ТЕРМИНОЛОГИЧЕСКИЙ БАЗИС В ОБЛАСТИ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

***Макаренко Сергей Иванович**, кандидат технических наук*
***Чукляев Илья Игоревич**, кандидат технических наук, доцент*

В работе предлагается однозначная и непротиворечивая система терминов и определений, в основу которой положены руководящие документы Вооруженных сил США в области информационного противоборства, дополненные материалом международных стандартов и отечественных публикаций данной предметной области.

***Ключевые слова**: информационная война, информационное пространство, информационные воздействия, информационное оружие.*

THE TERMINOLOGICAL BASIS OF THE INFORMATIONAL CONFLICT` AREA

***Sergey Makarenko**, Ph.D.*
***Ilia Chucklyaev**, Ph.D., Associate Professor*

The single–valued and consistent system of terms based on USA Armed Forces` direct documents in the area of informational conflict, which are complemented by international standards and Russian science publications is offered in this work.

***Keywords**: informational warfare, informational space, informational effect, informational weapon*

Адекватное описание противоборства в информационной сфере потребовало формирования соответствующего терминологического базиса. К сожалению, в настоящее время отечественная терминология в данной области, не утверждена официальными документами, а используемые различными авторами термины и определения являются весьма неоднозначными и зачастую противоречивыми. Вместе с тем, в США и странах НАТО еще с 90-х годов введены руководящие документы определяющие терминологию и, зачастую, именно ей руководствуются исследователи в области информационного противоборства.

В работе предлагается однозначная и непротиворечивая система терминов и определений, в основу которой положены открытые источники: руководящие документы Вооруженных сил (ВС) США в области информационного противоборства [1-10], дополненные материалом международных стандартов [11, 13] и публикаций отечественных специалистов [14-26] данной предметной области.

Информационная война

В качестве основного определения в руководящих документах ВС США сформулировано следующие определения информационной войны.

Информационная война – широкомасштабная информационная борьба с применением способов и средств информационного воздействия на противника в интересах достижения целей воздействующей стороны.

По направленности информационных воздействий информационная война, как правило, подразделяется на два основных вида:

- информационно-психологическую (психологическую) войну;
- информационно-техническую войну.

Эксперты ВС США считают, что информационная война может проводиться во всех сферах общественной жизни – в экономике, политике, военном деле, социальных отношениях, сфере духовной жизни и особенно в идеологии. При этом рядом специалистов США введены определения, расширяющие суть данного понятия относительно изложенных в руководящих документах.

Информационная война - комплексное воздействие на систему государственного и военного управления противостоящей стороны, на ее военно-политическое руководство, которое уже в мирное время приводило бы к принятию благоприятных для стороны-инициатора информационного воздействия решений, а в ходе конфликта полностью парализовало бы функционирование инфраструктуры управления противника.

Информационная война – соперничество и организованные действия (информационные операции) конфликтующих сторон в области информационных потенциалов, проводимые с целью снижения возможностей по использованию имеющегося государственного, военного и боевого потенциала противника и сохранения (повышения) возможностей по использованию собственного потенциала.

Информационный потенциал – совокупность информации, зафиксированной на материальных носителях или в любой другой форме, обеспечивающей ее передачу во времени и пространстве потребителям для решения широкого спектра задач, связанных с деятельностью государственных институтов, военно-промышленного комплекса и ВС, а также силы и средства, используемые для получения, обработки, хранения и представления информации; умонастроения людей, использующих эту информацию и способных запускать и контролировать вещественно-энергетические процессы.

Цель информационной войны – такое воздействие на противника, в результате которого он самостоятельно, без принуждения, принимает благоприятные для атакующей стороны решения.

Объекты ведения информационной войны – информационные системы и сети обмена информацией (включая соответствующие линии передач, обрабатывающие центры и человеческие факторы этих систем), а также информационные технологии, используемые в системах вооружений.

Информационная война состоит из совокупности информационных операций, проводимых в информационном пространстве в интересах достижения информационного превосходства.

В настоящее время, содержательная часть понятия «информационная война» применительно к действиям ВС изменились, и сейчас в руководящих документах США и НАТО в основном используется термин «информационная операция». В тоже время область применения термина «информационная война» сместилась в сферу описаний глобальных противоречий между государствами и стратегического информационного противоборства.

Информационное пространство

Информационное пространство – область ведения информационной войны.

Действия в информационном пространстве разворачиваются в:

- технической сфере;
- психологической сфере.

Техническая сфера – область информационного пространства, в которой создается, обрабатывается и накапливается информация. Кроме того, это область, в которой функционируют системы командования, управления, связи, коммуникаций и разведки.

Психологическая сфера – область информационного пространства, которая объединяет мышление личного состава ВС и мирного населения. То есть это область, в которой формируются намерения командиров, доктрины, тактика, методы противоборства, мораль, понятие сплоченности подразделений, уровень подготовки, опыт, понимание ситуации и общественное мнение.

Ряд экспертов ВС США считает целесообразным исключение участия физических средств поражения в информационных действиях (таких как поражение пунктов управления, разрушение инфраструктуры и др.), так как эти действия находятся в физическом пространстве, которое является традиционной областью войны, и объединяет традиционные сферы противоборства - землю, море, воздух и космическое пространство. То есть то пространство, в котором функционируют системы вооружения, военной техники и системы коммуникаций.

Одним из ключевых понятий, которым оперируют специалисты в области информационного противоборства США, является «информационная обстановка», оно по смысловому контексту созвучно «информационному пространству».

Информационная обстановка – совокупность людей, организаций и систем, собирающих, отрабатывающих, доводящих информацию или действующих на ее основе.

Элементы информационной обстановки – руководители, лица, принимающие решения, люди и организации.

Ресурсы информационной обстановки – материальные средства и системы, используемые для сбора, анализа, применения или доведения информации.

Включая понятия ресурса и элементов, можно сформулировать следующее определение информационной обстановки – это сфера, в которой функционируют люди и автоматизированные системы: ведут наблюдение, ориентируются, принимают решения и действуют на основе информации. С этой точки зрения информационная обстановка является «основной обстановкой принятия решений» на земле, на море, в воздухе, в космосе и информационном пространстве.

По взглядам специалистов США, информационная обстановка состоит из трех измерений.

Физическое измерение – это реальный мир, в котором ведутся военные действия на суше, на море, в воздухе и в космосе. Информационные системы и системы связи, их техническая составляющая находится в этом измерении для того, чтобы эти действия могли бы иметь место.

Информационное измерение – место, где информация создается, обрабатывается, распространяется и хранится. Это измерение связывает реальный физический мир с сознанием человека познавательного измерения в качестве входящего источника и преобразует ее в исходящий результат – решение.

Познавательное измерение существует в сознании лица принимающего решение. Это та область, где человек обрабатывает полученную информацию в соответствии с присущим ему комплексом норм, морали, убеждений, культуры и ценностей. Они действуют в качестве ограничений восприятия лицом, принимающим решения при фильтровании информации и получении сознания значимости и взаимосвязи. Информация оценивается и анализируется, чтобы сформировать решения, которые передаются через информационное измерение в область физического мира.

Каждая из составляющих информационной обстановки может быть подвергнута целевому воздействию и являться объектом, который в определенных обстоятельствах может оказать решающее влияние на исход операции (боевых действий) с учетом концептуальной взаимосвязи на основе цикла принятия решения.

Информационные операции

Информационные операции – действия, предпринимаемые для достижения информационного превосходства в обеспечении национальной военной стратегии путем воздействия на информацию и информационные системы противника с одновременным укреплением и защитой собственной информации и информационных систем и инфраструктуры.

Цель информационных операций – достижение информационного превосходства над противником.

Информационное превосходство – способность собирать, обрабатывать и распределять непрерывный поток информации различного характера, препятствуя противнику делать то же самое.

Информационное превосходство так же может быть определено и через показатели динамики обработки информации.

Информационное превосходство – способность обеспечивать такой темп проведения операции, который превосходит любой возможный темп противника, позволяя доминировать во все время ее проведения, оставаясь непредсказуемым, и действовать, опережая противника в его ответных акциях.

Основные объекты воздействия в ходе информационных операций:

- органы управления государства и его ВС;
- информационно-управляющие системы гражданской инфраструктуры (телекоммуникационные, включая средства массовой информации, транспортные, энергетического комплекса, финансового и промышленного секторов);
- информационно-управляющие элементы военной инфраструктуры (системы связи, разведки, боевого управления, тылового обеспечения, управления оружием);
- линии, каналы связи и передачи данных;
- информация, циркулирующая или хранящаяся в системах управления;
- общество в целом (как гражданское население, так и личный состав ВС), его государственные, экономические и социальные институты;
- средства массовой информации (в первую очередь – электронные);
- руководящий состав и персонал автоматизированных систем управления, участвующий в процессе принятия решений.

В период проведения миротворческих операций объектами воздействия могут быть также военизированные, партизанские и политические организации, религиозные и социальные группы, отдельные лица, открыто или тайно выступающие против присутствия ВС или союзников и препятствующие выполнению ими своей миссии.

Поскольку информационные операции связаны с использованием информации и информационных технологий для воздействия на военные и гражданские системы с целью достижения информационного превосходства над противником, ряд специалистов дают следующее определение информационным операциям.

Информационная операция – это комплекс взаимосвязанных по цели, месту и времени мероприятий и акций, направленных на инициализацию и управление процессами манипулирования информацией, с целью достижения и удержания информационного превосходства путем воздействия на информационные процессы в информационных системах противника.

При этом информационные системы рассматриваются в широком смысле, т.е. не только автоматические и автоматизированные технические системы, но и государство и общество, которые тоже рассматриваются как информационные системы.

Информационные операции есть основа ведения информационной войны. Информационные операции являются самостоятельным видом оперативного обеспечения, который реализует на поле боя концепцию информационной войны.

По целям и задачам информационные операции подразделяются на:

- информационное обеспечение;
- специальные информационные операции;
- информационное противоборство.

По уровню управления, на которое осуществляется воздействие, и масштабу воздействия информационные операции могут быть классифицированы на:

- стратегические операции, проводятся по решению военно-политического руководства страны, являются воздействием на элементы государственного устройства потенциальных противников (политические, военные, экономические и информационные) при одновременной защите своих государственных структур и призваны обеспечить достижение национальных стратегических целей;
- оперативные операции, проводятся для обеспечения успешного хода военной операции или кампании в целом или решения ее главных задач, являются воздействием на линии связи, системы тылового обеспечения и боевого управления ВС противника при одновременной защите аналогичных собственных систем, так и союзников;
- тактические операции, проводятся с целью обеспечения решения тактических военных задач и сосредоточены на воздействии на информацию и информационные системы, такие, как системы связи, боевого управления, разведки и другие, непосредственно обеспечивающие ведение боевых действий соединениями и частями противника при одновременной защите своих систем.

По характеру решаемых задач информационные операции могут быть:

- оборонительными,
- наступательными.

Оборонительные информационные операции – взаимосвязанные процессы по защите информационной среды, вскрытию признаков нападения, восстановлению боеспособности и организации ответных действий на агрессию (нападение).

Цель оборонительных информационных операций – обеспечение выполнения целевых задач информационными и управляющими системами в условиях ведения информационной войны, а также обеспечение сохранности информационных ресурсов и предотвращения утечки, искажения, утраты или хищения информации в результате несанкционированного доступа к ней со стороны противника.

Оборонительные информационные операции включают мероприятия по обеспечению безопасности собственных информационных ресурсов:

- оперативная маскировка;
- обеспечение физической безопасности информационной инфраструктуры;
- обеспечение безопасности информации и скрытности действий войск (сил);
- вскрытие мероприятий по оперативной маскировке противника;
- контрпропаганда и контрдезинформация;
- контрразведка;
- радиоэлектронная защита;
- специальные информационные операции.

Оборонительные информационные операции должны обеспечивать своевременность и точность передачи данных, гарантированный доступ к ним пользователей в условиях информационного воздействия противника. В ходе их предусматривается проведение мероприятий по восстановлению боеспособности информационных систем.

Наступательные информационные операции представляют собой комплексное проведение по единому замыслу и плану мероприятий по оперативной маскировке, радиоэлектронной борьбе, программно-математическому воздействию на информационно-управляющие системы, физическому уничтожению (или выводу из строя) объектов информационной инфраструктуры.

Цель наступательных информационных операций – достижение и удержание информационного превосходства в ходе информационной войны.

В ходе таких операций принимаются меры, оказывающие воздействие на сознание людей и направленные на срыв процесса принятия решений, а также действия с целью нарушения работы или уничтожения элементов информационной инфраструктуры.

Наступательные информационные операции включают следующие мероприятия по достижению и удержанию информационного превосходства:

- оперативная маскировка;
- психологические операции;
- радиоэлектронная борьба;
- физическое разрушение и уничтожение объектов информационной инфраструктуры;
- программно-математические воздействия и атаки на компьютерные сети противника.

При проведении наступательных информационных операций основными традиционными

методами являются психологические операции и мероприятия по оперативной маскировке, традиционно применявшиеся для оказания влияния на сознание людей в процессе принятия ими решений, а также такие действия, как радиоэлектронное подавление и использование средств физического уничтожения, направленные на нарушение функционирования или уничтожение элементов информационной инфраструктуры. К достаточно новым методам в данном случае можно отнести специальные программно-математические воздействия на компьютерные сети противника и специальные информационные операции.

Оперативная маскировка – мероприятия, проводящиеся под руководством командующих объединенными группировками войск (сил), в интересах оказания воздействий на органы принятия решений противника через его системы сбора, анализа и распределения информации путем предоставления им заведомо ложной информации и скрытия признаков реальной деятельности войск (сил).

Цель оперативной маскировки состоит в том, чтобы запутать, дезинформировать разведывательные органы противника, заставить их делать неправильные выводы и, как следствие, добиться от военного руководства противника неверных действий. Эти мероприятия позволяют также опередить противника в принятии решения.

Оперативная маскировка предполагает применение следующих способов:

- дезинформация – распространение заведомо ложной информации о составе, состоянии, дислокации, боеготовности своих войск, их группировках, характере и способах решения задач, планах, предназначении и состоянии военной техники и объектов;
- имитация – воспроизведение правдоподобных демаскирующих признаков, характерных для реальной деятельности войск (объектов), создание радиоэлектронной обстановки с использованием имитаторов, радиотехнических устройств, ложных сооружений и объектов, макетов военной техники и т. д.;
- демонстративные действия – преднамеренный показ противнику специально выделенными силами и средствами активной деятельности в целях его дезориентации и скрытия истинных намерений организаторов;
- обеспечение скрытности действий – определение признаков, распознаваемых разведывательными системами противника и позволяющих ему на основе их анализа получать особо важную и своевременную информацию; выбор и проведение мероприятий, которые обеспечивали бы скрытие этих признаков и тем самым снижали бы до приемлемого уровня уязвимость союзников от действий разведки противника.

Успех проведения мероприятий по оперативной маскировке в определяющей степени зависит от эффективности разведывательного обеспечения. Разведка в этом случае осуществляет вскрытие объектов противника, в отношении которых замышляются эти действия, оказывает помощь в разработке правдоподобной версии, предлагаемой для дезинформации, выборе наиболее перспективных объектов для реализации дезинформации и оценивает эффективность проведенных мероприятий.

Психологические операции – мероприятия по распространению специально подготовленной информации с целью оказания воздействия на эмоциональное состояние, мотивацию и аргументацию действий, принимаемые решения и поведение отдельных руководителей, организаций, социальных или национальных групп и отдельных личностей противника в благоприятном для государства и их союзников направлении.

Радиоэлектронная борьба подразделяется на:

- радиоэлектронное подавление;
- радиоэлектронную защиту;
- радиоэлектронное обеспечение.

Радиоэлектронное подавление – действия наступательного характера, предпринимаемые с целью дезорганизовать, нейтрализовать или снизить возможности противника по эффективному использованию им радиоэлектронных систем в различных звеньях управления ВС.

Радиоэлектронная защита – такие действия, как защита своих радиоэлектронных средств (РЭС) от помех, создаваемых противником, и осуществление контроля (наблюдения) за работой РЭС союзников, с целью исключения их взаимного влияния друг на друга.

Радиоэлектронное обеспечение представляет собой действия, направленные на обнаружение, идентификацию и определение местоположения РЭС противника, которые могут являться как источниками получения разведданных, так и источниками информационных угроз.

Физическое уничтожение элементов информационной инфраструктуры рассматривается как проводимые в ходе информационной операции действия по применению средств огневого поражения и физического уничтожения с целью вывода из строя ключевых элементов системы управления и связи противника.

Программно-математическое воздействие на компьютерные сети (компьютерные атаки)

определяется как действия с применением аппаратно-программных средств, направленные на использование, искажение, подмену или уничтожение информации, содержащейся в базах данных компьютеров и информационных сетей, а также на снижение эффективности функционирования либо вывод из строя самих компьютеров и компьютерных сетей.

Так же среди наступательных информационных операций в ВС США выделяют борьбу с системами управления как самостоятельный вид боевого обеспечения. При организации информационных операций, действия по борьбе с системами управления централизованно интегрируются в них и становятся их неотъемлемыми элементами.

Борьба с системами управления – деструктивное воздействие на информационные системы противника и циркулирующую в них информацию или уничтожение их. При этом целевыми объектами воздействия являются системы управления и связи противника.

Информационное воздействие

Информационное воздействие (информационное нападение) представляет собой наступательную составляющую информационной войны и реализуется посредством наступательных информационных операций.

Информационное воздействие – основной поражающий фактор информационной войны, представляющий собой воздействие информационным потоком на объект атаки – информационную систему или ее компонент, с целью вызвать в нем в результате приема и обработки данного потока заданные структурные и/или функциональные изменения.

Объект информационного воздействия – множество элементов информационной системы, принадлежащих или способных принадлежать сфере управления, и имеющих потенциальные ресурсы для перепрограммирования на достижение целей, чуждых данной системе, но выгодных противнику.

Объектами воздействия и защиты в ходе информационно-психологической борьбы являются психика личного состава ВС и населения противостоящих сторон, системы формирования общественного мнения и принятия решений.

Объектами воздействия и защиты в ходе информационно-технической войны являются информационно-технические системы (системы связи и управления, телекоммуникационные системы, радиоэлектронные средства, компьютерные сети и т.д.).

Для каждой информационной сферы характерны свои объекты воздействия и средства поражения. Различают следующие **объекты информационного воздействия**:

- одиночные (отдельные узлы связи или компьютерная сеть и др.);
- групповые (например, элементы территориально распределенной информационно-управляющей системы).

Средства воздействия также классифицируют по характеру поражающих свойств:

- высокоточное воздействие (на определенный ресурс в информационно-вычислительной сети);
- комплексное воздействие (вся телекоммуникационная инфраструктура информационно-вычислительной системы).

При этом тип воздействия может быть:

- разрушающим;
- манипулирующим;
- блокирующим.

Степень поражения информационным воздействием – емкость той части объекта информационного воздействия, которая либо уничтожена, либо работает на цели, чуждые собственной системе, но выгодные противнику.

Используемая в настоящее время концепция информационной войны предусматривает следующие информационные воздействия:

- подавление (в военное время) элементов инфраструктуры государственного и военного управления (поражение центров командования и управления);
- электромагнитное воздействие на элементы информационных и телекоммуникационных систем (радиоэлектронная борьба);
- получение разведывательной информации путем перехвата и дешифрования информационных потоков, передаваемых по каналам связи, а также по побочным излучениям и за счет специального внедрения технических средств перехвата информации;
- осуществление несанкционированного доступа к информационным ресурсам (путем использования программно-аппаратных средств, прорыва систем защиты информационных и телекоммуникационных систем противника) с последующим их искажением, уничтожением или хищением, либо нарушение нормального функционирования этих систем;
- формирование и массовое распространение по информационным каналам противника или глобальным сетям дезинформации или тенденциозной информации для воздей-

ствия на оценки, намерения и ориентацию населения и лиц, принимающих решения;
- получение интересующей информации путем перехвата и обработки открытой информации, передаваемой по незащищенным каналам связи, циркулирующей в информационных системах, а также публикуемой в открытой печати и средствах массовой информации.

Информационное оружие

Информационное оружие – совокупность методов и средств информационного воздействия на технику и людей.

При этом данное определение может быть сформулировано более развернуто.

Информационное оружие – это совокупность специально организованной информации и информационных технологий, позволяющая целенаправленно изменять (уничтожать, искажать), копировать, блокировать информацию, преодолевать системы защиты, ограничивать допуск законных пользователей, осуществлять дезинформацию, нарушать функционирование носителей информации, дезорганизовывать работу технических средств, компьютерных систем и информационно-вычислительных сетей, применяемая в ходе информационной борьбы для достижения поставленных целей.

В соответствие с видами информационной борьбы информационное оружие подразделяется на два основных вида:
- информационно-техническое (так же включает в себя **программно-математическое оружие**);
- информационно-психологическое (включает в себя психофизическое оружие).

Главными объектами информационного оружия первого вида является технические средства, второго – люди.

Психофизическое оружие – это совокупность всех возможных методов и средств (технотронных, суггестивных, психотропных, комплексных и др.) скрытого насильственного воздействия на подсознание человека с целью модификации его сознания, поведения и физиологического состояния в нужном для воздействующей стороны направлении. Психофизическое оружие представляет собой разновидность информационно-психологического оружия.

Информационное оружие, по сути, является информационной технологией, включающей в себя:
- анализ способов и механизмов активизации у конкретной системы – противника, заложенных в нее программ самоуничтожения;
- поиск программы самоуничтожения;
- разработка конкретного информационного оружия;
- применение информационного оружия по заданному объекту.

Средства информационного воздействия – средства, используемые в качестве информационного оружия.

Средства специального программно-математического воздействия – некоторая самостоятельная программа (набор инструкций), которая способна выполнить любое подмножество перечисленных ниже функций:
- скрывать признаки своего присутствия в программно-аппаратной среде системы;
- обладать способностью к самокопированию, ассоциированию себя с другими программами и/или переносу своих фрагментов в иные области оперативной или внешней памяти;
- разрушать (искажать) код программ в оперативной памяти;
- сохранять фрагменты информации из оперативной памяти в некоторой области внешней памяти прямого доступа (локальной и удаленной);
- искажать, блокировать и/или подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных;
- подавлять информационный обмен в телекоммуникационных сетях, фальсифицировать информацию в каналах управления;
- противодействовать работе тестовых программ и систем защиты информационных ресурсов.

Способы программно-математического воздействия можно подразделить на следующие:
- «логические бомбы» – скрытые управляющие программы, которые по определенному сигналу или в установленное время осуществляют несанкционированный доступ к информации, нарушает управление информационными ресурсами либо дезорганизует работу технических средств;
- компьютерные вирусы, представляющие собой специализированные программные продукты, которые способны воспроизводить «логические бомбы», внедрять их дистанционно в информационные сети противника, и обладают способностью к самокопированию;
- программные продукты типа «троянский конь» – программы, внедрение которых по-

зволяет осуществлять скрытый несанкционированный доступ к информационным ресурсам противника для добывания разведданных или проведения информационного воздействия;
- нейтрализаторы тестовых программ, обеспечивающие сохранение естественных и искусственных недостатков программного обеспечения;
- преднамеренно созданные, скрытые от обычного пользователя интерфейсы для входа в систему.

В соответствии с различными основаниями информационное оружие можно классифицировать следующим образом.

По цели использования информационное оружие подразделяют на:
- обеспечивающее;
- атакующее.

Обеспечивающее информационное оружие – оружие, с помощью которого оказываются информационные воздействия на средства защиты информации атакуемой системы.

В состав обеспечивающего информационного оружия входят:
- средства компьютерной разведки;
- средства преодоления системы защиты.

Успешное применение обеспечивающего информационного оружия позволяет осуществлять деструктивные воздействия на хранимую, обрабатываемую и передаваемую в системе информацию с использованием атакующего информационного оружия.

Атакующее информационное оружие – оружие, с помощью которого осуществляется воздействие на хранимую, обрабатываемую и передаваемую в системе информацию, нарушающее применяемые информационные технологии.

В составе атакующего информационного оружия выделяют четыре основных вида средств информационных воздействий:
- средства нарушения конфиденциальности информации;
- средства нарушения целостности информации;
- средства нарушения доступности информации;
- средства психологических воздействий на абонентов информационной системы.

Применение атакующего информационного оружия направлено на срыв выполнения информационной системой целевых задач.

По способу реализации информационное оружие можно разделить на три класса:
- математическое (алгоритмическое);
- программное;
- аппаратное.

Информационное оружие, относящееся к разным классам, может применяться совместно, а также некоторые виды информационного оружия могут нести в себе черты нескольких классов.

К **алгоритмическому информационному оружию** относится:
- алгоритмы, использующие сочетание санкционированных действий для осуществления несанкционированного доступа к информационным ресурсам;
- алгоритмы применения санкционированного (легального) программного обеспечения и программные средства несанкционированного доступа для осуществления незаконного доступа к информационным ресурсам.

К **программному информационному оружию** относятся программы с потенциально опасными последствиями своей работы для информационных ресурсов системы.

К **аппаратному информационному оружию** относятся средства функционального поражения информационных ресурсов системы, а также аппаратные закладки в интересах нарушения функционирования или несанкционированного доступа к информационным ресурсам.

В целом основные понятия концепции информационного противоборства в том виде, в каком они приняты в ВС США, не являются новыми для российской теории военного искусства. Теоретические основы информационного противоборства достаточно полно раскрыты в российской военной науке через понятия «борьба с системами управления противника», «радиоэлектронная война», «завоевание господства в эфире», «психологическая война», «дезинформация», «военная хитрость» и т. п. Новизна подхода ВС США к теории информационного противоборства заключается в комплексном использовании военно-теоретических разработок по данной тематике, основанных на своих технологических достижениях в области информатики. Данный комплексный подход представлен в настоящей работе и предлагается специалистам для использования в интересах развития отечественной теории информационного противоборства.

Литература

1. Cyber Space Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. - Washington D.C.: The White House, 2009.
2. Informational Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. - Washington D.C.: The White House, 2011.
3. Department of Defense Strategy for Operating in Cyberspace. - Washington D.C.: U.S. Department of Defense, 2011.
4. AFDD 3-12. Cyberspace Operations. USAF, 2010, 60 p.
5. AFDD 3-13. Information Operations. USAF, 2011, 65 p.
6. AFPD 10-7. Information Operations. USAF, 2006, 29 p.
7. DoDD 3600.1. Information Operations. US DoD, 2013, 12 p.
8. Information Operations Primer: Fundamentals of Information Operations. U.S. Army War College, 2011, 204 p.
9. JP 3-13. Information Operations. US Joint Chiefs of Staff, 2012. 69 p.
10. JP 3-13.1. Electronic Warfare. US Joint Chiefs of Staff, 2007. 115 p.
11. Стандарт ISO/IEC 27032:2012. Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности. 2012.
12. Стандарт ITU-T X.1205:2008. Обзор кибербезопасности. 2008. – Женева: МСЭ-Т, 2008. – 162 с. – URL: www.itu.int/ITU-T (дата доступа 20.01.2014)
13. Безопасность в электросвязи и информационных технологиях. Обзор содержания и применения действующих Рекомендаций МСЭ-Т для обеспечения защищенной электросвязи. – Женева: МСЭ-Т, 2009. – 162 с. – URL: www.itu.int/ITU-T (дата доступа 20.01.2014)
14. Гриняев С.Н. Поле битвы - киберпространство. Теория, приемы, средства, методы и системы ведения информационной войны. – М.: Харвест, 2004. – 426 с.
15. Расторгуев С.П. Информационная война. – М: Радио и связь, 1999. – 416 с.
16. Почепцов Г.Г. Информационные войны. – М.: Рефл-бук, К.: Ваклер, 2000. – 576 с.
17. Жуков В. Взгляды военного руководства США на ведение информационной войны // Зарубежное военное обозрение. № 1 2001. - URL: http://pentagonus.ru/publ/22-1-0-175
18. Куннакова Н.Л. Информационная война как объект научного анализа // Альманах современной науки и образования, №6 (61), 2012. – 93-96 с.
19. Антонович П.И., Шаравов И.В., Лойко В.В. Сущность операций в кибернетическом пространстве и их роль в достижении информационного превосходства // Вестник Академии военных наук. № 1 (38). 2012. С. 41-45.
20. Антонович П.И. Изменение взглядов на информационное противоборство на современном этапе // Вестник Академии военных наук. № 1 (34). 2011. С. 43-47.
21. Антонович П.И. О современном понимании термина «кибервойна» // Вестник Академии военных наук. № 2 (35). 2011. С. 89-96.
22. Антонович П.И. О сущности и содержании кибервойны// Военная мысль. № 7. 2011. С. 39-46.
23. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 1) // Вопросы кибербезопасности. № 1 (1). 2013. С. 2-9.
24. Зубарев И.В., Жидков И.В., Кадушкин И.В. Кибербезопасность автоматизированных систем управления военного назначения // Вопросы кибербезопасности. № 1 (1). 2013. С. 10-16.
25. Макаренко С. И. Проблемы и перспективы применения кибернетического оружия в современной сетецентрической войне // Спецтехника и связь. № 3. 2011. С. 41-47. - URL: http://www.st-s.su/sites/default/files/files/pdf/2011-03/2011-03-makarenko.pdf
26. Макаренко С. И. Информационная безопасность: учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М.А. Шолохова, 2009. – 372 с.

References

1. Cyber Space Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. - Washington D.C.: The White House, 2009.
2. Informational Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. - Washington D.C.: The White House, 2011.
3. Department of Defense Strategy for Operating in Cyberspace. - Washington D.C.: U.S. Department of Defense, 2011.
4. AFDD 3-12. Cyberspace Operations. USAF, 2010, 60 p.
5. AFDD 3-13. Information Operations. USAF, 2011, 65 p.
6. AFPD 10-7. Information Operations. USAF, 2006, 29 p.
7. DoDD 3600.1. Information Operations. US DoD, 2013, 12 p.
8. Information Operations Primer: Fundamentals of Information Operations. U.S. Army War College, 2011, 204 p.
9. JP 3-13. Information Operations. US Joint Chiefs of Staff, 2012. 69 p.
10. JP 3-13.1. Electronic Warfare. US Joint Chiefs of Staff, 2007. 115 p.
11. Standart ISO/IEC 27032:2012. Informatsionnye tekhnologii. Metody obespecheniia bezopasnosti. Rukovodiashchie ukazaniia po obespecheniiu kiberbezopasnosti. 2012.
12. Standart ITU-T X.1205:2008. Obzor kiberbezopasnosti. 2008. – Zheneva: MSE-T, 2008. – 162 p. – URL: www.itu.int/ITU-T (data dostupa 20.01.2014).
13. Bezopasnost' v elektrosviazi i informatsionnykh tekhnologiiakh. Obzor soderzhaniia i primeneniia deistvuiushchikh Rekomendatsii MSE-T dlia obespecheniia zashchishchennoi elektrosviazi. – Zheneva: MSE-T, 2009. – 162 p. – URL: www.itu.int/ITU-T (data dostupa 20.01.2014).
14. Griniaev S.N. Pole bitvy - kiberprostranstvo. Teoriia, priemy, sredstva, metody i sistemy vedeniia informatsionnoi voiny. – M.: Kharvest, 2004. – 426 p.
15. Rastorguev S.P. Informatsionnaia voina. – M: Radio i sviaz', 1999. – 416 p.
16. Pocheptsov G.G. Informatsionnye voiny. – M.: Refl-buk, K.: Vakler, 2000. – 576 p.
17. Zhukov V. Vzgliady voennogo rukovodstva SShA na vedenie informatsionnoi voiny. Zarubezhnoe voennoe obozrenie. No 1 2001. - URL: http://pentagonus.ru/publ/22-1-0-175
18. Kunnakova N.L. Informatsionnaia voina kak ob»ekt nauchnogo analiza. Al'manakh sovremennoi nauki i obrazovaniia, No 6 (61), 2012. – pp 93-96.
19. Antonovich P.I., Sharavov I.V., Loiko V.V. Sushchnost' operatsii v kiberneticheskom prostranstve i ikh rol' v dostizhenii informatsionnogo prevoskhodstva. Vestnik Akademii voennykh nauk. No 1 (38). 2012. pp. 41-45.
20. Antonovich P.I. Izmenenie vzgliadov na informatsionnoe protivoborstvo na sovremennom etape. Vestnik Akademii voennykh nauk. No 1 (34). 2011. pp. 43-47.
21. Antonovich P.I. O sovremennom ponimanii termina «kibervoina». Vestnik Akademii voennykh nauk. No 2 (35). 2011. pp. 89-96.
22. Antonovich P.I. O sushchnosti i soderzhanii kibervoiny. Voennaia mysl'. No 7. 2011. pp. 39-46.
23. Borodakii Iu.V., Dobrodeev A.Iu., Butusov I.V. Kiberbezopasnost' kak osnovnoi faktor natsional'noi i mezhdunarodnoi bezopasnosti XXI veka (Chast' 1). Voprosy kiberbezopasnosti. No 1 (1). 2013. pp. 2-9.
24. Zubarev I.V., Zhidkov I.V., Kadushkin I.V. Kiberbezopasnost' avtomatizirovannykh sistem upravleniia voennogo naznacheniia. Voprosy kiberbezopasnosti. No 1 (1). 2013. pp. 10-16.
25. Makarenko S. I. Problemy i perspektivy primeneniia kiberneticheskogo oruzhiia v sovremennoi setetsentricheskoi voine. Spetstekhnika i sviaz'. No 3. 2011. pp. 41-47. - URL: http://www.st-s.su/sites/default/files/files/pdf/2011-03/2011-03-makarenko.pdf.
26. Makarenko S. I. Informatsionnaia bezopasnost': uchebnoe posobie dlia studentov vuzov. – Stavropol': SF MGGU im. M.A. Sholokhova, 2009. – 372 p.