УДК 623.62

К вопросу об определении термина «информационно-техническое воздействие»

Забегалин Е. В.

Актуальность задачи: *Доктрина информационной безопасности (ИБ) Российской Федерации, утверждённая в новой редакции 5 декабря 2016 года, ввела в официальный оборот термин «информационно-техническое воздействие» («ИТВ») и отнесла деятельность ряда зарубежных стран по наращиванию возможностей ИТВ на информационную инфраструктуру в военных целях к числу негативных факторов, влияющих на состояние информационной безопасности страны. В тексте Доктрины ИБ нет определения термина «ИТВ». Нет его и в других государственных документах. Различные варианты определений термина «ИТВ» известны из опубликованных справочников и работ специалистов, но ни одно из них не подходит для нормативного использования. По мнению автора настоящей статьи данная ситуация нуждается в разрешении – термин «ИТВ» должен получить своё нормативное определение в интересах дальнейшего развития теории и практики информационного противоборства и информационной безопасности.* ***Целью работы*** *является разработка определения термина «ИТВ», которое может быть предложено для использования в руководящих и нормативных технических документах и которое может нести общую парадигму решения множества теоретических и практических задач во исполнение положений Доктрины ИБ.* ***Метод решения задачи:*** *сначала анализируются известные варианты определений термина «ИТВ» и выявляются их недостатки; потом принимается логический императив терминологического различения и разделения ИТВ и радиоэлектронного поражения/подавления целей; затем определяются природа, сущность и поражающие факторы ИТВ, которые отличаются от таковых в радиоэлектронном поражении целей; и в итоге формулируются определение термина «ИТВ» по образцу стандартизованной терминологии радиоэлектронной борьбы и определения других связанных с ИТВ терминов, в том числе определение термина «оружие ИТВ», которое согласуется со стандартизованной терминологией по военной технике.* ***Новизна решения*** *заключается в новом определении термина «информационно-техническое воздействие», которое отличается от известных определений тем, что оно базируется на предложенном автором исходном императивном различении природы, сущности и поражающих факторов ИТВ от таковых у радиоэлектронного поражения целей. Предложен отличительный признак ИТВ – нарушение компьютерной безопасности объектов (целей) информационно-технического воздействия.* ***Теоретическая значимость работы*** *состоит в том, что предложенные в ней новые определения терминов «ИТВ» и других связанных с ним терминов расширяют спектр современных взглядов специалистов на средства ведения информационного противоборства и могут быть учтены при построении терминологического базиса информационного противоборства.*

Ключевые слова: *информационно-техническое воздействие, ИТВ, оружие ИТВ, поражающие факторы ИТВ, информационно-техническое поражение, информационно-технический объект, информационное противоборство, информационная безопасность, компьютерная безопасность, радиоэлектронная борьба, радиоэлектронное поражение.*

Библиографическая ссылка на статью:
Забегалин Е. В. К вопросу об определении термина «информационно-техническое воздействие» // Системы управления, связи и безопасности. 2018. № 2. С. 121–150. URL: http://sccs.intelgr.com/archive/2018-02/08-Zabegalin.pdf.

Reference for citation:
Zabegalin E. V. A question of definition of the term «information and technical impact». *Systems of Control, Communication and Security*, 2018, no. 2, pp. 121–150. Available at: http://sccs.intelgr.com/archive/2018-02/08-Zabegalin.pdf (in Russian).

Актуальность

Доктрина информационной безопасности Российской Федерации [1] (далее – Доктрина ИБ) относит (в статье 11) деятельность ряда зарубежных стран по наращиванию возможностей *информационно-технического воздействия* на информационную инфраструктуру в военных целях к числу негативных факторов, влияющих на состояние информационной безопасности России.

Это положение Доктрины ИБ подтверждается множеством известных фактов. Вот лишь некоторые из них: в октябре 2016 года в США появились открытые заявления с угрозами начать кибервойну против России [2], а в марте 2017 года на Интернет-сайте Wikileaks началась публикация сведений об арсенале вредоносных компьютерных программ ЦРУ США [3, 4]. Однако и раньше российские эксперты утверждали то, что кибервойна США против России уже началась и идёт [5, 6].

Доктрина ИБ не определяет термин «информационно-техническое воздействие». Если привлечь из её текста содержательные моменты, которые раскрывают (в статьях 16, 17, 20, 23, 24) информационные угрозы, цели и основные направления обеспечения информационной безопасности, то можно предложить следующий вариант «доктринального» определения этого термина (от автора настоящей статьи):

«*Информационно-техническое воздействие (ИТВ)* – целенаправленное с использованием средств и возможностей информационных и иных технологий воздействие противоборствующей стороны на объекты критической информационной инфраструктуры, на автоматизированные системы управления, на образцы вооружения, военной и специальной техники, на процессы их функционирования и применения, нарушающее устойчивость их функционирования и их информационную, технологическую и промышленную безопасность, и приводящее к эскалации военных конфликтов, к возникновению чрезвычайных ситуаций, к нарушению государственного управления национальной обороной, безопасностью и правопорядком, к срыву выполнения военных задач вооружёнными силами».

Однако такой вариант «доктринального» определения термина «ИТВ» несёт лишь верхнеуровневое отражение угроз безопасности страны и больше подходит для использования в составе политической терминологии.

За основу научного анализа и синтеза технологической сущности ИТВ может быть принято вполне ясное понимание того, что реализация противником ИТВ на информационную инфраструктуру в военных целях возможна только путём создания и применения им специальных технических средств с целью нанесения ущерба объектам воздействия. Это даёт основания рассматривать технические средства ИТВ как оружие в рамках стандартизованной терминологии по военной технике [7], или в рамках словаря [8].

В таком ракурсе положение Доктрины ИБ о факторе военной направленности возможных информационно-технических воздействий на информационную инфраструктуру России даёт основание для военно-научных разработок терминов «ИТВ» и «оружие ИТВ» как в интересах исследований и разработок

эффективных мер защиты от ИТВ, так и возможно в интересах исследования целесообразности реализации ответных симметричных мер.

Автор настоящей статьи смог найти первое опубликованное использование термина «ИТВ» (без определения) в работе [9] 14-летней давности, а первое опубликованное технологическое определение термина «ИТВ» – в словаре [10] 10-летней давности. Начиная с работы [11], можно проследить появление в российских изданиях различных вариантов технологических определений терминов «информационное воздействие», «информационно-техническое воздействие», «информационно-техническое оружие» и различных классификаций этих воздействий и соответствующего им оружия. При анализе опубликованных вариантов технологических определений термина «ИТВ» и других близких по смыслу к нему терминов обнаруживается отсутствие нормативного определения термина «ИТВ». Это обстоятельство позволяет автору настоящей статьи участвовать в актуальном процессе составления терминологии, относящейся к ИТВ.

Что известно об ИТВ?

До утверждения в 2016 году новой редакции Доктрины ИБ были известны различные варианты понимания ИТВ, например, следующие:

а) «ИТВ – комплекс программных (программно-аппаратных) и радиоэлектронных средств, направленных на манипулирование функционированием информационно-технических объектов, а также прекращение (затруднение) работы или вывод их из строя на определенный период» [10];

б) «ИТВ – применение способов и средств информационного воздействия на информационно-технические объекты страны, на технику и вооружение противника в интересах достижения поставленных целей» [11, 12];

в) «ИТВ – основной поражающий фактор информационно-технического оружия, представляющий собой воздействие либо на информационный ресурс, либо на информационную систему или на средства получения, передачи, обработки, хранения и воспроизведения информации в её составе, с целью вызвать заданные структурные и/или функциональные изменения» [13, 14];

г) «ИТВ на ракетные комплексы стратегического назначения (РК СН) – целенаправленное аппаратно-программное (компьютерная атака) или программное воздействие, а также их комбинация на информационно-телекоммуникационные системы РК СН, приводящие к нарушению или снижению эффективности управления РК СН» [15].

Известны также определения иных терминов, близких по смыслу к термину «ИТВ»:

д) «Программное воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ» [16];

е) «Компьютерная атака – целенаправленное несанкционированное воздействие на информацию, на ресурс информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств» [17];

ж) «Информационное воздействие – основной поражающий фактор информационной войны, представляющий собой воздействие информационным потоком на объект атаки – информационную систему или ее компонент, – с целью вызвать в нём в результате приёма и обработки данного потока заданные структурные и/или функциональные изменения» [9, 14, 18];

з) «Программно-математическое воздействие на компьютерные сети – компьютерные атаки – 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» [18].

В работе [14] предложена широкая классификация ИТВ по различным признакам, в том числе по способам реализации воздействия: алгоритмическое, программное, аппаратное, физическое.

Если говорить о средствах непосредственной реализации ИТВ на цели, то возникают термины «информационное оружие» и «информационно-техническое оружие», для которых специалистами предлагаются, например, следующие определения:

- «Информационное оружие – это совокупность методов и средств подавления элементов инфраструктуры государственного и военного управления противника; электромагнитного влияния на элементы информационных и телекоммуникационных систем; несанкционированного доступа к информресурсам с последующей их деформацией, уничтожением или хищением; информационно-психологического воздействия на военнослужащих и гражданское население противоборствующей стороны» [19];
- «Информационно-техническое оружие – совокупность специально организованной информации, информационных технологий, способов и средств, позволяющих целенаправленно изменять (уничтожать, искажать), копировать, блокировать информацию, преодолевать системы защиты, ограничивать допуск законных пользователей, осуществлять дезинформацию, нарушать функционирование систем обработки информации, дезорганизовывать работу технических средств, компьютерных систем и информационно-вычислительных сетей, а также другой инфраструктуры высокотехнологического обеспечения жизни общества и функционирования системы управления государством, применяемое в ходе информационной операции для достижения поставленных целей» [14].

Электронный военный энциклопедический словарь, функционирующий на Интернет-сайте Минобороны России, даёт классификацию средств информационной борьбы и определяет в их числе «средства специального программно-технического воздействия (ССПТВ)» как компьютерные «программы, результатом выполнения которых является хищение, уничтожение, модификация информации (данных, баз данных, программного обеспечения), блокирование доступа, нарушение порядка функционирования вычислительных средств, а также поражение операторов ЭВМ, как правило, через зрительное восприятие информации» [20].

Из приведенных выше примеров складывается картина, показывающая, то, что известные варианты понимания термина «ИТВ» и близких к нему по смыслу терминов:

- различаются категориальным отнесением ИТВ – и к действиям, и к способам, и к средствам, и к поражающим факторам;
- различаются перечнями типов воздействия – ИТВ может быть и программным, и информационным, и радиоэлектронным, и прочим физическим;
- имеют смысловые пересечения и расхождения,

и вследствие всего этого не дают в целом, по мнению автора настоящей статьи, достаточных однозначности и полноты для чёткого понимания термина «ИТВ».

Представляется также существенным обратить внимание при разработке терминологии ИТВ на стандартизованную терминологию радиоэлектронной борьбы (РЭБ) [21], которая повторяется специалистами в научных и учебных изданиях (например, в [14, 22, 23]). Терминология РЭБ относит программные средства искажения информации противника к категории средств радиоэлектронного поражения (РЭПр). По мнению автора настоящей статьи, это категориальное расширение РЭПр нуждается в теоретическом обосновании необходимости и целесообразности включения нового типа поражения целей – программного – в один категориальный ряд с классическими видами РЭПр – преднамеренными радиопомехами и силовым электромагнитным излучением.

Не очевидны также логические основания для включения в объём термина «ИТВ» двух типов воздействий – программного и радиоэлектронного – в исторически первом его определении, данном в словаре [10], приведенном выше.

Нуждается также в прояснении и логика определения информационно-технического оружия в ряде научных публикаций, в которых в эту категорию оружия включаются и средства РЭПр, и средства программного воздействия. Так, например, утверждается, что информационно-технического оружие – это:

- «... совокупность специальных методов и средств, которые основаны на использовании электромагнитных волн (излучений) различной длины и мощности и вредительских (деструктивных) программ с целью воздействия на радиоэлектронные средства, элементы радиоэлектроники, программные средства АСУ и ЭВТ … и приводят к ухудшению их функционирования и (или) исключению нормального функционирования по своему предназначению» [24];

- «… средства и технологии: радиоэлектронного подавления приемников, поражения программного обеспечения и элементов радиоэлектронной аппаратуры, изменения условий распространения электромагнитных, акустических и гидроакустических волн, ускоренного старения элементов радиоэлектронной аппаратуры» [25].

Кроме формальной логики, не ясна также практическая целесообразность предлагаемой в указанных публикациях логической ассоциации программных и радиоэлектронных воздействий в рамках ИТВ, когда вполне понятному термину «преднамеренные радиопомехи» придаётся второй дополнительный смысл ИТВ, которое само пока ещё не определено достаточно ясно. Основную причину этого автор настоящей статьи усматривает в бесспорном понимании (продемонстрированном, например, в статье [26]) той причинно-следственной связи, в которой радиопомехи, изменяя информационные потоки в контурах управления войсками и оружием, в конечном итоге ухудшают качество этого управления. Однако понятно также и то, что радиопомехи в их классическом понимании никак «интеллектуальным» образом не изменяют компьютерные алгоритмы обработки информации и никак не профилируются под различные форматы и семантики цифровых данных, обрабатываемых компьютерными алгоритмами. Для того, чтобы радиопомехи могли алгоритмическим образом влиять на компьютерные алгоритмы и данные, они должны нести соответствующую «цифровую» нагрузку. Это, например, и показывают авторы, той же статьи [26], наделяя будущие средства РЭПр способностью бескомпроматно подавать ложные цифровые информационные потоки на аппаратно-программные интерфейсы сетей связи. Однако авторам статьи [26] остаётся сделать последний логический шаг и сказать то, что в таком случае природа воздействия перестаёт быть физической радиоэлектронной и становится программно-алгоритмической[1].

Завершая проведенный анализ, надо признать то объективное обстоятельство, что проблемное состояние вопроса определения термина «ИТВ» обусловлено небольшим, ещё прошедшим временем становления информационного противоборства (ИПб) в российских Вооружённых Силах [28] и вытекающим из этого обстоятельства, недостаточным прояснением объектовых и технологических границ ИТВ.

В данных обстоятельствах, не смотря на наличие стандартизованной терминологии РЭБ, включившей искажение информации противника специальными программными средствами в категорию радиоэлектронного поражения, остаются открытыми, по мнению автора настоящей статьи, возможности для научного обсуждения вопросов и научных разработок вариантов терминологии для ИТВ.

Учитывая фактически начавшуюся в Доктрине ИБ самостоятельную официальную жизнь термина «ИТВ», а также вне зависимости от организационных рамок ИТВ, представляется предпочтительным, по мнению автора настоящей

[1]*Примечание.* Уже появились первые уточнения смыслов РЭПр, рассматриваемого как ИТВ, например, в новейшей работе [27] её автор ввёл и использует новый термин «радиоэлектронное ИТВ».

статьи, логическое разведение (разделение) понятий и терминов РЭБ и ИТВ, которое может быть полезным и для складывающихся теории и практики ИПб, и для уже сложившихся теории и практики РЭБ. По меньшей мере, такая установка видится автору настоящей статьи более понятной и приемлемой, чем использование для преднамеренных радиопомех нового дополнительного названия «информационно-техническое воздействие».

Постановка задачи

Исходя из того, что в науке термины используются для точного названия строго определённых понятий [29], задача определения термина «ИТВ» может быть решена при условии предварительной разработки понятия «ИТВ».

Опираясь на известные рекомендации логической науки [29], согласно которым понятия логически представляются целостными совокупностями утвердительных суждений о наиболее общих и одновременно наиболее существенных признаках соответствующих им объектов, необходимо сначала определить природу и сущность ИТВ, которые позволили бы отличить ИТВ от других типов поражающих воздействий на целевые объекты.

Исходя из этого, при определении сущности ИТВ нужно проанализировать различные виды ИТВ и различные поражающие факторы ИТВ, в которых природа и сущность ИТВ проявляются в процессе непосредственной реализации ИТВ и которые представляют объективную основу для понятийного обобщения.

Разработка понятия и определения термина «ИТВ» должна быть выполнена в соответствии с известными логическими правилами определения понятий, в числе которых: отнесение к ближайшему роду и выявление видового отличия, соблюдение соразмерности определяемого и определяющего понятий, выделение существенных видовых признаков, отсутствие терминологического круга, применение позитивной формы суждений, недопущение логических противоречий и двусмысленности, достижение чёткости и ясности [29].

Далее, исходя из понятых природы и сущности ИТВ, нужно содержательно охарактеризовать соответствующий ему тип поражения/подавления объектов (целей).

Затем нужно разработать новое определение термина «ИТВ» и новые определения других связанных с ИТВ терминов, которые могут быть предложены для нормативного использования.

В завершение нужно разработать определение термина «оружие ИТВ», согласующееся со стандартизованной терминологией по военной технике [7], определяющей «оружие» как изделие военной техники, предназначенное для поражения цели или доставки к ней средств воздействия.

Схема решения задачи

Для решения задачи разработки нового определения термина «ИТВ» представляется рациональным и целесообразным воспользоваться методологическим багажом составления терминологии радиоэлектронной борьбы потому,

что у РЭБ значительно более солидный, чем у ИПб, возраст – уже более 100 лет [30].

Для этого можно привлечь из стандартизованной терминологии РЭБ [21] и из научных и учебных изданий специалистов РЭБ (например, из [14, 22, 23]) такие основополагающие термины РЭБ с их определениями, как радиоэлектронная борьба, радиоэлектронное поражение (РЭПр), поражение электромагнитным излучением (ЭМИ), радиоэлектронное подавление (РЭП), радиоэлектронная помеха, радиоэлектронный объект (РЭО), радиоэлектронное средство (РЭС).

Во множестве этих терминов РЭБ просматривается базовая логическая схема составления всей терминологии РЭБ, которая отражает следующие объективные рамки РЭБ:

1) класс объектов поражения составляют радиоэлектронные объекты;
2) изменения в РЭО, наступающие в результате радиоэлектронного поражения, проявляются в виде снижения эффективности функционирования РЭО или в виде физического повреждения элементов РЭО;
3) непосредственными механизмами поражения РЭО, которые можно назвать поражающими факторами оружия РЭБ, являются преднамеренные радиопомехи, силовое ЭМИ и самонаводящееся на излучение РЭС кинетическое оружие;
4) типом организации РЭБ и РЭПр является «совокупность мероприятий и действий».

Опираясь на эту схему как на логический образец, а также реализуя исходную установку автора настоящей статьи на разделение понятий и терминов ИТВ и РЭБ, можно для нового определения термина «ИТВ» императивно зафиксировать в качестве граничных условий следующие принципиальные позиции[2]:

1) мероприятия, действия и процессы ИТВ содержательно отличаются от мероприятий, действий и процессов РЭБ;
2) технические средства ИТВ существенно отличаются от средств РЭПр, им даются следующие обобщающие названия – «оружие ИТВ» или «информационно-техническое оружие» (ИТОр);
3) при ИТВ реализуется особый тип поражения/подавления целей (объектов) – информационно-техническое поражение/подавление (ИТПр), отличающееся по своим природе, сущности и поражающим факторам от РЭПр;
4) целевыми объектами для ИТВ являются «информационно-технические объекты (ИТОб)», отличающиеся по своим признакам от РЭО.

Данную схему можно назвать логическим императивом ИТВ, в рамках которого решение поставленной выше общей задачи складывается из последовательного решения следующих частных задач:

[2]*Примечание.* Словарь [10], хотя и использует термин «информационно-технический объект» в определении термина «ИТВ», которое приведено в начале настоящей статьи, но не содержит статьи, определяющей этот тип объектов.

- определение существенных отличительных признаков ИТОб;
- определение примерного круга различных типов и видов целевых ИТОб;
- определение природы и сущности ИТВ;
- определение информационно-технического типа поражения ИТОб;
- определение различных видов ИТВ и поражающих факторов ИТВ;
- разработка новых определений терминов «ИТВ», «ИТПр», «ИТОб», «оружие ИТВ», которые могут быть нормативными.

Целевые объекты ИТВ

В первую очередь сама Доктрина ИБ способствует определению круга объектов информационной инфраструктуры, которые могут быть целями для ИТВ, – она определяет эту инфраструктуру (в п. з ст. 2) как совокупность объектов информатизации, информационных систем, сайтов в Интернете и сетей связи.

Кроме того, Доктрина ИБ относит (в п. д ст. 23) повышение безопасности функционирования образцов вооружения, военной и специальной техники (ВВСТ), автоматизированных систем управления (АСУ) к числу основных направлений обеспечения информационной безопасности страны. Поэтому образцы ВВСТ и АСУ могут быть включены во множество потенциальных целевых объектов ИТВ.

В работах [24, 25] специалисты предлагают включать в число объектов ИТВ широкий ряд разнотипных объектов таких, как средства вычислительной техники, программное обеспечение, радиоэлектронные средства, элементы радиоэлектронной аппаратуры, среду распространения электромагнитных волн (ЭМВ), каналы связи. Этот перечень может быть расширен стандартизованной категорией «объект информатизации»[3].

Однако такие варианты выделения объектов (целей) для ИТВ не могут в целом быть приняты потому, что в объём термина «объект информатизации» не включены образцы ВВСТ, а РЭС и среда распространения ЭМВ не могут быть включены в круг целевых объектов ИТВ в соответствии с логическим императивом ИТВ, который был сформулирован выше.

Решающим приёмом для определения круга информационно-технических объектов (целей) ИТВ может быть использование такого родового признака объектов (целей) ИТВ, как наличие в их структуре электронных цифровых вычислительных устройств, называемых также компьютерными устройствами или просто компьютерами, которые могут быть универсальными или специализированными (это, например, сетевые маршрутизаторы и коммутаторы, навигационные радиоприёмники и др.).

[3]*Примечание*. «Объект информатизации: совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений или объектов, предназначенных для ведения конфиденциальных переговоров» [31].

В настоящее время термины «вычислительное устройство», «компьютерное устройство», «компьютер» не стандартизованы, но стандартизован равнозначный им по смыслу термин «средства вычислительной техники (СВТ)»[4].

Можно с полной уверенностью рассматривать и дальше использовать как синонимы термины «средство вычислительной техники», «вычислительное устройство/средство», «компьютерное устройство/средство», «компьютер».

Нет необходимости во введении термина «информационно-техническое средство» по аналогии с термином «радиоэлектронное средство» потому, что спектр различных типов и видов компьютерных средств очень широк (они могут быть отдельными устройствами и встраиваемыми вычислительными модулями, они могут иметь различные функциональные профили и различаться габаритами в диапазоне от десятков до единиц и долей сантиметров). Поэтому те технические средства, в которых компьютерные устройства являются их компонентами, можно и удобно именовать «компьютеризированными средствами».

Исходя из этого, «информационно-технический объект» (ИТОб) может быть определён как технический объект, в конструкцию которого включены одно или несколько компьютерных устройств, выполняющих функции приёма, обработки, отображения, передачи данных в электронных цифровых форматах.

Данное определение ИТОб позволяет теперь более конкретно очертить круг характерных типов и видов целевых объектов для ИТВ, включив в него:

1) автоматизированные системы (АС), в т. ч. АС военного назначения и АС управления производственными технологическими процессами, и др. виды АС, в структурах которых есть компьютеры-серверы, компьютеры-рабочие станции, компьютерные коммуникационные средства образования локальных (объектовых) вычислительных сетей;
2) компьютерные и коммуникационные узлы в распределённых информационно-телекоммуникационных сетях, в т. ч. в сети Интернет;
3) компьютерные компоненты сетей радиосвязи (в т. ч. спутниковой);
4) космические аппараты (КА) на орбитах;
5) наземные комплексы управления КА;
6) компьютеризированные транспортные средства;
7) компьютеризированные образцы ВВСТ;
8) компьютеризированные беспилотные летательные аппараты (БЛА);
9) компьютеризированные наземные и морские роботы;
10) компьютерные устройства в каналах приёма и передачи цифровых данных между удалёнными информационно-техническими объектами (в т. ч. цифровые каналы радиоуправления БЛА, наземными и морскими роботами, транспортными средствами, космическими аппаратами);
11) персональные компьютеры, планшеты и смартфоны;
12) цифровые навигационные приёмники, вычисляющие свои координаты по принимаемым радионавигационным сообщениям, транслируемым с

[4] *Примечание.* «СВТ – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем» [32].

орбит космическими аппаратами спутниковых радионавигационных систем.

Этот перечень не является исчерпывающим и может быть дополнен.

Опираясь на предложенное выше определение объектов (целей) для ИТВ, можно теперь определить природу и сущность ИТВ.

Природа и сущность ИТВ

Известно (например, из [33, 34]), что в большинстве случаев основными компонентами компьютерных устройств являются:

- центральные процессоры и модули оперативной памяти;
- системные платы с модулями общесистемной логики и аппаратными интерфейсами для инсталляции внутренних устройств, для подключения внешних устройств, для организации сетевых каналов приёма и передачи данных;
- программное обеспечение в памяти системной платы – BIOS (Basic Input/Output System – Базовая система ввода-вывода), UEFI (Unified Extensible Firmware Interface – Унифицированный расширяемый интерфейс («прошивка»);
- специализированные процессоры для обработки графических, видео и звуковых данных (т. ч. инсталлируемые на системной плате);
- внутренние устройства постоянной энергонезависимой памяти – магнитные диски или модули флэш-памяти;
- видеомониторы, звуковые устройства, устройства ввода данных;
- общее и специальное программное обеспечение в постоянной памяти;
- исходные данные для обработки и данные результатов обработки, размещаемые в постоянной памяти.

Принципиальный механизм функционирования любого компьютерного устройства заключается в выполнении центральным процессором совместно с оперативной памятью заранее составленных компьютерных программ обработки данных. При этом программные команды и данные для обработки извлекаются из постоянной памяти в оперативную память, откуда переносятся в исполнительные регистры процессора, а результирующие данные записываются в постоянную память, передаются на видеомонитор или в звуковое устройство компьютера, или же выдаются в сетевые каналы передачи данных[5].

Исходя из этого общего механизма, можно следующим образом определить *сущность ИТВ* – это преднамеренное навязывание процессорам компьютерных устройств выполнения ложных программ или обработки ложных данных, приводящее к получению (вычислению) ложных результирующих данных,

[5] *Примечание.*
1) «Программа для ЭВМ – представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определённого результата» [35].
2) «Данные – представление информации в формализованном виде, пригодном для передачи, интерпретации или обработки» [36].

которые вызывают ложное (нештатное) функционирование или блокирование функционирования компьютеризированных объектов.

Сущность ИТВ в таком понимании принципиально отличается от сущности классического РЭПр, состоящей в электромагнитном волновом зашумлении радиосигналов, принимаемых РЭО или в необратимом силовом изменении физических параметров электронных компонентов РЭО под действием ЭМИ. В отличие от электромагнитной природы РЭПр природа ИТВ является исключительно программно-алгоритмической и она даёт возможность осуществлять компьютерным образом вредоносные изменения штатных алгоритмов и процессов обработки данных в компьютерных устройствах, на которые направлено ИТВ.

ИТВ при таком понимании его природы и сущности может реализовываться различными средствами и способами, но его механизмы всегда однотипны – это внедрение (запись) в постоянную или в оперативную память компьютерного устройства ложных программ или ложных данных, причём так, чтобы с нужной для атакующей стороны вероятностью эти ложные программы были выполнены, а ложные данные были обработаны либо сразу после их «инъекции» в память устройства, либо в будущее необходимое атакующей стороне время.

Успешно реализованное ИТВ приводит к нарушению компьютерной безопасности объекта воздействия, когда в объекте нарушаются безопасность компьютерных программ, безопасность компьютерных данных и безопасность предписанных функций по назначению объекта [37]. Объективной основой возможности реализации ИТВ в большинстве случаев является наличие уязвимостей в программном обеспечении компьютерных устройств [38-41], которые должны быть предварительно разведаны атакующей стороной[6].

Таким образом, отличительными признаками ИТВ являются:

- тип целевых объектов воздействия – компьютеризированные объекты;
- особый тип поражения/подавления целевых объектов воздействия – информационно-технический, – который состоит в преднамеренном скрытном несанкционированном внедрении в компьютеризированный объект ложных программ или ложных данных и в их последующем выполнении или обработке, вызывающем в итоге ложное функционирование и снижение эффективности функционирования объекта или блокирование его функционирования.

Поражающие факторы ИТВ

Термин «поражающий фактор оружия» можно определить (как видится автору настоящей статьи) как материальную или информационную причину, которая возникает в процессе целевого применения оружия и которая непосредственно вызывает поражение или подавление объектов (целей) противника

[6] *Примечание.* «Уязвимость: недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть использована для реализации угроз безопасности информации» [42].

с нанесением им ущерба, или же вызывает их ложное функционирование или поведение[7].

Если обратиться к стандартизованным терминам и определениям РЭБ [21] и к книгам специалистов РЭБ (например, [14, 22, 23]), которые используют такие же основополагающие термины, то из них можно логически определить и составить следующий перечень поражающих факторов оружия РЭБ:

- преднамеренные активные и пассивные радиопомехи, приводящие к временному снижению эффективности целевого функционирования РЭС;
- преднамеренное силовое ЭМИ, приводящее к необратимому снижению эффективности или к полному прекращению целевого функционирования РЭС вследствие получения необратимых ущербных изменений электрофизических параметров полупроводниковых элементов РЭС в результате их перегрева или электрического пробоя;
- самонаводящиеся на излучение РЭС боеприпасы авиационных или ракетно-артиллерийских систем.

В логической схеме «причина-следствие» и в рамках определённой выше сущности ИТВ просматривается однотипность поражающих факторов ИТВ – как непосредственных причин поражения/подавления ИТОб, – это всегда массивы ложных программных команд или данных, которые будучи скрытно и не санкционировано установлены и активированы в компьютерном устройстве объекта, вызывают ложное его функционирование или же блокируют его функционирование. В некоторых частных случаях для обозначения поражающих факторов ИТВ может быть использован термин «вредоносная программа»[8].

В ситуациях, когда программные команды или данные ИТВ заранее внедряются в компьютерное устройство различными способами и средствами и лишь потом, спустя продолжительное время, активируются в нужный атакующей стороне момент времени, можно использовать вместе с термином «ИТВ» термин «программное воздействие».

В ситуациях, когда программные команды или данные ИТВ начинают исполняться или обрабатываться компьютерным устройством сразу после подключения к нему атакующей стороной своего внешнего технического устройства, несущего эти команды или данные (механическим присоединением или по радиоканалу передачи данных), и переноса их в память устройства, можно

---

[7] *Примечание.*
1) «Поражение объектов, целей – воздействие различными средствами поражения на объекты (цели), в результате которого они полностью или частично (временно) теряют способность работать по предназначению, решать боевые задачи (утрачивают боевую способность). В зависимости от величины ущерба, нанесённого объектам (целям), достигаются их уничтожение (разрушение), подавление, дезорганизация и изнурение (живой силы объекта)» [43].
2) «Подавление объектов, целей – нанесение объекту (цели) ущерба (повреждений) и создание условий, при которых он временно лишается боеспособности, ограничивается (воспрещается) его манёвр или нарушается управление» [44].

[8] *Примечание.* «Вредоносная программа: программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы автоматизированной информационной системы» [16]).

использовать вместе с термином «ИТВ» термин «программно-аппаратное воздействие».

Конкретные виды ИТВ могут быть разнообразными. Автор настоящей статьи не ставил себе задачу дать в статье исчерпывающие перечень и характеристики различных видов ИТВ, которые уже раньше были достаточно информативно проанализированы во множестве публикаций специалистов, например, в [14, 38, 39, 41, 45-51], и на фирменных Интернет-порталах, например, в [52-56]. Задача настоящей статьи состоит в построении принципиальных логических рамок определения ИТВ. Поэтому, в следующей таблице перечислены лишь некоторые достаточно показательные виды ИТВ.

Таблица 1 – Возможные виды ИТВ

ИТО – цели для ИТВ	Виды ИТВ
Серверы и рабочие станции автоматизированных систем.	- Занесение и выполнение различных вредоносных программ: вирусов, червей, троянских коней. - Фальсификация (подмена) специального программного обеспечения (ПО) и специальных данных.
Сетевые коммутаторы и маршрутизаторы.	- «Перепрошивка» устройства. - Фальсификация (подмена) таблиц коммутации и маршрутизации.
DNS-серверы Интернет.	- Фальсификация записей доменов. - Искажение кэша данных. - Перегрузка высоко интенсивными потоками входящих ложных заявок на обслуживание – «DDoS-атаки».
Web-серверы Интернет.	- Занесение и выполнение различных вредоносных программ: вирусов, червей, троянских коней. - SQL-инъекции. - «DDoS-атаки».
Сети спутниковой связи. Космические аппараты на орбитах.	- Фальсификация абонентов спутниковой связи и выполнение с них по каналам связи ИТВ на узловые маршрутизаторы наземных станций спутниковой связи и на абонентские компьютерные устройства.
Космические аппараты на орбитах.	- Фальсификация командных радиолиний и закладка на борт КА ложных вредоносных команд управления.
Наземные комплексы управления космическими аппаратами.	- Занесение и выполнение на серверах и рабочих станциях различных вредоносных программ: вирусов, червей, троянских коней. - Фальсификация (подмена) специального ПО и специальных данных технологического управления.
Вычислительные модули цифровых каналов радиоуправления в составе компьютеризированных объектов (например, БЛА, роботов и пр.).	- «Перехват радиоуправления» – формирование и радиотрансляция ложных цифровых команд дистанционного управления по предварительно разведанному протоколу информационного обмена «оператор управления – объект управления».

ИТО – цели для ИТВ	Виды ИТВ
Цифровые навигационные приёмники сообщений, транслируемых КА спутниковых радионавигационных систем.	- «Постановка ложных навигационных полей» – формирование и радиотрансляция ложных навигационных сообщений в пределах локальных областей пространства, в которых находятся и движутся объекты с навигационными приёмниками.
Компьютеризированные наземные транспортные средства (в т.ч. беспилотные).	- Занесение и выполнение различных вредоносных программ: вирусов, троянских коней. - Подмена (фальсификация) специального ПО и специальных данных. - «Перехват радиоуправления». - «Постановка ложных навигационных полей».
Компьютеризированные БЛА, наземные и морские роботы.	- «Перехват радиоуправления». - «Постановка ложных навигационных полей».
Другие компьютеризированные образцы ВВСТ.	- Занесение и выполнение различных вредоносных программ: вирусов, троянских коней. - Фальсификация (подмена) ПО и данных. - «Постановка ложных навигационных полей».

Итак, видно, что поражающие факторы ИТВ при их выявленной общей однотипности могут различаться семантикой и характером воздействия.

Следующая таблица содержит перечень некоторых известных и потенциально возможных поражающих факторов ИТВ, который может быть расширен.

Таблица 2 – Некоторые поражающие факторы ИТВ

Виды ИТВ	Поражающие факторы ИТВ
Занесение и выполнение программных вирусов.	Наборы самокопирующихся программных команд в границах одного компьютера, занимающие его полезную память.
Занесение и выполнение сетевых программных червей.	Наборы программных команд, распространяющие свои копии по каналам передачи данных на другие компьютеры и занимающие полезную компьютерную память.
Занесение и выполнение программных троянских коней (иногда используется термин «логическая бомба» [10]).	Наборы программных команд: а) удаляющие, блокирующие, изменяющие, шифрующие, копирующие и пересылающие данные на компьютерах; б) замедляющие функционирование компьютеров и сетей; в) генерирующие исходящий поток удалённых запросов DDoS-атак к сетевым серверам.
Занесение и выполнение многофункциональных вредоносных компьютерных программ.	Наборы программных команд и данных с композицией функций вирусов, червей и троянских коней.
SQL-инъекции.	Наборы программных команд вредоносных SQL-запросов к реляционным базам данных.

Виды ИТВ	Поражающие факторы ИТВ
Фальсификация (подмена) специального программного обеспечения и данных.	Изменённые версии программ и данных с вредоносными свойствами, скрытно и не санкционировано установленные в компьютерные устройства взамен штатных версий (например, ложные таблицы коммутации и маршрутизации).
Высоко интенсивные потоки входящих заявок на обслуживание сетевым серверам или маршрутизаторам – «DDoS-атаки».	Огромная очередь принятых цифровых заявок на обслуживание, с обработкой которой не справляется обслуживающий их компьютер-сервер.
«Перехват радиоуправления» – «фальсификация радиомодема».	Цифровые команды радиоуправления, предварительно выявленные технической компьютерной разведкой и затем транслируемые на цели по разведанному цифровому коммуникационному протоколу.
«Постановка ложных навигационных полей».	Ложные цифровые навигационные сообщения, имитирующие с преднамеренными искажениями сообщения КА спутниковых радионавигационных систем.

Данные таблицы подтверждают правильность выделенных сущностных признаков ИТВ, которые отличают ИТВ от других типов поражающих воздействий.

Определение термина «ИТВ» и других связанных с ним терминов

На основе составленного выше перечня поражающих факторов ИТВ и, ориентируясь на систему стандартизованных терминов и определений РЭБ [21] как на логический образец (шаблон) составления специальной терминологии, можно следующим образом сформулировать определения терминов «ИТВ», «ИТПр», «ИТОб», которые могут быть нормативными:

- *информационно-техническое воздействие* (*в широком понимании*) – это совокупность мероприятий и действий, направленных на информационно-техническое поражение/подавление информационно-технических объектов (целей) противника;
- *информационно-техническое воздействие* (*в узком понимании*) – это процесс непосредственного информационно-технического поражения/подавления информационно-технических объектов (целей) противника;
- *информационно-техническое поражение/подавление* (*ИТПр*) – это тип поражения/подавления объектов (целей) противника, которое заключается в преднамеренном скрытном несанкционированном внедрении ложных программ или ложных данных в компьютерные устройства информационно-технических объектов (целей) и в последующих выполнении этих программ или обработке этих данных, приводящем к ложному функционированию и снижению эффективности функционирования, либо к блокированию функционирования этих объектов (целей);

- *информационно-технический объект* (*ИТОб*) – это технический объект, в конструкцию которого включены одно или несколько компьютерных устройств, выполняющих функции приёма, обработки, отображения и передачи данных в электронных цифровых форматах.

Теперь на основе этих определений и в логике стандартизованной терминологии по военной технике [7] можно следующим образом определить термин «оружие ИТВ» (или же «Информационно-техническое оружие» (ИТОр).

Оружие ИТВ – это изделие военной техники, предназначенное для информационно-технического поражения/подавления информационно-технических объектов (целей) противника. Поражающими факторами оружия ИТВ являются различные виды ложных программ или ложных данных, которые различными путями и способами преднамеренно, скрытно и не санкционировано внедряются в компьютерные устройства информационно-технических объектов (целей), и последующее выполнение или обработка которых приводит к ложному функционированию и снижению эффективности функционирования, либо к блокированию функционирования этих объектов (целей).

Какая от этого может быть польза?

Сформулированные выше определения терминов «ИТВ», «оружие ИТВ», «ИТПр», «ИТОб» могут оказаться полезными:

1) при решении практических задач реализации положений Доктрины ИБ, когда эти задачи получали бы в качестве компонента своего методического обеспечения взаимно однозначное смысловое и содержательное контрпозиционирование защищаемых объектов информационной инфраструктуры и видов предполагаемого ИТВ на них;
2) при реализации требования Доктрины ИБ по повышению безопасности функционирования образцов ВВСТ, когда для этого мог бы использоваться критерий выделения образцов ВВСТ, которые могут быть объектами (целями) для ИТВ, – это компьютеризированные образцы ВВСТ;
3) при реализации заданных Доктриной ИБ основных направлений обеспечения информационной безопасности в области обороны страны, в т. ч. (в п. а ст. 21) реализации направления по стратегическому сдерживанию и предотвращению военных конфликтов, провоцируемых применением информационных технологий, когда при определении необходимых мер по реализации этого направления рассматривались бы оружие ИТВ (информационно-техническое оружие) и средства защиты от него, имеющие программно-алгоритмическую природу;
4) при проектировании возможных будущих стендовых полигонов, которые оснащались бы программно-техническими имитаторами ИТВ и предназначались для проведения испытаний компьютеризированных образцов ВВСТ и компьютерных компонентов АС и АСУ военного назначения на устойчивость функционирования в условиях модельного натурного ИТВ;

5) при разработке документов информационного противоборства, когда чётко и ясно обозначались бы границы, с одной стороны, для системы, мероприятий и действий, связанных с ИТВ, и, с другой стороны, для системы, мероприятий и действий РЭБ;
6) при разработке профессиональных стандартов возможных новых специальностей, непосредственно связанных с ИТВ, которые отличались бы от профессиональных стандартов по специальностям РЭБ.

Этот перечень возможных вариантов полезного использования новых определений терминов «ИТВ», «ИТПр», «ИТО», «оружие ИТВ» подтверждает правильность предложенного выше логического императива ИТВ.

Что дальше?

Выполненное выше логическое разделение (разведение) ИТВ и РЭПр позволяет предложить выделение отдельного вида противоборства, которое может вестись с использованием оружия ИТВ и средств защиты от него, и которое можно назвать термином *«информационно-техническая борьба»* (ИТБ).

Подобным же образом может быть рассмотрена возможность применения термина *«информационно-психологическая борьба»* для названия вида противоборства, ведущегося с применением информационно-психологического воздействия (ИПВ)[9].

В дальнейшем могут потребоваться определения и других терминов, связанных с понятиями и терминами «ИТВ» и «ИПВ», например, понятий и терминов для обозначения систем, комплексов, действий и операций информационно-технической борьбы и информационно-психологической борьбы[10].

Заключение

Проведен анализ недостатков известных вариантов понимания термина «информационно-техническое воздействие» и разработано его новое определение, которое опирается на предложенное автором настоящей статьи понимание природы, сущности и поражающих факторов ИТВ, которые отличаются от природы, сущности и поражающих факторов оружия РЭБ. Это отличие является основой для логического разведения (разделения) двух типов оружия – оружия ИТВ и оружия РЭБ.

На основе предложенного нового понимания ИТВ разработаны определения других связанных с ИТВ терминов: «информационно-технический объект», «информационно-техническое поражение/подавление», «оружие ИТВ», кото-

[9] *Примечание.* «Информационно-психологическое воздействие – комплекс мероприятий по воздействию на интеллектуальную, рационально-волевую и эмоционально-чувственную сферу психики и подсознание информационно-психологических объектов, направленных на формирование у них прогнозируемых мнений и взглядов, мировоззренческих и психологических установок, поведенческих реакций» [10]).

[10] *Примечание.* Нельзя не отметить то, что идеи этих двух видов борьбы уже высказывались ранее военными специалистами, например, авторы статьи [50] уверенно используют термины «информационно-техническое противоборство» и «информационно-психологическое противоборство».

рые вместе с разработанным новым определением термина «ИТВ» могут быть предложены для нормативного использования.

Показаны возможные направления практического приложения выполненного логического разведения (разделения) информационно-технического воздействия и радиоэлектронного поражения в задачах реализации Доктрины ИБ в области обороны страны.

Обозначена возможность типизации вооружённой борьбы с применением оружия ИТВ и средств защиты от него, которая может именоваться термином «информационно-техническая борьба». Ещё один термин информационного противоборства – «информационно-психологическая борьба» – может стать предметом понятийной и терминологической разработки, исходя из сущности и поражающих факторов информационно-психологического воздействия.

Методология и результаты решения задач разработки понятий и возможных нормативных определений терминов «информационно-техническая борьба» и «информационно-психологическая борьба» могут быть рассмотрены в отдельных будущих публикациях.

Литература

1. Доктрина информационной безопасности Российской Федерации. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 // Российская газета [Электронный ресурс]. 06.12.2018. – URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 18.04.2018).

2. Кибервойна против России – США посылают сигнал // BFM.ru [Электронный ресурс]. 15.10.2016. – URL: http://www.bfm.ru/news/336185 (дата обращения: 18.04.2018).

3. Wikileaks приступила к публикации серии утечек данных ЦРУ // ТАСС [Электронный ресурс]. 07.03.2017. – URL: http://tass.ru/mezhdunarodnaya-panorama/4077820 (дата обращения: 18.04.2018).

4. Опубликована коллекция хакерских инструментов ЦРУ // Geektimes [Электронный ресурс]. 08.03.2017. – URL: http://geektimes.ru/post/286702 (дата обращения: 18.04.2018).

5. Ларина Е. С. Кибервойна США против России уже началась // REGNUM [Электронный ресурс]. 24.02.2015. – URL: https://regnum.ru/news/polit/1898308.html (дата обращения: 18.04.2018).

6. Горбачёв Ю. Кибервойна уже идёт. Армия втягивается в информационное противоборство // Независимая газета [Электронный ресурс]. 12.04.2013. – URL: http://nvo.ng.ru/armament/2013-04-12/1_cyberwar.html (дата обращения: 18.04.2018).

7. ГОСТ РВ 51540–2005. Военная техника. Термины и определения. – М.: Стандартинформ, 2011. – 12 с.

8. Война и мир. Военно-политический словарь. Статья 9.1.4 ОРУЖИЕ / под общей ред. Д. О. Рогозина [Электронный ресурс]. 2018. – URL: http://www.voina-i-mir.ru/article/434 (дата обращения: 18.04.2018).

9. Гриняев С. Н. Поле битвы — киберпространство. Теория, приемы, средства, методы и системы ведения информационной войны. – М.: Харвест, 2004. – 416 с.

10. Словарь терминов и определений в области информационной безопасности / Военная академия Генерального штаба Вооружённых Сил Российской Федерации. Научно-исследовательский центр информационной безопасности. – М.: Воениформ, 2008. – 208 с.

11. Информационная война и защита информации. Словарь основных терминов и определений. – М.: Центр стратегических прогнозов и оценок, 2011. – 68 с. – URL: http://csef.ru/media/articles/2176/2176.pdf (дата обращения: 18.04.2018).

12. Гражданская защита: Энциклопедический словарь / под общей ред. В. А. Пучкова. – М.: ФГБУ ВНИИ ГОЧС (ФЦ), 2015. – 664 с. – URL: http://www.mchs.gov.ru/upload/site1/document_file/4DadHaPBwt.pdf (дата обращения: 18.04.2018).

13. Макаренко С. И. Информационное оружие в технической сфере: терминология, классификация, примеры // Системы связи, управления и безопасности. 2016. № 3. С. 292–376. – URL: http://sccs.intelgr.com/archive/2016-03/11-Makarenko.pdf (дата обращения: 18.04.2018).

14. Макаренко С. И. Информационное противоборство и информационная война в сетецентрических войнах начала XXI века. Монография. – СПб.: Наукоемкие технологии, 2017. – 546 с. – URL: http://publishing.intelgr.com/archive/Makarenko-InfPro.pdf (дата обращения: 18.4.2018).

15. Климов С. М., Зорин Э. Ф., Половников А. Ю., Антонов С. Г. Основные направления обеспечения информационной безопасности ракетных комплексов стратегического назначения в условиях информационно-технических воздействий // Военная мысль. № 6. 2016. С. 24–29.

16. Рекомендации по стандартизации Р 50.1.053–2005. Информационные технологии. Основные термины и определения в области технической защиты информации. Ст. 3.2.16. – М.: Стандартинформ, 2005. – 16 с.

17. Рекомендации по стандартизации Р 50.1.056–2005. Техническая защита информации. Основные термины и определения. Ст. 3.2.8. – М.: Стандартинформ, 2006. – 16 с.

18. Макаренко С. И., Чукляев И. И. Терминологический базис в области информационного противоборства // Вопросы кибербезопасности. 2014. № 1(2). С. 13–21. – URL: http://cyberrus.com/wp-content/uploads/2014/03/13-21.pdf (дата обращения: 18.04.2018).

19. Буренок В. М., Ивлев А. А., Корчак В. Ю. Развитие военных технологий XXI века: проблемы, планирование, реализация. – Тверь: ООО «Купол», 2009. – 624 с.

20. Средства информационной борьбы («Информационное оружие») // Военный энциклопедический словарь Министерства обороны Российской Федерации [Электронный ресурс]. 2018. – URL:

http://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=14342 (дата обращения: 18.04.2018).

21. ГОСТ РВ 0158-002–2008. Борьба радиоэлектронная. Термины и определения. – М.: Стандартинформ, 2009. – 12 с.

22. Леньшин А. В. Бортовые системы и комплексы радиоэлектронного подавления. Воронеж: Научная книга, 2014. – 90 с.

23. Осипов А. С. Военно-техническая подготовка. Военно-технические основы построения средств и комплексов РЭП : учебник / под науч. ред. Е. Н. Гарина. – Красноярск: Сибирский федеральный университет, 2013. – 344 с. – URL: http://vii.sfu-kras.ru/images/libs/Osnovi_repp.pdf (дата обращения: 18.04.2018).

24. Новиков В. К. Информационное оружие – оружие современных и будущих войн. – М.: Горячая линия - Телеком, 2016. – 288 с.

25. Сироткин Д. В., Мартьянов А. Н., Новиков В. К., Пономаренко А. В. Модель информационного противоборства в Вооруженных силах Российской Федерации // Отечественная юриспруденция. 2016. № 8(10). С. 49–51. – URL: https://legalscience.ru/images/PDF/2016/10/Otechestvennaja-jurisprudencija-8-10.pdf (дата обращения: 18.04.2018).

26. Антонович П. И., Макаренко С. И., Михайлов Р. Л., Ушанев К. В. Перспективные способы деструктивного воздействия на системы военного управления в едином информационном пространстве // Вестник Академии военных наук. 2014. № 3 (48). С. 93–101. – URL: http://sccs.intelgr.com/editors/Makarenko/Makarenko-podavlenie.pdf (дата обращения: 18.04.2018).

27. Макаренко С. И. Подавление сетецентрических систем управления радиоэлектронными информационно-техническими воздействиями // Системы управления, связи и безопасности. 2017. № 4. С. 15–59. – URL: http://sccs.intelgr.com/archive/2017-04/02-Makarenko.pdf (дата обращения: 18.04.2018).

28. Военные РФ впервые отработали информационное противоборство на учениях «Кавказ» // ТАСС [Электронный ресурс]. 14.09.2016. – URL: http://tass.ru/armiya-i-opk/3619816 (дата обращения: 18.04.2018).

29. Кондаков Н. И. Логический словарь-справочник. – М.: Наука, 1975. – 720 с.

30. Колесов Н. А., Носенков И. Г. Радиоэлектронная борьба. От экспериментов прошлого до решающего фронта будущего / М. С. Барабанов, С. А. Денисенцев, В. Б. Кашин, А. В. Лавров, Р. Н. Пухов, Д. В. Федутинов, А. А. Хетагуров, М. Ю. Шеповаленко; под ред. Н. А. Колесова и И. Г. Насенкова. – М.: Центр анализа стратегий и технологий, 2015. – 248 с.

31. ГОСТ Р 51275–2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ст. 3.1. – М.: Стандартинформ, 2007. – 11 с.

32. ГОСТ Р 50739–95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Гл. 1. – М.: Стандартинформ, 2006. – 8 с.

33. Воройский Ф. С. Информатика. Энциклопедический систематизированный словарь-справочник: введение в современные информационные и телекоммуникационные технологии в терминах и фактах. – М.: Физматлит, 2008. – 767 с.

34. Таненбаум Э., Остин Т. Архитектура компьютера. – СПб.: Питер, 2013. – 816 с.

35. Гражданский кодекс Российской Федерации от 18 декабря 2006 г. N 230-ФЗ Часть четвертая. Ст. 1261 // Российская газета [Электронный ресурс]. 22.12.2018. – URL: https://rg.ru/2006/12/22/grazhdansky-kodeks.html (дата обращения: 18.04.2018).

36. ГОСТ Р ИСО/МЭК 12119–2000. Информационная технология. Пакеты программ. Требования к качеству и тестирование. Ст. А.3.1. – М.: Стандартинформ, 2006. – 19 с.

37. Забегалин Е. В. Определение термина «компьютерная безопасность» // Системы связи, управления и безопасности. 2017. № 4. С. 102–111. – URL: http://sccs.intelgr.com/archive/2017-04/05-Zabegalin.pdf (дата обращения: 18.4.2018).

38. Бирюков А. А. Информационная безопасность: защита и нападение. – М.: ДМК Пресс, 2017. – 434 с.

39. Климов С. М. Методы и модели противодействия компьютерным атакам. – Люберцы: КАТАЛИТ, 2008. – 316 с.

40. Марков А. С., Фадин А. А. Систематика уязвимостей и дефектов безопасности программных ресурсов // Защита информации. INSIDE. 2013. № 3. С. 2–7. – URL: https://www.npo-echelon.ru/doc/is_taxonomy.pdf (дата обращения: 18.04.2018).

41. Шелухин О. И., Сакалема Д. Ж., Филинова А. С. Обнаружение вторжений в компьютерные сети (сетевые аномалии). Учебное пособие для вузов / Под ред. профессора О. И. Шелухина. – М.: Горячая линия - Телеком, 2016. – 220 с.

42. ГОСТ Р 56545-2015. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей. – М.: Стандартинформ, 2015. – 12 с.

43. Поражение объектов, целей // Военный энциклопедический словарь Министерства обороны Российской Федерации [Электронный ресурс]. 2018. – URL: http://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=9201 (дата обращения: 18.04.2018).

44. Подавление объектов, целей // Военный энциклопедический словарь Министерства обороны Российской Федерации [Электронный ресурс]. 2018. – URL: http://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=8995 (дата обращения: 18.04.2018).

45. Егоров М. Выявление и эксплуатация SQL-инъекций в приложениях // Защита информации. INSIDE. 2011. № 2. С. 2–8. – URL: http://www.inside-zi.ru/pages/2_2011/76.html (дата обращения: 18.04.2018).

46. Жук А. П., Осипов Д. Л., Гавришев А. А., Бурмистров В. А. Анализ методов защиты от несанкционированного доступа беспроводных каналов

связи робототехнических систем // Наукоемкие технологии в космических исследованиях Земли, 2016. Т. 8. № 2. С. 38–42. – URL: https://cyberleninka.ru/article/v/analiz-metodov-zaschity-ot-nesanktsionirovannogo-dostupa-besprovodnyh-kanalov-svyazi-robototehnicheskih-sistem (дата обращения: 18.04.2018).

47. Климов С. М. Модель бескомпроматного аудита информационной безопасности сети спутниковой связи // Двойные технологии. 2013. № 3(64). С. 15–20. – URL: http://pstmprint.ru/wp-content/uploads/2016/11/dt-3-2013-3.pdf (дата обращения: 18.04.2018).

48. Оганесян А. А. Повышение функциональной надёжности координатно-временного навигационного обеспечения робототехнических комплексов // Сборник материалов деловой программы XVIII Международной выставки средств обеспечения безопасности государства «Интерполитех-2014», 2014. С. 47–50. – URL: http://e-edition.ru/katalog/materials-ipx-2014/files/assets/basic-html/page47.html (дата обращения: 18.04.2018).

49. Петренко С. А. Методы информационно-технического воздействия на киберсистемы и возможные способы противодействия // Труды ИСА РАН. 2009. Т. 41. С. 104–146. – URL: http://www.isa.ru/proceedings/images/documents/2009-41/104-146.pdf (дата обращения: 18.04.2018).

50. Скоков С. И., Грушка Л. В. Информационное противоборство во внутреннем вооружённом конфликте как следствие стратегического информационного противоборства // Вестник Сибирского отделения Академии военных наук. 2014. № 27. С. 25–36. – URL: http://www.avnrf.ru/attachments/article/726/%D0%90%D0%92%D0%9D27%20%D0%B8%D1%81%D0%BF%D1%80.doc (дата обращения: 18.04.2018).

51. Cyber Attacks in Space // Israel Defense [Электронный ресурс]. 29.07.2013. – URL: http://www.israeldefense.co.il/en/content/cyber-attacks-space (дата обращения: 18.04.2018).

52. Классификация вредоносного ПО // Интернет-сайт компании «Элика Плюс» [Электронный ресурс]. 29.01.2010. – URL: http://virus.e-pls.ru/index.php/home/2010-01-29-14-24-20 (дата обращения: 18.04.2018).

53. Классификация вредоносных программ // Интернет-сайт компании «Лаборатория Касперского» [Электронный ресурс]. 2018. – URL: http://www.kaspersky.ru/internet-security-center/threats/malware-classifications (дата обращения: 18.04.2018).

54. Что такое компьютерный вирус и компьютерный червь? // Интернет-сайт компании «Лаборатория Касперского» [Электронный ресурс]. 2018. – URL: http://www.kaspersky.ru/internet-security-center/threats/viruses-worms (дата обращения: 18.04.2018).

55. Что такое троянская программа? // Интернет-сайт компании «Лаборатория Касперского» [Электронный ресурс]. 2018. – URL: http://www.kaspersky.ru/internet-security-center/threats/trojans (дата обращения: 18.04.2018).

56. Что такое вредоносные утилиты? // Интернет-сайт компании «Лаборатория Касперского» [Электронный ресурс]. 2018. – URL: http://www.kaspersky.ru/internet-security-center/threats/malicious-tools (дата обращения: 18.04.2018).

References

1. Doctrine of Information Security of the Russian Federation. *Rossiiskaia hazeta* [Russian Newspaper], 06 December 2016. Available at: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (accessed 18 April 2018) (in Russian).

2. Kibervoina protiv Rossii – SShA posylaiut signal [Cyberwar Against Russia – US Sends Signal]. *BFM.ru*, 10 October 2016. Available at: http://www.bfm.ru/news/336185 (accessed 18 April 2018) (in Russian).

3. Wikileaks pristupila k publikatsii serii utechek dannykh TsRU [Wikileaks started publishing a series of data leakage of the CIA]. *TASS*, 07 March 2017. Available at: http://tass.ru/mezhdunarodnaya-panorama/4077820 (accessed 18 April 2018) (in Russian).

4. Opublikovana kollektsiia khakerskikh instrumentov TsRU [Published a Collection of Hacking Tools of the CIA]. *Geektimes*, 08 March 2017. Available at: http://geektimes.ru/post/286702 (accessed 18 April 2018) (in Russian).

5. Larina E. S. Kibervoina SShA protiv Rossii uzhe nachalas' [Cyberwar of the United States Against Russia Has Already Begun]. *REGNUM*, 24 February 2015. Available at: https://regnum.ru/news/polit/1898308.html (accessed 18 April 2018) (in Russian).

6. Gorbachev Iu. Kibervoina uzhe idet. Armiia vtiagivaetsia v informatsionnoe protivoborstvo [The Cyberwar Already is. The Army is Drawn into the Information Confrontation]. *Nezavisimaia hazeta* [Independent Newspaper], 12 April 2013. Available at: http://nvo.ng.ru/armament/2013-04-12/1_cyberwar.html (accessed 18 April 2018) (in Russian).

7. State Standard RV 51540–2005. Military equipment. Taxonomy. Moscow, Standartinform Publ., 2011. 12 p. (in Russian).

8. Voina i mir. Voenno-politicheskii slovar', 9.1.4 ORUZHIE [War and Peace. Military-Political Dictionary, 9.1.4 WEAPONS]. 2018. Available at: http://www.voina-i-mir.ru/article/434 (accessed 18 April 2018) (in Russian).

9. Griniaev S. N. *Pole bitvy — kiberprostranstvo. Teoriia, priemy, sredstva, metody i sistemy vedeniia informatsionnoi voiny.* [The Battlefield is Cyberspace. Theory, Methods, Means, Methods and Systems of Information Warfare]. Moscow, Kharvest Publ., 2004. 416 p. (in Russian).

10. Slovar' terminov i opredelenii v oblasti informatsionnoi bezopasnosti [Dictionary of Terms and Definitions in the Field of Information Security]. Moscow, Voennaia akademiia General'nogo shtaba Vooruzhennykh Sil Rossiiskoi Federatsii, Nauchno-issledovatel'skii tsentr informatsionnoi bezopasnosti. Voeninform Publ., 2008. 208 p. (in Russian).

11. Informatsionnaia voina i zashchita informatsii. Slovar' osnovnykh terminov i opredelenii. [Information War and Information protection. Dictionary of Basic

Terms and Definitions]. Moscow, The Centre of Strategic Estimations and Forecasts, 2011. 68 p. Available at: http://csef.ru/media/articles/2176/2176.pdf (accessed 18 April 2018) (in Russian).

12. Grazhdanskaia zashchita: Entsiklopedicheskii slovar' [Civil Protection: Encyclopedic Dictionary]. Moscow, All-Russian Institute for Research of Civil Defense and Emergencies Situations of the Emergencies Ministry of Russia (the Federal Science and High Technology Center), 2015. 664 p. Available at: http://www.mchs.gov.ru/upload/site1/document_file/4DadHaPBwt.pdf (accessed 18 April 2018) (in Russian).

13. Makarenko S. I. Information Weapons in the Technical Sphere: Terminology, Classification, Examples. *Systems of Control, Communication and Security*, 2016. no. 3, pp. 292–376. Available at: http://sccs.intelgr.com/archive/2016-03/11-Makarenko.pdf (accessed 18 April 2018) (in Russian).

14. Makarenko S. I. *Informatsionnoe protivoborstvo i informatsionnaia voina v setetsentricheskikh voinakh nachala XXI veka. Monografiia* [Information Confrontation and Information War in the network-centric Wars of the Beginning of the XXI century. Monography]. St. Petersburg, Naukoemkie tekhnologii Publ., 2017. 546 p. Available at: http://publishing.intelgr.com/archive/Makarenko-InfPro.pdf (accessed 18 April 2018) (in Russian).

15. Klimov S. M., Zorin E. F., Polovnikov A. Iu., Antonov S. G. Main Directions of Ensuring Information Security of Strategic Missile Systems in Terms of Informational-and-Technical Influences. *Military Thought*, no. 6, 2016, pp. 24-29. (in Russian).

16. State Standard Recommendation R 50.1.053–2005. Information Technology. Taxonomy on technical protection of information. Article 3.2.16. Moscow, Standartinform Publ., 2005. 16 p. (in Russian).

17. State Standard Recommendation R 50.1.056–2005. Technical protection of information. Taxonomy. Article 3.2.8. Moscow, Standartinform Publ., 2006. 16 p. (in Russian).

18. Makarenko S. I., Chukliaev I. I. The Terminological Basis of the Informational Conflict Area. *Voprosy kiberbezopasnosti*, 2014. no. 1(2), pp. 13–21. Available at: http://cyberrus.com/wp-content/uploads/2014/03/13-21.pdf (accessed 18 April 2018) (in Russian).

19. Burenok V. M., Ivlev A. A., Korchak V. Iu. *Razvitie voennykh tekhnologii XXI veka: problemy, planirovanie, realizatsiia* [Development of Military Technologies of the XXI Century: Problems, Planning, Implementation]. Tver', OOO "Kupol" Publ., 2009. 624 p, p. 473. (in Russian).

20. Sredstva informacionnoj bor'by ("Informacionnoe oruzhie") [Means of Information Struggle ("Information weapons")]. *Military Encyclopedic Dictionary of the Ministry of Defence of the Russian Federation*, 2018. Available at: http://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=14342 (accessed 18 April 2018) (in Russian).

21. State Standard RV 0158-002–2008. Radio-electronic warfare. Taxonomy. Moscow, Standartinform Publ., 2009. 12 p. (in Russian).

22. Len'shin A. V. *Bortovye sistemy i kompleksy radioelektronnogo podavleniia* [On-board Systems and Radio-electronic Suppression Systems]. Voronezh, Nauchnaia kniga Publ., 2014. 90 p. (in Russian).

23. Osipov A. S. *Voenno-tekhnicheskaia podgotovka. Voenno-tekhnicheskie osnovy postroeniia sredstv i kompleksov REP* [Military-technical training. Military-technical foundations for constructing means and complexes for Radio-electronic suppression]. Krasnoiarsk, Siberian Federal University, 2013. 344 p. Available at: http://vii.sfu-kras.ru/images/libs/Osnovi_repp.pdf (accessed 18 April 2018) (in Russian).

24. Novikov V. K. *Informatsionnoe oruzhie – oruzhie sovremennykh i budushchikh voin.* [Information Weapons – Weapons of Modern and Future Wars]. Moscow, Goriachaia liniia - Telekom Publ., 2016. 288 p. (in Russian).

25. Sirotkin D. V., Mart'ianov A. N., Novikov V. K., Ponomarenko A. V. *Model' informatsionnogo protivoborstva v Vooruzhennykh silakh Rossiiskoi Federatsii* [Model of Information Confrontation in the Armed Forces of the Russian Federation]. *National Law*, 2016, no. 8 (10), pp. 49–51. Available at: https://legalscience.ru/images/PDF/2016/10/Otechestvennaja-jurisprudencija-8-10.pdf (accessed 18 April 2018) (in Russian).

26. Antonovich P. I., Makarenko S. I., Mikhailov R. L., Ushanev K. V. New Means of Destructive Effects on Network Centric Military Command, Control and Communication Systems in the Common Information Space. *Vestnik Akademii voennykh nauk*, 2014, № 3 (48), pp. 93–101. Available at: http://sccs.intelgr.com/editors/Makarenko/Makarenko-podavlenie.pdf (accessed 18 April 2018) (in Russian).

27. Makarenko S. I. Suppression of a Net-Centric Control System with Radio Cyber Attacks. *Systems of Control, Communication and Security*, 2017, no. 4, pp. 15–59. Available at: http://sccs.intelgr.com/archive/2017-04/02-Makarenko.pdf (accessed 18 April 2018) (in Russian).

28. Voennye RF vpervye otrabotali informatsionnoe protivoborstvo na ucheniiakh "Kavkaz" [The Military of Russia for the First Time Worked out Information Confrontation in the Exercises "Caucasus"]. *TASS*, 14 September 2016. Available at: http://tass.ru/armiya-i-opk/3619816 (accessed 18 April 2018) (in Russian).

29. Kondakov N. I. *Logicheskii slovar'-spravochnik.* [The Logical Dictionary-directory]. Moscow, Nauka Publ., 1975. 720 p. (in Russian).

30. Kolesov N. A., Nosenkov I. G. *Radioelektronnaia bor'ba. Ot eksperimentov proshlogo do reshaiushchego fronta budushchego* [Radio-electronic Warfare. From the Experiments of the Past to the Decisive Front of the Future]. Moscow, Tsentr analiza strategii i tekhnologii, 2015. 248 p. (in Russian).

31. State Standard R 51275–2006. Data protection. The object of informatization. Factors affecting information. General provisions. Article 3.1. Moscow, Standartinform, Publ., 2007. 11 p. (in Russian).

32. State Standard R 50739–1995. Means of computer facilities. Protection against unauthorized access to information. General technical requirements. Ch.1. Moscow, Standartinform Publ., 2006. 8 p. (in Russian).

33. Voroiskii F. S. *Informatika. Entsiklopedicheskii sistematizirovannyi slovar'-spravochnik: vvedenie v sovremennye informatsionnye i telekommunikatsionnye tekhnologii v terminakh i faktakh* [Computer Science. Encyclopaedic Systematized Dictionary-reference: Introduction to Modern Information and Telecommunication Technologies in Terms and Facts]. Moscow, Fizmatlit Publ., 2008. 767 p. (in Russian).

34. Tanenbaum A. S., Austin T. *Structured Computer Organization (6th Edition)*. Amsterdam, Pearson Education Limited, 2012. 800 p.

35. Civil Code of the Russian Federation. Fourth Part. Article 1261 // *Rossiiskaia hazeta* [Russian Newspaper], 18 December 2006. Available at: https://rg.ru/2006/12/22/grazhdansky-kodeks.html (accessed 18 April 2018) (in Russian).

36. ISO/IEC 12119:1994. Information technology – Software packages – Quality requirements and testing. International Organization for Standardization, 1994, 20 p.

37. Zabegalin E. V. Definition of the Term "Computer Security". *Systems of Control, Communication and Security*, 2017, no 4, pp. 102-111. Available at: http://sccs.intelgr.com/archive/2017-04/05-Zabegalin.pdf (accessed 18 April 2018) (in Russian).

38. Biriukov A. A. *Informatsionnaia bezopasnost': zashchita i napadenie.* [Information Security: Protection and Attack]. Moscow, DMK Press, 2017. 434 p. (in Russian).

39. Klimov S.M. *Metody i modeli protivodeistviia komp'iuternym atakam* [Methods and Models for Countering Computer Attacks]. Liubertsy, KATALIT Publ., 2008. 316 p. (in Russian).

40. Markov A. S., Fadin A. A. Sistematika uiazvimostei i defektov bezopasnosti programmnykh resursov [Systematics of Vulnerabilities and Security Flaws in Software Resources]. *Zasita informacii. Inside*, 2013, no. 3, pp. 2–7. Available at: https://www.npo-echelon.ru/doc/is_taxonomy.pdf (accessed 18 April 2018) (in Russian).

41. Shelukhin O. I., Sakalema D. Zh., Filinova A. S. *Obnaruzhenie vtorzhenii v komp'iuternye seti (setevye anomalii)* [Detection of Intrusions into Computer Networks (Network Anomalies)]. Moscow, Goriachaia liniia - Telekom Publ., 2016. 220 p. (in Russian).

42. State Standard R 51275–2006. Data protection. Vulnerabilities of information systems. Vulnerability description rules. Moscow, Standartinform Publ., 2015. 12 p. (in Russian).

43. Porazhenie ob"ektov, celej [Defeat of Objects, Targets]. *Military Encyclopedic Dictionary of the Ministry of Defence of the Russian Federation*, 2018. Available at: http://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=9201 (accessed 18 April 2018) (in Russian).

44. Podavlenie ob"ektov, celej [Suppression of Objects, Targets]. *Military Encyclopedic Dictionary of the Ministry of Defence of the Russian Federation*, 2018. Available at: http://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=8995 (accessed 18 April 2018) (in Russian).

45. Egorov M. Vyiavlenie i ekspluatatsiia SQL-in"ektsii v prilozheniiakh [Identifying and Exploiting SQL Injections in Applications]. *Zasita informacii. Inside*, 2011, no 2, pp. 2–8. Available at: http://www.inside-zi.ru/pages/2_2011/76.html (accessed 18 April 2018) (in Russian).

46. Zhuk A. P., Osipov D. L., Gavrishev A. A., Burmistrov V. A. Analysis Methods of Protection Against Unauthorized Access Wirelessly Robotic systems. *H&ES Research*, 2016, vol. 8, no. 2, pp. 38–42. Available at: https://cyberleninka.ru/article/v/analiz-metodov-zaschity-ot-nesanktsionirovannogo-dostupa-besprovodnyh-kanalov-svyazi-robototehnicheskih-sistem (accessed 18 April 2018) (in Russian).

47. Klimov S.M. The Audit Model Information Safety Satellite Communications Network Without Compromising. *Dual technology*, 2013. no. 3(64), pp. 15–20. Available at: http://pstmprint.ru/wp-content/uploads/2016/11/dt-3-2013-3.pdf (accessed 18 April 2018) (in Russian).

48. Oganesian A. A. Povyshenie funktsional'noi nadezhnosti koordinatno-vremennogo navigatsionnogo obespecheniia robototekhnicheskikh kompleksov [Increase of the Functional Reliability of the Coordinate-time Navigation Support of Robotic Complexes]. *Sbornik materialov delovoi programmy XVIII Mezhdunarodnoi vystavki sredstv obespecheniia bezopasnosti gosudarstva "Interpolitekh-2014"*, 2014, pp. 47–50. Available at: http://e-edition.ru/katalog/materials-ipx-2014/files/assets/basic-html/page47.html (accessed 18 April 2018) (in Russian).

49. Petrenko S. A. Metody informatsionno-tekhnicheskogo vozdeistviia na kibersistemy i vozmozhnye sposoby protivodeistviia [Methods of Information and Technical Impact on Cyber Systems and Possible Ways of Counteraction]. *Trudy Instituta sistemnogo analiza Rossiiskoi akademii nauk*, 2009, vol. 41, pp. 104–146. Available at: http://www.isa.ru/proceedings/images/documents/2009-41/104-146.pdf (accessed 18 April 2018) (in Russian).

50. Skokov S. I., Grushka L. V. Informatsionnoe protivoborstvo vo vnutrennem vooruzhennom konflikte kak sledstvie strategicheskogo informatsionnogo protivoborstva [Information Confrontation in the Internal Armed Conflict as a Consequence of the Strategic Information Confrontation]. *Vestnik Sibirskogo otdeleniia Akademii voennykh nauk*, 2014, no. 27, pp. 25–36. Available at: http://www.avnrf.ru/attachments/article/726/%D0%90%D0%92%D0%9D27%20%D0%B8%D1%81%D0%BF%D1%80.doc (accessed 18 April 2018) (in Russian).

51. Cyber Attacks in Space. *Israel Defens*, 29 July 2013. Available at: http://www.israeldefense.co.il/en/content/cyber-attacks-space (accessed 18 April 2018).

52. Klassifikatsiia vredonosnogo PO [Malware Cassification]. *"Elika Plius" company Internet-site*, 2018. Available at: http://virus.e-pls.ru/index.php/home/2010-01-29-14-24-20 (accessed 18 April 2018) (in Russian).

53. Klassifikatsiia vredonosnykh programm [Malware Cassification]. *"Kaspersky Laboratory" company Internet-site*, 2018. Available at: http://www.kaspersky.ru/internet-security-center/threats/malware-classifications (accessed 18 April 2018) (in Russian).

54. Chto takoe komp'iuternyi virus i komp'iuternyi cherv'? [What is a Computer Virus and a Computer Worm?]. *"Kaspersky Laboratory" company Internet-site*, 2018. Available at: http://www.kaspersky.ru/internet-security-center/threats/viruses-worms (accessed 18 April 2018) (in Russian).

55. Chto takoe troianskaia programma? [What is a Trojan?]. *"Kaspersky Laboratory" company Internet-site*, 2018. Available at: http://www.kaspersky.ru/internet-security-center/threats/trojans (accessed 18 April 2018) (in Russian).

56. Chto takoe vredonosnye utility? [What are Malicious Tools]. *"Kaspersky Laboratory" company Internet-site*, 2018. Available at: http://www.kaspersky.ru/internet-security-center/threats/malicious-tools (accessed 18 April 2018) (in Russian).

Статья поступила 19 апреля 2018 г.

Информация об авторе

Забегалин Евгений Викторович – кандидат технических наук. Старший научный сотрудник. 4 Центральный научно-исследовательский институт. Область научных интересов: информационная безопасность. E-mail: ezabex@yandex.ru

Адрес: 141092, Россия, Московская обл., г. Королёв, мкр. Юбилейный, ул. М.К. Тихонравова, д. 29.

A question of definition of the term «information and technical impact»

E. V. Zabegalin

The relevance of the task. *The Doctrine of Information Security of the Russian Federation (DIS), approved on December 5, 2016 in a new edition, introduced the official term "information and technical impact" ("ITI") and referred the activities of a number of foreign countries to increase ITI capabilities for information infrastructure for military purposes to the number of negative factors affecting the state of information security of the country. In the text of the DIS there is no definition of the term "ITI". There is no it in other government documents. Various variants of definitions of the term "ITI" are known from published directories and works of specialists, but none of them is suitable for regulatory use. In the author's opinion, this situation needs to be resolved – the term "ITI" should receive its normative definition in the interests of further development of the theory and practice of information confrontation and information security.* ***The purpose of the work*** *is to develop a definition of the term "ITI", which can be proposed for use in guidance and regulatory technical documents and which can carry a common paradigm for solving a variety of theoretical and practical tasks in accordance with the provisions of the DIS.* ***Method for solving the problem:*** *first, the known variants of the definition of the term "ITI" are analyzed and their shortcomings are identified; then the logical imperative of the terminological distinction and separation of ITI and radio-electronic defeat of targets are determined; then the nature, essence and striking factors of ITI, which are differ from those in the radio-electronic defeat of targets, are defined; and at the end, the definition of the term "ITI" is modeled on the standardized terminology of radio-electronic warfare and also definitions of other ITI-related terms are modeled, including the definition of the term "ITI weapons", which is consistent with the standardized terminology on military equipment.* ***The novelty of the solution*** *lies in the new definition of the term "information and technical impact", which differs from the known definitions in that it is based on the author's initial imperative distinction of the nature, essence and striking factors of ITI from those of radio-electronic defeat of targets. Also a distinctive feature of ITI is proposed – violation of computer security of objects (targets) of information and technical impact.* ***The theoretical significance of the work*** *is that the new definitions of the term "ITI" and other related terms expand the range of modern views of specialists on the means of information confrontation and can be taken into account in the construction of terminological basis of information confrontation.*

Keywords: *information and technical impact, ITI, ITI-weapon, striking factors of ITI, information and technical defeat, information and technical object, information confrontation, information security, computer security, radio-electronic warfare, radio-electronic defeat.*

Information about Author

Evgeniy Viktorovich Zabegalin – Ph.D. of Engineering Sciences. Senior Research Officer. The 4th Central Research Institute of the Ministry of Defence of the Russian Federation. Field of research: information security. E-mail: ezabex@yandex.ru

Address: Russia, 141092, Moskovskaya oblast, Korolev, mkr. Yubileyny, ulica M.K. Tikhonravova, 29.