МЕТОДИЧЕСКИЙ ПОДХОД К ОЦЕНКЕ ЖИВУЧЕСТИ ИНФОРМАЦИОННЫХ ОБЪЕКТОВ В УСЛОВИЯХ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

УДК 365.42

Ю. Е. Кулешов, С. И. Паскробка, А. А. Родионов*

В условиях ведения информационного противоборства одним из важнейших факторов, оказывающих влияние на функционирование информационных объектов, является их живучесть. Авторами в статье предлагается методический подход к расчету показателей живучести информационных объектов в условиях информационного противоборства.

Under the information counterstruggle conditions one of the most important factors affecting the functioning information objects is vitality. The authors in the article propose methodical step an approach to calculating the data of vitality information objects in information counterstruggle conditions.

Широкая информатизация процесса управления в современных условиях создала в военном деле качественно новую ситуацию. С середины XX века произошел бурный рост роли средств получения, передачи, обработки и представления военной информации в ходе и исходе операций (боевых действий) войск. В военном деле сложилась ситуация, когда дальнейший рост боевой эффективности оружия потребовал информатизации, т. е. преодоления ограничений информационно-управляющих возможностей людей.

Создание и развитие технических средств осуществления информационных процессов, их внедрение в военное дело, а также развитие информатики как комплексной области научно-технической деятельности, изучающей информацию и информационные потоки, построение мощных информационно-коммуникационных систем создали предпосылки к научному определению сущности и содержания информационного противоборства.

В настоящее время под информационным противоборством понимается борьба в информационной сфере, которая предполагает комплексное деструктивное воздействие на информацию, информационные системы и информационную инфраструктуру противоборствующей стороны с одновременной защитой собственной информации, информационных систем и информационной инфраструктуры от подобного воздействия.

Как показывает анализ зарубежной и отечественной военно-научной литературы, главной целью информационного противоборства являются завоевание и удержание информационного превосходства над противоборствующей стороной, что определяется как способность собирать, обрабатывать и распределять непрерывный поток информации об обстановке, препятствуя противнику делать то же самое.

Цель информационного противоборства достигается путем решения задач комплексного опережающего информационного воздействия: вывод из строя, подавление систем разведывательно-информационного обеспечения противника (средства и системы разведки, сетеобразующие узлы, центры обработки информации и управления), формирование общественного сознания населения, соответствующая подготовка политического и военного руководства и защита собственной информационной среды.

Анализ взглядов на теорию информационного противоборства, приведенный в [1], показывает, что, например, в США разработаны и совершенствуются руководящие и методические документы по вопросам информационного противоборства, создаются и развиваются органы управления и подразделения для их ведения. Так, 13 февраля 2006 г. комитетом начальников штабов была утверждена новая редакция доктрины «Информационные операции» (JP 3-13), в которой пересмотрены взгляды американского военного руководства на подготовку и ведение информационных операций вооруженными силами, уточнены цели, задачи и основные принципы информационного противоборства, а также обязанности долж-

ностных лиц по подготовке и проведению информационных операций как в мирное, так и в военное время.

До последнего времени в США решающую роль в информационном противоборстве играли психологические операции, мероприятия по оперативной маскировке и по обеспечению безопасности собственных сил и средств. В новую редакцию доктрины включены сетевые операции и РЭБ как основной вид ведения информационных операций.

Вспомогательные мероприятия информационного противоборства, такие как обеспечение безопасности информации (ОБИ), физическое уничтожение критически важных информационных объектов противника и контрразведка, по взглядам военно-политического руководства США, являются неотделимыми от основного содержания информационного противоборства США.

Следует особо подчеркнуть, что в обновленном документе уточнены роль и сущность физического уничтожения информационных объектов противника. Физическое уничтожение критически важных объектов информационной инфраструктуры противника рассматривается как вспомогательный элемент информационного противоборства и представляет собой проводимые в ходе информационной операции действия по применению средств огневого поражения и физического уничтожения в целях вывода из строя ключевых элементов системы управления и связи противника. Основные объекты информационного воздействия показаны на рисунке 1.

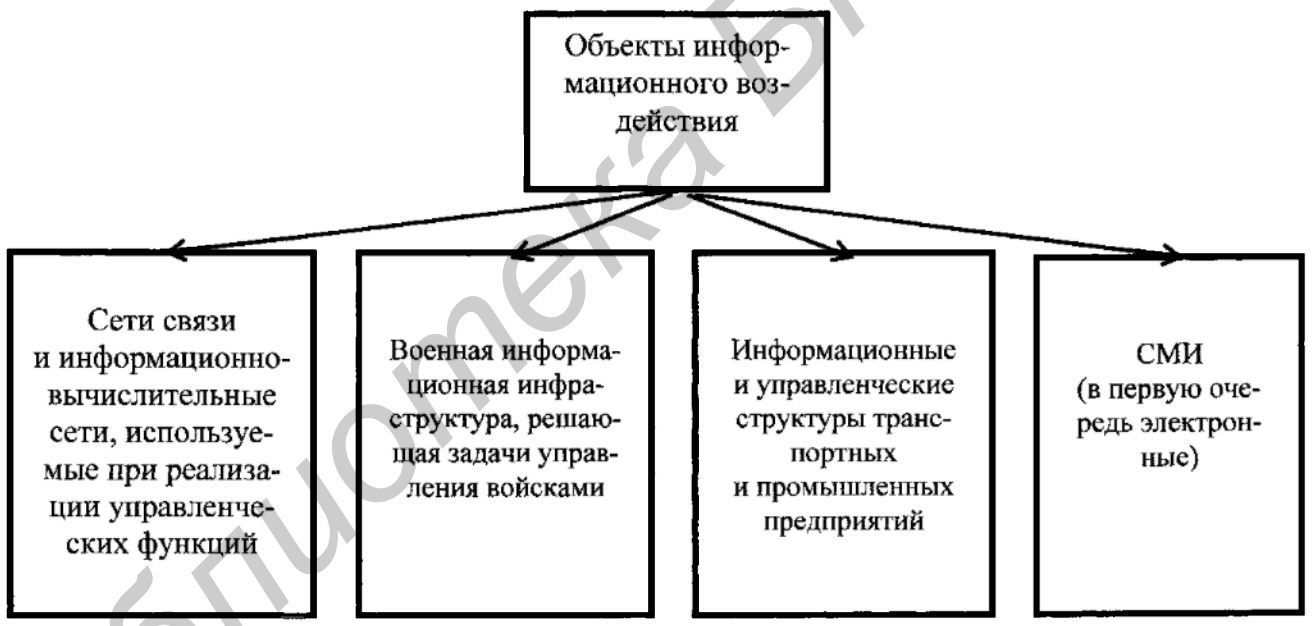

Рисунок 1 – Объекты информационного воздействия

Особую остроту и актуальность приобретает проблема оценки живучести информационных объектов. Авторами статьи предлагается методический подход к оценке живучести информационных объектов в условиях информационного противоборства.

Будем исходить из того, что информационное противоборство прежде всего направлено на решение задач информационного воздействия на информацию и информационные системы противника (системы связи и боевого управления, системы разведки и другие), непосредственно обеспечивающие ведение боевых действий противником, при одновременной защите аналогичных систем своих войск.

В этих условиях вероятность скрытого управления войсками с j-го звена управления – $P_j^s(t)$ в работе [2] автором предлагается рассчитывать следующим образом:

$$P_j^s(t) = 1 - \prod_{i=1}^{n_j} \left[1 - P_{ij}^s(t)\right], \ (i = \overrightarrow{1,n}, \ \ j = \overrightarrow{1,m}), \tag{1}$$

где n_j – количество пунктов управления на j-м звене управления;

$P_{ij}^s(t)$ – вероятность скрытого управления с i-го пункта j-го звена в момент времени t.

При условии, что информационный объект, в качестве которого авторами рассматривается система управления, состоящая из j звеньев (оперативного, тактического), каждый из которых включает i пунктов (КП, ЗКП, ТПУ):

$$P_{ij}^s(t) = \left[1 - P_{ij}^o(t)\right] \cdot P_{ij}^y(t) \cdot P_{ij}^c(t), \ (i = \overrightarrow{1,n}, \ \ j = \overrightarrow{1,m}), \qquad (2)$$

где $P_{ij}^o(t)$ – вероятность обнаружения противником i-го пункта j-го звена управления к моменту t;

$P_{ij}^y(t)$ – условная вероятность уничтожения противником i-го пункта j-го звена управления к моменту времени t;

$P_{ij}^c(t)$ – вероятность скрытной выдачи в систему управления выходной информации с i-го пункта j-го звена управления в момент t.

Возникает закономерный вопрос, каким же образом рассчитывать вероятности $P_{ij}^o(t)$, $P_{ij}^y(t)$ и $P_{ij}^c(t)$. В работах [2, 3, 4] разъяснений мы не находим. Вместе с тем первые два показателя $P_{ij}^o(t)$ и $P_{ij}^y(t)$ являются показателями, характеризующими живучесть рассматриваемой системы управления. Рассуждая далее, авторы предлагают метод расчета приведенных выше показателей, в основе которого лежат основные положения теории вероятности [6].

Уточним основные понятия: информационный объект и его живучесть [7].

Информационный объект – системы и средства разведки и управления войсками (силами) и оружием, в том числе автоматизированные, а также комплексы средств автоматизации; информатизированные образцы вооружения и военной техники; центры обработки и анализа информации, каналы информационного обмена и телекоммуникации, системы и средства защиты информации; средства массового информирования населения (войск); компьютерная и электронно-вычислительная техника; программное обеспечение; автоматизированные системы управления технологическими процессами в ключевых сегментах инфраструктуры государства (транспорт, энергетика, химическая и нефтяная промышленность, водоснабжение, телекоммуникации и связь, банки, финансы и др.).

Под живучестью информационного объекта мы будем понимать его способность сохранять или быстро восстанавливать свои функции в условиях всех видов информационного воздействия противника. Живучесть информационных объектов обеспечивается: рассредоточением, тщательной маскировкой и размещением в прочных фортификационных сооружениях; применением дублирующих средств и видов связи с организацией прямых, обходных и резервных каналов связи; организацией защиты, охраны и обороны; устройством ложных (имитирующих) элементов; принятием эффективных мер радиоэлектронной защиты и др.

В рассматриваемом информационном объекте – системе управления $P_{ij}^o(t)$ можно рассчитать следующим образом:

$$P_{ij}^o(t) = \prod_{z=1}^{3} P_{ijz}(t), \ (i = \overrightarrow{1,3}, \ \ j = \overrightarrow{1,n_i}), \qquad (3)$$

где P_{ijz} – вероятность того, что на i-м уровне в j-м подразделении противником будут вскрыты все z пунктов управления.

Вероятность того, что на i-м уровне в j-м подразделении в период t хотя бы один пункт управления будет функционировать скрытно, рассчитывается следующим образом:

$$P_{ij}^{o'}(t) = 1 - \prod_{z=1}^{3} P_{ijz}(t), \ (i = \overrightarrow{1,3}, \ \ j = \overrightarrow{1,n_i}). \qquad (4)$$

Вероятность уничтожения противником на i-м уровне в j-м подразделении всех пунктов управления при условии, что они обнаружены, можно рассчитать:

$$P_{ij}^{y}(t) = \prod_{z=1}^{3} P_{ijz}(t) \prod_{z=1}^{3} P_{ijz}^{y}(t). \quad (5)$$

В этом случае вероятность того, что на i-м уровне в j-м подразделении будет функционировать хотя бы один пункт управления при условии его обнаружения, рассчитывается:

$$P_{ij}^{y'}(t) = \prod_{z=1}^{3} P_{ijz}(t) \cdot \left[1 - \prod_{z=1}^{3} P_{ijz}^{y}(t)\right]. \quad (6)$$

Расчет вышеприведенных вероятностей позволяет ввести комплексный показатель живучести информационного объекта – $K_1(t)$, который характеризует вероятность того, что хотя бы один пункт управления на любом уровне и в любом подразделении в момент t будет функционировать:

$$K_1(t) = 1 - K_2(t), \quad (7)$$

где $K_2(t)$ – вероятность того, что все пункты управления, входящие в систему, в момент t будут уничтожены противником.

Этот показатель может быть рассчитан:

$$K_2(t) = \prod_{i} \prod_{j} \prod_{z} P_{ijz}(t)\, P_{ij}^{y}(t). \quad (8)$$

Для примера произведем расчет $P_{ij}^{o}(t)$ – вероятности обнаружения противником i-го пункта j-го звена управления к моменту t.

Сущность расчета.

Этап 1. Рассчитываем P_{ijz} – вероятность того, что на i-м уровне в j-м подразделении противником будут вскрыты все z пунктов управления.

Этап 2. Рассчитываем $P_{ij}^{o}(t)$ – вероятность обнаружения противником i-го пункта j-го звена управления к моменту t.

Этап 3. Анализ решения. Графическое представление результатов расчета.

Исходные данные для расчета.

Противником (синими) выслана разведывательно-диверсионная группа численностью 10 человек с задачей – вскрыть местонахождение информационных объектов воинского формирования (красных). Район поиска составляет 40 км^2. Нормативная площадь разведки местности, производимой разведывательно-диверсионной группой противника в единицу времени, $S_{\text{р}}^{-1}$ – 10 км^2/сут. Вероятность выполнения задачи $P_{\text{вып}} = 60\,\%$ с учетом вероятности обнаружения и уничтожения группы.

Этап 1. Рассчитываем вероятности того, что на тактическом уровне в воинском формировании (красных) противником (синими) будут вскрыты все информационные объекты (КП, ЗКП, ТПУ).

В соответствии с положениями теории вероятностей [5] вероятность того, что на i-м уровне в j-м подразделении противником будут вскрыты все z пунктов управления, P_{ijz} может быть рассчитана по формуле

$$P_{ijz} = P_{\text{вып}} \cdot \frac{S_{\text{р}}}{S_{\text{р.п}}}, \quad (9)$$

где $P_{\text{вып}}$ – вероятность выполнения задачи разведывательно-диверсионной группой (синими);

$S_{\text{р}}$ – площадь разведки;

$S_{\text{р.п}}$ – район поиска.

Принимаем, что площадь разведки, производимой разведывательно-диверсионной группой (синими), будет равна площади разведки, производимой группой в единицу времени t, т. е. $S_{\text{р}} = S_{\text{р}}^{1}$.

С учетом исходных данных получаем:

площадь района поиска $S_{\text{р.п}} = 40$ км^2;

нормативная площадь разведки местности, производимой разведывательно-диверсионной группой противника в единицу времени, $S_{\text{р}}^{1} = 10$ км^2/сут $\approx 0{,}42$ км^2/ч;

вероятность выполнения задачи с учетом вероятности обнаружения и уничтожения разведывательно-диверсионной группы – $P_{\text{выд}} = 0{,}6$. Тогда

$$P_{ijz}(t) = 0{,}6 \cdot \frac{0{,}42t}{40}. \qquad (10)$$

Из приведенной формулы видна прямая зависимость рассчитываемой вероятности от времени поиска. В целях проверки адекватности расчета рассчитаем P_{ijz} для начального момента времени, т. е. $t = 0$:

$$P_{ijz}(0) = 0{,}6 \cdot \frac{0{,}42 \cdot 0}{40} = 0. \qquad (11)$$

Логично, что для разведывательно-диверсионной группы, не начавшей поиск, вероятность обнаружения командного пункта воинского формирования будет равна нулю. В то же время, изменяя время поиска, мы имеем возможность наблюдать динамику изменения искомой вероятности – P_{ijz} (таблица 1).

Таблица 1 – Показатели зависимости вероятности обнаружения всех информационных объектов от времени поиска

Время поиска t, ч	Расчет вероятности P_{ijz}	Значение P_{ijz}, %
$t_1 = 1$	$P_{ijz} = 0{,}6 \cdot \frac{0{,}42 \cdot 1}{40} = 0{,}00625$	0,625
$t_2 = 24$	$P_{ijz} = 0{,}6 \cdot \frac{0{,}42 \cdot 24}{40} = 0{,}15$	15
$t_3 = 48$	$P_{ijz} = 0{,}6 \cdot \frac{0{,}42 \cdot 48}{40} = 0{,}3$	30
$t_4 = 72$	$P_{ijz} = 0{,}6 \cdot \frac{0{,}42 \cdot 72}{40} = 0{,}45$	45
$t_5 = 96$	$P_{ijz} = 0{,}6 \cdot \frac{0{,}42 \cdot 96}{40} = 0{,}6$	60

Дальнейшее увеличение времени не принесет желаемого возрастания вероятности, так как разведывательно-диверсионная группа исследует всю площадь разведки. Это видно из расчета:

$$S_{\text{р.п}} = 0{,}42 \cdot 96 \approx 40 \text{ км}^2. \qquad (12)$$

Этап 2. Рассчитываем вероятность обнаружения противником информационного объекта (командного пункта) воинского формирования (красных) к исходу четвертых суток поиска.

Подставив рассчитанные значения показателя вероятности P_{ijz} в (3), получим значения вероятностей обнаружения противником командного пункта бригады $P_{ij}^{\text{о}}(t)$ к моменту t (таблица 2).

Таблица 2 – Показатели зависимости вероятности обнаружения информационного объекта (командного пункта) воинского формирования от времени поиска

Время поиска, t, ч	Расчет вероятности P_{ij}^{o}	Значение $P_{ij}^{o}(t)$, %
$t_1 = 1$	$P_{ij}^{o}(1) = \prod_{z=1}^{3} 0{,}00625 = 0{,}00000024$	0,000024
$t_2 = 24$	$P_{ij}^{o}(24) = \prod_{z=1}^{3} 0{,}15 = 0{,}0034$	0,34
$t_3 = 48$	$P_{ij}^{o}(48) = \prod_{z=1}^{3} 0{,}3 = 0{,}027$	2,7
$t_4 = 72$	$P_{ij}^{o}(72) = \prod_{z=1}^{3} 0{,}45 = 0{,}09$	9,0
$t_5 = 96$	$P_{ij}^{o}(96) = \prod_{z=1}^{3} 0{,}6 = 0{,}216$	21,6

Этап 3. Анализ решения. Графическое представление результатов расчета.

Зависимость вероятности обнаружения информационных объектов воинского формирования от времени ведения разведки показана на рисунке 2.

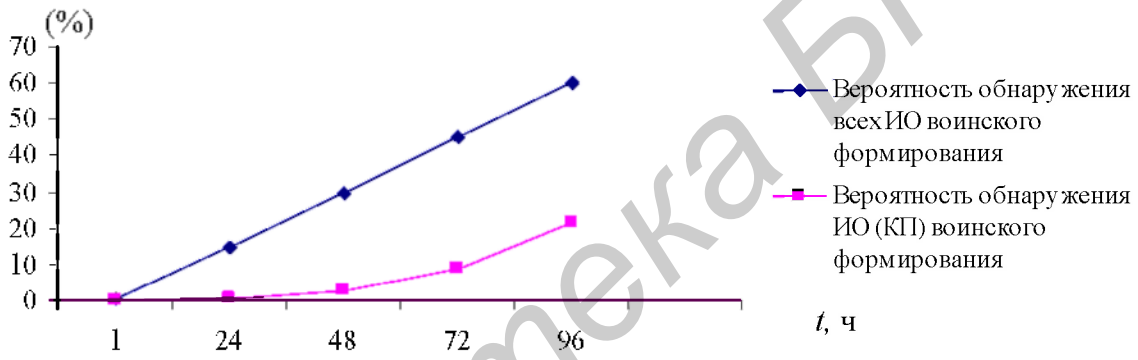

Рисунок 2 – Зависимость вероятности обнаружения информационных объектов воинского формирования от времени ведения разведки

Таким образом, предложенный методический подход, характеризующий живучесть информационных объектов, дает представление об объеме и характере задач, решаемых командирами при обеспечении безопасности информационных объектов в условиях информационного противоборства. Несомненно, в целях дальнейшего развития теории информационного противоборства потребуются дальнейшие глубокие и всесторонние исследования и проверка полученных результатов в ходе моделирования процесса информационного противоборства, мероприятий оперативной и боевой подготовки.

Литература

1. Кулешов, Ю. Е. Анализ взглядов на теорию информационного противоборства и необходимость ее развития / Ю. Е. Кулешов // Вестн. Воен. акад. Респ. Беларусь. – 2012. – № 1 (34). – С. 10–20.

2. Рябчук, В. Д. Теория управления: воен.-теорет. тр. / В. Д. Рябчук. – М.: ВА им. М. В. Фрунзе, 1995. – 386 с.

3. Рябчук, В. Д. Теория управления боем (науковедческий и методологические аспекты) / В. Д. Рябчук. – Минск: ВА РБ, 2011. – 105 с.

4. Рябчук, В. Д. Философия войны и теория управления современным противоборством / В. Д. Рябчук, В. И. Ничипор // Воен. мысль. – 2007. – № 8.

5. Глод, И. В. Пути решения проблемы обеспечения устойчивого управления войсками (силами) / И. В. Глод, Г. С. Казаков, В. К. Синявский // Наука и воен. безопасность. – 2009. – № 1.

6. Феллер, В. Введение в теорию вероятностей и ее приложения: в 2 т. / В. Феллер; пер. с англ. – М.: Мир, 1984. – Т.1. – 528 с.

7. О Сборнике основных военных терминов и понятий: Приказ начальника Генерального штаба Вооруженных Сил – первого заместителя Министра обороны Респ. Беларусь от 11.05.2009 № 222.

*Сведения об авторах:
Кулешов Юрий Евгеньевич,
УО «Военная академия Республики Беларусь»;
Паскробка Сергей Иванович,
УО «Белорусский государственный университет информатики и радиоэлектроники»;
Родионов Андрей Александрович,
ГУ «Научно-исследовательский институт Вооруженных Сил Республики Беларусь».
Статья поступила в редакцию 1.11.2012 г.