, называется наземным компонентом объединённых сил. Командующий наземным компонентом объединённых сил создаёт свою группу операций в ЭМС путём введения руководителя по управлению спектром в отделение CEMA. Объединённая оперативно-тактическая группа обеспечивает проведение объединённых операций в ЭМС в районе объединённых операций в соответствии с правилами, установленными боевыми командованиями. Более подробную информацию об объединённых операциях в ЭМС спектре см. в JP 3-85.

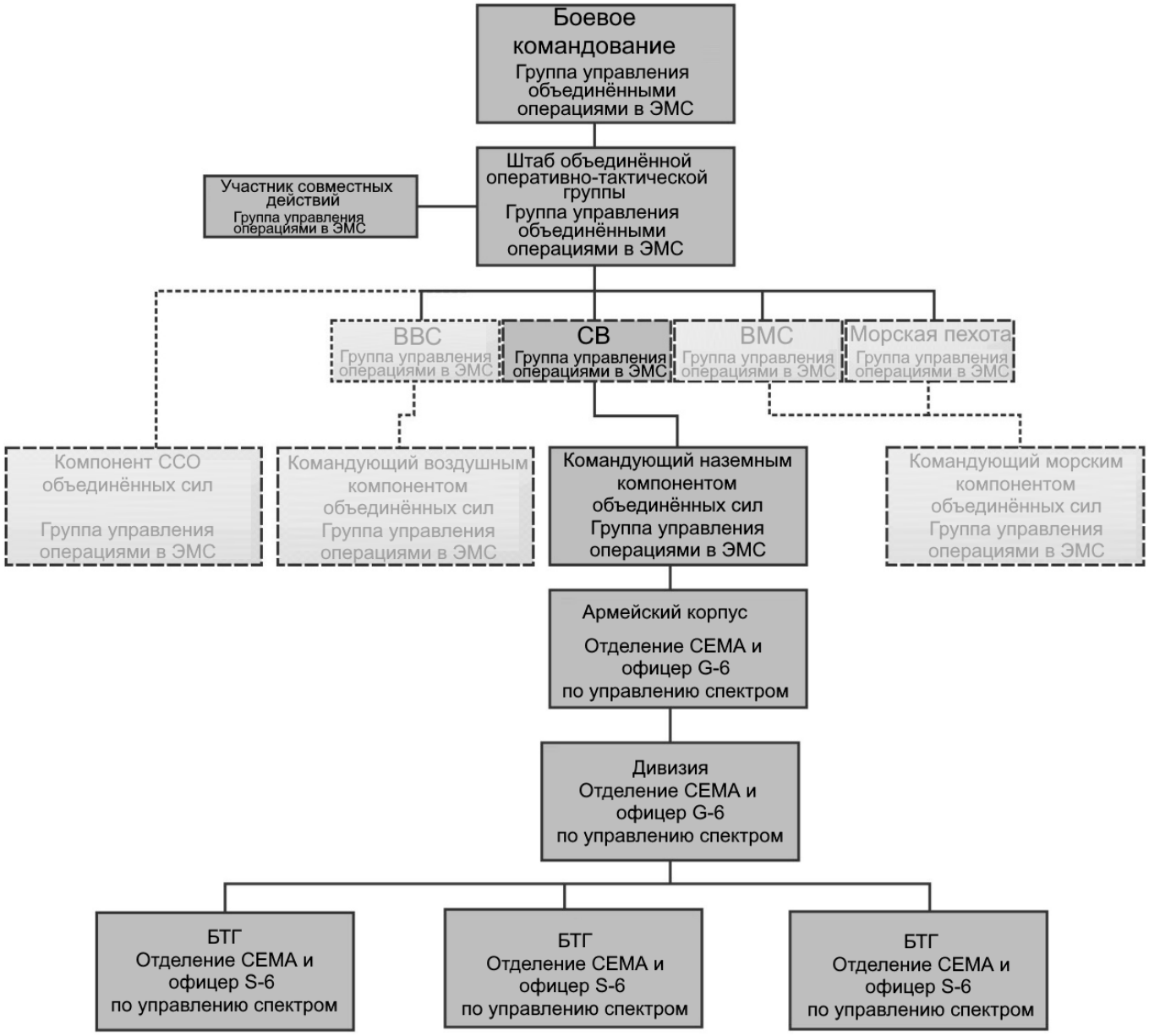


Рис. D-2. – *Организационная структура операций в ЭМС*

Приложение E. Запрос на поддержку

В данном приложении рассматривается, как подразделения сухопутных войск запрашивают поддержку для кибероперации и РЭБ в ходе объединённых операций. Сухопутным войскам может потребоваться поддержка наступательных кибероперации для идентифицированных целей, требующих поражения с использованием кибератак. Оперативная поддержка в области защиты киберпространства может оказаться необходимой, когда выявленная угроза в своём или союзном киберпространстве выходит за рамки обеспечения кибербезопасности. Поддержка РЭБ может потребоваться, когда подразделению сухопутных войск требуется усиление, или когда их возможности или полномочия в области РЭБ не способны выполнить требования для поддержки операций или замысла командира.

E-1. Запрос на поддержку в киберпространстве и РЭБ

E-1. Данный раздел описывает процедуры по запросу поддержки ОКбО-ВМО, НКбО и ОкБО-МР на уровне армейских корпусов и ниже. В нём также представлено, как подразделения сухопутных войск запрашивают не штатное обеспечение РЭБ в качестве дополнения для устранения пробелов целеуказаний.

E-1.1. Обзор запроса на получение поддержки

E-2. В совокупности с необходимыми правовыми и оперативными полномочиями командиры выбирают штатные средства РЭБ для создания желаемого воздействия на цели, определённые для ЭМА. Если штатные средства РЭБ подразделения не удовлетворяют требованиям по целеуказаниям, необходимых для реализации замысла командира, или командир не имеет полномочий на применение тех или иных средств РЭБ, подразделение СЕМА запрашивает поддержку у следующего вышестоящего уровня. Для запроса ЭМА с применением авиационных средств группа СЕМА использует совместный запрос на проведение совместного тактического авиаудара (*англ. Joint Tactical Air Strike Request*, *JTASR*) и инструмент поддержки запросов.

E-3. По мере передачи запросов от уровня к уровню каждый из них обрабатывает запрос на проведение совместного тактического авиаудара, чтобы оценить свои возможности по оказанию поддержки, отвечающей требованиям запрашивающего подразделения. Уровень запроса повышается либо до тех пор, пока оно не достигнет уровня, который в состоянии обеспечить поддержку для запрашивающего подразделения, либо до тех пор, пока вышестоящий уровень не откажет в удовлетворении запроса. Поддержка запрашивающего подразделения может быть невозможна из-за приоритетности, сроков, возможностей, разрешений или конфликта с другими требованиями к возможностям РЭБ.

Командиры несут окончательную ответственность за отклонение запросов на ресурсы и могут делегировать это право своему штабу. Отклонить запрос на использование объединённых воздушных ресурсов может командующий объединёнными силами, но не командующий воздушным компонентом объединённых сил.

E-4. Армейский корпус и подразделения более низкого уровня не обладают штатными возможностями в киберпространстве для решения задач ОКбО-ВМО, ОКбО-МР или НКбО. Структурное подразделение штаба G-3 или S-3 запрашивает поддержку через вышестоящий штаб. Группы G-6 или S-6 и отделение CEMA координируют запрос ОКбО-ВМО после установления того, что угроза в киберпространстве, используемом своими войсками, выходит за рамки обеспечения безопасности киберпространства. ОКбО-ВМО является инструментом для реализации ОКбО-МР. Силы кибероперацій, выполняющие ОКбО-ВМО, запрашивают меры реагирования после принятия решения о том, что угроза в киберпространстве требует оборонительной атаки за пределами киберпространства, используемого своими войсками или войсками союзников. НКбО используются для создания желаемого воздействия на цели, выбранные для кибератак, которые включены в объединённый список целей. ОКбО-МР и НКбО схожи, за исключением того, что ОКбО-МР используются только для сдерживания угрозы, тогда как НКбО применяется для проецирования силового воздействия.

E.1-2. Запрос на поддержку наступательных кибероперацій

E-5. Для выполнения задач НКбО рабочая группа CEMA определяет цели, которые соответствуют установленным стандартам выбора целей в целеуказания (см. Глава 4) и соответствуют указаниям командиров по целеуказанию. После утверждения группа огневой поддержки добавляет эти цели в список приоритетных целей подразделения со всеми другими идентифицированными целями, не связанными с киберпространством. Рабочая группа CEMA также выносит рекомендации по списку объектов, запрещённых к поражению, и списку объектов с ограничениями на поражение, что оказывает поддержку руководящим указаниям командующего по целеуказанию.

E-6. Боевые оперативные группы предоставляют возможности НКбО армейским корпусам и нижестоящим подразделениям через процедуру запросов на поддержку. После утверждения командиром отделение CEMA представляет запрос на поддержку вместе со списком приоритетных целей, списком запрещённых к поражению целей и списком с ограничениями в вышестоящий штаб через Командование наземным компонентом объединённых сил в штаб объединённой оперативно-тактической группы на рассмотрение в качестве предложений для объединённого цикла целеуказания и включения в объединённый список запрещённых или ограниченных к поражению целей.

Цели, требующие решения задач, связанных с НКбО, должны включать такие данные, как известные IP-адреса, по возможности, известные физические местоположения, а также любые известные киберперсоны, связанные с целью.

E-7. После того, как штаб объединённой оперативно-тактической группы утвердит цели, связанные с НКбО, определённые в списке приоритетных целей корпуса, он включает их в объединённый цикл целеуказаний. Командование объединённой оперативно-тактической группой продолжает процедуру продвижения запроса на поддержку с целью получения поддержки НКбО от киберштаба объединённых сил (рис. E-1).

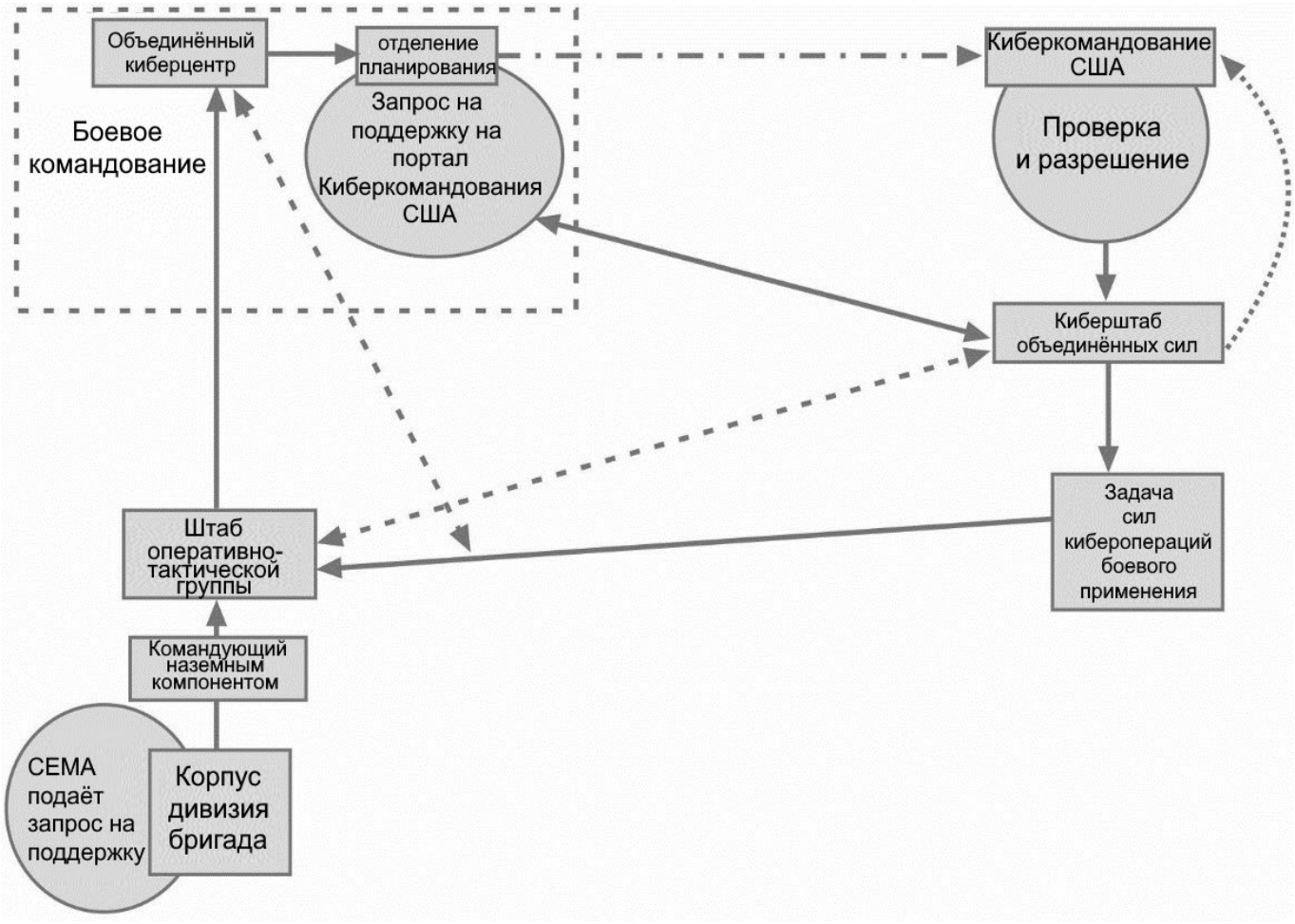


Рис. E-1. – *Процесс маршрутизации при запросе обеспечения НКбО*

Примечание.

> Киберкомандование США не принимает форму запроса для воздействия в киберпространстве (*англ. cyber effects request format, CERF*). Штаб использует запрос на поддержку для запроса помощи в проведении наступательных кибероперациий в условиях совместной боевой операции. Прежде чем запрашивать поддержку штаб объединённой оперативно-тактической группы и подчинённые ему подразделения должны ознакомиться с запросом на поддержку или любым другим стандартизированным форматом запроса, установленным Киберкомандованием США и боевым командованием. Командование наземным компонентом объединённой группировки войск преобразует все запросы для воздействия в киберпространстве, полученные от сухопутных войск, в формат запросов на поддержку, перед их направлением в штаб объединённой оперативно - тактической группы.

Е.1.3. Запрос на поддержку оборонительных кибероперациий

Е-8. Подразделения армейского корпуса и ниже не имеют штатных средств оборонительных кибероперациий-внутригосударственных мероприятий по обороне и должны запрашивать поддержку выполнения задач, связанных с ОКбО-ВМО в рамках процесса запроса поддержки. Поддержка в рамках ОКбО-ВМО необходима при возникновении угроз на рамках информационной сети МО – сухопутные войска, выходящих за рамки возможностей штатных средств кибервойск, обеспечивающих безопасность киберпространства. Подразделения запрашивают поддержку ОКбО-ВМО в качестве быстрой меры для защиты от угрозы в киберпространстве. Отдел связи армии (G-6) или штаба бригады (S-6) согласовывает с оперативным управлением армии (G-3) или штаба бригады (S-3) подготовку запроса на поддержку для предоставления поддержки в рамках ОКбО-ВМО.

Е-9. После утверждения командующим запроса на поддержку, он представляется, утверждается и направляется в вышестоящие штабы через Командование наземным компонентом объединённой группировки войск в штаб объединённой оперативно-тактической группы, пока не попадает в объединённый киберцентр боевого командования. Запрашивающее подразделение дополнительно информирует поставщика сервисов кибербезопасности (Агентство оборонных информационных систем или Командование сетевых технологий СВ) об угрозе в киберпространстве. Штаб объединённой оперативно-тактической группы направляет запрос на поддержку; поставщику услуг кибербезопасности, также уведомляет штаб объединённых сил – информационная сетей МО о выявленной угрозе в киберпространстве. Боевое командование имеет штатные группы киберзащиты, которые проводят ОКбО-ВМО в киберпространстве, используемом своими войсками и союзниками. Командиры имеют директивные полномочия на операции в киберпространстве, которые разрешают ОКбО-ВМО в рамках назначенной им зоны ответственности без запроса разрешения от Киберкомандования США.

E-10. Боевое командование использует штатные группы по киберзащите для проведения ОКбО-ВМО во всей зоне ответственности, которые осуществляют ОКбО-ВМО. Группы киберзащиты проводят ОКбО-ВМО исключительно за пределами информационной сети МО в киберпространстве своих войск или союзников. Если группы киберзащиты боевого командования недоступны, объединённый центр управления киберпространством направляет запрос на поддержку через подразделение комплексного планирования кибероперациий в штаб объединённых сил – информационная сеть МО через портал Киберкомандования США. Подразделение комплексного планирования кибероперациий обеспечивает для Киберкомандования США ситуативную осведомлённость обо всех миссиях ОКбО-ВМО, проводимых в зоне ответственности.

Примечание:

> Когда поставщику услуг кибербезопасности становится известно об угрозе в информационной сети МО он направляет информацию в штаб объединённых сил – информационная сеть МО. Штаб объединённых сил – информационная сеть МО использует уведомление от поставщика услуг кибербезопасности для начала процесса привлечения групп киберзащиты (либо информационной сети МО, либо вида ВС) до получения запроса на поддержку по каналам связи. Однако запрашивающее подразделение по-прежнему несёт ответственность как за инициирование процесса запроса на поддержку, так и за информирование поставщика услуг кибербезопасности.

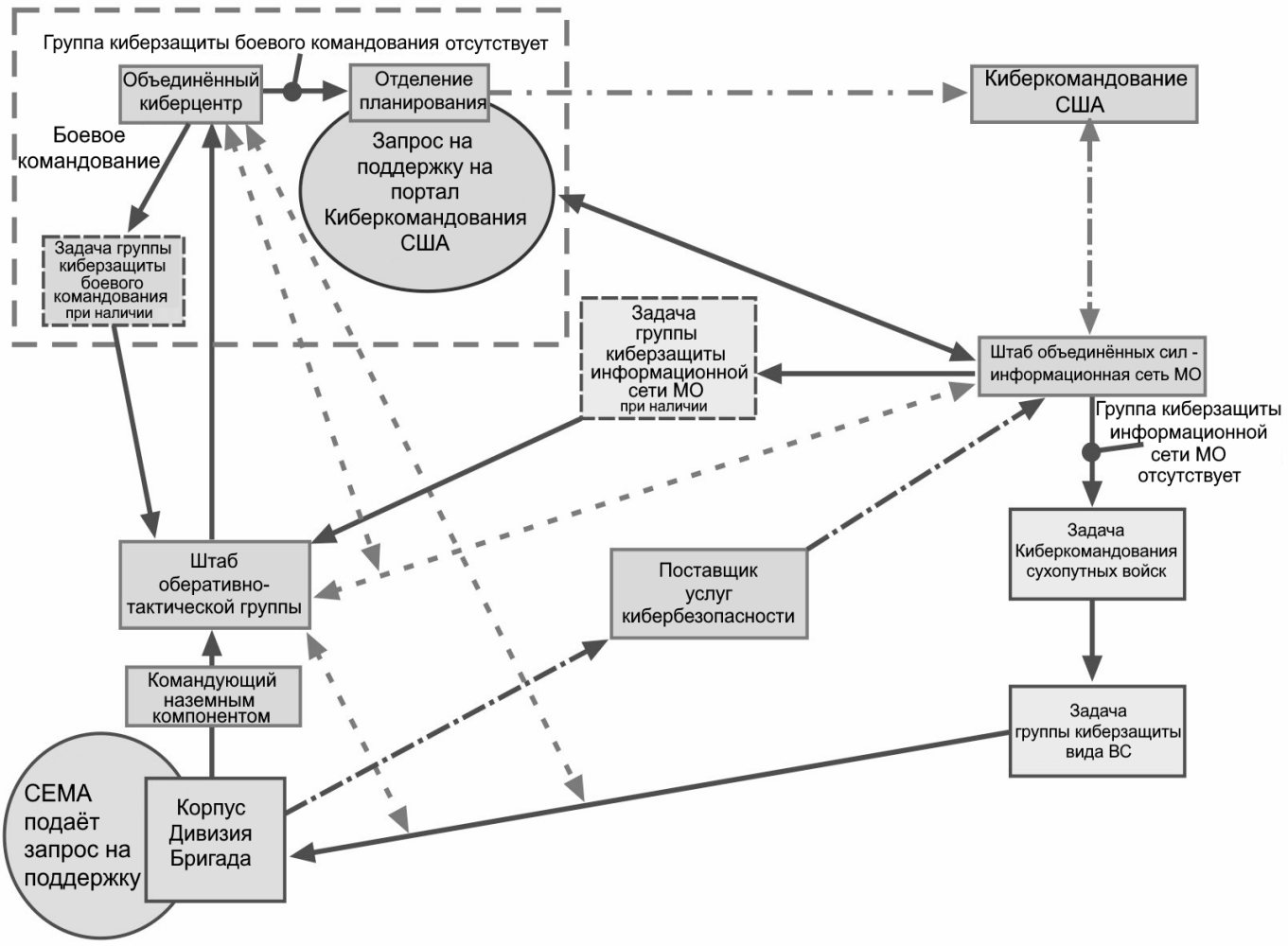
E-11. Штаб объединённых сил – информационная сеть МО обладает директивными полномочиями по проведению операций в киберпространстве для осуществления ОКбО-ВМО в глобальном масштабе в рамках сетей и систем, входящие в инфраструктуру информационной сети МО. Штаб объединённых сил – информационная сеть МО обеспечивает ситуативную осведомлённость Киберкомандования США в отношении всех ОКбО-ВМО.

Штаб объединённых сил – информационная сеть МО также осуществляет тактическое управление всеми кибер-командованиями видов ВС, занимающимися вопросами киберпространства, только для операций в рамках сетей и систем, входящие в инфраструктуру информационной сети МО и ОКбО-ВМО.

В штабе объединённых сил – информационная сеть МО имеются свои группы киберзащиты информационной сети МО, которые проводят ОКбО-ВМО; однако их основное внимание, как правило, сосредоточено на мониторинге и реализации проактивных ОКбО-ВМО для ослабления угроз в киберпространстве для сетей и систем, входящих в инфраструктуру информационной сети МО в глобальном масштабе.

E-12. Если группы киберзащиты информационной сети МО недоступны для удовлетворения запроса на поддержку, штаб объединённых сил – информационная сеть МО контролирует процесс совместного утверждения поручения одному из киберкомандований видов ВС предоставить группы киберзащиты для проведения ОКбО-ВМО в поддержку запроса подразделения. Назначенная группа киберзащиты может выполнять ОКбО-ВМО удалённо или совместно со штабом объединённой оперативно-тактической группы или запрашивающим подразделением. При нахождении в составе другого подразделения группа киберзащиты по-прежнему подчиняется командованию своего подразделения.

Рисунок E-2 иллюстрирует процесс маршрутизации для запроса поддержки ОКбО-ВМО для корпуса и ниже.



Условные обозначения:

координация

ситуативная оценка и обновления

запрос на процесс поддержки ОКбО-ВМО

Информирование поставщика услуг кибербезопасности

Рис. E-2. Процесс маршрутизации при запросе ОКО-ВМО

Примечание:

> Инициирование ОКбО-ВМО для упреждающего реагирования на угрозы в киберпространстве осуществляется по принципу «сверху вниз». Упреждающие ОКбО-ВМО имеют место, когда штаб объединённых сил – информационная сеть МО выявляет угрозу киберпространству в сетях и системах, входящие в инфраструктуру информационной сети МО до получения запроса на поддержку или информации от поставщика услуг по кибербезопасности и заблаговременно развёртывает группы киберзащиты (либо информационной сети МО, либо вида ВС) для ослабления угрозы в киберпространстве.

E-1.3.1. Поддержка оборонительных кибероперaций для киберпространства, не относящегося к министерству обороны

E-13. Запрос на поддержку запрашивает помощь в связи с угрозой, обнаруженной в критической сети, расположенной в киберпространстве, используемом своими войсками и не являющемся частью информационной сети МО, направляется в Штаб национальных сил кибероперaций для привлечения национальной группы киберзащиты для проведения ОКбО-ВМО. Национальные группы киберзащиты проводят ОКбО-ВМО только в киберпространстве, не являющемся частью киберпространства, которое контролирует министерство обороны. Киберпространство, не входящее в зону ответственности министерства обороны, т.е. сетей и систем, входящих в инфраструктуру информационной сети МО включает в себя критически важные сети, в которых союзные структуры выполняют кибероперации, а также области киберпространства, защищаемые МО по приказу министра обороны.

Штаб национальных сил кибероперaций обладает директивными полномочиями в отношении кибероперaций, которые позволяют ему проводить ОКбО-ВМО в киберпространстве, не входящим в зону ответственности министерства обороны, без разрешения Киберкомандования США. Тем не менее, штаб национальных сил кибероперaций отвечает за обеспечение ситуативной осведомлённости Киберкомандования США во всех ОКбО-ВМО.

E-1.3.2. Поддержка оборонительных кибероперaций-меры реагирования

E-14. Национальные силы кибероперaций, состоящие из национальных оперативных групп и национальных групп обеспечения, приписанных к штабу национальных сил кибероперaций, проводят ОКбО-МР по запросам групп киберзащиты (на любом уровне), когда более агрессивный оборонительные действия выходят за пределы сетей и систем, входящих в инфраструктуру информационной сети МО или в нейтральное, или вражеское киберпространство. В зависимости от более широкого оперативного контекста ОКбО-МР могут быть доведены до уровня применения силы, приводящей к физическому повреждению или уничтожению систем противника.

Тактика операций ОКбО-МР имеет много общего с НКбО, требуя скоординированных военных приказов и тщательного рассмотрения вопросов масштаба, правил ведения боевых действий и оценки целей. По этим причинам штаб национальных сил кибероперацій должен получить подтверждение и разрешение от Киберкомандования США на проведение ОКбО-МР. На рисунке Е-3 показан процесс маршрутизации при запросе поддержки ОКбО-ВМО для киберпространства, не относящегося к МО, и поддержки ОКбО-МР.

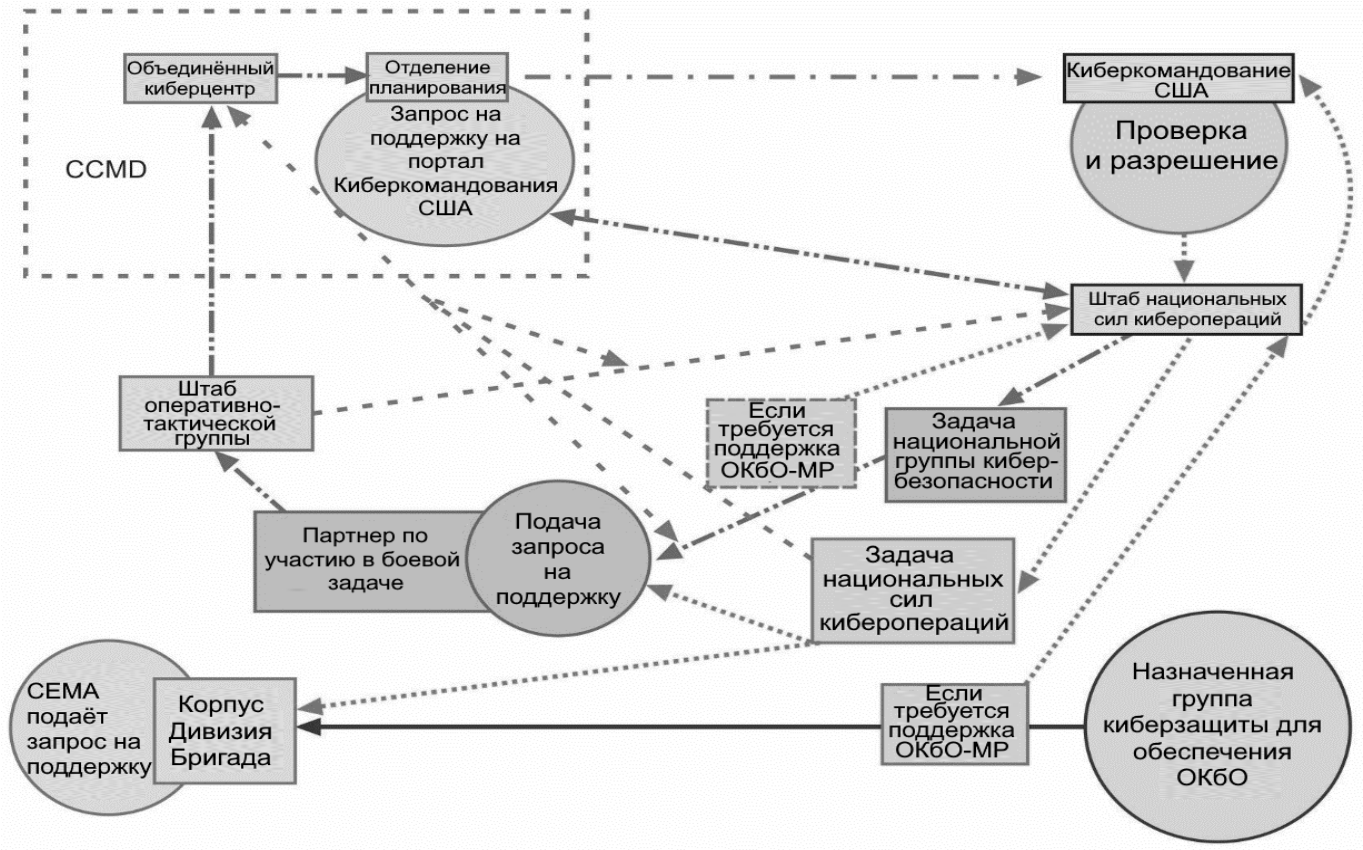


Рис. Е-3. – *Процесс маршрутизации для ОКбО-ВМО (для информационной сети, не относящейся к министерству обороны) и ОКбО-МР*

Е-1.4. Запрос на кибервоздействие (уровень корпуса и ниже)

Е-15. Запрос на кибервоздействие – это форма, используемая корпусом и нижестоящими подразделениями. для запроса на воздействие в киберпространстве. Обеспечение поддержки в ответ на запрос на кибервоздействие может осуществляться объединёнными силами кибервойск, такими как боевые группы, другими объединёнными силами или силами других видов ВС, а также силами кибероперацій, находящимися в распоряжении этих видов ВС.

E-1.4.1. Утверждение воздействий на уровнях корпуса и ниже

E-16. В процессе оперативного процесса на уровнях корпуса и ниже командир и штаб определяют желаемые воздействия в киберпространстве и через киберпространство для поддержки операций против конкретных целей. Если запрашивающий и вышестоящий уровни определяют, что имеющихся возможностей недостаточно, командир и штаб утверждают и обрабатывают запрос на кибервоздействие. Процесс маршрутизации продолжается на каждом уровне до тех пор, пока критически важные требования к информации командира не доходит до Командования наземного компонента объединённой группировки войск, где он преобразуется в запрос на поддержку и направляется в штаб объединённой оперативно-тактической группы. Процесс утверждения запроса на кибервоздействие на уровнях эшелонов корпуса и ниже проходит по следующим этапам:

1. Определить цели воздействия в киберпространстве.
2. Проверить, могут ли штатные средства обеспечить желаемый результат.
3. Утвердить цель для воздействия в киберпространстве.
4. Передать на следующий вышестоящий уровень сухопутных войск для устранения конфликтов и согласования действий.
5. Проверить, могут ли другие штатные средства обеспечить желаемый эффект, если штатные средства для воздействия на киберпространство отсутствуют.
6. Если текущие возможности удовлетворяют требованию, следует провести работы по согласованию.
7. Если имеющиеся возможности не удовлетворяют требованиям, утвердить цель для воздействия в киберпространстве.
8. Передать на утверждение на следующий вышестоящий уровень сухопутных войск до тех пор, пока запрос на кибервоздействие не войдет в объединённый процесс.
9. Согласовывать операции с поражающими воздействиями в киберпространстве (если это возможно).

Примечание:

> Командование наземного компонента объединённой группировки войск может потребовать от запрашивающего корпуса преобразовать запрос на кибервоздействие в формат запроса на поддержку перед передачей его в объединённый процесс.

E-1.4.2. Утверждение воздействий на уровнях выше корпуса

E-17. Кибероперации предоставляют средства, с помощью которых сухопутные войска могут добиваться временного или моментального превосходства в киберпространстве, создавая воздействия, поддерживающие цели командующего.

Возможности атак в киберпространстве нацелены на создание конкретных результатов и должны планироваться, готовиться и выполняться с использованием существующих процессов и процедур. Командир и штаб на всех уровнях предпринимают дополнительные меры для определения места, времени и способов использования киберпространственных воздействий.

E-18. Командиры и штабы на каждом уровне должны осуществлять координацию и взаимодействие независимо от того, будет ли кибероперация проводиться по указанию вышестоящего штаба или по запросу подчинённых подразделений. Разведка сухопутных войск, опираясь на процесс объединённой разведки (осуществляемой несколькими видами ВС), обеспечивает необходимый анализ и получение данных, на основе которых проверяются и утверждаются цели, а также определяются точки поражения. В результате процесса разведывательной подготовки поля боя и во взаимодействии с процессом объединённой разведки по подготовке оперативной обстановки личный состав разведки определяют сетевые топологии технических сетей противника, неприятеля и принимающей страны.

E-19. Цели, определяемые в процессе планирования, описываются в общем виде как физические и логические объекты в киберпространстве, состоящие из одного или нескольких сетевых устройств, используемых противником и силами неприятеля. Подразделение G-2 штаба может обозначить эти цели как именованные зоны повышенного интереса и зоны повышенного риска. Кроме того, анализ сетей своих подразделений позволит получить критическую информацию и создать основу для формирования ключевой зоны в киберпространстве. Критические сетевые узлы являются ключевой зоной киберпространства. К ним относятся физические и логические объекты в технических сетях своих подразделений, имеющие такую исключительную важность, что любое нарушение их функционирования будет иметь пагубные последствия для выполнения задач.

E-20. При определении типов кибератак на цели и защитных мер для критически важных узлов сети отделение CEMA готовит, подаёт и отслеживает запрос на кибервоздействие. Этот запрос направляется выше уровня корпуса и включается в объединённый цикл целеуказаний для последующей обработки и утверждения.

E-1.5. Подготовка формата запроса на кибервоздействие

E-21. Хотя запрашивающее подразделение может не иметь информации о топологии конкретной целевой сети, оно должно предоставить имеющуюся текущую информацию о цели. Процесс утверждения воздействия в киберпространстве может занять больше времени, чем для других средств целеуказания. Ниже приводится описание каждого из трёх разделов запроса на кибервоздействие в быстром формате «пули». Запрашивающее подразделение предоставляет всю информацию из приведённых ниже списков в вышестоящий штаб через рабочую группу CEMA или через другие установленные процессы целеуказания.

E-1.5.1. Раздел 1 – информация о запрашивающем подразделении

E-22. В разделе 1 запроса запрашивается следующая информация о подразделении:

а. Поддержка главного командования. Указать главное командование, уполномоченное утверждать и определять приоритеты запроса на кибервоздействие. Для подразделений сухопутных войск уровня армейского корпуса и ниже эта запись обычно включает географическое или функциональное боевое командование.

б. Дата. Указать дату, когда запрашивающее подразделение представило запрос на кибервоздействие в вышестоящий штаб.

в. Время отправления. Указать время, когда запрашивающее подразделение передало запрос на кибервоздействие в вышестоящий штаб.

г. Запрашивающее подразделение. Указать название запрашивающего подразделения.

д. Кем. Указать звание, фамилию и имя контактного лица запрашивающего подразделения, поставившего временную отметку и обработавшего запрос на кибервоздействие.

е. Контактное лицо. Указать звание, фамилию и имя контактного лица запрашивающего подразделения. Также указать номер телефона и e-mail.

ж. Гриф секретности. Указать общий гриф секретности документа. Обеспечить нанесение обозначений грифа ограничения доступа в каждом разделе и сопроводительной документации.

E-1.5.2. Раздел 2 – информация о поддерживаемых операциях

E-23. В разделе 2 запроса на кибервоздействие запрашивается следующая информация о поддерживаемых операциях:

а. Поддерживаемый оперативный план/план действий в чрезвычайных ситуациях/приказ. Описать ключевые детали плана, которые будут обеспечены запрашиваемой кибератакой.

б. Поддерживаемые задачи операции. Описать основную задачу (задачи) подразделения и цель, которую будет поддерживать запрашиваемое воздействие (воздействия).

в. Поддерживаемый замысла командира. Описать ключевую информацию в рамках замысла командира, которую будет поддерживать запрашиваемое воздействие (воздействие).

г. Поддерживаемый конечный замысел командира. Описать ключевую информацию в рамках конечной цели командира, которую будет поддерживать запрашиваемое воздействие(воздействия).

д. Поддерживаемая концепция операций. Описать ключевую информацию в рамках замысла операции, которую будет поддерживать запрашиваемое воздействие (воздействия).

е. Поддерживаемая цель (стратегическая, оперативная и тактическая). Описать поддерживаемую цель (цели), для достижения которой (которых) будет непосредственно использоваться запрашиваемое воздействие (воздействия).

ж. Поддерживаемая тактическая цель/задача. Описать тактические цели и задачи, которые будут прямо или косвенно решаться с помощью запрашиваемого воздействия (воздействий).

Е-1.5.3. Раздел 3 – операции с компьютерной сетью

Е-24. В разделе 3 запроса на кибервоздействие запрашиваются следующие операции с компьютерными сетями и конкретная информация:

а. Тип цели:

- указать, известны ли конкретные даты, время и/или другие вспомогательные условия;
- Указать на наличие дежурных, или если известно, триггерных событий или вспомогательных условий.

б. Приоритетность цели:

- указать «*экстренно*», если цель требует немедленных действий. Указать «*приоритет*», если цель требует определённой степени срочности;
- указать «*обычно*», если цель не требует немедленных действий или степени срочности, выходящей за рамки стандартной обработки.

в. Название цели. Указать название цели, кодифицированное в обновлённой интегрированной базе данных.

г. Местонахождение цели:

- указать местоположение цели;
- не учитывать, если запрос относится к ОКбО-ВМО.

д. Описание цели:

- привести описание цели;
- описать сетевой(ые) узел(ы), в котором(ых) конкретные действия должны поддерживать ОКбО-ВМО.

е. Необходимый результат:

- введите для ОКО такие понятия, как «отказ», «деградация», «нарушение», «уничтожение» или «манипуляция».

- указать сроки: *менее 96 часов, от 96 часов до 90 дней или более 90 дней*.

ж. Функция цели. Указать основную функцию цели (целей) и дополнительные функции, если они известны.

з. Значимость цели. Описать, почему цель (цели) важна для системы (систем) целей противника или неприятеля или представляет ценность в дополнение к своим функциям и ожиданию.

и. Подробности о цели. Описать дополнительную информацию о цели (целях), если она известна. Эта информация должна включать все необходимые данные об оборудовании, такие как:

- тип, количество пользователей;
- активность;
- дружественные субъекты в районе операций;
- окружающие/соседние/параллельные устройства.

к. Концепция кибероперaций:

- описать, каким образом запрашиваемое воздействие (воздействия) будет способствовать достижению целей командира и общей концепции операций;
- включить задачу, цель, метод и конечное состояние;
- описать план сбора разведданных и план конкретной оценки, если известен;
- дать ссылки на ключевые директивы и приказы.

л. Отчёт о выявлении целей. В соответствии с документом CJCSI 3370.01C в приложении D описывается, как запрашиваемое воздействие повлияет на целевую систему (системы). В этом описании должны быть рассмотрены следующие вопросы:

- Как повлияет на систему-мишень её нейтрализация, замедление, повреждение или деградация функций мишени (Два примера – оперативное воздействие и психологическое воздействие).
- Какова предполагаемая степень воздействия на целевую систему (системы)?
- Каково предполагаемое время восстановления работоспособности целевой системы (систем) при нейтрализации, замедлении, повреждении или деградации её функций?
- Какие краткосрочные или долгосрочные военные или политические преимущества/недостатки, которые мы ожидаем в случае уничтожения, замедления, разрушения или деградации функции цели?
- Какова ожидаемая реакция противника или неприятеля на воздействие на функцию цели?

E-2. Запрос на воздушную поддержку

E-25. Как правило, подразделения сухопутных войск уровня корпуса и ниже имеют штатные возможности для ведения РЭБ в пределах назначенного района операций. Командующий объединёнными силами, как правило, делегирует полномочия по управлению ЭМА подчинённым командирам, выполняющим задачи РЭБ в пределах назначенного им района операций. Командиры должны обеспечить интеграцию и согласование РЭБ операций в штабе в соответствии с указаниями вышестоящего командира.

E-26. Подразделениям могут потребоваться средства РЭБ, которых нет в наличии, или дополнительные средства РЭБ для выполнения требований, определенных в ходе цикла целеуказания, или процесса разведки целей. Командир и офицер по кибервойне и РЭБ запрашивают усиление через вышестоящий, соседний или нижестоящий штаб для удовлетворения своих потребностей. В этом разделе описаны процедуры запроса на воздушную поддержку в киберпространстве и ЭМА. В нём также рассматривается использование пяти строчного запроса на ЭМА для немедленной воздушной ЭМА.

E-2.1. Обеспечение воздушной электромагнитной атаки

E-27. В межвидовой оперативной среде подразделения сухопутных войск могут инициировать запрос на проведение воздушной кибератаки, ЭМА или ЭМП. Целеуказание с помощью средств воздушного базирования в киберпространстве и ЭМА может осуществляться как по плановым, так и по внезапно возникшим динамическим целям. В этом случае подразделение подаёт заявку по форме DD 1972 Запрос на проведение совместного тактического авиаудара (*англ. Joint Tactical Air Strike Request*, *JTASR*), к которой прилагается запрос на воздушную кибератаку, ЭМА или ЭМП. Каждый из этих запросов имеет уникальные информационные требования и свой маршрут движения. Группа огневого обеспечения запрашивающего подразделения добавляет цель в список своих целей. Цель также добавляется в объединённый интегрированный список приоритетных целей в штабе объединённой оперативно-тактической группы и передаётся Командованию воздушным компонентом объединённой группировки войск с присвоенным ей номером запроса на совместный тактический авиаудар DD Form 1972 (см. ATP 3-09.32). После того как Командованию воздушного компонента объединённой группировки войск утверждает запрос на совместный тактический авиаудар он передаётся в центр управления воздушными операциями для выполнения атаки.

E-28. Ниже в таблице E-1 приведён пример формы запроса, используемого для подачи заявки на воздушную электромагнитную атаку или для электромагнитной поддержки и сопровождающую форму запроса на совместный тактический авиаудар DD 1972.

Nonkinetic Effect Discipline (Space, Airborne Electro-magnetic Attack, Information Operations, or Cyber)	Applicable phase or Find, Fix Track, Target, Engage, Assess	Nonkinetic Effect	Risk			Aproval Timeline (idea to Approved Execution Order)	Employ ment Timeline (initial Access to Effect Ready to Fire)	Authority Level (for use in Area of Responsibility	Execution Authority (Tactical Employ ment)
			Technical Gain/ Loss	Intel Gain/ Loss	Commander's Acceptable Level or Risk				
---	---	---	---	---	---	---	---	---	---
---	---	---	---	---	---	---	---	---	---
Airborne EA	Target	Jam	Gain	Gain	Acceptable	180 mins	180 mins	Local	Local
---	---	---	---	---	---	---	---	---	---
---	---	---	---	---	---	---	---	---	---

Рис. E-3. – *Средства запроса на воздушную кибератаку, ЭМА или ЭМП*

На рис. E-4 ниже показана форма запроса на совместный тактический авиаудар DD 1972.

E-29. Центр воздушных операций отвечает за контроль применения средств ЭМА в соответствии с Планом воздушных операций (*англ. Air Tasking Order, ATO*). Воздушные средства ЭМА предоставляют своим войскам возможности для снижения угроз и дают командирам дополнительные возможности для целеуказаний. Воздушные средства ЭМА могут иметь различные конфигураций и возможности для нейтрализации объектов в наземной, морской и воздушной зонах. Список доступных возможностей и конфигураций бортовых средств ЭМА см. в Наставлении ATP 3-60.1. Центр управления воздушными операциями является основным контактным лицом для определения возможностей целеуказания авиацией.

JOINT TACTICAL AIR STRIKE REQUEST | See Joint Pub 3-09.3 for preparation instructions.

SECTION I - MISSION REQUEST

DATE

1. UNIT CALLED: Chieftan	THIS IS: Gator 01	REQUEST NUMBER: IA9501-A	SENT — TIME: 1615 — BY: Maj Smith
2. PREPLANNED: A PRECEDENCE 4 B PRIORITY II; IMMEDIATE: C PRIORITY			RECEIVED — TIME: 1615 — BY: SrA Ford

3. TARGET IS/NUMBER OF

A PERS IN OPEN 20-30	B PERS DUG IN	C WPNS/MG/RR/AT	D MORTARS, ARTY
E AAA ADA	F RKTS MISSILE	G ARMOR 3xBTR in line	H VEHICLES 4 Stationary
I BLDGS 2	J BRIDGES	K PILLBOX, BUNKERS	L SUPPLIES, EQUIP
M CENTER (CP, COM)	N AREA	O ROUTE	P MOVING N E S W
Q REMARKS			

4. TARGET LOCATION IS — CHECKED — BY: SSgt Intel

A 11SUG8005 (COORDINATES)	B (COORDINATES)	C (COORDINATES)	D (COORDINATES)
E TGT ELEV 10	F SHEET NO. 2875 II	G SERIES V795S	H CHART NO.

5. TARGET TIME/DATE

A ASAP	B NLT 1600	C AT	D TO

6. DESIRED ORD/RESULTS — A ORDNANCE LGB/Guns

B DESTROY	C NEUTRALIZE X	D HARASS/INTERDICT

7. FINAL CONTROL

A FAC/RABFAC II	B CALL SIGN GATOR 20	C FREQ Orange 17	
D CONT PT JACKS			

8. REMARKS

SECTION II - COORDINATION

9. NSFS: 4XTLAM FLA 1 SS	10. ARTY		11. AIO/G-2/G-3
12. REQUEST: [X] APPROVED [ ] DISAPPROVED	13. BY: Maj Hughes	14. REASON FOR DISAPPROVAL	
15. RESTRICTIVE FIRE/AIR PLAN: A IS NOT IN EFFECT B NUMBER		16. IS IN EFFECT: A (FROM TIME) B (TO TIME)	
17. LOCATION: A (FROM COORDINATES) B (TO COORDINATES)		18. WIDTH (METERS)	19. ALTITUDE/VERTEX: A (MAXIMUM/VERTEX) B (MINIMUM)

SECTION III - MISSION DATA

20. MISSION NUMBER: 3021/3022	21. CALL SIGN: Razor 51/52 Venom 16-17	22. NO. AND TYPE AIRCRAFT: (2) AV-8B (2) AH-1Z	23. ORDNANCE: SCL 1/3
24. EST/ACT TAKEOFF: 1424	25. EST TOT: 1438	26. CONT PT (COORDS): Breaker	27. INITIAL CONTACT
28. FAC/FAC(A)/TAC(A) CALL SIGN/ FREQ	29. AIRSPACE COORDINATION AREA	30. TGT DESCRIPTION	*31. TGT COORD/ELEV

32. BATTLE DAMAGE ASSESSMENT (BDA) REPORT (USMTF INFLTREP)

LINE 1/CALL SIGN Razor 51/52	LINE 4/LOCATION 18SUG8005
LINE 2/MSN NUMBER 3021/3022	LINE 5/TOT 1454
LINE 3/REQ NUMBER 1A9501-A	LINE 6/RESULTS Neutralize/Destory
	REMARKS

*TRANSMIT AS APPROPRIATE

DD FORM 1972, MAY 2019 PREVIOUS EDITION MAY BE USED. Adobe Professional 7.0

Рис. E-4. – *Форма запроса на проведение совместного тактического авиаудара*

E-2.2. Запрос на электромагнитную атаку

E-30. Динамичное целеуказание – это обнаружение целей, которые были идентифицированы слишком поздно или не были своевременно отобраны для воздействия, чтобы быть включёнными в число целей для целенаправленного целеуказания. Динамичное целеуказание обычно используется при планировании текущих операций, поскольку характер и сроки, связанные с текущими операциями, обычно требуют более оперативного реагирования, чем при плановом целеуказании (JP 3-60). Динамичное целеуказание используется для целей, которые могут внезапно появиться, включая незапланированные и непредвиденные цели. Если для целеуказания требуется немедленная ЭМА, например, когда наземному манёвренному подразделению необходимо заглушить средства связи противника перед вступлением в бой, подразделение может запросить поддержку с помощью запроса на ЭМА. Подразделения также подают запрос на оказание поддержки ЭМА, когда задача не может быть спланирована заранее в связи с тем, что некоторые операции носят срочный характер. В запросе на ЭМА указывается подготовка экипажа, обеспечивающего ЭМА (см. ATP 3-09.32). Штаб оперативно-тактической группы, Командование наземным компонентом объединённых сил, Командование воздушным компонентом объединённых сил и Центр воздушных операций должны совместно планировать проведение авиационных ЭМА до начала операции. Такое планирование и взаимодействие дают Командованию воздушным компонентом объединённых сил необходимое время для определения и подготовки эскадрильи РЭБ, которая будет находиться в готовности на протяжении всей операции. На рис. E-5 представлен образец запроса на ЭМА.

Electromagnetic Attack Request

Do not transmit line numbers. Units of measure are standard unless briefed.

Lines 1,2 and 4 are mandatory readback (*). Jam Control Authority (JTAC) may request additional readback.

JCA; "Foxfire 06 (aircraft call sign). this is Forward 09 (JTAC call sign);"

1. Target/ or Effect Description:" Disrupt ;"

   a. Rapper or Target Name radio transmitter
   b. Frequency (if known) 107.1 MHZ
   c. Modulation FM

2. Target Location; "N 46° 47 33.[illegible]8" / W 120° 947.2322" (latitude and longitude or MGRS);"

3. Remarks:" No current remarks or special instructions ;"

EXAMPLE

Legend

JTAC	joint terminal attack controller	N	North
MGRS	military grid reference system	W	West

Рис. E-5 – *Запрос на электромагнитную атаку*

Примечание:

> Запрос на ЭМА является общим форматом запроса на воздушную ЭМА. При запросе немедленной ЭМА Центр управления некинетическими операциями может потребовать использование особой процедуры запроса для немедленной поддержки ЭМА. Штаб оперативно-тактической группы и его подчинённые подразделения должны ознакомиться с формализованным форматом запроса на ЭМА, установленным Центром некинетических операций или боевым командованием, прежде чем запрашивать ЭМА. Кроме того, тактическая группа управления воздушным пространством или диспетчер объединённого пункта управления атакой могут быть привлечены для управления ЭМА ввиду уникальности и необходимости наличия особых тактических знаний и опыта, требуемых для данной операции.

Приложение F. Действия по улучшению приёмов и возможностей РЭБ

В данном приложении описываются общие процедуры улучшения приёмов и возможностей РЭБ, разделённые на четыре этапа. Будут описаны три основные типа улучшения приёмов и возможностей РЭБ и связанные с этим действия. Также обсуждается, как координируют процедуры улучшения приёмов и возможностей РЭБ.

F-1. Цели улучшения приёмов и возможностей

F-1. Целью улучшения приёмов и возможностей РЭБ является поддержание или повышение эффективности оборудования РЭБ и программного обеспечения систем целеуказания. Улучшение приёмов и возможностей РЭБ включает изменения в системах самообороны, наступательного вооружения и сбора разведданных. Каждое подразделение сухопутных войск ответственно за улучшение приёмов и возможностей систем РЭБ и целеуказания с использованием программы поддержки улучшения приёмов и возможностей РЭБ.

F-2. Подразделения всех видов вооружённых сил, выявившие изменения в сигнатурах угроз, докладывают об этих изменениях через вышестоящий штаб боевому командованию зоны ответственности, в которой они проводят операции. Центр сбора разведывательной информации вида вооружённых сил [Национальный центр наземной разведки сухопутных войск]; и управление поддержки оборудования вида вооружённых сил осуществляют поддержку для систем РЭБ и программного обеспечения целеуказания.

F-3. Боевое командование обеспечивает распространение выявленных изменений в сигнатурах угроз по всем подразделениям и видам вооружённых сил, действующих в зоне ответственности, следуя правилам и процедурам улучшения приёмов и возможностей РЭБ, разработанных объединённым штабом. Центр сбора разведданных собирает данные для обработки и анализа, чтобы распознавать и понимать изменения сигнатур. Управление поддержки оборудования вида вооружённых сил подтверждает запрос и оценивает совместимость и воздействие на систему оборудования РЭБ и программного обеспечения целеуказания.

Примечание.

> Улучшение приёмов и возможностей РЭБ требуется только для программного обеспечения РЭБ и целеуказания, нуждающегося в обновлении сигнатур угроз. В этих системах улучшение приёмов и возможностей РЭБ производится при изменении сигнатур угроз. РЭБ с динамичными возможностями не нуждаются в загрузке сигнатур угроз и, соответственно, не требуют улучшения своих приёмов и возможностей.

F-2. Категории улучшения приёмов и возможностей РЭБ

F-4. В улучшении приёмов и возможностей РЭБ входит несколько типов изменений. Эти изменения делят на три основные категории. Это:

1. **Тактические**. Включают изменения в процедурах, оборудовании, настройках или данных планирования боевой задачи систем РЭБ. Эти изменения обычно проводятся на сервисном уровне и выполняются подразделениями с задействованием штатного личного состава и оборудования.
2. **Программные.** Включают перепрограммирование программного обеспечения РЭБ и целеуказания. Эти изменения требуют от поставщиков программного обеспечения менять запрограммированные таблицы поиска, библиотеки угроз или процедуры сортировки сигналов.
3. **Аппаратные**. Аппаратные изменения или сложная модификация могут быть необходимы из-за тактических и программных изменений, необходимых для устранения недостатков. Эти изменения нужны при сложных тактических и программных изменениях, диктующих модификацию или модернизацию оборудования.

F-2.1. Действия по улучшению приёмов и возможностей РЗБ

F-5. В критических ситуации или при ЭМА противника улучшение приёмов и возможностей РЭБ обеспечивает командирам возможность своевременно реагировать на изменения систем угроз и корректировать системы РЭБ для целеуказания. С помощью улучшение приёмов и возможностей РЭБ командиры также могут корректировать РЭБ и целеуказание, адаптировать их к особым требованиям задачи. Улучшение приёмов и возможностей РЭБ достигает этой цели используя три типа изменений по отдельности или вместе. Эти действия:

1. **Корректировка угрозы**. Любые изменения в рабочей или электромагнитной сигнатуре системы угроз. Суть улучшения приёмов и возможностей РЭБ в реагировании на изменения угроз, влияющих на боевую эффективность РЭБ и целеуказания.
2. **Корректировка географических особенностей**. Улучшение приёмов и возможностей РЭБ и систем программного обеспечения целеуказания для операций в конкретном районе или регионе. Географическая адаптация оптимизирует использование системной памяти, сокращает время обработки и уменьшает отображение ошибок.
3. **Корректировка задачи**. Улучшение приёмов и возможностей РЭБ и систем программного обеспечения целеуказания для работы несущей платформы – аппаратной части компьютера или терминала. Корректировка задачи может улучшить реакцию системы на приоритетные угрозы, определённые несущей платформой.

F-2.2. Действия по улучшению приёмов и возможностей РЭБ

F-6. Процесс улучшения приёмов и возможностей РЭБ состоит из четырёх этапов. Подразделения могут дополнительно усовершенствовать последние три этапа процесса улучшения приёмов и возможностей РЭБ для решения специфических задач. Четыре этапа процесса улучшение приёмов и возможностей РЭБ:

1. Определение угрозы.
2. Определение ответа.
3. Разработка корректировок.
4. Применение корректировок.

F-2.2.1. Определение угрозы

F-7. При определении проблемы или угрозы подразделения создают и ведут детальное описание оперативной электромагнитной обстановки, т.е. системы угроз и действия. Документируются информационные требования для постоянного ведения точного описания оперативной электромагнитной обстановки. Информационные требования важны, поскольку оборудование РЭБ и целеуказания запрограммировано для идентификации и реагирования на конкретную угрозу или данные сигнатуры цели. Точное описание оперативной электромагнитной обстановки требует соединения известных данных сигнатуры угрозы с собранными, анализированными и верифицированными, в три этапа:

1. **Сбор данных.** Сбор данных сигнатур угроз представляет собой сбор данных о параметрах системы угроз и является обязанностью G-2 или S-2. Сбор данных сигнатур может быть вопросом обычного сбора разведданных о целевых системах. Могут проводиться другие сборы данных при срочных запросах разведки. Независимо от цели сбора данные сигнатур посылают по каналам разведки в Национальный центр наземной разведки и каналам управления поддержки оборудования видов ВС РЭБ и программного обеспечения целеуказания для анализа и предупреждения.
2. **Выявление изменений.** Управление поддержки оборудования видов ВС РЭБ и программного обеспечения целеуказания анализирует собранные данные на совместимость. Несовместимые данные помечаются для дальнейшего анализа и оценки воздействия на систему. Национальный центр наземной разведки обрабатывает и анализирует собранные данные для выявления изменений сигнатур угроз в оперативной электромагнитной обстановке. Выявленные изменения дополнительно анализируются.
3. **Проверка изменений.** После того, как выявленное изменение сигнатуры соотносится с системой угроз и анализируется принимается решение о том, фактическое ли это изменения параметров системы или ошибка. На этом этапе

очень важна информация о технических данных системы угроз и об её тактическом использовании. Технический анализ и проверку изменений сигнатур угроз обычно проводит Национальный центр наземной разведки или РУМО. На объединённом уровне боевое командование должно оперативно представить идентификацию, техническое описание и анализ сообщений о подтверждении изменения угрозы в подразделения командований и центры перепрограммирования (Группа анализа улучшения приёмов и возможностей РЭБ для сухопутных войск) (*англ. Army Reprogramming Analysis Team for the Army, ARATA*).

F-2.2.2. Определение ответа

F-8. Центры улучшения приёмов и возможностей видов ВС оценивают проверенную информацию об изменениях угроз на предмет её влияния на оборудование РЭБ и программное обеспечение целеуказания союзников. Принимается решение о начале улучшения приёмов и возможностей. Оборудование может не обеспечить распознавание и предупреждения или противодействие в ответ на изменение угрозы. В этом случае центр улучшения приёмов и возможностей видов ВС определяет, требуется ли исправление недостатка тактическими, программными или аппаратными изменениями.

F-9. Управление поддержки оборудования видов ВС сообщением о воздействии на систему информирует боевое командование и подразделения командований об оперативном воздействии изменения угрозы на работу оборудования РЭБ и программного обеспечения целеуказания. Боевое командование пересылает сообщение о результатах воздействия на систему, через штаб объединённой оперативно-тактической группы подчинённым подразделениям. Сообщение о воздействии на систему часто содержит рекомендации как правильно реагировать на каждое выявленное изменение угрозы; однако каждое подразделение в конечном итоге ответственно за определение верных мер реагирования.

F-2.2.3. Разработка корректировок

F-10. Подразделение разрабатывает тактические, программные или аппаратные изменения, чтобы сохранить или улучшить работу оборудования и боевую эффективность. Разрабатывая корректировку, в первую очередь рассматривают использование тактических методов избежания угрозы. Тактические изменения рассматриваются первыми, т.к. изменения программного и аппаратного обеспечения требуют времени, которого может не быть. Подразделения решают применить тактических изменений в качестве первой меры, чтобы продолжать работу, пока управление поддержки оборудования видов ВС не подготовит изменения программ и аппаратной части.

F-11. Сочетание корректировок (тактических и программных) часто обеспечивает скорое и долговременное устранение недостатков оборудования. Изменения программ и аппаратного обеспечения требуют содействия управления поддержки оборудования видов ВС РЭБ и программного обеспечения целеуказания. Управление поддержки оборудования видов ВС помогает улучшению приёмов и возможностей, проверяя боевую эффективность оборудования моделированием и симуляцией, стендовыми испытаниями или испытаниями на полигонах, имитирующих реальные условия.

F-2.2.4. Проведение корректировки

F-12. Применение корректировок гарантирует, что подразделения сохранят или повысят боевую эффективность с помощью тактических, программных или аппаратных изменений. Боевые командования заботятся, чтобы подчинённые подразделения включали тактические изменения в брифинг перед началом выполнения боевой задачи. Управление поддержки оборудования видов ВС работает с другими службами над применением программных и аппаратных корректировок носителя оборудования РЭБ и программного обеспечения целеуказания.

Приложение G. Подготовка

Подготовка призвана подготовить военнослужащих к выполнению задач по определению оперативной обстановки, предотвращению конфликтов и ведению крупномасштабных боевых действий против равных угроз (противника). Сухопутные войска должны быть организованы, обучены и оснащены для решения глобальных задач. Сухопутные войска планируют и проходят жёсткую, максимально приближённую к боевой обстановке подготовку, включающую непрерывную подготовку подразделений в местах дислокации, в центрах боевой подготовки и во время развёртывания в ПВД (за границей).

G-1. Обзор программы подготовки

G-1. Командиры обеспечивают подготовку военнослужащих и подразделений в сложных и максимально приближённых к боевой обстановке условиях, которые в точности повторяют условия оперативной обстановки и при этом учитывают принципы подготовки сухопутных войск:

- Тренируйся так, как будешь сражаться.
- Тренируйся согласно боевому уставу.
- Тренируйся, чтобы превозмогать.
- Тренируйся для поддержания силы и навыков.

G-2. Индивидуальная подготовка затрагивает три части обучения: профессиональную, оперативную и самостоятельную подготовку. Основная подготовка включает начальную и длительную индивидуальную подготовку, согласованную с индивидуальным планом развития каждого специалиста по киберпространству и РЭБ. Кроме того, военнослужащие проходят индивидуальную и групповую подготовку в ходе боевой подготовки, чтобы быть в курсе постоянно развивающихся методов, технологий и тенденций, происходящих в киберпространстве и ЭМС.

G-1.1. Профессиональная подготовка

G-3. Офицеры, уорент-офицеры и военнослужащие по контракту, желающие получить профессию в области кибероперaций и РЭБ, проходят интенсивную основную подготовку в учебных заведениях перед отправкой в своё первое подразделение. Основная подготовка продолжается на протяжении всей службы этих военнослужащих. Общетехнический колледж подготовки специалистов по кибероперациям (*англ. Cyber Common Technical College*) и Колледж подготовки специалистов радиоэлектронной борьбы (*англ. Electronic Warfare College*) находятся

в Головном центре кибероперaций сухопутных войск США. Эти учебные заведения обеспечивают профессиональную подготовку действующих военнослужащих сухопутных войск, резерва сухопутных войск и Национальной гвардии в области киберпространства и РЭБ с уровнем понимания кибероперaций, радиоэлектронной борьбы и связанной с ними доктрины. Специалисты по кибероперациям учатся сочетать такие операции сухопутных войск, как: разведку и тактику малых подразделений с основополагающими навыками в наступательных и оборонительных задачах в киберпространстве. Специалисты по РЭБ изучают операции сухопутных войск и тактику малых подразделений с основополагающими навыками в задачах ЭМА, ЭМП и ЭМЗ. Занятия, проводимые в рамках профессиональной учебной подготовки, обеспечивают повышение квалификации специалистов по кибероперациям и РЭБ в соответствующих областях профессиональной деятельности и включают такие учебные мероприятия, как:

а. Обучение в аудитории (теория), состоящее из занятий с гражданскими и военными преподавателями.

б. Учебные курсы.

в. Завершающий этап обучения.

G-1.2. Подготовка в пункте постоянной дислокации.

G-4. Офицер по кибервойне и РЭБ отвечает за координацию работы с каждым подчинённым из личного состава по разработке и реализации годового плана обучения в ППД. Он согласовывает план подготовки с перечнем основных задач подразделения, состоящим из основных индивидуальных и групповых задач, которые должны выполнять военнослужащие. Офицер по кибервойне и РЭБ согласует подготовку в ППД с тем, как подразделение будет действовать во время аттестации в центре боевой подготовки. План подготовки включает тематику, обеспечивающую профессионализм специалистов подразделения по кибероперациям и РЭБ в соответствующих областях профессиональной деятельности, и может состоять из таких учебных мероприятий, как:

а. Обучение в аудитории (теория) и инструктаж в мобильной учебной группе (*англ. mobile training team, MTT*).

б. Учебные курсы.

в. Полевые учения.

G-5. Как минимум, обучение (теория) военнослужащих, проводящих кибероперации, должно включать инструктаж, связанный с оборонительными кибероперациями-внутренними мероприятиями по обороне, в том числе:

- защита операционных систем Windows;
- компьютерная криминалистика;

- реагирование на инциденты;
- выявление и полный анализ вторжений;
- хакерские приёмы;
- эксплойты и предотвращение инцидентов;
- тестирование на проникновение в сеть;
- этичный взлом;
- аудит сетей, периметров и информационно-технологических систем.

G-6. Как минимум, обучение (теория) военнослужащих по РЭБ должна включать.

- общие математические и алгебраические понятия;
- основные принципы и расчёты радиочастот;
- теория антенн;
- основы пеленгования;
- принципы обнаружения и идентификации частот, представляющих интерес;
- составление текущих оценок РЭБ.
- совместный доклад и процедуры доклада об электромагнитных помехах.
- цифровая обработка сигналов;
- знакомство с инструментами планирования и управления РЭБ и планирование сценариев;
- основы манёвра.

G-7. Подготовка и инструктажи, проводимые мобильными учебными группами, позволяют специалистам по кибероперациям и РЭБ взаимодействовать с военными и коммерческими экспертами. Мобильные учебные группы позволяют получить дополнительные знания и практические навыки, а также создать и поддерживать профессиональные связи для повышения эффективности работы на месте службы. Групповая подготовка даёт возможность специалистам по кибероперациям и РЭБ отрабатывать общевойсковые действия, которые завершают подготовку в ППД и помогают обеспечить боеготовность и живучесть подразделений. Групповая подготовка может включать такие имитационные действия, как подавление связи, для обеспечения реалистичности, которая подчёркивает важность основных, запасных, резервных и чрезвычайных планов. Подчинённые подразделения могут использовать информацию, полученную в ходе учебных занятий, проводя анализ их результатов для разработки основных, запасных, резервных и чрезвычайных планов.

G-2. Центры боевой подготовки

G-8. В настоящее время в сухопутных войсках имеется три центра боевой подготовки: Национальный учебный центр в Форт Ирвине, штат Калифорния; Объединённый учебный центр отработки вопросов боевой готовности в Форт Полке, штат Луизиана; и Объединённый многонациональный центр отработки вопросов боевой готовности в Хоэнфельсе, Германия, и Программа подготовки по управлению выполнением боевой задачи *(англ. Mission Command Training Program, MCTP*).

Обучение в центре боевой подготовки имитирует реальные события, создавая реальные сценарии, с которыми могут столкнуться подразделения во время развёртывания. Оперативные силы, подчиняющиеся центрам боевой подготовки, создают для подразделений такие реальные сценарии. Центры боевой подготовки оценивают боевую готовность готовящихся на ротацию учебных подразделений, определяемую превентивными и ответными мерами, принимаемыми для предотвращения или устранения препятствий, возникающих в ходе выполнения реальных сценариев.

G-9. В сценарии решительных действий кибероперации и РЭБ играют важную роль в получении и сохранении тактических преимуществ, необходимых для благоприятного разрешения конфликта. Центры боевой подготовки постоянно следят за способностью учебных подразделений действовать в условиях оперативной обстановки, включающих моделирование конфликтов и соревнований.

Центры боевой подготовки помогают командирам оценивать общую боеготовность подразделений, умение выполнять задачи, связанные с выполнением списка основных задач, а также те критические и основные задачи, которые требуют дополнительной подготовки. После этого командиры могут контролировать внесение необходимых изменений в процесс обучения в ППД для повышения квалификации военнослужащих.

СЛОВАРЬ

В данном глоссарии перечислены аббревиатуры и термины с сухопутными войсками, межвидовыми или объединёнными определениями, а также другие отдельные термины. В скобках после определения приводится публикация разработчиков термина.

Раздел I. Акронимы и аббревиатуры

Сокращение	Полное словосочетание и сокращаемое понятие	
	на английском языке	на русском языке
AOR	area of responsibility	зона ответственности
ARCYBER	United States Army Cyber Command	Киберкомандование сухопутных войск
CCMD	combatant command	боевое командование
CEMA	cyberspace electromagnetic activities	кибер-электромагнитная деятельность
CERF	cyber effects request format	форма запроса для кибервоздействия
CEWO	cyber electromagnetic warfare officer	офицер по кибервойне и РЭБ
CNMF	cyber national mission force	Национальные силы кибероперaций
CNMF-HQ	Cyber National Mission Force-Headquarters	штаб Национальных сил кибероперaций
COA	course of action	вариант действий
CPT	cyber protection team	группа киберзащиты
D3A	decide, detect, deliver, and assess	решать, обнаруживать, поражать и оценивать
DCO	defensive cyberspace operations	оборонительные кибероперации
DCO-IDM	defensive cyberspace operations-internal defensive measures	оборонительные кибероперации-внутригосударственные мероприятия по обороне
DCO-RA	defensive cyberspace operations-response actions	оборонительные кибероперации-меры реагирования
DODIN	Department of Defense information network	информационная сеть министерства обороны
DODIN-A	Department of Defense information network-Army	информационная сеть министерства обороны – сухопутные войска
EA	electromagnetic attack	электромагнитная атака
EMI	electromagnetic interference	электромагнитные помехи
EMOE	electromagnetic operational environment	электромагнитная оперативная обстановка
EMS	electromagnetic spectrum	электромагнитный спектр

Сокращение	Полное словосочетание и сокращаемое понятие	
	на английском языке	на русском языке
EMSO	electromagnetic spectrum operations	операции в электромагнитном спектре
EP	electromagnetic protection	электромагнитная защита
ES	electromagnetic support	электромагнитная поддержка
EW	electromagnetic warfare	радиоэлектронная борьба
I2CEWS	intelligence, information, cyber, electromagnetic warfare and space	разведка, информация, киберпротиводействие, РЭБ и космос
IO	information operations	информационные операции
IP	Internet Protocol	Интернет-протокол
IPB	intelligence preparation of the battlefield	разведывательная подготовка района боевых действий
JEMSO	joint electromagnetic spectrum operations	объединённые операции в электромагнитном спектре
JEMSOC	joint electromagnetic spectrum operations cell	группа управления объединёнными операциями в электромагнитном спектре
JFHQ-C	Joint Force Headquarters-Cyber	Киберштаб объединённых сил
JFHQ-DODIN	Joint Force Headquarters-Department of Defense Information Network	Штаб объединённых сил – информационная сеть министерства обороны
JTF	joint task force	объединённая оперативно-тактическая группа
NCO	noncommissioned officer	сержантский состав (сержант)
NETCOM	United States Army Network Enterprise Technology Command	Командование сетевых технологий сухопутных войск
OCO	offensive cyberspace operations	наступательная кибероперация
OE	operational environment	оперативная обстановка
OPLAN	operation plan	план операции
OPORD	operation order	боевой приказ
OPSEC	operations security	безопасность операций
RFS	request for support	запрос на поддержку
SIGINT	signals intelligence	радио и радиотехническая разведка
TSS	targeting sensing software	программное обеспечение для систем целеуказаний
USC	United States Code	Кодекс (Свод законов) США
USCYBERCOM	United States Cyber Command	Киберкомандование США

Раздел II. Термины

Термин	Определение
безопасность операций	Способность к выявлению и управлению критически важной информации, признаков действий своих войск в ходе военных операций и принятия мер противодействия для снижения риска использования противником уязвимостей. Сокращённо: **БЗПО** (англ. OPSEC). (JP 3-13,3)
боевая устойчивость / боевое обеспечение	Взаимосвязанные задачи и системы, обеспечивающие поддержку и обслуживание для обеспечения свободы действий, расширения оперативного охвата и повышения выносливости. (ADP 3-0)
боевое обеспечение	Группа задач и систем, объединённых общей целью, которую командиры используют для выполнения боевых и учебных задач. (ADP 3-0)
боевые возможности	Совокупность разрушительных, созидательных и информационных возможностей, которые может использовать воинская часть или подразделение в данное время. (ADP 3-0)
важная цель	Цель противника, которая необходима командиру противника для успешного выполнения задачи. (JP 3-60)
война направленной энергией	Военные действия с применением вооружения, устройств и средств противодействия направленной энергии. Сокращённо: **ВНЭ** (*англ. DEW*). (JP 3-85)
выполнение	Распоряжение на приведение плана в действие путём применения боевых возможностей для выполнения поставленной задачи и изменения операций в зависимости от изменения обстановки. (ADP 5-0)
гибридная угроза	Гибридная угроза – это разнообразное и динамичное сочетание регулярных сил, нерегулярных сил, террористов или криминальных элементов, действующих согласованно для достижения взаимовыгодных результатов. (ADP 3-0)
динамическое целеуказание	Целеуказание, при котором сопровождаются цели, идентифицированные слишком поздно или не выбранные для своевременного включения в плановое целеуказание. (JP 3-60)
дипольный отражатель	Отражатели радиолокационных сигналов, представляющие собой тонкие узкие металлические полоски различной длины и частотной характеристики, которые используются для отражения эхо-сигналов с целью создания помех. (JP 3-85)

Термин	Определение
защита киберпространства	Действия, предпринимаемые в защищённом киберпространстве для борьбы с конкретными угрозами, которые нарушили или угрожают нарушить систему безопасности киберпространства. Включают действия по обнаружению, определению характеристик, противодействию и ослаблению угроз, включая вредоносное программное обеспечение или несанкционированные действия пользователей, а также по восстановлению системы до безопасной конфигурации. (JP 3-12)
информационная сеть министерства обороны	Совокупность информационных возможностей и соответствующих процессов для сбора, обработки, хранения, распространения и управления информацией по запросу военнослужащих, политических деятелей и вспомогательного персонала, как взаимосвязанных, так и самостоятельных. Сокращённо: **ИСМО** (*англ. DODIN*). (JP 6-0)
информационная сеть министерства обороны – сухопутные войска	Управляемый сухопутными войсками анклав информационной сети МО, включающий все информационные возможности СВ по сбору, обработке, хранению, отображению, распространению и защите информации по всему миру. Сокращённо: **ИСМО-СВ** (*англ. DODIN-A*). (ATP 6-02.71)
информационные операции	Комплексное использование в ходе военных операций информационных возможностей в сочетании с другими направлениями деятельности для оказания воздействия, срыва, подрыва или нарушения процесса принятия решений неприятелем и потенциальным неприятелем при одновременной защите собственных возможностей. Сокращённо: **ИО** (*англ. IO*). (JP 3-0)
использование киберпространства	Действия, предпринимаемые в киберпространстве для получения разведывательных сведений, выполнения манёвра, сбора информации или других действий, необходимых для подготовки к будущим военным операциям. (JP 3-12)
кибератака	Действия, предпринимаемые в киберпространстве и создающие заметные поражающие факторы (ухудшение, нарушение функций или уничтожение) в киберпространстве, или манипуляции, приводящие к отказу, который проявляется в физическом домене, и рассматриваются как форма огневого поражения. (JP 3-12)
кибербезопасность	Действия, предпринимаемые в защищённом киберпространстве для предотвращения несанкционированного доступа, использования или повреждения компьютеров, электронных коммуникационных систем и других информационных технологий, включая платформенные информационные технологии, а также содержащейся в них информации, для обеспечения её доступности, целостности, аутентификации, конфиденциальности и безотказности. (JP 3-12)

Термин	Определение
кибероперации (операции в киберпространстве)	Применение средств воздействия на киберпространство (кибервозможностей), при котором основной целью является достижение целей в киберпространстве или с его помощью. Сокращённое наименование – **КбО** (*англ. CO*) CO. (JP 3-0)
киберпространство	Глобальная сфера в информационной среде, состоящая из взаимосвязанных сетей технологий инфраструктуры информации и находящихся в нем данных, включая Интернет, телефонные сети, компьютерные системы и встроенные процессоры и контроллеры (JP 3-12)
кибер-электромагнитная деятельность	Процесс планирования, внедрения и согласования киберопераций и РЭБ для поддержки совместных наземных операций. Сокращённо: **СЕМА.** (ADP 3-0)
конкретная задача	Задача, специально поставленная подразделению вышестоящим штабом. (FM 6-0)
косвенная задача	Задача, которая должна быть выполнена для реализации конкретного задания или задачи, но не указанная в приказе вышестоящего штаба. (FM 6-0)
меры противодействия	Форма военной науки, которая посредством применения устройств и/или методов ставит своей целью снижение оперативной эффективности действий противника
Методика выработки и принятия комплексных решений сухопутных войск	Методика применения критического и творческого мышления для понимания, визуализации и описания проблем и подходов к их решению. Сокращённо: **МВПКР** (*англ. Army design methodology*). (ADP 5-0)
назначенный район интересов	Геопространственная область, узел или канал системы, по которым может быть собрана информация, удовлетворяющая определенному информационному требованию. Сокращённо: **НРИ** (*англ. NAI*). (JP 2-01.3)
направленная энергия	Универсальный термин, охватывающий технологии, связанные с получением пучка концентрированной электромагнитной энергии или атомных или субатомных частиц. Сокращённо: **НЭ** (*англ. DE*). (JP 3-85)
наступательные кибероперации	Задачи, направленные на проецирование силы в киберпространстве и через него. Сокращённо: **НКО** (*англ. OCO*). (JP 3-12).
неприятель	Сторона, признанная потенциально враждебной по отношению к своим войскам, против которой может быть предусмотрено применение силы. (JP 3-0)

Термин	Определение
оборонительные кибероперации	Задачи по сохранению способности использовать возможности «голубого» киберпространства и защите данных, сетей, киберустройств и других указанных систем путём поражения текущей или надвигающейся злонамеренной киберпространственной активности. Сокращённо: **ОКбО** (*англ. DCO*). (JP 3-12).
оборонительные кибероперации-внутригосударственные мероприятия по обороне	Операции, в которых санкционированные действия по защите происходят в пределах защищаемой части киберпространства. Сокращённо: **ОКбО-ВМО** (*англ. DCO-IDM*). (JP 3-12).
оборонительные кибероперации-меры реагирования	Операции, являющиеся частью задач оборонительных кибероперациий, которые проводятся вне защищаемой сети или части киберпространства без разрешения владельца поражённой системы. Сокращённо: **ОКбО-МР** (*англ. DCO-RA*). (JP 3-12).
ограничение	Ограничивающие условие, наложенное на командование вышестоящим командованием. (FM 6-0)
опасность	Состояние, которое может привести к травме, заболеванию или гибели личного состава, повреждению или утрате оборудования или имущества, а также к ухудшению выполнения задачи. (JP 3-0)
оперативная инициатива	Установление или темп и сроки действий на протяжении всей операции. (ADP 3-0)
оперативная обстановка	Совокупность условий, обстоятельств и воздействий, которые влияют на использование возможностей и влияют на решения командира, несущего за них ответственность. Сокращённо: **ОО** (англ. OE). (JP 3-0)
оперативный процесс	Основные действия командования и управления, выполняемые в ходе операций: планирование, подготовка, выполнение и постоянная оценка операции. (ADP 5-0)
операции в информационной сети министерства обороны	Операции по обеспечению безопасности, конфигурированию, эксплуатации, расширению, обслуживанию и поддержанию киберпространства министерства обороны для создания и сохранения конфиденциальности, доступности и целостности информационной сети МО. Сокращённо: **операции в ИСМО** (*англ. DODIN operations*). (JP 3-12).
определение направления	Процедура получения пеленгов на радиоизлучения с помощью узконаправленной антенны и блока отображения на приёмнике перехвата или вспомогательном оборудовании. Сокращённо: **ОН** (англ. DF). (JP 3-85)
оружие направленной энергии	Оружие или система, использующая направленную энергию для вывода из строя, повреждения или уничтожения техники, объектов и/или личного состава противника. (JP 3-85)

Термин	Определение
основная задача	Конкретное или косвенное задание, которое должно быть выполнено для завершения боевой задачи. (FM 6-0)
оценка	**1)** Непрерывный процесс, измеряющий общую эффективность применения сил и средств в ходе боевых действий. **2)** **Определение хода выполнения задачи, создания условий для достижения цели.** **3)** Анализ уровня безопасности, эффективности и потенциала существующей или планируемой разведывательной деятельности. **4)** Оценка мотивов, квалификации и характеристик настоящих или будущих сотрудников или «агентов». (JP 3-0)
очерёдность огня	Указания командира штабу, подчинённым командирам, ответственным за планирование огневых задач и вспомогательным службам по применению огневых средств в соответствии с относительной важностью задачи подразделения. (FM 3-09)
очерёдность поддержки	Приоритет, устанавливаемый командиром для обеспечения поддержки подчинённого подразделения в соответствии с его относительной важностью для выполнения задачи. (ADP 5-0)
планирование	Искусство и наука понимания ситуации, представления желаемого будущего и определения эффективных путей его достижения. (ADP 5-0)
подготовка	Мероприятия, выполняемые подразделениями и военнослужащими для улучшения их способности достичь цели операции. (ADP 5,0)
положение относительного преимущества	Место или создание благоприятных условий в районе боевых действий (операций), которые предоставляют командиру временную свободу действий для усиления своих боевых возможностей над противником или воздействия на него с целью принятия риска и перехода в невыгодное положение. (ADP 3.0)
поражение	Лишение вооружённых сил возможности достичь поставленных целей. (ADP 3-0)
постановка электромагнитных помех	Преднамеренное излучение, переизлучение или отражение электромагнитной энергии с целью предотвращения или снижения эффективности использования противником электромагнитного спектра, а также с целью ослабления или нейтрализации боевого потенциала противника. (JP 3-85)
превосходство в электромагнитном спектре	Такая степень контроля в электромагнитном спектре, которая позволяет проводить операции в определённое время и в определённом месте без запретительных помех, при этом оказывая воздействие на способность угрозы (противника) делать то же самое. (JP 3-85)

Термин	Определение
приоритетная цель	Цель, потеря которой противником будет в значительной степени способствовать своему варианту действий. Сокращённо: **ПЦ** (*англ. HPT*). (JP 3-60)
противник	Противник – это сторона, идентифицированная как враждебная, против которой разрешено применение силы. (ADP 3-0)
радиочастотные меры противодействия	Любые устройства или технологии, использующие радиочастотные средства или технологии, предназначенные для снижения эффективности действий противника, особенно в отношении систем высокоточного наведения и средств обнаружения. (JP 3-85)
радиоэлектронная борьба	Военные действия, связанные с использованием электромагнитной и направленной энергии для контроля электромагнитного спектра или для нападения на противника. Сокращённо: **РЭБ** (*англ. EW*). (JP 3-85)
Радиоэлектронная разведка	Обнаружение, местоопределение, идентификация и оценка посторонних электромагнитных излучений. (JP 3-85)
разведка	**1)** Результат сбора, обработки, внедрения, оценки, анализа и интерпретации имеющейся информации об иностранных государствах, враждебных или потенциально враждебных силах или элементах, районах реальных или потенциальных операций. **2)** Деятельность, результатом которой является продукт. **3)** Организации, осуществляющие такую деятельность. (JP 2-0)
разведывательная подготовка района боевых действий	Систематический процесс анализа переменных условий задачи: противника, местности, погоды и гражданских факторов в районе ответственности с целью определения их влияния на операции. Сокращённо: **РПРБД** (*англ. IPB*). (ATP 2-01,3)
разведывательные операции	Задачи, решаемые подразделениями военной разведки в рамках ведения разных видов разведки с целью получения информации для удовлетворения утверждённых требований. (ADP 2-0)
район расположения цели	Географическая область, в которой важные цели могут быть обнаружены и поражены своими войсками. (JP 2-01.3)
резервные режимы работы военного времени	Характеристики и порядок работы средств обнаружения, связи, навигации, распознавания угроз, вооружения и систем противодействия, которые способствуют повышению военной эффективности, если неизвестны или не распознаны командованием противника до их применения, но могут быть задействованы в интересах противника или нейтрализованы, если заранее будут обнаружены. (JP 3-85)
сбор информации	Деятельность, при которой согласовывается и интегрируется планирование и использование информационных возможностей, а также систем обработки, использования и распространения информации для непосредственного обеспечения текущих и будущих операций. (FM 3-55)

Термин	Определение
схема огня	Детальная, логическая последовательность целей и мероприятий огневой поддержки для поиска и поражения целей в интересах обеспечения выполнения задач командира. (JP 3-0)
улучшение приёмов и возможностей РЭБ	Преднамеренное изменение или модернизация систем РЭБ или систем обнаружения целей, а также использующих их тактики и процедур в ответ на подтверждённые изменения в оборудовании, тактике или электромагнитной обстановке. (JP 3-85)
управление знаниями	Процесс обмена знаниями для улучшения общего понимания, обучения и принятия решений. (ADP 6-0)
управление рисками	Процесс выявления, оценки и контроля рисков и принятия решений, обеспечивающих баланс между ценой риска и результатами выполнения задачи. (JP 3-0)
целеуказание	Процесс выбора и определения приоритетности целей и подбора соответствующих ответных мер с учётом оперативных требований и возможностей. (JP 3-0)
цель	Субъект или объект, выполняющий какую-либо роль для противника, рассматриваемый для возможного поражения или других действий. См. также целевой район (*англ. objective area*). (JP 3-60)
электромагнитная атака	Направление РЭБ, связанное с использованием электромагнитной энергии, направленной энергии или противорадиолокационного оружия для поражения личного состава, объектов или техники с целью повреждения, нейтрализации или уничтожения боевого потенциала противника и рассматриваемое как разновидность огневого поражения. Сокращённо: **ЭМА** (*англ. EA*). (JP 3-85)
электромагнитная безопасность	Защита, обусловленная всеми мерами, направленными на лишение посторонних лиц информации, представляющей ценность, которая может быть получена в результате перехвата и изучения ими электромагнитных излучений, не относящихся к средствам связи (например, РЛС). (JP 3-85)
электромагнитная защита	Направление РЭБ, включающее действия по защите личного состава, объектов и оборудования от любых последствий использования электромагнитного спектра противником или своими войсками, которые снижают, нейтрализуют или уничтожают свой боевой потенциал. Сокращённо: **ЭМЗ** (*англ. EP*). (JP 3-85)
электромагнитная маскировка	Контролируемое излучение электромагнитной энергии на частотах, используемых своими войсками, таким образом, чтобы защитить излучения своих систем связи и электроники от действий противника в процессе электромагнитной поддержки радио и радиотехнической разведки без существенного ухудшения работы своих систем. (JP 3-85)

Термин	Определение
электромагнитная поддержка	Направление РЭБ, включающее действия, выполняемые по задаче или под непосредственным управлением командира с целью поиска, перехвата, местоопределения или локализации источников преднамеренного и непреднамеренного излучения электромагнитной энергии для немедленного определения угрозы, целеуказания, планирования и проведения будущих операций. Сокращённо: **ЭМП** (*англ. ES*). (JP 3-85)
электромагнитная совместимость	Способность радиоэлектронных систем, оборудования и устройств работать в предназначенных для них условиях, не вызывая или не подвергаясь неприемлемому или непреднамеренному ухудшению работы, электромагнитным излучением или отражением. (JP 3-85)
электромагнитная устойчивость	Действия, предпринимаемые для защиты личного состава, объектов и/или оборудования путём подавления, фильтрации, ослабления, заземления, соединения и/или экранирования от нежелательного воздействия электромагнитной энергии (JP 3-85).
электромагнитная уязвимость	Характеристики системы, приводящие к её определённому ухудшению (неспособности выполнить поставленную задачу) в результате воздействия электромагнитного излучения определённого уровня. (JP 3-85)
электромагнитное вторжение	Преднамеренное введение электромагнитной энергии в каналы передачи любым способом. Цель электромагнитного вторжения – дезинформировать операторов угрозы или вызвать у них замешательство. (JP 3-85)
электромагнитное зондирование	Преднамеренное излучение, предназначенное для введения в устройства или системы противника с целью изучения функций и эксплуатационных возможностей этих устройств или систем. (JP 3-85)
электромагнитный импульс	Мощный всплеск электромагнитного излучения, вызванный ядерным взрывом, энергетическим оружием или природным явлением, который может взаимодействовать с электрическими или электронными системами, вызывая повреждающие скачки тока и напряжения. (JP 3-85)

ИСТОЧНИКИ И ССЫЛКИ

Все ссылки были доступны на 24 мая 2021 года.

ИС-1. Необходимые публикации

Эти документы должны быть доступны для предполагаемых пользователей данной публикации.

1. DOD Dictionary of Military and Associated Terms – МО США. Словарь военных терминов и словосочетаний, январь 2021 года.

2. FM 1-02.1. Operational Terms – Оперативные термины, 9 марта 2021 года.

3. FM 1-02.1. Military Symbols – Военные условные обозначения и сокращения, 10 ноября 2020 года.

ИС-2. Дополнительные публикации

ИС-2.1. Издания министерства обороны

Большинство публикаций министерства обороны доступны на веб-сайте Директората исполнительных служб по адресу: https://www.esd.whs.mil/DD/DoD-Issuances.

4. DODI O-3115.07. Радио и радиотехническая разведка. 15 сентября 2008 г. с изменением 2 от 25 августа 2020 года.

5. DODM 5240.01. Процедуры, регулирующие проведение разведывательной деятельности МО. 8 августа 2016 года.

ИС-2.2. Совместные публикации

Большинство публикаций председателя Комитета начальников штабов доступны по адресу: https://www.jcs.mil/Library/CJCS-Instructions/

Большинство совместных публикаций доступны по адресу: https://www.jcs.mil/Doctrine/Joint-Doctine-Pubs/.

6. CJCSI 3211.01F. Объединённая политика военной дезинформации.14 августа 2015 года.

7. CJCSI 3370.01C. Стандарты выявления целей. 14 августа 2018 года. Ограничено (только .mil/.gov).

8. JP 2-0. Объединённая разведка. 22 октября 2013 года.

9. JP 2-01. Объединённая и национальная разведывательная поддержка военных операций. 05 июля 2017 года.

10. JP 2-01.3. Объединённая разведывательная подготовка оперативной обстановки. 21 мая 2014 года.

11. JP 3-0. Объединённые операции. 17 января 2017 года.

12. JP 3-09. Объединённая огневая поддержка. 10 апреля 2019 года.

13. JP 3-12. Кибероперации. 8 июня 2018 года.

14. JP 3-13. Информационные операции. 27 ноября 2012 года с изменением 1 от 20 ноября 2014 года.

15. JP 3-13.3. Безопасность операций. 6 января 2016 года.

16. JP 3-14. Операции в космическом пространстве. 10 апреля 2018 года с изменением 1 от 26 октября 2020 года.

17. JP 3-33. Штаб объединённой оперативной группы. 31 января 2018 года.

18. JP 3-60. Совместное целеуказание. 28 сентября 2018 года.

19. JP 3-85. Объединённые операции в электромагнитном спектре. 22 мая 2020 года.

20. JP 5-0. Совместное планирование. 1 декабря 2020 года.

21. JP 6-0. Объединённая система связи. 10 июня 2015 г. с изменением 1 от 4 октября 2019 года.

ИС-2.3. Публикации сухопутных войск

Если не указано иное, публикации сухопутных войск доступны по адресу: https://armypubs.army.mil.

22. ADP 1. Сухопутные войска. 31 Июля 2019 года.

23. ADP 2-0. Разведка. 31 Июля 2019 года.

24. ADP 3-0. Операции. 31 Июля 2019 года.

25. ADP 3-19. Огонь. 31 Июля 2019 года.

26. ADP 3-37. Защита. 31 Июля 2019 года.

27. ADP 3-90. Наступление и оборона. 31 Июля 2019 года.

28. ADP 5-0. Оперативный процесс 31 Июля 2019 года.

29. ADP 6-0. Командование: Командование и управление сухопутными войсками. 31 Июля 2019 года.

30. AR 195-2. Уголовно-следственная деятельность. 21 июля 2020 года.

31. AR 380-10. Раскрытие информации за рубежом и контакты с иностранными представителями. 10 июля 2015 года.

32. AR 380-5. Программа информационной безопасности сухопутных войск. 22 октября 2019 года.

33. AR 381-10. Разведывательная деятельность сухопутных войск США. 3 мая 2007 года.

34. AR 381-12. Программа информирования и оповещения об угрозах. 1 июня 2016 года.

35. AR 525-21. (HC) Программа военной дезинформации сухопутных войск (C). 28 октября 2013 года.

36. AR 530-1. Безопасность операций 21 февраля 2014 года.

37. ATP 2-01.3. Разведывательная подготовка района боевых действий. 1 марта 2019 года.

38. АТП 3-09.32. Общий набор тактических приёмов, методов и процедур, методы и процедуры совместного применения огневой мощи. 18 октября 2019 года.

39. ATP 3-12.3. Методы радиоэлектронной борьбы. 16 июля 2019 года.

40. ATP 3-13.3. Безопасность операций для дивизии и ниже. 16 июня 2019 г.

41. ATP 3-60. Целеуказание. 1 июня 2015 года.

42. ATP 3-60.1/MCRP 3-31.5/NTTP 3-60.1/AFTTP 3-2.3. Межвидовая тактика, методы и процедуры динамического целеуказания. 10 сентября 2015 года.

43. ATP 3-94.2. Глубокие операции. 1 сентября 2016 года.

44. ATP 5-19. Управление рисками. 14 апреля 2014 года.

45. ATP 6-01.1. Методы эффективного управления знаниями. 6 марта 2015 года.

46. ATP 6-02.70. Методы управления спектром. 16 октября 2019 года.

47. ATP 6-02.71. Методы операций в информационной сети министерства обороны. 30 апреля 2019 года.

48. FM 2-0. Разведка. 6 июля 2018 года.

49. FM 3-0. Операции. 6 октября 2017 года.

50. FM 3-09. Огневая поддержка и действия артиллерии. 30 апреля 2020 года.

51. FM 3-13. Информационные операции. 6 декабря 2016 года.

52. FM 3-13.4. Поддержка сухопутными войсками действий по дезинформации. 26 Февраля 2019 года.

53. FM 3-14. Космические операции сухопутных войск. 30 октября 2019 года.

54. FM 3-55. Сбор информации. 3 мая 2013 года.

55. FM 6-0. Командир, организация штаба и операции. 17 мая 2014 года.

56. FM 6-02. Обеспечение связью в боевых действиях (операциях). 13 сентября 2019 года.

57. FM 6-27. MCTP 11-10C. Справочник командира по правовым нормам ведения наземных боевых действий. 7 августа 2019 года.

ИС-2.4. Другие публикации

58. Большинство положений Кодекса США по адресу: https://www.ecfr.gov/.

59. Стратегия превосходства в электромагнитном спектре министерства обороны. октябрь 2020 года. https:// www.defense.gov/Newsroom/Publications/

60. Европейско-американская программа «Щит конфиденциальности». 12 июля 2016 года. https://www.privacyshield.gov/

61. Исполнительный приказ 12333. Разведывательная деятельность США. 4 декабря 1981 года. Изменено указами президента № 13284 (2003) и № 13470 (2008). http://www.archives.gov/federal-register/codification/executive-order/12333.html

62. Билль Палаты представителей № 4081 – Закон о защите конфиденциальности потребителей 2017 года. https://www.congress.gov/bill/115th-congress/house-bill/4081

63. Раздел 17, Свод федеральных нормативных актов. Товарные и фондовые биржи.

64. Раздел 21, Свод федеральных нормативных актов. Продукты питания и лекарства.

65. Раздел 45, Свод федеральных нормативных актов. Государственное социальное обеспечение

66. Раздел 48, Свод федеральных нормативных актов. Федеральное положение о закупках для нужд обороны.

67. Конституция США. https://www.whitehouse.gov/1600/constitution

ИС-2.5. Законодательство США

Большинство актов и публичных законов доступны по адресу https://uscode.house.gov/.

68. Раздел 6, Кодекс США. Внутренняя безопасность

69. Раздел 10, Кодекс США. Вооружённые силы

70. Раздел 10, Кодекс США. Глава 47, Унифицированный военный уголовный кодекс.

71. Раздел 15, Кодекс США. Коммерция и торговля.

72. Раздел 18, Кодекс США. Преступления и уголовное судопроизводство.

73. Раздел 28, Кодекс США. Судоустройство и судебный процесс.

74. Раздел 32, Кодекс США. Национальная гвардия

75. Раздел 40, Кодекс США. Публичные здания, собственность и общественные работы.

76. Раздел 44, Кодекс США. Печать, полиграфия и документооборот.

77. Раздел 50, Кодекс США. Война и национальная оборона.

ИС-2.6. Установленные формы

Данный раздел не содержит записей.

ИС-2.7. Справочные формы

Если не указано иное, формы DA доступны на сайте Директората изданий сухопутных войск по адресу https://armypubs.army.mil/.

Формы DD доступны на сайте Дирекции исполнительных служб по адресу https://www.esd.whs.mil/Directives/forms/.

78. Форма DA 2028. Рекомендуемые изменения в публикациях и бланках. Формы министерства обороны доступны на веб-сайте штаб-квартиры в Вашингтоне: https://www.esd.whs.mil/Directives/forms/

79. Форма DD 1494. Заявка на распределение частот оборудования.

80. Форма DD 1972. Запрос на совместный тактический авиаудар.