DOI 10.37882/2223–2966.2022.06–2.22

СОДЕРЖАТЕЛЬНОЕ ОПИСАНИЕ МОДЕЛИ КОНФЛИКТА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ В КИБЕРПРОСТРАНСТВЕ

A MEANINGFUL DESCRIPTION OF THE CONFLICT MODEL OF SPECIAL-PURPOSE INFORMATION AND TELECOMMUNICATION SYSTEMS IN CYBERSPACE

K. Lukin
A. Sagdeev
I. Staheev
O. Titova

Summary. A meaningful description of the model of the antagonistic conflict arising in cyberspace during the mutual confrontation of special-purpose information and telecommunication systems, each of which has its own strategy for achieving the goal, is carried out.

Keywords: information and telecommunication system, cyberspace, information warfare, combat cybernetic system.

Лукин Константин Игоревич
К.т.н., генеральный директор, ОАО «Супертел», Санкт-Петербург
ki@supertel.ru
Сагдеев Александр Константинович
К.т.н., доцент, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
brother-aks@yandex.ru
Стахеев Иван Геннадиевич
К.т.н., доцент, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
kisasig@yandex.ru
Титова Ольга Викторовна
К.т.н., доцент, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
olga1110.spb@mail.ru

Аннотация. Осуществлено содержательное описание модели антогонистического конфликта, возникающего в киберпростанстве при взаимном противоборстве информационно-телекоммуникационных систем специального назначения, каждая из которых имеет свою стратегию достижения цели.

Ключевые слова: информационно-телекоммуникационная система, киберпространство, информационное противоборство, боевая кибернетическая система.

Боевая кибернетическая система (БКС) представляет собой объединенную целью совокупность элементов управления, добывания информации и исполнения, предназначенную для обеспечения конфликтно-устойчивых действий пространственно-распределенной ИТКС СН в динамике различного уровня конфликтов. Обеспечивающие действия, основная форма применения БКС в целях выполнения комплекса мероприятий, направленных на поддержание высокой боевой готовности, устойчивости, разведзащищенности, доступности и управляемости ИТКС СН, создание благоприятных условий для организованного и своевременного выполнения возложенных задач по обмену всеми видами информации между органами военного управления, а также на предупреждение и воспрещение внезапного нападения противника, снижение эффективности его ударов. [1] В качестве её элементов возможно рассмотрение различного рода систем (средств, комплексов) защиты информации и реализации информационно-технических воздействий. Информационно-техническое воздействие — комплекс мероприятий, направленных на дезорганизацию или полное прекращение (нарушение, срыв, вывод из строя) функционирования информационно-технических объектов. Информационно-техническое воздействие подразделяется на программное (программно-аппаратное), радиоэлектронное и другие виды воздействий. [2]

Программное воздействие (ПВ) (программно-аппаратное (ПАВ)) — комплекс организационно-технических мероприятий, проводимых с преодолением систем защиты информационных (локальных, локально распределенных, распределенных) вычислительных сетей и автономных программных комплексов с целью

дезорганизации функционирования информационных (вычислительных) сетей (глобальных, региональных, локальных), автономных вычислительных комплексов (электронно-вычислительных машин, персональных компьютеров и др.) программно-управляемых устройств (модулей, блоков, накопителей информаций и др.), электронно-программных продуктов (операционных систем, прикладных программ и др.), технических средств приёма, передачи и обработки информации, организуемый и осуществляемый с целью нарушения их штатных режимов функционирования или свойств безопасности информации (добывания, разрушения, уничтожения или искажения информации).

Программное воздействие осуществляется с использованием преднамеренно созданных и определенным образом сконфигурированных специализированных вредоносных программных средств (компьютерных вирусов, программ-сканеров, программных закладок, программ удаленного управления информационно-телекоммуникационными системами и др.), предназначенных для нарушения работы информационных систем противника и свойств безопасности информации, обрабатываемой в этих системах.

Аппаратное воздействие осуществляется скрытой установкой технических устройств контроля функционирования информационно-технических объектов и информации, циркулирующей в них, а также аппаратных закладок, предназначенных для нарушения работы информационных систем критически важных информационно-технических объектов (КВИТО) противника и свойств безопасности информации, обрабатываемой в этих системах, а также специальные средства проникновения в информационные системы КВИТО противника.

Для общности средства ПВ/ПАВ в дальнейшем будем именовать исполнительными элементами (ИЭ).

Защита от ПАВ — комплекс организационно-технических мероприятий по предотвращению, выявлению, срыву, нейтрализации, ослаблению программно-аппаратного воздействия противоборствующей стороны на информационно-технические объекты.

Радиоэлектронное воздействие осуществляется посредством радио-, оптико-электронного, гидроакустического и иного подавления, а также поражения электромагнитным излучением информационно-технических объектов.

Обоснование облика БКС основывается на результатах оценки эффективности в антагонистических конфликтах уровня БКС {К} — БКС {С} (система «красные» и система «синие»). В настоящее время в теории сложных систем преимущественное внимание уделяется развитию методов анализа, направленных на разрешение конфликтов, связанных с неопределенностью: [3]

а) знания исходной информации о целях, задачах, функциях, ресурсах, типах и ТТХ средств, а также внешних условий применения;

б) вопросов развития методов оценки эффективности технических систем (ТС) на конечном интервале в условиях детерминированных способов противодействия, оставляя в стороне задачи их применения в условиях стохастического конфликта иерархических организационно-технических систем (ОТС). На практике разработано и используется значительное число методов оценки эффективности, разработанных для конкретных типов ТС, функционирование которых осуществляется применительно к первым двум типам конфликтов. Требования же обеспечения функционирования ОТС в условиях динамического стохастического конечного конфликта с последействием делают невозможным в полной мере воспользоваться данными методами (принципами, постановками и подходами к решению задач, используемых математических методов) и обусловливают необходимость их теоретического обобщения и дальнейшего методологического развития применительно к новому специфическому классу исследуемых объектов — БКС. Исходя из этого, предлагается метод обоснования оперативно-технических требований к ИТКС СН посредством оценки «внешней» и «внутренней» эффективности ее БКС, под которым понимается взаимообусловленная совокупность принципов и научных подходов, раскрывающих общее содержание, состав и структуру постановки задачи оценки эффективности БКС, способов и моделей её решения.

Их разработка наталкивается на ряд специфических особенностей, связанных с организованным противодействием (функционированием подсистем наступательных и оборонительных действий (ПНД, ПОД) БКС ИТКС СН — С при решении задач снижения эффективности действий ИТКС СН — К.

1. Применение ИТКС СН осуществляется в режимах централизованного, децентрализованного или автономного управления на основе взаимосвязанной по цели, задачам, месту, времени и ресурсу совокупности организационных, организационно-технических и технических методов, мероприятий или средств, комплексов и подсистем, направленных на выполнение с заданной эффективностью поставленных задач по передаче информации независимо от различного рода внешних возмущающих воздействий. [4]

Достижение целей ИТКС СН осуществляется, в том числе, проведением ее БКС различного рода действий (акций) в виде совокупности одиночных, групповых и массированных действий (ОД, ГД и МД) для активного подавления (снижения эффективности функционирования) или воздействия ИЭ на элементы ИТКС СН — С и ее БКС. Это достигается распределением ИТКС СН ограниченного ресурса ИЭ (в том числе и ресурса ИЭ старшей инстанции, взаимодействующих систем) для парирования эффективности действий БКС {С} и выполнения с заданной эффективностью поставленных задач. Исходя из этого, процесс конфликтного функционирования ИТКС СН представляется в виде взаимообусловленного обмена совокупностью ОД, ГД и МД их БКС на основе оптимального распределения имеющегося ресурса реализации ПАВ и защиты от ПАВ противоборствующей стороны.

Выполнение ИТКС СН задач в условиях конфликта в киберпространстве сопряжено с преодолением ИЭ пространственно-распределенной эшелонированной ПОД БКС {С} в определенном районе (зоне, сегменте), основу которой составляет множество различных организационных, организационно-технических, технических (аппаратных) и программных способов или средств, комплексов и подсистем противодействия (для общности, оборонительных элементов — ОБЭ), отличающихся друг от друга назначением, алгоритмами и эффективностью применения. [5] Применение ОБЭ основывается на использовании в их составе различного типа, количества, эффективности и условий применения (уровня ЭМВОС, возможности размещения на средствах информационно-телекоммуникационной инфраструктуры (ИТКИ), времени, технических характеристик, наличия информационных средств (систем) (ИС) для обнаружения, распознавания ИЭ, целераспределения средств нейтрализации ИЭ и т.п.) средств и/или способов противодействия (СП). Наличие большой номенклатуры ОБЭ (а, соответственно, в их составе и СП) позволяет БКС {С}, исходя из пространственно-временных параметров способов применения ИЭ, осуществлять оптимизацию стратегий своего поведения на основе целераспределения имеющегося ресурса ОБЭ по возможным рубежам противодействия.

Исходя из топологического построения ПОД, БКС {С} при отражении ИЭ в МД может функционировать в режиме централизованного управления, ГД — в режиме децентрализованного управления и при отражении ОД — автономного управления. При отражении МД БКС {К} ПОД БКС {С} осуществляет целераспределение ресурса ОБЭ для защиты групп объектов в районе (зоне, сегменте) действий. При отражении же ГД БКС {К} ПОД БКС {С} реализует оптимальное распределение ресурса ОБЭ для снижения эффективности групп ИЭ с последующей нейтрализацией (обслуживанием) каждого ИЭ. После этого процесс преодоления ИЭ ПОД БКС {С} представляется в виде совокупности последовательно или параллельно проводимых ОД.

Принятие решений в подсистемах наступательных и оборонительных действий БКС {С} сопряжено с получением, обработкой и анализом данных от различного типа ИС, объединенных единством цели в пространственно-распределенные информационно-управляющие системы (ИУС) добывания информации и управления ИЭ и ОБЭ. В этих условиях выполнение задач ИТКС СН — К может обеспечиваться ее БКС за счет разрушения и/или снижения эффективности обработки информации в иерархических контурах принятия решений ИТКС СН — С и ее БКС за счет подавления наиболее важных элементов и/или информационно-технического воздействия на их ИС для снижения эффективности её функционирования до некоторого минимального уровня.

В этих условиях методологические основы исследования эффективности БКС в условиях конфликта ИТКС СН противоборствующих сторон должны удовлетворять основным требованиям к принципам, составу, структуре и содержанию моделирования: [6]

- соответствие показателя эффективности (ПЭ) применения БКС действиям ИТКС СН, основным из которых является сохранение (не ниже заданного) среднего количества работоспособных элементов и объектов ИТКС СН от воздействия ПНД противостоящей стороны в конфликте;
- соответствие иерархической декомпозиции целевых ПЭ, вытекающих из содержания выполняемых задач БКС, структурной декомпозиции характеристик конфликта уровня сценариев, эпизодов, ситуаций и дуэлей, а также возможность агрегатирования частных ПЭ от уровня дуэлей до уровня сценариев на основе преобразования в интегральный показатель эффективности функционирования ИТКС СН в соответствии со структурой ОТТ к БКС;
- обеспечение структурно-обоснованного взаимодействия целевого (между ИТКС СН) и информационного (между БКС) конфликтов, обеспечивающего последовательное иерархическое обоснование частных ОТТ к элементам и БКС в целом;
- учет межуровневых взаимосвязей ПЭ, исходных данных и ограничений, возникающих в конфликте нижних уровней с верхними, обеспечивающих приращение эффективности как по уровням иерархии, так и во времени.

Рассмотрим принципы моделирования БКС.

а) информационный конфликт рассматривается в рамках структуры целевого конфликта;
б) информационный конфликт элементов БКС является симметричным, а действия сторон — ассиметричными;
в) внутренне содержание конфликта определяется номенклатурой способов и средств реализующих управление, добывание информации, наступательные и оборонительные действия.

Оценка эффективности БКС проводится по основному критерию — эффективности ИТКС СН в условиях ограничений на техническую, технологическую и экономическую эффективность и неопределенности:
а) цели и задач, стоящих перед ИТКС СН — С;
б) способов развязывания, продолжительности ведения и окончания конфликта.

Это затрудняет разработку сценариев стратегий действий ИТКС СН, функционирующих в интересах противоборствующих органов военного (государственного) управления, а рассмотрение конфликтов на уровне ситуаций и эпизодов не отражает как внешних, так и внутренних условий и противоречий конфликта на уровне сценария.

Основным способом разрешения данных противоречий является проведение детального анализа порядка синтеза БКС, краткосрочный (среднесрочный) прогноз развития ИТКС СН противоборствующих сторон, а также способов развязывания и продолжительности ведения информационного противоборства в киберпространстве. Последняя задача по сложности определения целевой функции является проблемной вследствие отсутствия объективной информации о текущих процессах снижения эффективности противоборствующих ИТКС СН, тем более на упреждающий период прогноза. Исходя из этого, целесообразно рассматривать обобщенную структуру различных типов конфликтов и возможные способы их развязывания и ведения по интегральным ПЭ применения ИТКС СН, базирующихся на принципе гарантированного результата.

Весь процесс синтеза структурируется по этапам применения БКС в конфликтах уровня сценариев, эпизодов, ситуаций и дуэлей. Из него следует единое многоцелевое и многоуровневое их соответствие (например, сценарии — совокупность частных эпизодов; совершаемых последовательно или ассиметрично в пространстве и во времени, эпизоды — совокупность частных ситуаций; и т.д.). Оценки на частных этапах конфликта агрегатируются, вследствие чего необходима структуризация внутренних процессов конфликта на основе выделения, в нем особых («узловых») состояний, обеспечивающих дискретный иерархический характер взаимодействий в конфликте.

Основными принципами, реализующими совокупность требований к методам исследования эффективности применения БКС являются:
- принцип развития, как основы разработки методов оценки эффективности БКС, предполагающий адекватное наращивание их вычислительных возможностей в соответствии с нарастающей структурной сложностью конфликта;
- принцип условной математической адекватности методов оценки эффективности реальным процессам, протекающих в моделируемых БКС;
- принцип гомотопической инвариантности, предполагающий, иерархическое преобразование и выбор значений частных ПЭ для множества стратегий поведения БКС в динамике конфликта;
- принцип учета межуровневых взаимосвязей по управлению, информации и взаимодействию элементов в структуре общей модели оценки эффективности БКС с учетом динамических ресурсных, пространственных и временных ограничений;
- принцип временного баланса, предполагающий учет динамического изменения состояния элементов ИТКС СН — С под воздействием различных ИЭ противника в особых («узловых») состояниях. [7]

Основные допущения при построении методов оценки эффективности БКС.
1. Процесс воздействия БКС на эффективность применения ИТКС СН — С является динамическим, отражающим особенности конфликта противодействующих сторон;
2. Процесс воздействия БКС по количеству взаимодействий является ветвящимся временным процессом и может быть представлен, исходя из протекающих физических процессов в иерархических контурах принятия решений на основе методов логико-вероятностного математического моделирования. При этом простейшие конфликтные взаимодействия на нижних уровнях принятия решений возможно заменить аналитическими зависимостями расчета частных ПЭ, полученных по результатам математического моделирования.
3. При разработке методов оценки результатов конфликта предполагается, что применительно к прогнозируемым, условиям процесс функционирования ИТКС СН является условно стационарным. Такое допущение возможно, поскольку математические методы, предназначены для исследования стохастического процесса и его случайных состояний (событий) в «среднем» на основе использования его статистических характеристик — математического ожидания и дисперсии.

4. Так как в конфликте применяется множество элементов, размерности $m \times n$, где m и $n >> 1$, то по теореме Стьюдента стационарный процесс с вероятностью не ниже 0,97 при m и $n > 10$ гарантированно сходится к эргодическому. [8]

Исходя из этого, структуру методологических основ исследования эффективности БКС возможно представить в виде иерархической системы математических моделей и способов оценки эффективности средств и способов информационного противоборства в киберпространстве, которые по сложности построения и возможности оценки эффективности физических процессов возможно рассмотреть на различных уровнях конфликта и различной его интенсивности.

ЛИТЕРАТУРА

1. Сагдеев А.К., Чукариков А.Г. Обоснование оперативно-технических требований к информационно-телекоммуникационным сетям специального назначения, функционирующих с использованием ресурсов ЕСЭ РФ, в условиях конфликта в киберпространстве // Труды учебных заведений связи: сб. науч. ст. том 2 № 4/ под ред. С.В. Бачевского, М.В. Буйневич, Е.А. Аникевич — СПб.: Санкт-Петербургский университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2016.— 103 с. С. 99–103.
2. Сагдеев А.К., Сидоренко Е.Н., Суюндукова А.А., Тихомиров Д.А. Применение теории игр для исследования радиоэлектронного конфликта // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научнотехническая и научно-методическая конференция; сб. науч. ст. в 4 т. / Под. ред. С.В. Бачевского; сост. А.Г. Владыко, Е.А. Аникевич. СПб.: СПбГУТ, 2019. Т. 4. 708 с. С. 518–521.
3. Кощеев А.В., Лашин Ю.Ф., Сагдеев А.К., Халепа С.Л. Вопросы конфликтологии в системах военного назначения // Научно-практический журнал. Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки № 1–2 2022. С. 27–31.
4. Горбачева М.А., Сагдеев А.К. Проблемы обеспечения защищенности инфотелеком-муникационной сети военного назначения при ведении информационной войны // Труды Северо-Кавказского филиала Московского технического университета связи и информатики, часть I.— Ростов-на-Дону.: ПЦ «Университет» СКФ МТУСИ, 2015, 552с. С. 426–429.
5. Лепешкин М.О., Лепешкин О.М., Сагдеев А.К. Анализ возможности реализации ролевого разграничения доступом в системах государственного управления // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 3 т./ под ред. С.В. Бачевского, сост. А.Г. Владыко, Е.А. Аникевич, Л.М. Минаков.— СПб.: Санкт-Петербургский университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2016.— 550 с. С. 290–294.
6. Лепешкин М.О., Лепешкин О.М., Сагдеев А.К. Методологический подход оценки функциональной безопасности критической социотехнической информационной системы // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 3 т./ под ред. С.В. Бачевского, сост. А.Г. Владыко, Е.А. Аникевич, Л.М. Минаков.— СПб.: Санкт-Петербургский университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2016.— 550 с. С. 294–299.
7. Дробяскин А.Н., Сагдеев А.К., Сидоренко Е.Н., Янбулатова К.И. Модель воздействия технической компьютерной разведки и деструктивных программных воздействий на информационно-телекоммуникационную сеть военного назначения // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. / Под. ред. С.В. Бачевского; сост. А.Г. Владыко, Е.А. Аникевич. СПб.: СПбГУТ, 2020. Т. 4. 503 с. С. 125–129.
8. Новак А.В., Сагдеев А.К., Сидоренко Е.Н., Суюндукова А.А. Методика мониторинга информационно-телекоммуникационной сети военного назначения во время техносферной борьбы // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. / Под. ред. С.В. Бачевского; сост. А.Г. Владыко, Е.А. Аникевич. СПб.: СПбГУТ, 2018. Т. 4. 746 с. С. 367–370.

© Лукин Константин Игоревич (ki@supertel.ru), Сагдеев Александр Константинович (brother-aks@yandex.ru),
Стахеев Иван Геннадиевич (kisasig@yandex.ru), Титова Ольга Викторовна (olga1110.spb@mail.ru).
Журнал «Современная наука: актуальные проблемы теории и практики»