ПОСТРОЕНИЕ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ УПРАВЛЕНИЯ СИЛ БЫСТРОГО РЕАГИРОВАНИЯ

Евсеев *Сергей* Петрович,
Дорохов *Александр* Васильевич,
Король *Ольга* Григорьевна,
Украина, Харьков,
Харьковский национальный экономический университет,
кафедра информационных систем

DOI: 10.2298/vojtehg1202071E

ОБЛАСТ: компьютерные науки, криптография
ВИД СТАТЬИ: оригинальная научная работа

Краткое содержание:

Анализируются новые подходы (асимметричность и идиосинкритичность) к ведению боевых действий, вскрываются факторы, непосредственно влияющие на построение и особенности функционирования подсистемы защиты информации перспективной автоматизированной системы управления войсками. Исследуются возможные пути построения подсистем криптографической защиты информации в автоматизированной системе управления оперативной группировкой объединенных сил быстрого реагирования в условиях асимметричных и идиосинкритичных подходов к ведению боевых действий.

Ключевые слова: *криптографическая защита информации, автоматизированная система управления войсками.*

Введение

В последнее время ведущие мировые военные специалисты рассматривают вооруженные конфликты (локальные войны) как асимметричные, идиосинкритичные войны [1]. Появление новых форм и способов ведения вооруженной борьбы, высокая интенсивность изменения обстановки и динамика боевых действий, широкое применение средств вычислительной техники и компьютерных систем обуславливают высокие вероятностно-временные требования к показателям эффективности боевого управления и связи [1–4].

aleks.dorokhov@meta.ua

Evseev, S. P. et al, Construction of cryptographic information protection in automated control systems for rapid reaction military forces, pp. 71–83

В этих условиях построение подсистем защиты информации перспективной автоматизированной системы управления войсками (АСУВ) сопряжено со многими противоречивыми факторами, непосредственно влияющими на эффективность АСУВ в целом. Целью статьи является обоснование путей построения подсистем криптографической защиты информации в АСУ оперативной группировки объединенных сил быстрого реагирования.

Современные тенденции и изменения в средствах и способах вооруженной борьбы

Анализ боевых возможностей вооруженных сил ряда развитых государств и характера локальных военных конфликтов последнего времени позволяет выделить некоторые основополагающие тенденции и эволюционные изменениями в средствах и способах современной вооруженной борьбы.

Основными чертами таких изменений являются:

• практический отказ от широкомасштабной ядерной войны;

• ориентация на ведение вооруженной борьбы, прежде всего с использованием высокоточного обычного оружия и сохранением ядерных сил как средства сдерживания;

• повышенное внимание к локальным войнам и вооруженным конфликтам как наиболее возможным формам вооруженного столкновения государств;

• повышение роли начального периода войны, завоевание стратегической инициативы, а при благоприятных условиях – достижение основных военных целей вооруженной борьбы;

• рассмотрение в составе первоочередных объектов одновременного поражения массированными ракетно-авиационными ударами не только развернутых группировок вооруженных сил противника, но и важнейших центров государственного и военного управления, ключевых элементов экономической и военной инфраструктуры, районов формирования стратегических резервов и тому подобное;

• рост роли обычных средств вооруженной борьбы, возложение на некоторые из них функций сдерживания (для ядерных государств, как дополнение к ядерному сдерживанию);

• объединение усилий всех видов вооруженных сил по единому замыслу и плану, что является необходимым условием стратегического успеха, особенно на начальном этапе боевых действий;

• повышение внимания к защите от нападения с воздуха и космоса, как стратегической задачи вооруженных сил;

• повышение способности к быстрому перемещению на значительные расстояния больших группировок войск и их развертывание в кратчайшие сроки (стратегическая мобильность), появление в связи с этим в составе вооруженных сил таких функциональных элементов, как силы быстрого реагирования [2].

Асимметричность и идиосинкритичность, как новые подходы к ведению боевых действий

По мнению ведущих мировых военных специалистов, характер войн XXI столетия будет носить асимметричный и идиосинкритичный характер [1]. Под асимметричностью понимается нетрадиционное ведение боевых действий, разнообразие способов и форм ведения войны, которые предопределяют победу, отсутствие общего основания для сравнения, аспект возможностей, которые трудно сопоставить с накопленным войсками опытом.

Под идиосинкритичностью понимается специальный, нетрадиционный подход к использованию новых и (или) старых средств вооруженной борьбы. При этом важной составляющей начального этапа вооруженного конфликта (локальной войны) является нанесение главного удара в наиболее уязвимое место противника, что позволит сломить его волю к сопротивлению. Даже при наличии мощного интеллекта и реальных сил для ведения борьбы, противник, потеряв психологическую устойчивость, будет сломлен и побежден [1].

Ассиметричность и идиосинкритичность на начальном этапе вооруженного конфликта реализуется путем нанесения мощных ударов по стратегически важным объектам противника, что может деморализовать противоборствующую сторону и произвести эффект «опрокидывания» фронта с полным его разгромом.

Другим важным аспектом современных вооруженных конфликтов является стирание граней масштабности боевых действий. Фактически исчезают резкие грани между уровнями масштабности ведения боевых действий – тактических, оперативных, стратегических [5,8–10].

Тактика нередко влияет определяющим образом на оперативный и даже стратегический уровень. При этом для обеспечения асимметричности и идиосинкритичности проводится замена основных боевых единиц оперативно тактических группировок новыми компьютеризированными боевыми соединениями, использующими единую компьютерную сеть управления, увеличиваются огневые возможности боевых подразделений за счет введения новых образцов высокоточного оружия.

Анализ локальных войн показывает, что перед началом боевых действий создаются воздушно-космические и наземно-морские силы

Evseev, S. P. et al, Construction of cryptographic information protection in automated control systems for rapid reaction military forces, pp. 71–83

под единым командованием, которые, в зависимости от военной мощи противника, могут проводить двухфазную воздушно-космическую и наземную операции или однофазную наземную операцию [9, 10].

Анализируя первичные космические массированные ракетно-авиационные удары (КМРАУ), можно обобщить их типичный состав: от 600 до 1000 крылатых ракет морского и воздушного базирования и от 1200 до 1600 самолетов различного предназначения, из которых до 60% составляют ударные истребители, с поражением до до 1800–2800 целей. Так, общая численность при проведении КМРАУ в первые сутки может составлять от 1800 до 2600 самолетов (крылатых ракет воздушного, морского базирования, тактических ракет, оперативно-тактических ракет наземного базирования).

В состав наземной группировки на второй фазе, как правило, входят силы сухопутных войск до 4 армейских корпусов (16–20 дивизий), до 13–40 дивизионов палубной авиации, до 8 зенитно-ракетных дивизионов противовоздушной обороны, 1200–2000 танков; 400–1500 противотанковых ракетных комплексов; 650–2150 боевых машин пехоты, до единиц 1150 армейской авиации.

Очевидно, что характерной чертой военных операций ближайшего будущего будет возможность достижения их целей посредством проведения огневого поражения без вторжения группировки сухопутных войск на территорию противника. Такие операции будут представлять собой совокупность массированных, групповых и сосредоточенных ударов авиации, ракетных войск и артиллерии с использованием средств радиоэлектронной борьбы, автоматизированных систем управления, самонаведения оружия, разведки и анализа данных.

Таким образом, современные вооруженные конфликты характеризуются асимметричностью, идиосинкритичностью, внезапностью нанесения КМРАУ по стратегически важным объектам противника, широким использованием новейших образцов высокоточного оружия, авиации, крылатых ракет морского и воздушного базирования.

Анализ показывает, что при проведении КМРАУ в первые сутки общая численность средств поражения целей с воздуха может составлять от 1800 до 2800 единиц (самолетов, крылатых ракет воздушного, морского базирования, тактических ракет, оперативно-тактических ракет наземного базирования). При проведении наземной фазы наступательной операции на усиление выделяется от 300 до 400 самолетовылетов для каждого армейского корпуса.

Следовательно, при отражении нападения наземной группировки средствам разведки необходимо обнаружить от 10000 до 15000 наземных подвижных целей. При этом и воздушная, и наземная фазы наступления сопровождаются целенаправленными действиями частей и подразделений радиоэлектронной борьбы противника (РЭБ), навязыванием ложной информации с его стороны.

Поэтому для устойчивого, непрерывного, оперативного и скрытного управления силами и средствами активной компоненты объединенных сил быстрого реагирования (ОСБР) необходимо развернуть до 200 пунктов управления оперативно-тактического и тактического уровня. При этом перспективная АСУВ должна обеспечить доведение команд до подразделений в условиях резко возросших объемов обрабатываемых и передаваемых данных, активных действий подразделений РЭБ противника. Возникает необходимость проанализировать состояние и общие принципы построения системы управления и связи ОСБР.

Особенности построения АСУВ ОСБР

Отличительной особенностью построения систем боевого управления и связи является иерархическая централизованная структура, включающая подсистему принятия решений, которая распределена по нескольким подчиненным уровням, а информационные сообщения циркулируют по соответствующим направлениям и сетям связи [4,7,8].

Перспективная система управления и связи ОСБР, как совокупность взаимоувязанных и согласованных по задачам, месту, времени действий пунктов управления, узлов и линий связи различного назначения, развертываемых и создаваемых по единому плану, должна обеспечивать устойчивое, непрерывное, оперативное, скрытное управление объектами и решать следующие задачи:

- сбор, обработку, документирование и отображение информации об общей воздушной обстановке, оповещение подразделений о воздушной обстановке;
- сбор, обработку документирования и выдачу боевых распоряжений и донесений;
- сбор, обработку информации о наземной обстановке;
- поддержку процессов принятия решений лицами боевых дежурных смен;
- отображение обобщенной информации характеристик целей и боевых действий;
- управление подчиненными подразделениями;
- управление информационными потоками в пунктах • управления;
- передачу боевой и оперативной информации на пункты управления различных уровней, обеспечение информационного взаимодействия;
- обеспечение безопасности информационных и других ресурсов.

Для решения задач управления подчиненными силами и средствами разворачиваются автоматизированные командные пункты (АКП), способные функционировать в различных режимах: боевом режиме, режиме боевого дежурства, режиме технического обслуживания [7,8].

Evseev, S. P. et al, Construction of cryptographic information protection in automated control systems for rapid reaction military forces, pp. 71–83

В боевом режиме АКП обеспечивают полномасштабное решение задач управления всеми подчиненными силами и средствами полной боевой сменой. В режиме боевого дежурства дежурной сменой АКП обеспечивается управление дежурными силами при приведении частей оперативной группировки в высшую степень боевой готовности, развертывание в предбоевые порядки и организацию боевого дежурства. В режиме технического обслуживания обеспечивается обслуживание основных аппаратных и программных средств системы для ее поддержания в работоспособном состоянии [4].

В рамках трехступенчатой системы оперативного управления (генеральный штаб, объединенное оперативное командование, межвидовые группировки), функционального и структурного совершенствования системы оперативного управления войсками целесообразным является создание органа управления межвидовой группировкой, объединенного оперативного командования (ООК).

В состав модульной автоматизированной системы управления на основе организационной структуры объединенного оперативного командования, функционального предназначения структурных составляющих ООК необходимо выделить ряд подсистем, реализующихся путем создания соответствующего программного обеспечения базовых модулей:

• информационно-справочный модуль, предназначенный для обеспечения планирования боевого применения подчиненных войск (сил), всестороннего обеспечения боевых действий, получения и обработки разведывательной информации;

• информационно-расчетный модуль динамического моделирования, предназначенный для проведения предварительных расчетов оценки боевых возможностей конкретного состава и определения ожидаемой эффективности боевых действий своих войск, моделирования возможных действий противника, оценки возможного нанесенного ущерба, выработки предложений для непосредственного управления войсками (силами);

• модуль отображения обстановки, предназначенный для выведения в режиме реального времени с различной детализацией и масштабом информации в зависимости от необходимого анализа обстановки;

• модуль коммутации, предназначенный для организации информационного обмена между АКП по действующим каналам связи, создания межрегиональных сетей управления и оповещения, а также для обеспечения информационного взаимодействия базовых комплектов аппаратуры, реализующих функции конкретного АКП.

Таким образом, перспективная АСУВ ОСБР должна обеспечивать автоматизацию процессов сбора, анализа и оценки данных обстановки, принятия решения, планирования, постановки и доведения задач до войск (сил), контроль за ходом их выполнения [4–6,9,10]. При этом важным

направлением совершенствования АСУВ является разработка подсистемы защиты информации, предназначенной для обеспечения безопасности и достоверности обрабатываемых и передаваемых данных. В современных условиях основными объективно сложившимися факторами, резко усложнившими обеспечение безопасности и достоверности информации в системе управления ОСБР, следует считать [4,9,10]:

• асимметричность (разносторонность, непохожесть подходов) и идиосинкритичность (новые способы использования средств) ведения боевых действий возможным противником;

• резкое увеличение численности и разнообразия применяемых средств ведения вооруженной борьбы, прежде всего во время проведения КМРАУ и ведения наземной фазы операции;

• высокую интенсивность и динамику изменения обстановки в условиях современной высокотехнологичной войны;

• широкое применение средств информационного и радиоэлектронного воздействия и другие.

Проведенный анализ показал, что современные вероятностно-временные требования к перспективным средствам защиты информации существенно возросли [4,7,8]. Это обусловлено наличием следующих объективно сложившихся противоречивых факторов:

• резким увеличением объемов обрабатываемых и передаваемых данных в современных системах управления и связи;

• развитием современной вычислительной техники и компьютерных систем, их широкой доступностью;

• появлением новых форм и способов обработки информации, в том числе, технологий распределенных вычислений и вычислений в облаках, их широкой доступностью;

• развитием методов криптографического анализа, появлением новейших технологий несанкционированного доступа к информации, возникновением новых угроз конфиденциальности, целостности, аутентичности и доступности.

Таким образом, появление новых методов криптоанализа в совокупности с возможностями современной вычислительной техники, новыми формами и способами обработки информации выдвигают повышенные требования к стойкости криптографических средств защиты информации. Повышение объемов обрабатываемой и передаваемой информации в системах управления и связи также выдвигает повышенные требования к быстродействию криптографических средств защиты информации.

Резкое обострение объективно сложившихся противоречивых факторов ведет к стремительному повышению вероятностно-временных требований, предъявляемых к перспективным криптографическим средствам защиты информации, которые должны обеспечивать:

• быстрое (10–100 Мбит/с) криптографическое преобразование больших объемов данных с возможностью частой смены ключевых данных;

• высокий уровень стойкости к современным методам криптоанализа (безопасное время $T_Б$ > 100–200 лет, вероятность вскрытия ключевых данных и вероятность бесключевого чтения $P_К$, $P_И < 10^{-25}$–10^{-30}), теоретически хорошо обоснованную модель безопасности информации;

• комплексное обеспечение безопасности и достоверности (вероятность ошибки $P_{ош}<10^{-9}$) информации в системах управления и связи специального назначения.

Учитывая изложенное, рассмотрим возможности существующих средств защиты по обеспечению требуемых показателей безопасности информации в перспективной АСУВ ОСБР.

Анализируя возможностей существующих средств защиты информации следует подчеркнуть, что традиционно решение задач обеспечения безопасности информации возлагается на засекречивающую аппаратуру связи (ЗАС).

В настоящее время на вооружении в подразделениях связи видов вооруженных сил стоят как аналоговые, так и цифровые ЗАС. Большинство типов ЗАС обеспечивает засекречивание только определенного вида информации с небольшой скоростью передачи и не имеет защиты от навязывания ложной информации. В то же время, в современных условиях остро стоит вопрос обеспечения конфиденциальности, целостности и аутентичности при передаче предварительных боевых распоряжений, начиная с первых часов возможного военного конфликта, а нередко – еще до его начала.

Построение подсистем криптографической защиты информации в современных АСУВ

Проведенный анализ показал, что в условиях резкого обострения объективно сложившихся негативных факторов эффективное функционирование подсистемы защиты информации перспективной АСУ ОСБР сопряжено с частой сменой ключевых данных, реализацией быстрого криптографического преобразования с обеспечением требуемых показателей безопасности и достоверности информации.

Следуя основным теоретическим положениям современной криптографии, требуемые параметры функционирования подсистем защиты информации в системах управления и связи специального назначения можно реализовать путем применения симметричных криптоалгоритмов в сочетании с несимметричными протоколами распространения секретных ключевых данных [4].

Использование симметричных криптоалгоритмов позволяет реализовать быстрое криптографическое преобразование больших

объемов данных. В то же время, это направление сопряжено со следующими существенными недостатками:

• несимметричные протоколы обмена ключами подразумевают самостоятельное формирование частей секретного ключа двумя различными абонентами, что нарушает принцип централизованного управления и распространения ключей;

• использование несимметричных протоколов обмена ключами подразумевает формирование общего ключа для двух абонентов; при формировании секретного ключа совместно с другими абонентами соответствующие секретные ключи будут различны, что делает невозможным организацию управления и связи в циркулярном режиме, а это в свою очередь затрудняет своевременное управление подчиненными объектами и, в конечном счете, ведет к снижению непрерывности и оперативности управления;

• использование несимметричных протоколов обмена ключами подразумевает применение криптоалгоритмов, сложность реализации которых на 3–5 порядков превосходит сложность реализации классических (симметричных) криптоалгоритмов, что в условиях частой смены ключевых данных может привести к значительным задержкам в управлении.

Решение возможно также путем применения несимметричных алгоритмов шифрования. В этом случае один (общий для группы абонентов ключ) распространяется по открытым каналам связи, и нет необходимости поочередного выполнения алгоритмов распространения секретных ключевых данных с каждым абонентом информационного обмена в отдельности. В то же время, этот подход связан со следующими существенными недостатками:

• сложность реализации существующих алгоритмов несимметричного шифрования существенно (на 3-5 порядков) выше по сравнению с симметричными криптоалгоритмами, что в условиях стремительного увеличения объемов обрабатываемых и передаваемых данных и повышения вероятностно-временных требований к безопасности и достоверности информации недопустимо;

• применение существующих несимметричных протоколов обмена секретными сообщениями с использованием открытых ключей приводит к значительному (в 2–4 раза) увеличению избыточности передаваемых данных, что существенно снижает эффективность связи.

Таким образом, существующие классические подходы к построению подсистем обмена секретными сообщениями не позволяют на сегодняшний день в полной мере обеспечить выполнение современных требований безопасности информации в системах управления и связи специального назначения.

Возникает противоречие между резко возросшими объемами обрабатываемых и передаваемых данных, повышением вероятност-

но-временных требований к безопасности и достоверности информации при частой смене ключевых данных и существующими подходами теории защиты информации к построению подсистем обмена секретными сообщениями.

Применяемый математический аппарат криптографического преобразования данных не позволяет в полной мере обеспечить эффективную защиту информации в системах управления и связи специального назначения. Перспективным направлением в разрешении выявленного противоречия являются криптографические средства защиты информации, построенные с использованием алгебраических блоковых кодов [4,9,10]. Фактически, речь идет о построении средств защиты информации, основанных на специальных режимах функционирования аппаратуры канального кодирования. Их применение позволяет:

• реализовать быстрые криптографические преобразования больших объемов данных с использованием открытых ключей, что с одной стороны не требует распространения секретных ключевых данных по закрытым каналам связи, а с другой стороны – не требует усложнения существующей аппаратуры передачи данных;

• обеспечить высокий уровень стойкости к современным методам криптоанализа за счет сведения задачи бесключевого чтения к решению теоретико-сложностной задачи декодирования случайного кода при обеспечении доказуемой стойкости криптографических средств защиты информации;

• строить интегрированные механизмы канального кодирования и криптографического преобразования данных, что позволяет комплексно решать задачи обеспечения безопасности и достоверности информации в системах управления и связи специального назначения.

Таким образом, решение важной научно-технической проблемы, состоящей в разработке теоретических основ построения быстрых криптографических преобразований доказуемой стойкости с использованием алгебраических блоковых кодов и создания на их основе криптографических средств защиты информации с использованием открытых ключей, является актуальным.

Решение указанной проблемы имеет важное значение как для развития теории защиты информации, так и для решения прикладных вопросов обеспечения безопасности и достоверности информации в перспективной АСУВ ОСБР.

Заключение

Таким образом, в современных условиях требования к системам управления и связи резко возросли. Перспективная АСУВ должна обеспечить доведение сигналов и команд до адресатов в условиях

резко возросших объемов обрабатываемых и передаваемых данных, активных действий частей и подразделений РЭБ противника. Поэтому важным направлением совершенствования АСУВ является разработка эффективных подсистем защиты информации.

При этом стоящие на вооружении средства защиты информации на сегодняшний день морально и физически устарели и не обеспечивают выполнение современных требований по обеспечению ее безопасности и достоверности. Однако существующие классические подходы к построению подсистем обмена секретными сообщениями не позволяют в полной мере обеспечить выполнение современных требований.

Поэтому перспективным направлением в разрешении выявленного противоречия являются криптографические средства защиты информации, построенные с использованием алгебраических блоковых кодов. Их применение позволяет строить быстрые криптографические преобразования доказуемой стойкости и создавать на их основе средства защиты информации с использованием открытых ключей. Решение указанной проблемы имеет важное значение как для развития общей теории защиты информации, так и для решения прикладных вопросов обеспечения безопасности и достоверности информации в перспективных АСУВ.

Литература/References

[1] Montgomeri, M., *The era of strategic asymmetry,* Independent Military Review*,* 37/2002, pp. 3–12*.*

[2] Gorodnov, V. P., Drobaha, G. A., Ermošin, M. O., Tkačenko, V. I., *Simulation of fighting air defense forces and information management processes of its (theory, practice and history),* HVU, Harkov, 2004.

[3] Bereza, A*. S., System integrators basis for the development of ASM,* HVU, Harkov, 1996.

[4] Evseev, S. P., Dorokhov, O. V., Korol, O. G., *Mechanisms of protection of information in computer networks and systems,* Military Technical Courier/Vojnotehnički glasnik, Vol. 59, No. 4, pp. 15–39, Ministry of Defence of the Republic of Serbia, Belgrade, 2011.

[5] *Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity and Encryption,* 2004.

[6] Salomaa A., *Cryptography with open keys*, Mir, Moskva, 1995.

[7] Kuznecov, A. A., Evseev, S. P., *The development of theoretical coding schemes using elliptic codes*, Information processing systems, 5/2004, pp. 127–132.

[8] Kuznecov, O. O., Evseєv, S.P., Kavun, S. V., Information security and economic security of the enterprise, HNUE, Harkiv, 2008.

[9] Palьčik, M., *Conceptual foundations of a model of the Armed Forces of Ukraine in 2010,* Science and Defence*,* 1/2009, pp. 6–14.

[10] White paper*, 2006., Ukraine defence Policy,* MoD of Ukraine, Kiev, 2006.

CONSTRUCTION OF CRYPTOGRAPHIC INFORMATION PROTECTION IN AUTOMATED CONTROL SYSTEMS FOR RAPID REACTION MILITARY FORCES

Evseev Sergey Petrovich, Dorokhov Oleksandr Vasilievich,
Korol Olga Grigorievna, Kharkov National University of Economics,
Faculty of Economics Informatics, Ukraine

FIELD: Computer Sciences, Cryptography
ARTICLE TYPE: Original Scientific Paper

Summary

New approaches to realizations of military operations are analyzed. The main factors that directly affect the construction and operation of information security subsystems in prospective automated command and control military systems are described. Possible ways of the construction of cryptographic subsystems of information protection in automated operation management systems for united military force groups are investigated.

Introduction

New forms of warfare, high dynamics of combat operations, and the use of computers result in the growth of performance requirements in combat control and communications. Especially important is the protection of information in automated systems for command and control.

Characteristics of modern military conflicts

The features of modern military conflicts are: absence of a large-scale nuclear war; focus on precise conventional weapons with a nuclear one as a deterrent; increased role of the initial period of war; primary lesion of centers of state and military governance, infrastructure, reserves; increased attention to the protection against attacks from the air and space; and high speed of movement of troops and their mobility.

New approaches to the conduct of military operations

It should be noted that the main attacks occur on strategically important objects, blurring the scale of the fight - tactical, operational, and strategic one. Air forces are widely used as well as primary massive missile and air strikes without the invasion of ground troops into the enemy territory.

It is necessary to transmit signals and commands to military units within increased mass of transmitted data and during enemy actions.

Features of military automated control and communication systems

These systems must be able to solve the problems of collection, processing, and displaying information on a combat situation, thus offering support for decision making by commanders at various levels.

They are composed of some basic modules: data bases; calculation tools for dynamic modeling and assessment of combat capabilities, expected enemy action; mapping of the situation; information management and communication units.

Information protection, security and reliability of processed and transmitted data are important as well.

They are made difficult due to the increase of the number and diversity of warfare means and data mass; dynamic changes of the situation; intensive use of information and electronic effect technologies; development of cryptographic analysis methods as well as new technologies of unauthorized access to information for violation of their confidentiality, integrity, authenticity and accessibility.

Therefore, requirements for cryptographic protection of information are intensified. Traditionally, the security of information is provided by equipment for secret communications. However, this works only with certain types of information and with insufficient transmission speed, without protection from false information.

Construction of subsystems for the cryptographic protection of information

Data protection involves frequent changes of key data and the implementation of cryptographic transformations. They can be implemented using symmetric cryptographic algorithms combined with asymmetric distribution of secret protocols of key data. However, this direction is associated with major drawbacks.

It is also possible to use asymmetric encryption algorithms. In this case, a common group key is distributed through open communication channels. There is no distribution of secret key data to each subscriber individually. However, this approach has several drawbacks.

The existing approaches to secret exchange of messages and mathematical tools for cryptographic transformation of data cannot thus fully ensure the security of information management systems and communications for special purposes.

A prospective solution of this problem can be found in a cryptographic information protection means which uses algebraic block codes, based on special modes of operation of equipment channel coding.

It allows the implementation of fast cryptographic transformations of large volumes of data using open public keys. What is more, it does not require the distribution of secret key data through special telecommunication channels. In addition, it does not require the complexity of the existing equipment of data transmission.

It also provides a high level of resistance to modern methods of cryptanalysis by reducing the keyless read problem to a solution of the theoretic complexity problem of decoding a random code with provable security strength of cryptographic information protection.

Conclusions

The requirements for military control and communication systems are dramatically increased now. An important problem is the protection and safety of information in them. A prospective solution for this purpose is to protect information using algebraic block codes.

Key words: *cryptographic information protection, automated command control and communication military systems, algebraic block codes.*

Datum prijema članka: 24. 11. 2011.
Datum dostavljanja ispravki rukopisa: 26. 12. 2011.
Datum konačnog prihvatanja članka za objavljivanje: 27. 12. 2011.