DOI 10.37882/2223–2966.2022.06–2.21

ОБОСНОВАНИЕ ИСПОЛЬЗОВАНИЯ БОЕВЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ В ИНФОРМАЦИОННОМ ПРОТИВОБОРСТВЕ

JUSTIFICATION OF THE USE OF COMBAT CYBERNETIC SYSTEMS IN INFORMATION WARFARE

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

Summary. The problems of information and telecommunication systems when transferring the antagonistic conflict of the parties to cyberspace are considered. the justification of the use of combat cybernetic systems in the emerging information confrontation 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. Рассмотрена проблематика информационно-телекоммуникационных систем при переносе антогонистического конфликта сторон в киберпространство. проведено обоснование использования боевых кибернетических систем, в возникающем информационном противоборстве.

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

Использование государством своих возможностей: дипломатических, информационных, военных и экономических — позволяют достигать ему поставленных целей. Применение таких возможностей в киберпространстве требует безопасной передачи, хранения и обработки информации в масштабе времени, близком к реальному. Государства, которые используют эти возможности в киберпространстве, получают превосходство в использовании Вооружённых Сил в традиционных сферах их применения. Такие реалии превращают киберпространство в современное поле боя, дополняющее традиционные сферы применения Вооружённых Сил. [1]

Киберпространство является информационно-технической основой информационного пространства, т.е. находится только в физическом и информационном аспекте информационного пространства. В связи с этим, большая часть противоборства в информационной сфере будет происходить в киберпространстве. [2]

Выполнение задач информационно-телекоммуникационных систем специального назначения (ИТКС СН) по обеспечению обмена всеми видами информации в системе управления войсками в условиях информационного противоборства (борьбы) в киберпространстве (киберконфликтах) достигается нейтрализацией действий противоборствующих систем на основе дополнения целевой функции оборонительной и наступательной функциями, что обуславливает необходимость рассмотрения в границах киберпространства нового класса систем — боевых кибернетических систем (БКС).

Под боевыми кибернетическими системами следует понимать выделенную совокупность функционально связанных и взаимодействующих аппаратных,

программных и аппаратно-программных средств, реализующих добывание информации (разведывательные действия), наступательные и оборонительные действия в киберпространстве, а также автоматизированные системы управления ими и должностных лиц их эксплуатирующих.

Совокупность элементов БКС представляют объединенную единством цели пространственно-распределенную иерархическую структуру элементов киберпространства, предназначенных для выполнения с заданным качеством поставленных задач в условиях конфликта с одной или несколькими аналогичными системами противника (противников). [3] Элементы в структуре БКС составляют иерархическую совокупность взаимообусловленных и взаимосвязанных элементов, дополняющих друг друга при реализации поставленных задач. Связи между элементами в системе, исходя из характера выполняемых задач, организационно определяются отношениями управления, исполнения и обеспечения.

Функционирование ИТКС СН базируется на оптимизации применения тех или иных видов (типов) ресурсов транспортной сети, построенной на ресурсах операторов связи, являющейся в свою очередь элементом общемирового единого информационно-телекоммуникационного пространства (ОМЕИТП), находящихся в сфере интересов одной или нескольких ИТКС, обусловливая тем самым возникновение ресурсных конфликтов. В свою очередь конфликт является основной формой функционирования БКС и характеризуется наличием одной или нескольких целей, представляющих интерес для противоборствующих сторон. Достижение целей функционирования ИТКС СН в конфликте осуществляется проведением ее БКС наступательных и оборонительных действий за овладение и поддержание целевого превосходства — оперативно-тактической инициативы для выполнения с заданным качеством поставленных задач на основе методов программно-аппаратных воздействий (ПАВ) на элементы ИТКС СН противника в целях снижения эффективности ее функционирования, а так же на элементы БКС противоборствующей стороны для снижения их боеспособности до необходимого, а в некоторых случаях и минимального уровня. [4]

Рассмотрим две взаимно конфликтующие системы «красную» и «синюю», и соответственно их представляющие ИТКС СН — К и ИТКС СН — С.

При применении ИТКС СН — К, актуальной является задача обеспечения заданной эффективности их функционирования в условиях реализации противоборствующей стороной ПАВ. Предполагается, что из состава ИТКС СН — К выделяется ресурс организационно объединяемый в БКС. БКС включает совокупность функционально объединенных единством цели элементов информационно-телекоммуникационной инфраструктуры (ИТКИ), которые обеспечивают управление, добывание информации, создание, хранение, передачу исполнительного элемента (ИЭ) (программного кода) и средства и комплексы защиты информации (СКЗИ) (для общности — оборонительный элемент (ОБЭ)) для обеспечения действий ИТКС СН — К в конфликте методами и средствами информационного противоборства в киберпространстве. [5]

ИТКС СН — С для обеспечения своих действий симметрично применяет БКС, структурно включающую:

- подсистему управления (ПУ);
- подсистему добывания информации (ПДИ), использующей множество различного типа ИС добывания информации об элементах ИТКС СН — К;
- подсистему наступательных действий (ПНД), использующей множество различного типа ИЭ для воздействия на элементы ИТКС СН — К;
- подсистему оборонительных действий (ПОД), использующей множество различного типа ОБЭ для пресечения ИЭ противника. [6]

В условиях случайностей начала, продолжительности и исхода конфликта процесс функционирования ИТКС СН — К оказывается стохастическим на конечном интервале времени до достижения одной из сторон минимального уровня эффективности функционирования. Для исследования этого требуется разработка модели функционирования ИТКС СН — К в условиях использования для обеспечения эффективных действий БКС, эффект применения которой состоит в воздействии на элементы управляющей, информационной и исполнительной подсистем ИТКС СН — С и ее БКС на различных этапах конфликта для неустановившегося переходного стохастического процесса конфликтного взаимодействия противоборствующих систем. [7]

Таким образом, представляется возможным выдвинуть гипотезу: эффективность функционирования ИТКС СН применительно к условиям конфликта в киберпространстве возможно оценить через эффективность обеспечивающей ее системы — БКС. Причем оценке подлежит как «внешняя» эффективность БКС по показателям, характеризующими способность ИТКС СН выполнять функциональные задачи в условиях реализации противником информационно-технического воздействия (ИТВ) (в частности ПАВ), так и «внутренняя» эффективность БКС по показателям, характеризующими степень достижения цели функционирования при реализации оборонительных и наступательных действий. Полученные оценки позволят научно обосновывать оперативно-технические требования (ОТТ) непосредственно к ИТКС СН.

ЛИТЕРАТУРА

1. Лепешкин О.М., Сагдеев А.К. Подход к оценке конфликтных ситуаций в информационных системах управления // Сборник трудов № 53 СВИС РВ г. Ставрополь, СВИС РВ, 2010- С. 58–64.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. 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.

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича