УДК 519.876

Боевая эффективность кибератак: практические аспекты

Бойко А. А.

Постановка задачи. *В современных боевых действиях и вооруженных конфликтах широко применяются информационно-технические воздействия, к которым относятся электромагнитные воздействия (радиоэлектронное подавление и поражение электромагнитным излучением) на физическом уровне модели OSI и кибератаки на вышестоящих уровнях этой модели. Вопросам обеспечения защиты образцов вооружения и военной техники и воинских формирований в целом от электромагнитных воздействий традиционно уделяется пристальное внимание. В то же время не менее значимые вопросы защиты этих объектов от кибератак в боевых условиях являются мало изученными и потому остаются без требуемого понимания военными и техническими специалистами. Настоящая статья является второй частью материалов, рассматривающих методические основы оценки боевой эффективности кибератак на уровне соотношения боевых потенциалов воинских формирований. В первой части предложен темпоральный подход к аналитическому моделированию современного боя, позволяющий оценить эффект от системного влияния огневого поражения, электромагнитного воздействия и кибератак на временные и вероятностные характеристики подсистем разведки, связи, управления и огневого поражения, функционирующих в рамках единого боевого цикла воинского формирования.* ***Цель работы:*** *исследование аналитической модели современного боя и разработка на ее основе методики обоснования требований к защищенности образцов вооружения и военной техники от кибератак.* ***Идея методики****:* 1) *моделирование боя двух одинаковых воинских формирований с защищаемыми образцами вооружения и военной техники, одному из которых дополнительно придается подсистема кибератак; 2*) *оценка соотношения боевых потенциалов сторон;* 3) *определение требований к защищенности образцов вооружения и военной техники от кибератак на основе такой допустимой вероятности успешной реализации на них кибератак, при которой соотношение боевых потенциалов сторон не превышает необходимое значение и стоимость устранения уязвимостей не выше максимально допустимой.* ***Новизна*** *состоит в получении возможности количественной оценки влияния кибератак на соотношение боевых потенциалов противоборствующих воинских формирований.* ***Результат****. Показано, что электромагнитные воздействия в бою дают эффект, являющийся частным случаем эффекта кибератак в различных вариантах их применения. В интересах повышения оперативности применения предложенной методики выявлена универсальная аналитическая зависимость остаточной доли численности воинского формирования от вероятности реализации кибератак в бою двух одинаковых воинских формирований, одно из которых дополнено подсистемой информационно-технических воздействий. Для этой закономерности предложены формулы оценки коэффициентов при тотальном воздействии кибератак на все подсистемы и выборочном воздействии на подсистему связи, управления, разведки или огневого поражения. Приведены диаграммы максимальных абсолютных отклонений значений, полученных с применением предложенных формул, от результатов моделирования. Показаны примеры обоснования требований к обеспечению конфликтной устойчивости воинских формирований при различных вариантах реализации кибератак.* ***Практическая значимость****: решение можно использовать при обосновании требований к конфликтной устойчивости информационно-технических средств существующих и перспективных образцов вооружения и военной техники в условиях кибератак противника.*

Ключевые слова: *аналитическая модель боя, кибератака, боевой потенциал, воинское формирование, боевой цикл*

Библиографическая ссылка на статью:
Бойко А. А. Боевая эффективность кибератак: практические аспекты // Системы управления, связи и безопасности. 2020. № 4. С. 134-162. DOI: 10.24411/2410-9916-2020-10405.

Reference for citation:
Boyko A. A. Combat Effectiveness of Cyber-attacks: Practical Aspects. *Systems of Control, Communication and Security*, 2020, no. 4, pp. 134-162. (in Russian). DOI: 10.24411/2410-9916-2020-10405.

Введение

В современных боевых действиях и вооруженных конфликтах широко применяются информационно-технические воздействия (ИТВ). Не прибегая к витиеватым и нередко противоречащим друг другу классификациям, будем полагать, что к ИТВ относятся электромагнитные воздействия (ЭМВ) (то есть радиоэлектронное подавление (РЭП) и поражение электромагнитным излучением (ЭМИ)) на физическом уровне модели OSI и компьютерные или кибератаки (КА) на вышестоящих уровнях этой модели [1]. КА называют также разрушающими программными воздействиями, функциональным поражением специальными программными средствами, программно-математическими воздействиями, программно-техническими воздействиями, радиоэлектронно-информационными воздействиями, программно-аппаратными воздействиями и т.п.

По мере внедрения информационных и телекоммуникационных технологий в военное дело вопросы оценки защищенности образцов ВВТ от КА в боевых условиях становятся все более актуальными. Однако сегодня уделяется пристальное внимание вопросам обеспечения защиты образцов ВВТ и в целом воинских формирований (ВФ) от ЭМВ, в то время как не менее значимые вопросы защиты этих объектов от КА еще только изучаются и потому остаются без требуемого понимания военными и техническими специалистами.

Настоящая статья продолжает цикл работ автора [2-11]. Она является второй частью материалов, рассматривающих методические основы оценки боевой эффективности КА на уровне соотношения боевых потенциалов (БП) ВФ. В первой части [12] предложен темпоральный подход к аналитическому моделированию современного боя, позволяющий оценить эффект от системного влияния огневого поражения (ОП), ЭМВ и КА на временные и вероятностные характеристики функционирования подсистем разведки, связи, управления и ОП при их совместном применении в едином боевом цикле ВФ (OODA-цикле, цикле «разведка-поражение», цикле Дж. Бойда и т.д.). Настоящая статья посвящена исследованию практических аспектов применения КА в современном бою и обоснованию требований к защищенности образцов ВВТ от КА на уровне соотношения БП.

Постановка задачи

Анализ известных работ. В последнее десятилетие вопросам обоснования требований к защищенности от КА различных объектов специального назначения (СН) в научной литературе уделяется значительное внимание. Довольно подробный обзор таких работ приводится, например, в монографии Е.Б. Дроботуна [13]. Однако все известные работы в этой области имеют общую особенность. Они рассматривают в качестве объекта исследования некоторую «сущность», которая крайне условно привязана к своей надсистеме. Этими «сущностями», в частности, являются автоматизированные системы управления СН [13], автоматизированные информационно-управляющие системы СН [14], информационно-коммуникационное пространство эргатических систем СН [15], информационные системы СН [16], автоматизированные системы СН в целом [17], сети [18] и узлы [19] связи СН, информационно-

телекоммуникационные сети [20] и системы [21] СН, информационно-вычислительные сети СН [22], комплексы средств автоматизации СН [23], объекты критической информационной инфраструктуры [24] и т.п. Перечень таких терминов, которые, очевидно, определяют во многом пересекающиеся множества объектов реального мира, можно продолжать долго.

Результаты анализа известных работ показывают, что в рассматриваемой молодой и, несомненно, пока еще мало изученной научной области имеет место ситуация, наиболее полно характеризующаяся классической «метафорой поликлиники», в которой каждый специалист лечит только свой орган, терапевты выполняют функции координаторов, но никто не отвечает за здоровье пациента в целом. Совокупность известных работ по рассматриваемой тематике сегодня разрознена, но такое состояние проходит любая зарождающаяся сфера научных знаний. Вероятно, именно поэтому, как было отмечено во введении, вопросы защиты объектов СН от КА в боевых условиях и в целом в условиях антагонистического конфликта на межгосударственном уровне пока еще не находят требуемого понимания военными и техническими специалистами. Сейчас остро ощущается потребность в подходах, способных устранить создавшуюся разрозненность, то есть подходах, рассматривающих каждый из указанных объектов в качестве элемента единой надсистемы, представляющей собой процесс антагонистического конфликта сложных организационно-технических систем или ВФ. Настоящая работа является попыткой автора создать такой подход применительно к боевым действиям ВФ на тактическом уровне.

Цель работы – исследование аналитической модели современного боя и разработка на ее основе методики обоснования требований к защищенности образцов ВВТ от КА.

Исследование процесса применения КА в современном бою

Рассмотрим пример боя с применением ИТВ, в котором участвуют два одинаковых ВФ – Красные и Синие. Аналитические выражения, описывающие модель такого боя, приведены в [12]. Тип ВФ – самоходный артиллерийский дивизион. Состав сторон включает подсистемы разведки, связи, управления и ОП. Наступающим Синим дополнительно придана подсистема ИТВ, включающая наземное средство ИТВ. Подсистемы разведки, управления, связи и ИТВ (в части КА) являются скрытными, средства ОП сторон поражают друг друга, а средства ОП Красных дополнительно могут поражать нескрытное средство РЭП. Восстановление средств в бою не происходит. Подсистема управления может работать в режиме сетецентрического управления, когда средства подсистемы ОП получают целеуказания напрямую из подсистемы разведки. «По умолчанию» управление не сетецентрическое. После уничтожения средства ОП огонь автоматически переводится на еще не уничтоженные средства ОП противника. При применении РЭП Красные обнаруживают местоположение источника помех своей подсистемой разведки и в связи с высокой заметностью средств РЭП применяют средства ОП в режимах с приоритетом «ОП$\succ$РЭП» или «РЭП$\succ$ОП». Структурная схема боя показана на рис. 1. Параметры боя, принятые «по умолчанию», приведены в таблице 1.

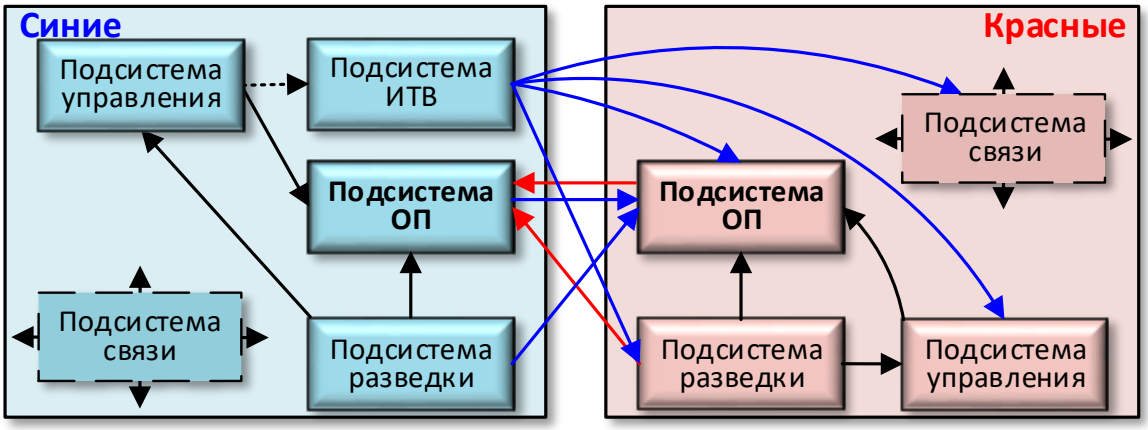


Рис. 1. Структурная схема современного боя с применением ИТВ

Таблица 1 – Параметры моделируемого боя (модель приведена в [12])

№	Обозначение	Физический смысл	Значение
Общие показатели			
1	U	ослабление ущерба обороняемым позициям	1
2	$P_{гар}$	требуемая вероятность гарантированного ОП цели	0,94
3	Δ	уровень информатизации Красных	от 0 до 1
Подсистема ОП			
4	$N_{кр}$, $N_{син}$	количество средств ОП Красных и Синих	18 18
5	$P_{1бп\_кр}$, $P_{1бп\_син}$	вероятность поражения цели одним боеприпасом средства ОП Красных и Синих	0,3 0,3
6	$T_{оп\_кр}$, $T_{оп\_син}$	время подготовки подсистемы ОП Красных и Синих (количество каналов не создает очереди)	30 с 30 с
7	$T_{1бп\_кр}$, $T_{1бп\_син}$	время воздействия одним боеприпасом в подсистеме ОП Красных и Синих	8 с 8 с
8	$K_{бп\_кр}$, $K_{бп\_син}$	количество боеприпасов в боекомплекте одного средства ОП Красных и Синих	∞ ∞
9	$N_{им\_кр}$ $N_{им\_син}$	количество имитируемых средств ОП Красных и Синих	0 0
Подсистема разведки			
10	$T_{р\_кр}$, $T_{р\_син}$	время работы подсистемы разведки Красных и Синих	30 с 30 с
11	$P_{р\_кр}$, $P_{р\_син}$	вероятность вскрытия и распознавания цели подсистемой разведки Красных и Синих	0,99 0,99
Подсистема управления			
12	$T_{упр\_кр}$, $T_{упр\_син}$	время работы подсистемы управления Красных и Синих	20 с 20 с
Подсистема связи			
13	$T_{св\_кр}$, $T_{св\_син}$	время передачи информации по каналу связи Красных и Синих	30 с 30 с
14	$P_{св\_кр}$, $P_{св\_син}$	вероятность гарантированной передачи информации по каналу связи Красных и Синих	0,9 0,9
Подсистема ИТВ			
15	$P_{ИТВ}$	вероятность ИТВ Синих	от 0,01 до 0,99
Примечание: среднеквадратическое отклонение для времен равно 10% от математ. ожидания.			

В этом бою, по мнению органа управления Синих, техника ИТВ должна обеспечить увеличение БП, достаточное для победы. То есть, зная заранее уязвимости ВВТ Красных к ИТВ, орган управления Синих полагает, что его техника ИТВ способна изменить соотношение БП, как минимум, на 33,3% с 1:1 (100%:100%) до 1,5:1 (100%:66,7%) для выполнения классического критерия соотношения БП для успешного наступления во встречном бою.

Применительно к такой ситуации возникает два вопроса.

1) При каких параметрах Красных орган управления Синих ошибается?

2) Как защитить от КА Красных, чтобы не допустить их поражения?

Для ответа на эти вопросы рассмотрим различные варианты этого боя.

Вариант боя №1. Сравнение боевой эффективности КА и РЭП на подсистему связи. Схема этого варианта показана на рис. 2.

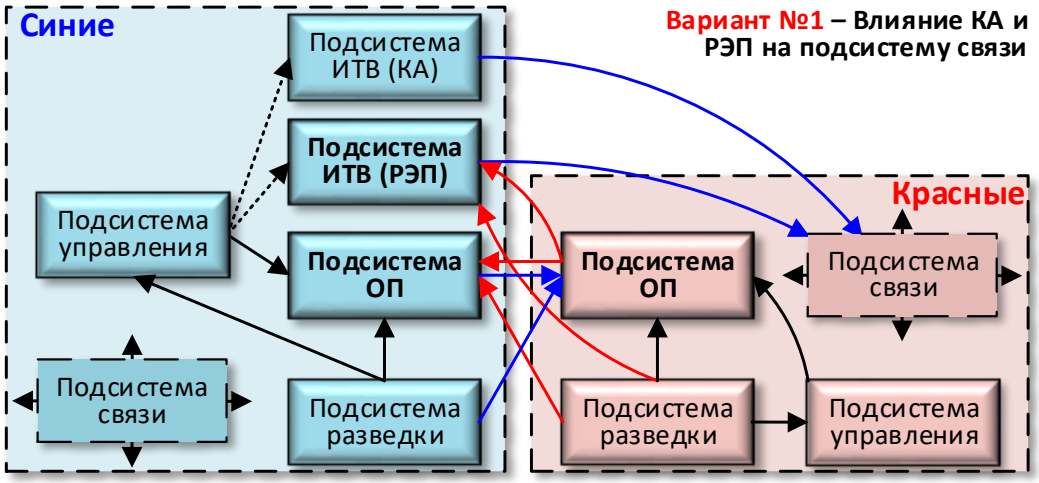


Рис. 2. Схема влияния КА и РЭП на подсистему связи

БП ВФ для удобства отображения на графиках будем оценивать по остаточной доле численности победившей стороны $\Delta N^*_{\text{син}}$. Зависимость $\Delta N^*_{\text{син}}(P_{\text{ИТВ}})$ при реализации КА (или в этом варианте боя скрытного РЭП, поскольку оба вида воздействия оказывают влияние только на время связи) для различных значений Δ показана на рис. 3. Сравнение боевой эффективности КА (скрытного РЭП) и не скрытного РЭП для рассматриваемого варианта показана на рис. 4 для Δ=100% (далее для наглядности Δ может выражаться процентами).

На рис. 4 показан «мнимый парадокс», когда КА или скрытное РЭП оказывается в основном менее эффективно, чем не скрытное РЭП, высокий энергопотенциал электромагнитного излучения которого хорошо заметен для средств разведки Красных. Дело в том, что, сберегая численность средств ОП, в случае применения нескрытного РЭП Синие жертвуют своей подсистемой ИТВ. При этом следует отметить, что длительность боя составляет около 20 мин, а **время жизни нескрытного средства РЭП в нем около 5 мин** (при $P_{\text{ИТВ}}$=0,5 и Δ=100%). Задавшись вопросом о стоимости нескрытного средства РЭП и самоходной артиллерийской установки с боекомплектом, можно оценить военно-экономическую целесообразность использования техники, реализующей нескрытное РЭП на подсистему связи Красных в этом бою.

№4. 2020
ISSN 2410-9916

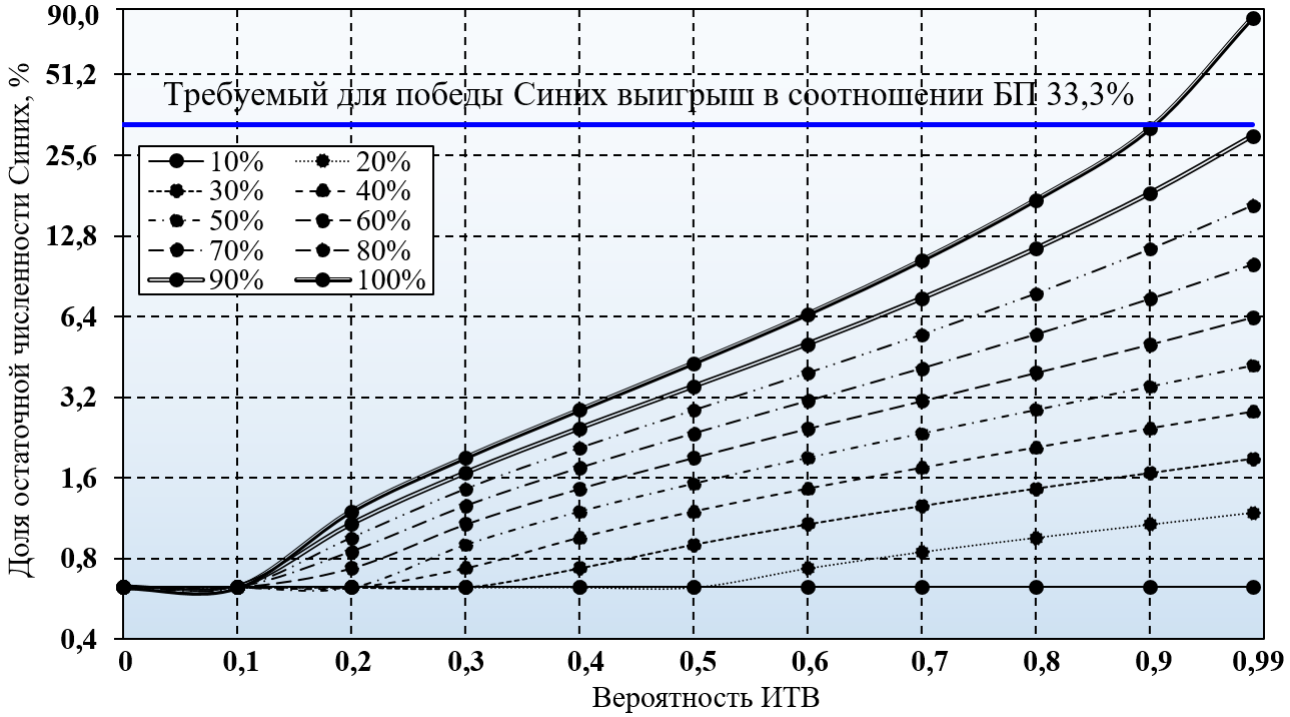


Рис. 3. Боевая эффективность КА или скрытного РЭП на подсистему связи при различных уровнях Δ (в логарифмическом масштабе по основанию 2)

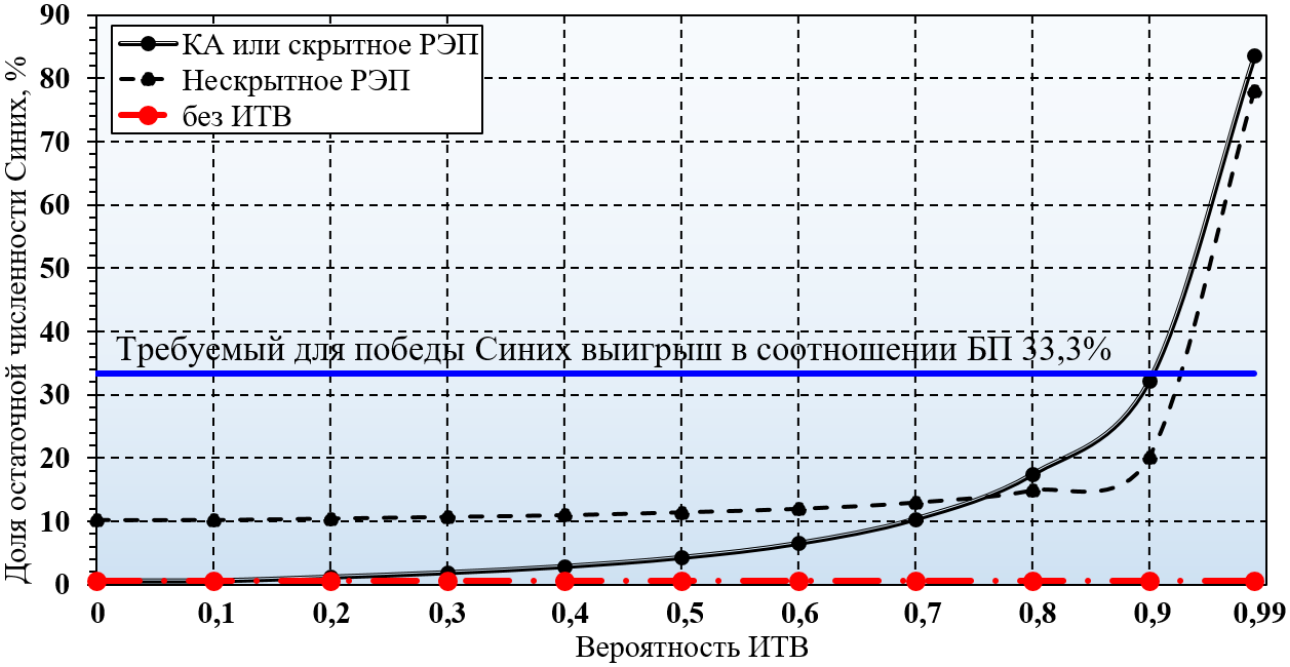


Рис. 4. Сравнение боевой эффективности КА и РЭП для подсистемы связи

Здесь следует пояснить, что понимается под скрытностью РЭП. Как известно, сам по себе этот вид воздействия не может являться скрытным ввиду необходимости обеспечения определенного превышения сигнала помехи над полезным сигналом в радиоприемнике цели. Скрытным РЭП в данном контексте является в том случае, если местоположение средства РЭП невозможно, крайне трудно или нецелесообразно определять. Например, когда средство РЭП является целевой нагрузкой беспилотного летательного аппарата (БПЛА), низкие параметры заметности которого не позволяют поразить его имеющимися у

DOI: 1024411/2410-9916-2020-10405
URL: http://sccs.intelgr.com/archive/2020-04/05-Boyko.pdf

Красных средствами ОП, либо, когда применяются забрасываемые передатчики помех, которые из-за их большого количества и малых габаритов делают применение по ним средств ОП бесполезным. По этой причине далее рассматривается только скрытное РЭП.

Выводы по варианту боя №1:

1) орган управления Синих ошибается в том случае, если уровень информатизации Красных менее 100%, но даже в таком случае вероятность успешного КА или скрытного РЭП должна составлять не менее 0,9;

2) в интересах недопущения поражения Красных им достаточно либо, не прибегая к устранению уязвимостей к ИТВ, обеспечить свой уровень информатизации менее 90%, либо использовать хотя бы 10% неуязвимых для ИТВ средств связи.

В контексте варианта боя №1 представляют интерес результаты оценки боевой эффективности КА или скрытного РЭП на подсистему связи для различных времен сеанса связи при наиболее часто встречающемся на практике случае, когда Δ=100%. Они показаны на рис. 5.

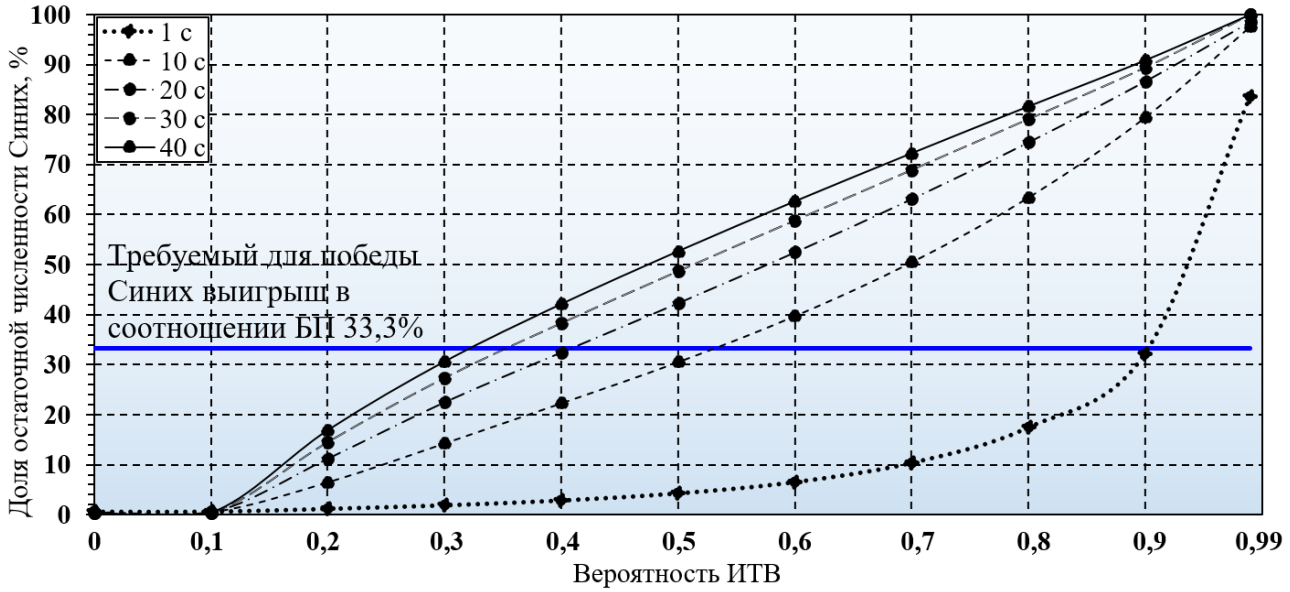


Рис. 5. Боевая эффективность КА или скрытного РЭП на подсистему связи для различных времен сеанса связи при Δ=100%

На рис. 5 наглядно прослеживается известный из практики факт, что в бою лучше передавать сообщения по каналам передачи данных, чем использовать голосовые средства радиосвязи, в том числе цифровые.

Также представляет интерес оценка коэффициентов боевой соизмеримости (КБС) подсистем сторон в этом варианте боя. Этот показатель вычисляется с использованием метода, предложенного в [7]. Результаты такой оценки для Синих показаны на рис. 6 (сумма КБС для каждой стороны равна 100%).

Из анализа рис. 6 следует, что вес средства ИТВ Синих превышает вес их средства ОП в 3,7 (при $P_{ИТВ}$ = 0,15) – 10,7 (при $P_{ИТВ}$ = 0,75) раз. Снижение КБС средства ИТВ после достижения максимума обусловлено тем, что блокирование связи на уровне $P_{ИТВ}$=0,75 приводит к такой задержке боевого цикла Крас-

№4. 2020
ISSN 2410-9916

ных, после которой дальнейшее увеличение КБС подсистемы ИТВ Синих сдерживается возрастанием КБС их других подсистем. Тем не менее, это увеличение необходимо для снижения боевых потерь. На рис. 7 показано, как отличаются КБС компонентов Синих при $P_{ИТВ}$=0,75 и $P_{ИТВ}$=0,99.

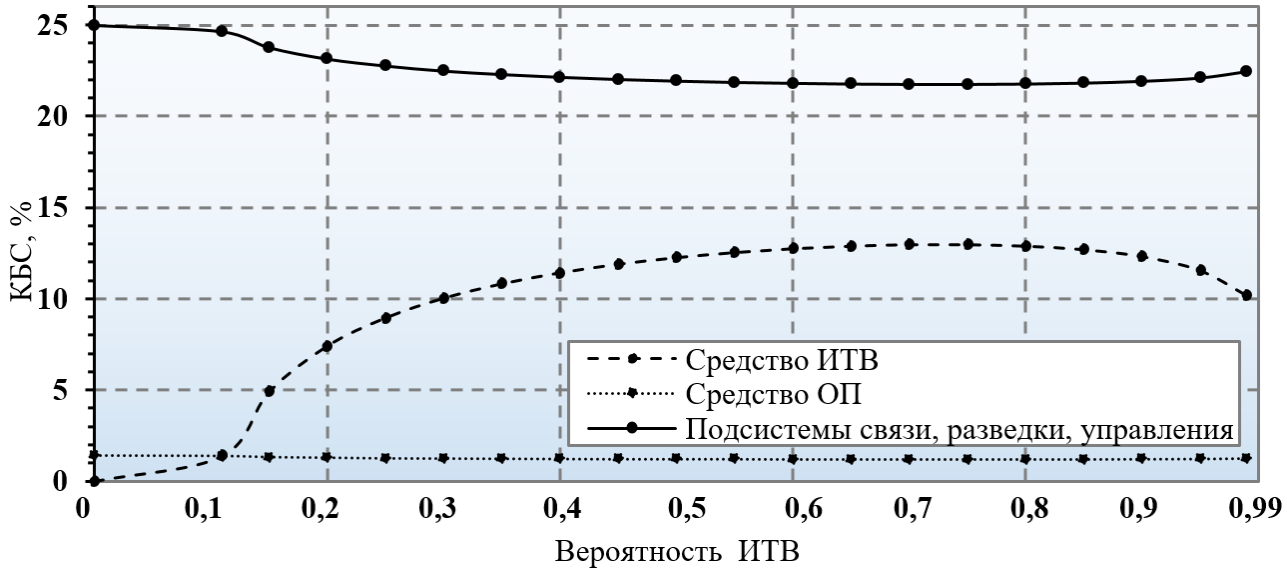


Рис. 6. КБС компонентов Синих в рассматриваемом варианте боя №1

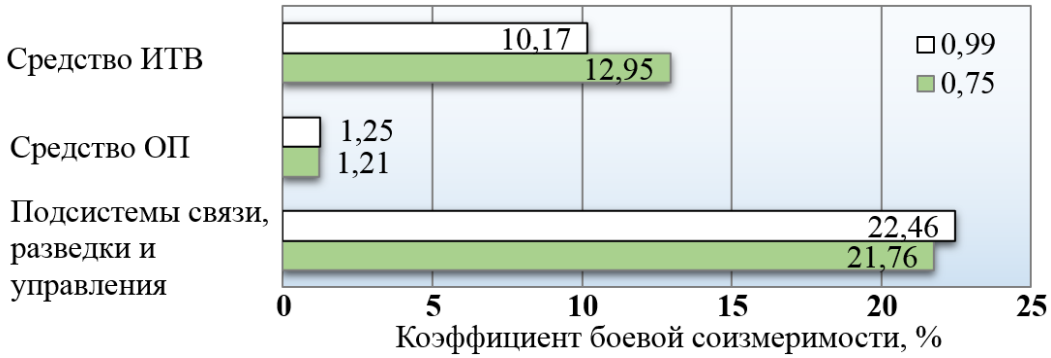


Рис. 7. КБС компонентов Синих при $P_{ИТВ}$=0,75 и $P_{ИТВ}$=0,99

Вариант боя №2. Сравнение боевой эффективности КА и скрытного РЭП подсистемы разведки. Схема этого варианта показана на рис. 8.

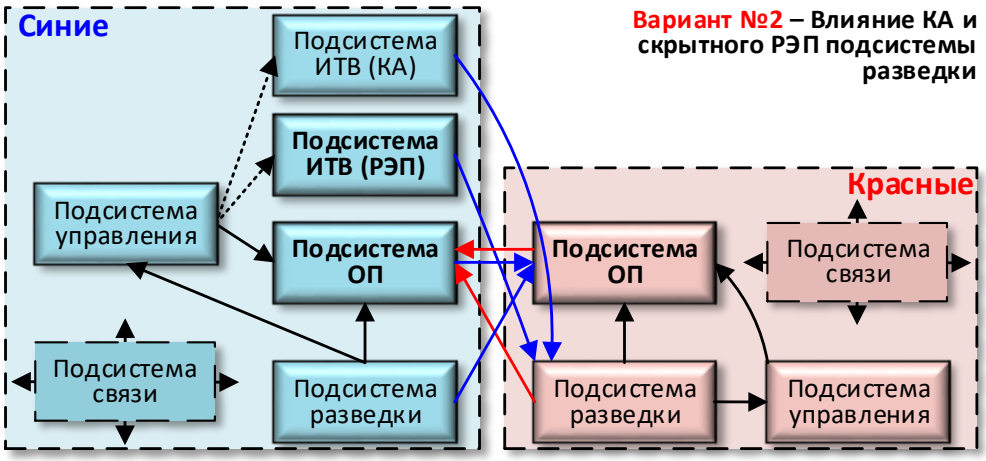


Рис. 8. Схема влияния КА и скрытного РЭП на подсистему разведки

DOI: 1024411/2410-9916-2020-10405
URL: http://sccs.intelgr.com/archive/2020-04/05-Boyko.pdf

Боевая эффективность КА и скрытного РЭП для различных уровней информатизации Δ показана на рис. 9-10, соответственно. Сравнение боевой эффективности этих видов ИТВ в данном варианте боя приведено на рис. 11 для Δ=100%.

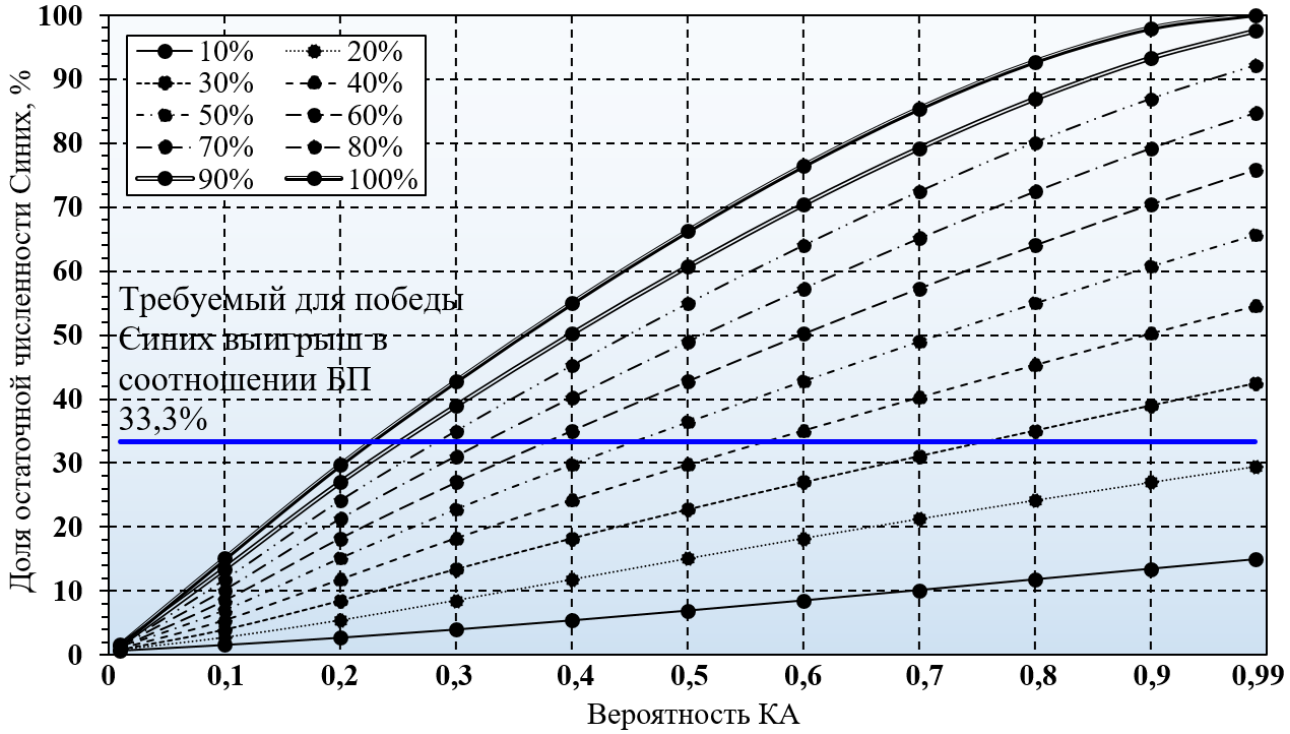


Рис. 9. Боевая эффективность КА на подсистему разведки при различных Δ

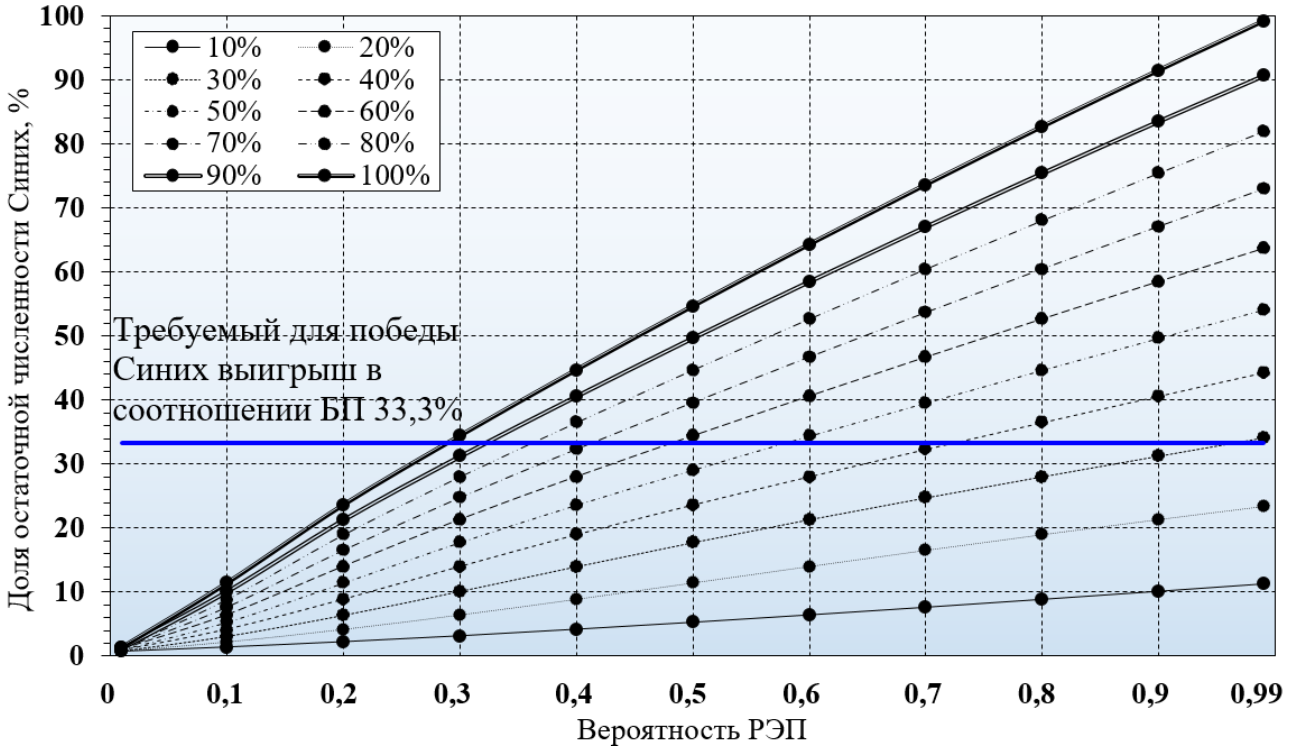


Рис. 10. Боевая эффективность скрытного РЭП подсистемы разведки при различных Δ

№4. 2020
ISSN 2410-9916

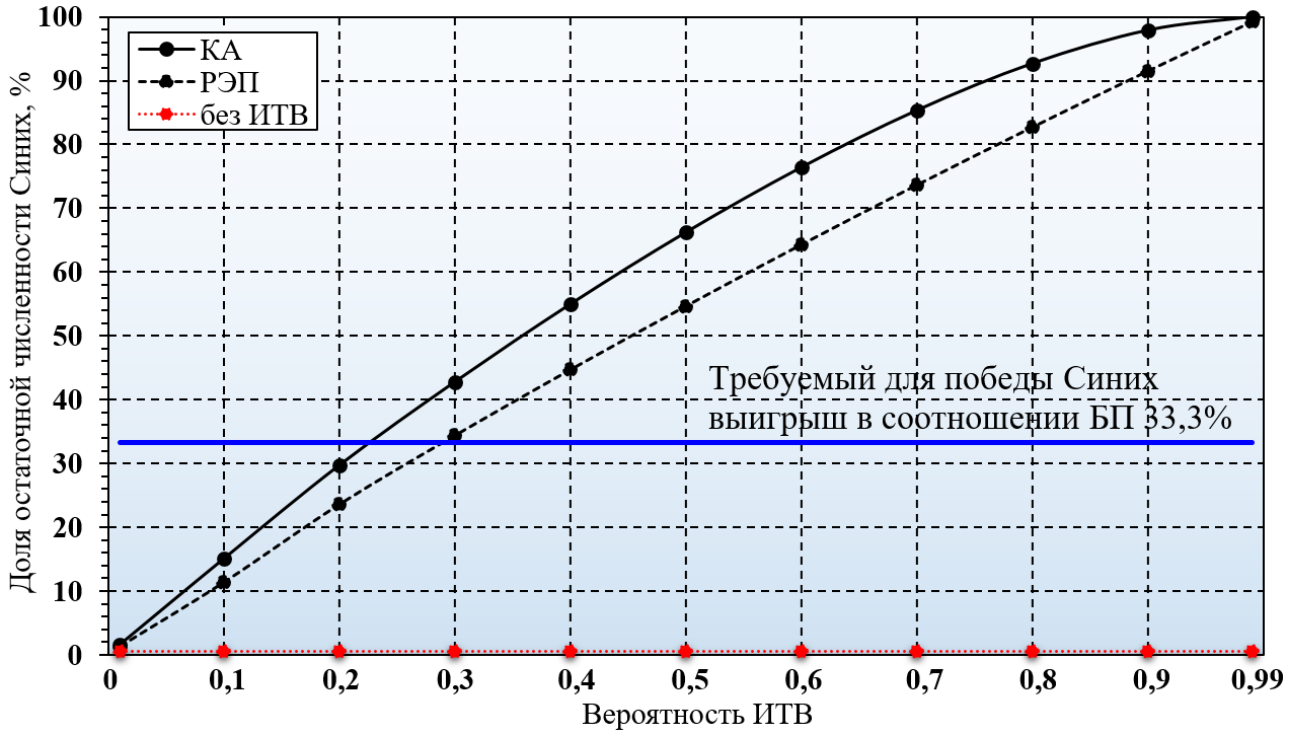


Рис. 11. Боевая эффективность КА и скрытного РЭП подсистемы разведки при Δ=100%

На рис. 11 видно, что боевая эффективность КА выше боевой эффективности скрытного РЭП. Это обусловлено тем, что КА влияют на вероятность разведки и время выполнения задач (операций) в подсистеме разведки, а РЭП только на вероятность разведки.

Выводы по варианту боя №2:

1) орган управления Синих ошибается при выполнении следующих критериев:

$$P_{\text{ИТВ}} < 0,23/\Delta \text{ – для КА;} \quad (1)$$

$$P_{\text{ИТВ}} < 0,29/\Delta \text{ – для скрытного РЭП;} \quad (2)$$

2) если уровень информатизации средств разведки Красных более 30%, то она требует значительных мер для обеспечения защиты от КА.

Вариант боя №3. Боевая эффективность КА на подсистему огневого поражения. Схема этого варианта показана на рис. 12.

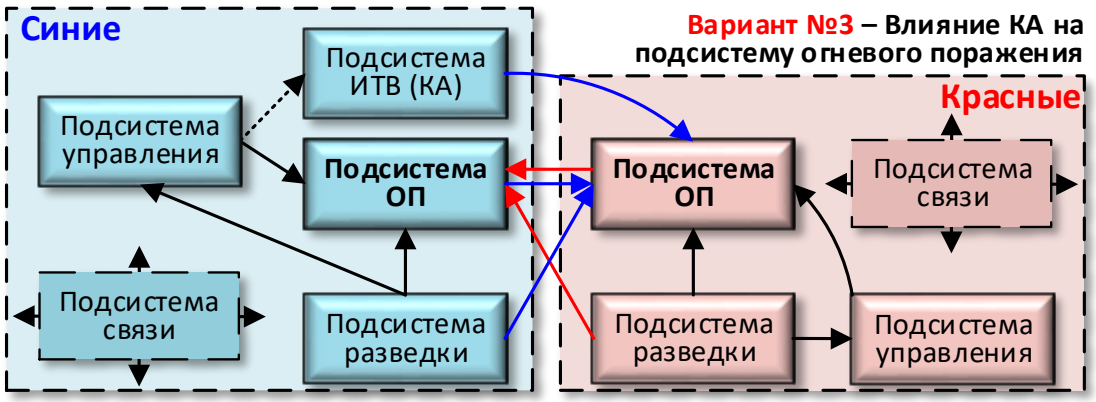


Рис. 12. Схема влияния КА на подсистему ОП

DOI: 1024411/2410-9916-2020-10405
URL: http://sccs.intelgr.com/archive/2020-04/05-Boyko.pdf

Влияние КА и скрытного РЭП на подсистему ОП с позиции математических конструкций аналогично их влиянию на подсистему разведки. Однако на практике РЭП и КА на подсистему ОП отличаются от РЭП и КА на подсистему разведки. Под РЭП на подсистему ОП понимается подавление приемных устройств навигационно-временного обеспечения средств ОП, позволяющих осуществить геопривязку своего местоположения и цели по сигналам радионавигационных систем (в первую очередь спутниковых систем GPS, ГЛОНАСС, Бейдоу и Галилео), а под КА на подсистему ОП понимается нарушение работы информационно-технических средств управления средством ОП. В случае эффективного нарушения работы средств ОП более некоторого порога (он может составлять 10-20%) Красные по низкой эффективности стрельбы, которую обнаружит их подсистема разведки, поймут, что подверглись ИТВ и перейдут на ручной режим управления. Исключение составляют дистанционно-управляемые роботизированные средства ОП. То есть для нероботизированных средств ОП справедливыми будут только части графиков на рис. 10-11 в диапазоне вероятности ИТВ от 0 до 0,2. Тем не менее, ввиду того, что в рассматриваемом бою вероятность ОП значительно ниже вероятности разведки, на рис. 13 показана боевая эффективность КА на подсистему ОП.

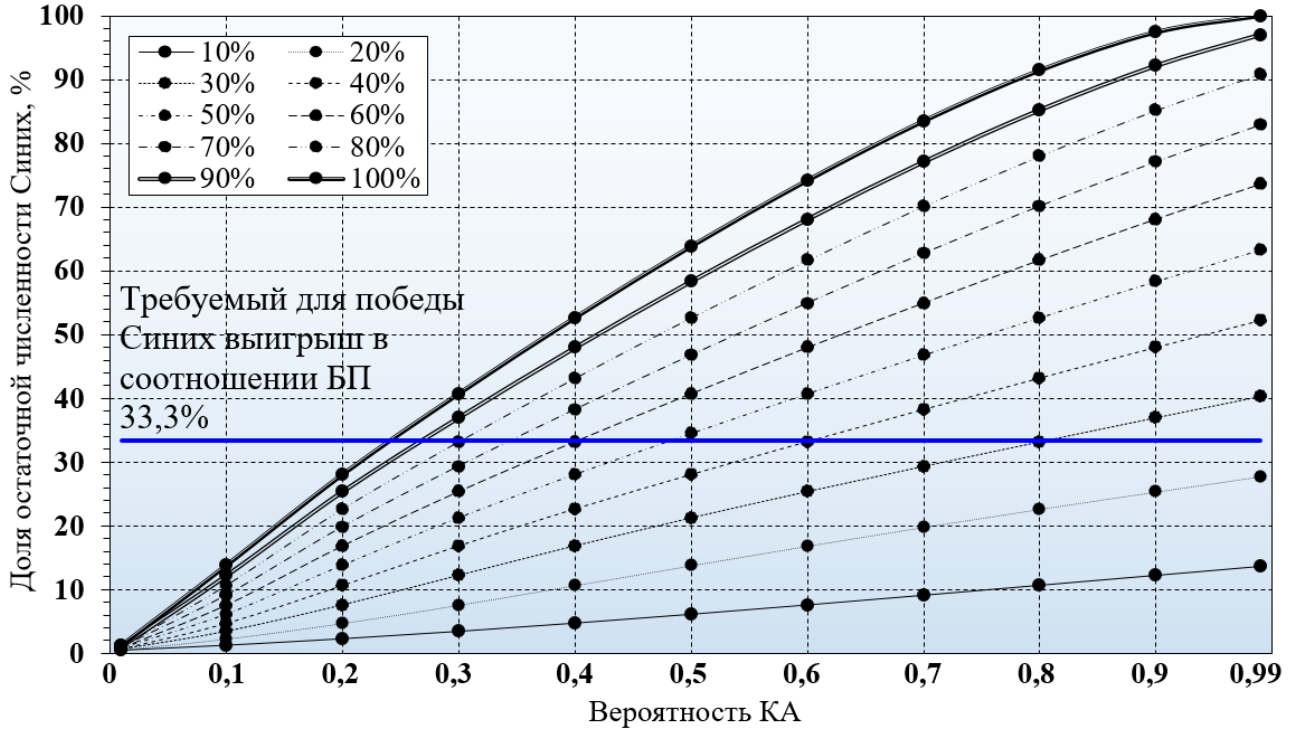


Рис. 13. Боевая эффективность КА на подсистему ОП при различных Δ

Выводы по варианту боя №3:

1) орган управления Синих ошибается при выполнении следующего критерия:

$$P_{\text{ИТВ}} < 0,24/\Delta \text{ – для КА;} \quad (3)$$

2) если Δ для средств разведки Красных более 25%, то их подсистема ОП требует значительных мер для обеспечения защиты от КА.

№4. 2020
ISSN 2410-9916

Вариант боя №4. Боевая эффективность КА на подсистему управления. Схема этого варианта показана на рис. 14. Боевая эффективность КА для различных значений уровня информатизации Δ показана на рис. 15.

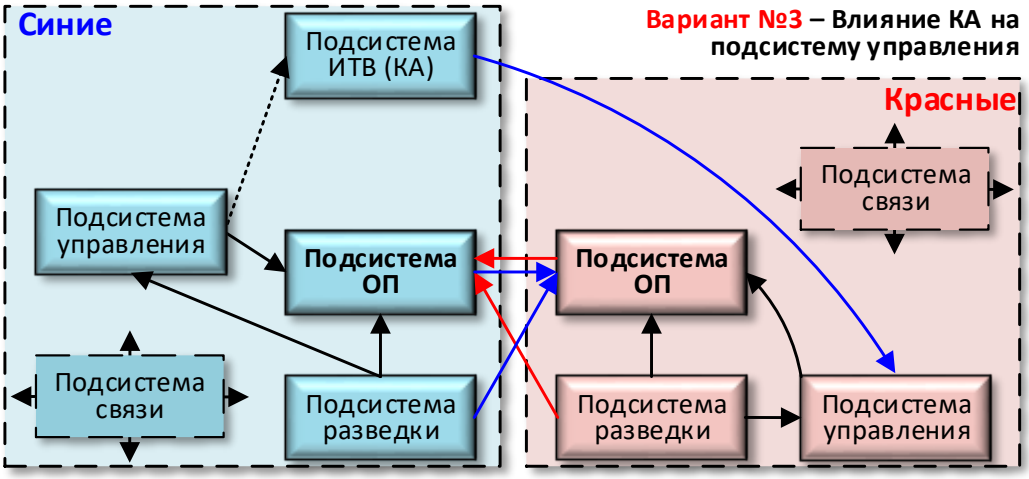


Рис. 14. Схема влияния КА на подсистему управления

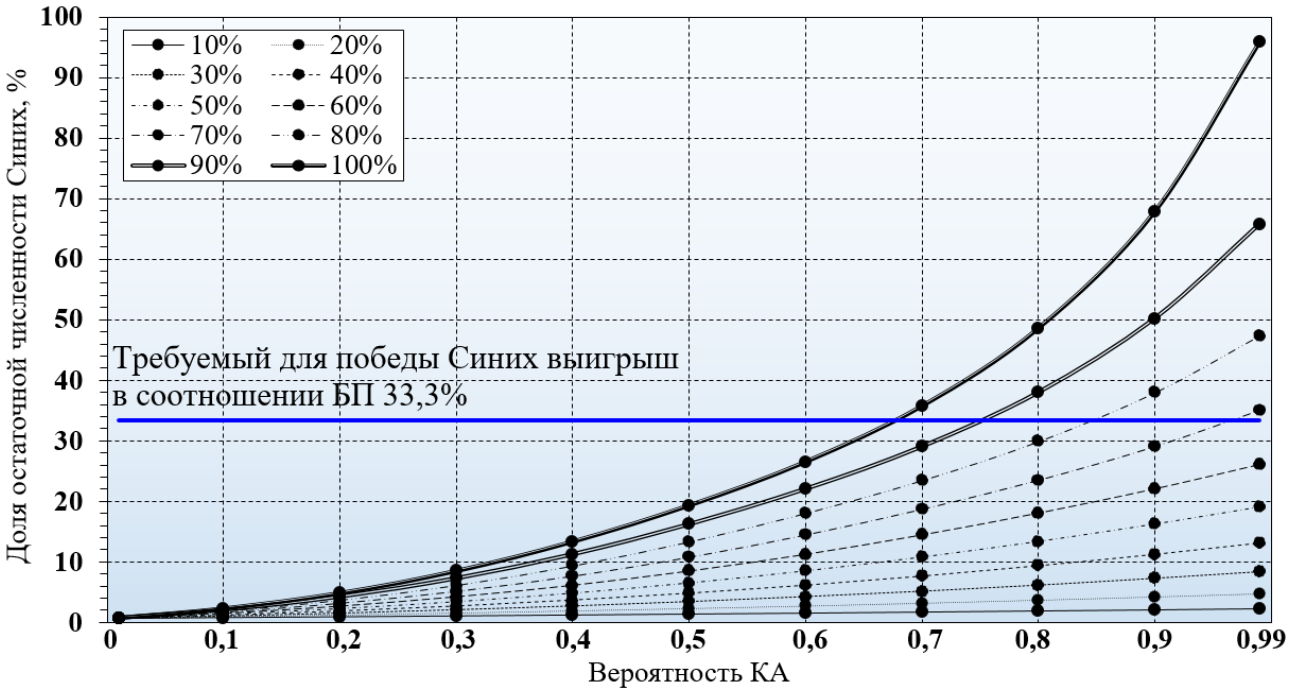


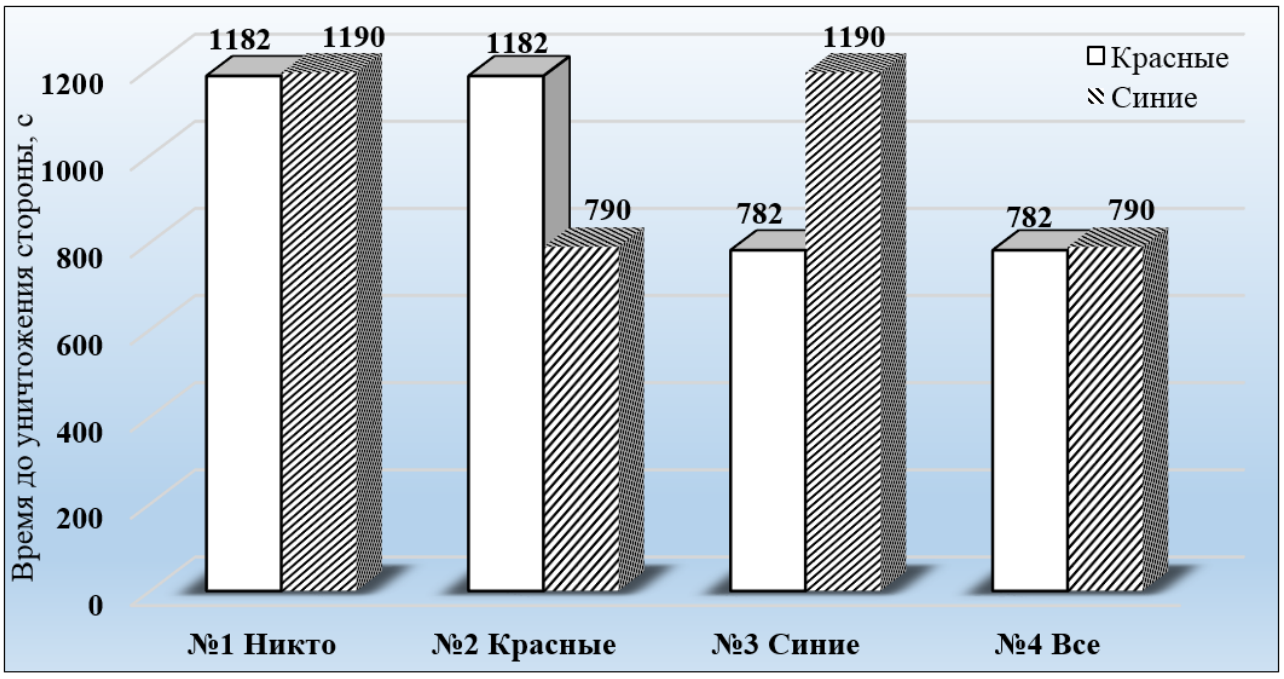
Рис. 15. Боевая эффективность КА на подсистему управления при различных Δ

Очевидно, при наличии сетецентрического доступа средств ОП Красных к развединформации КА на подсистему их управления не являются эффективными. В этом контексте предлагается обратить внимание на целесообразность сетецентрического доступа средств ОП к развединформации.

На рис. 16 показаны времена до уничтожения Красных при различных схемах доступа сторон к развединформации без применения КА. На нем видно, что Синие, наступая, тем не менее, терпят поражение при схеме №2, когда они сетецентрический доступ не применяют, а Красные применяют. Условия, при которых Синие побеждают при схеме №2, показаны на рис. 17.

DOI: 1024411/2410-9916-2020-10405
URL: http://sccs.intelgr.com/archive/2020-04/05-Boyko.pdf

№4. 2020
ISSN 2410-9916



Схемы применения сетецентрического доступа к развединформации

Рис. 16. Времена до уничтожения Красных при различных схемах доступа сторон к развединформации без применения КА

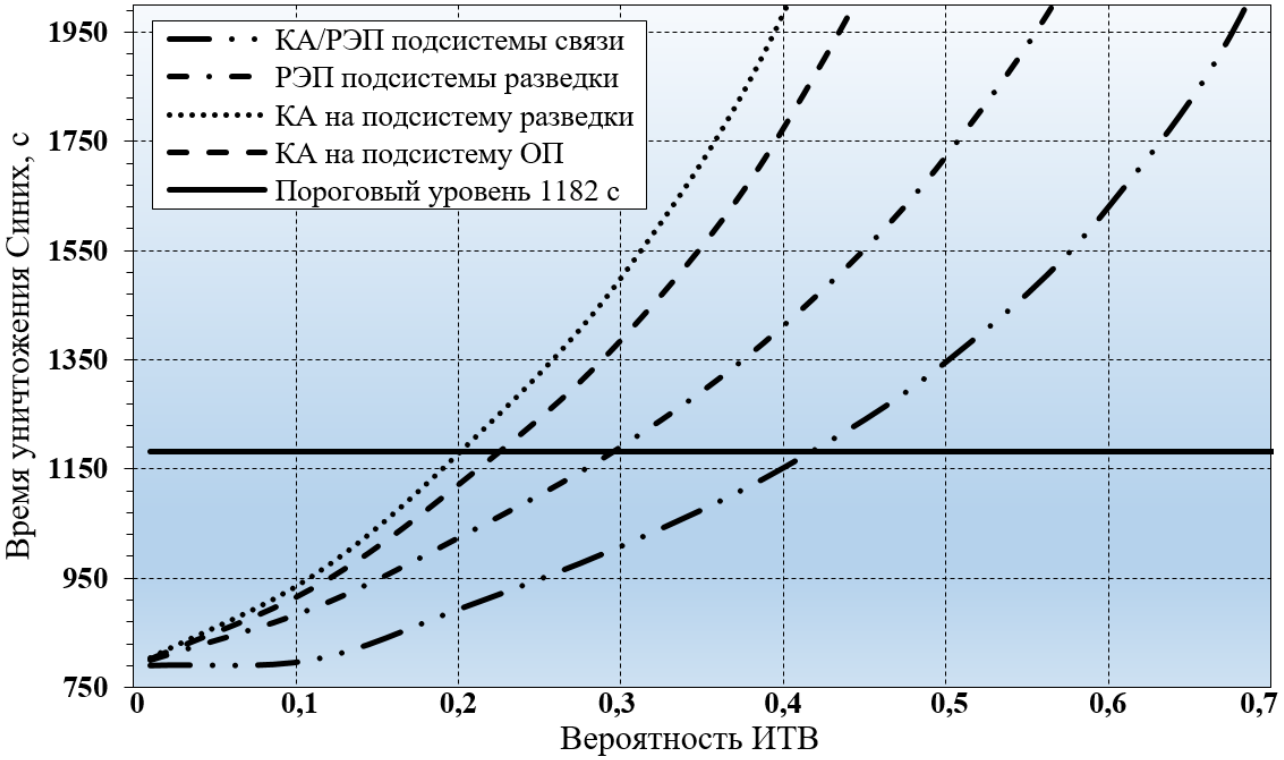


Рис. 17. Времена до уничтожения Красных для различных вариантов ИТВ при Δ=100%

Выводы по варианту боя №4:

1) орган управления Синих ошибается при выполнении следующего критерия:

$$P_{\text{ИТВ}} < 0,67/\Delta; \quad (4)$$

DOI: 1024411/2410-9916-2020-10405
URL: http://sccs.intelgr.com/archive/2020-04/05-Boyko.pdf

2) если ⅓ и более операций в подсистеме управления Красных выполняются без применения информационно-технических средств, то повышение защищенности командно-наблюдательных и командных пунктов от КА не окажет влияния на исход боя, но будет способствовать снижению боевых потерь.

Вариант боя №5. Боевая эффективность тотального воздействия КА, РЭП и поражения ЭМИ. Схема этого варианта показана на рис. 18. Здесь под тотальным воздействием понимается одновременное воздействие на все подсистемы, которые потенциально доступны для соответствующего вида ИТВ. Боевая эффективность КА и скрытного РЭП для различных значений Δ показана на рис. 19 и 20, соответственно. Сравнение боевой эффективности КА и скрытного РЭП для этого варианта показано на рис. 21 для Δ=100%.

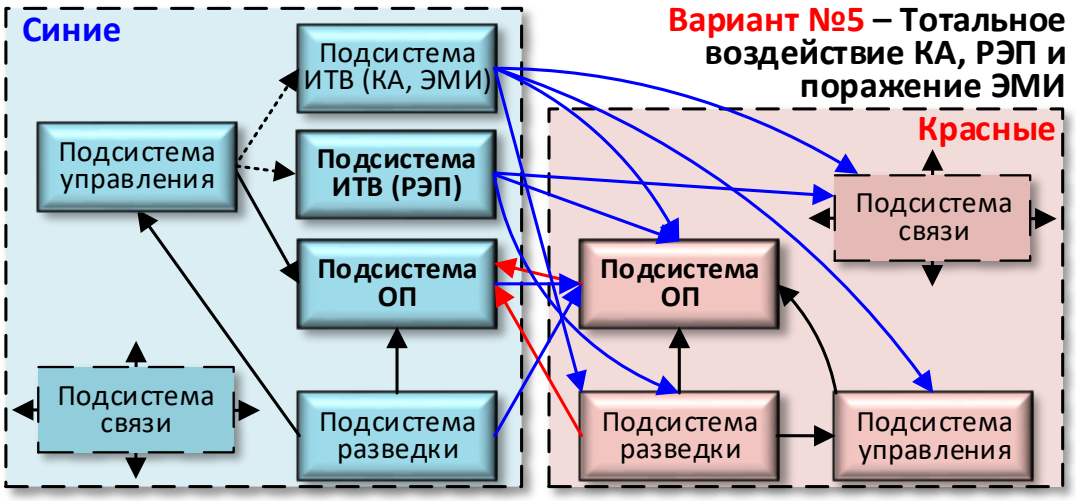


Рис. 18. Схема тотального воздействия КА и РЭП

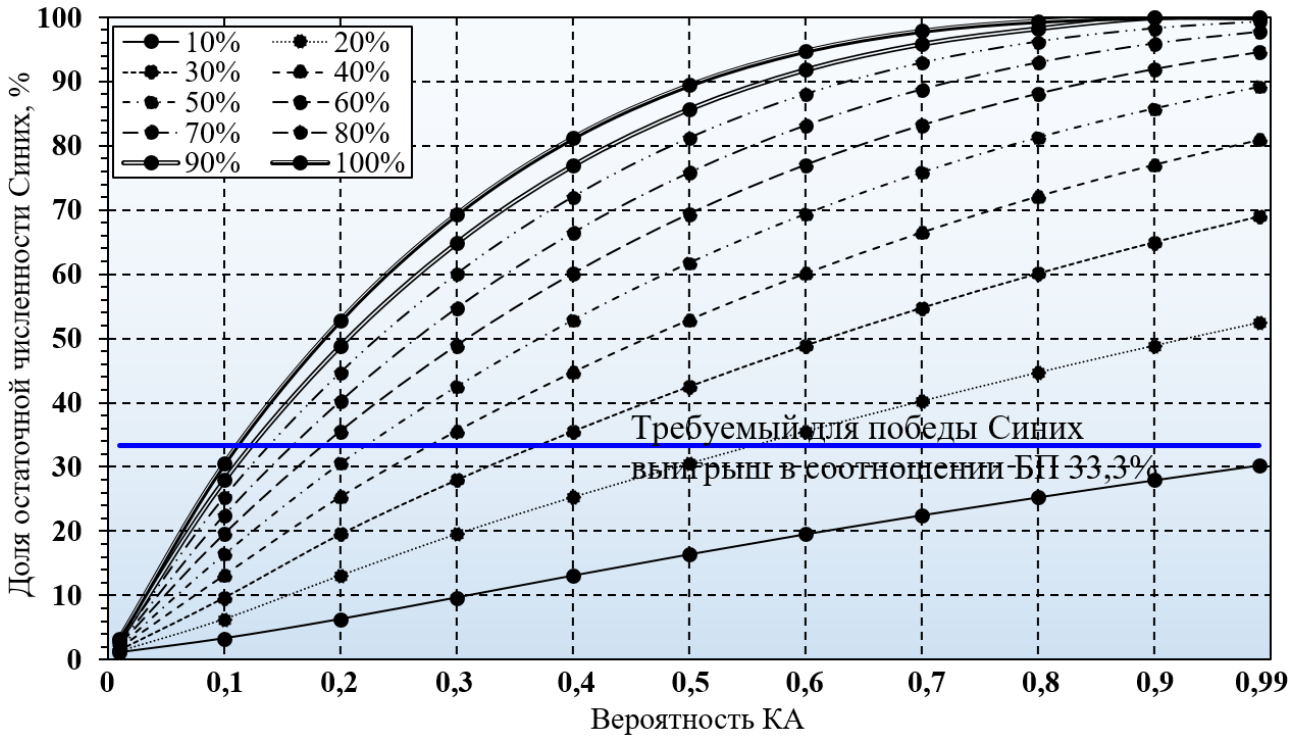


Рис. 19. Боевая эффективность тотального воздействия КА при различных Δ

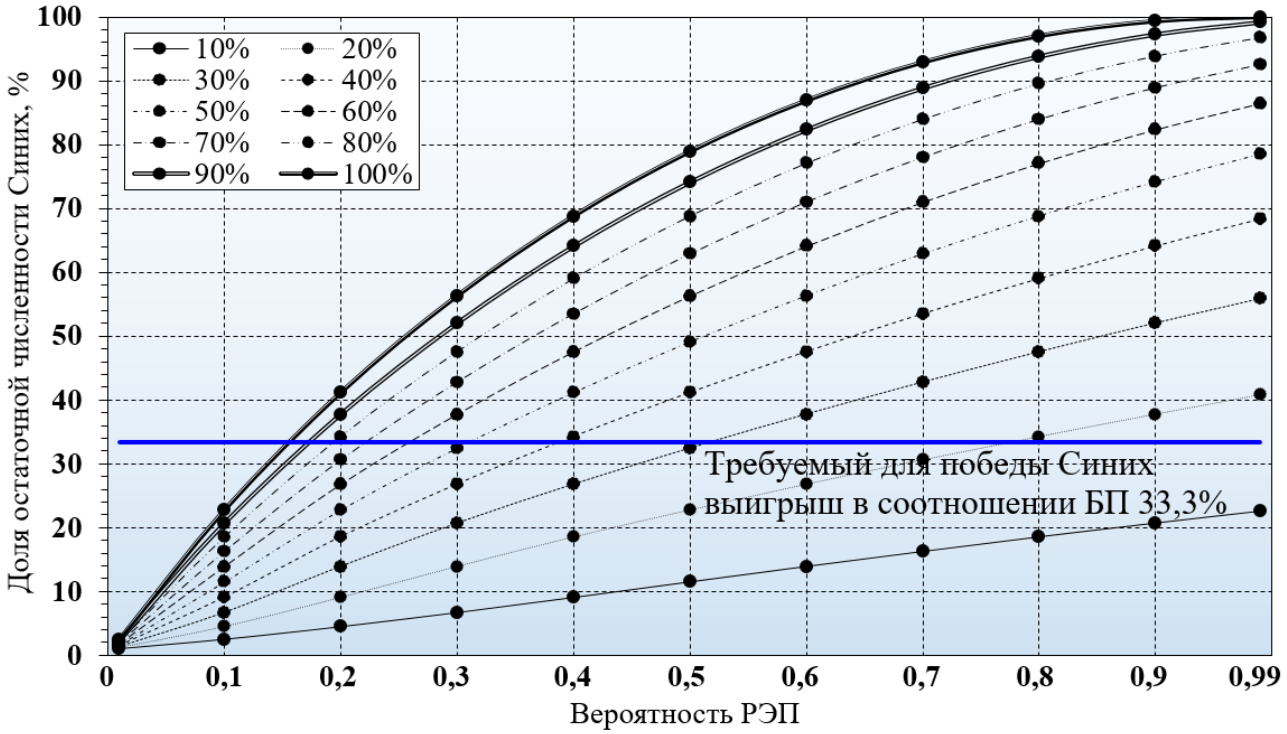


Рис. 20. Боевая эффективность тотального скрытного РЭП при различных Δ

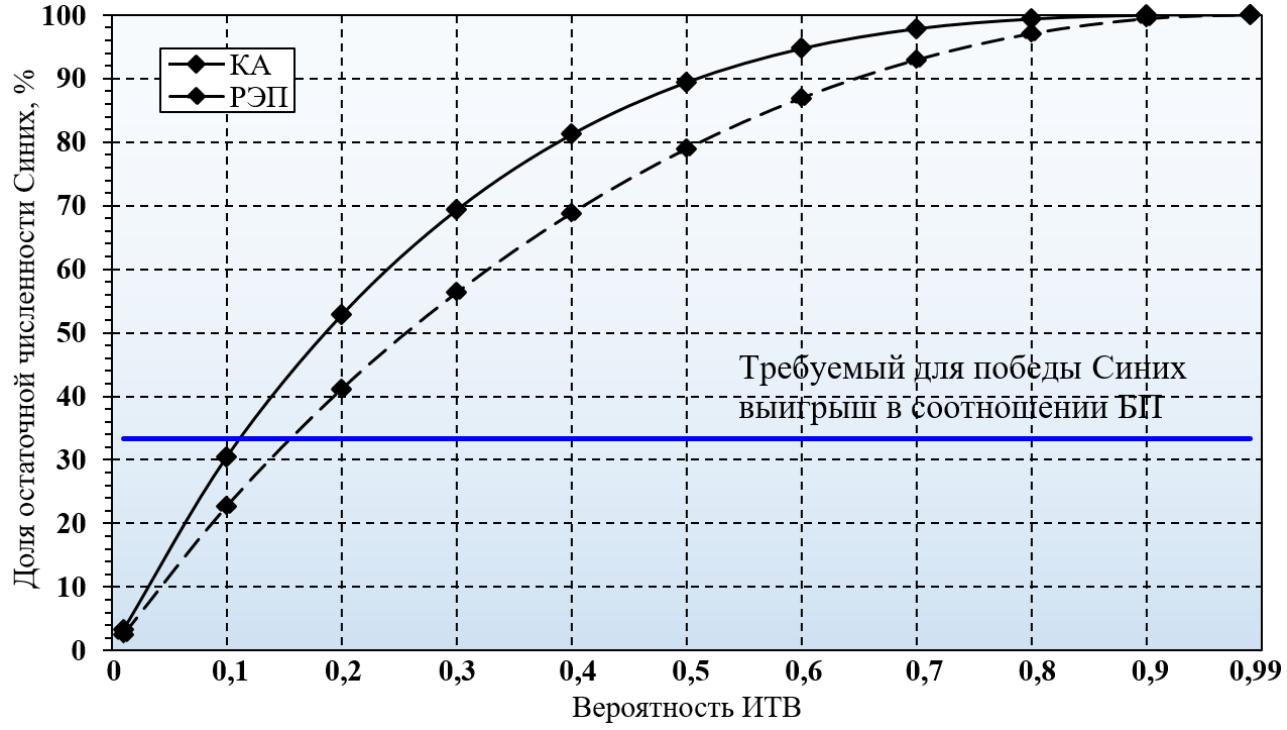


Рис. 21. Боевая эффективность тотальных КА и скрытного РЭП при Δ=100%

Выводы по варианту боя №5:

1) орган управления Синих ошибается при выполнении следующих критериев:

$$P_{\text{ИТВ}} < 0{,}11/\Delta \text{ – для КА;} \quad (5)$$

$$P_{\text{ИТВ}} < 0{,}16/\Delta \text{ – для скрытного РЭП;} \quad (6)$$

2) в интересах недопущения поражения Красных их ВВТ требуют значительных мер для обеспечения защиты от ИТВ.

№4. 2020
ISSN 2410-9916

Вариант боя №6. Боевая эффективность КА, тотальное поражение ЭМИ, имитация боевой обстановки и занятие Красными оборудованных позиций. Схема этого варианта показана на рис. 22.

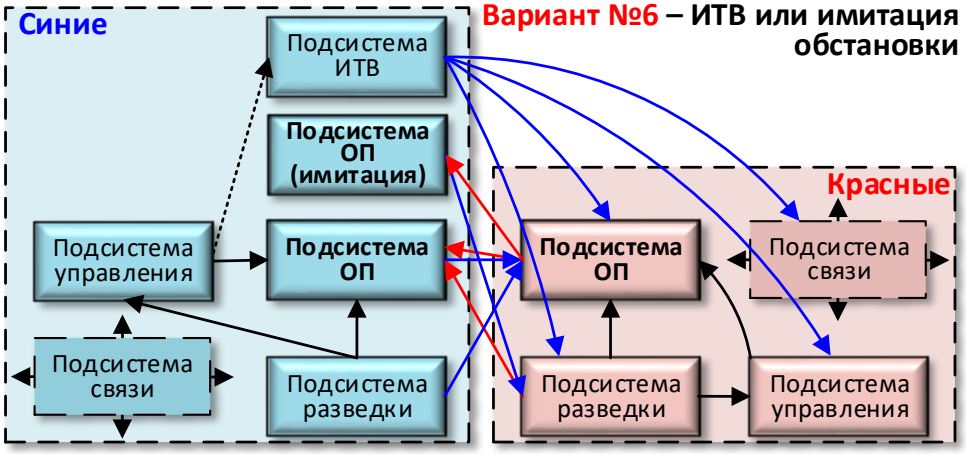


Рис. 22. Схема применения КА и имитации боевой обстановки

Под имитацией боевой обстановки понимается применение Синими имитационных средств ОП, создаваемых любыми способами (в том числе постановкой активных и пассивных имитирующих помех, развертыванием муляжей), на которые Красные расходуют свой боекомплект и ресурс скорострельности. На рис. 23 показана боевая эффективность КА на различные подсистемы для Δ=100%, тотального поражения ЭМИ для Δ=100% и имитации боевой обстановки Синими без дополнительной защиты Красных и с дополнительной защитой, предполагающей занятие ими обороны на оборудованных позициях.

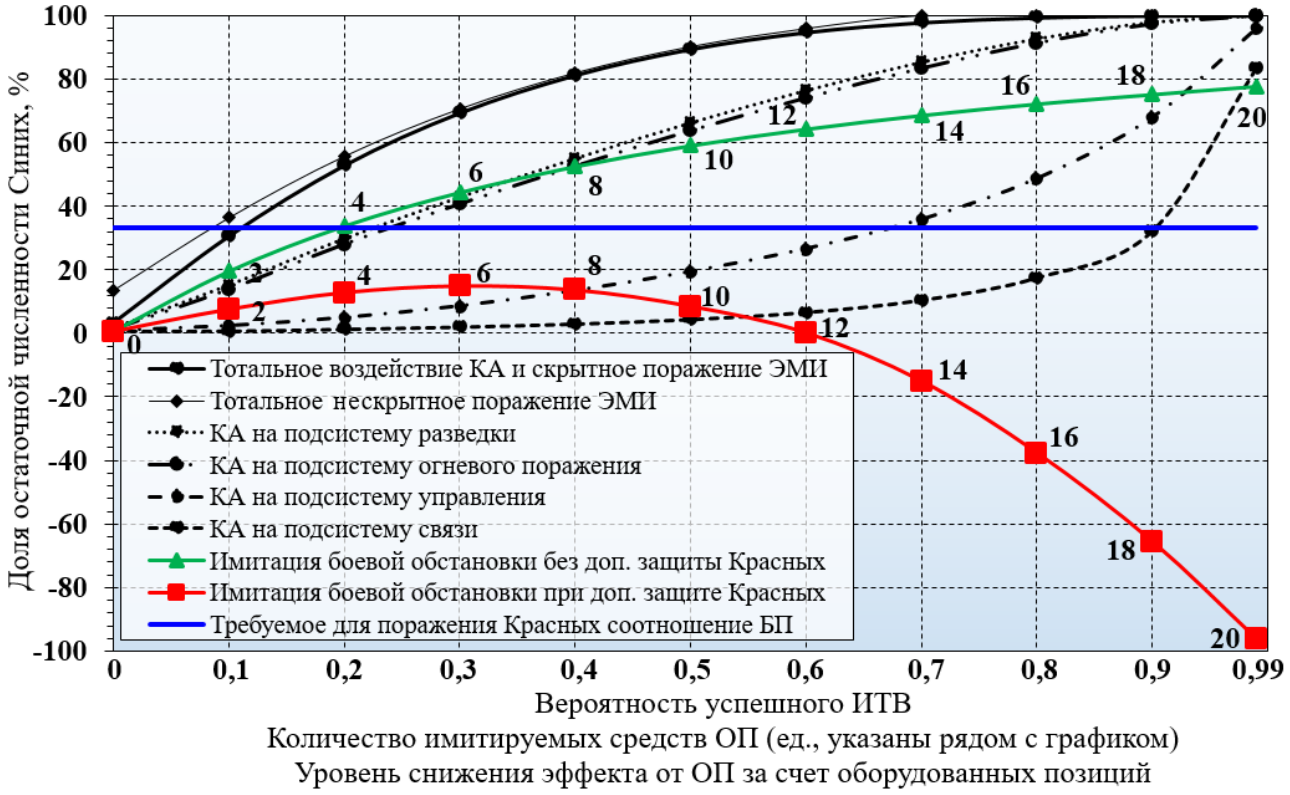


Рис. 23. Сравнение боевой эффективности ИТВ и имитации боевой обстановки

DOI: 1024411/2410-9916-2020-10405
URL: http://sccs.intelgr.com/archive/2020-04/05-Boyko.pdf

Выводы по варианту боя №6:

1) орган управления Синих ошибается, если количество имитируемых средств ОП составляет менее 4;

2) в интересах недопущения поражения Красных их подсистема разведки должна распознавать не менее 80% ложных целей;

3) при применении Синими средств имитации боевой обстановки или ИТВ Красным следует как можно быстрее занять оборону.

Во всех рассмотренных вариантах применения ИТВ в современном бою вместо КА или РЭП может использоваться поражение ЭМИ. Если поражение ЭМИ является скрытным (например, если массогабаритные характеристики средства ИТВ позволяют поместить его на БПЛА), то его боевая эффективность аналогична таковой для КА. В противном случае эффект от применения ЭМИ будет несколько выше эффекта тотального воздействия КА, как показано на рис. 23, но за этот незначительный эффект, наблюдаемый при Δ=0%…30%, Синим придется пожертвовать средством поражения ЭМИ.

Приведенные результаты аналитического моделирования современного боя показывают, что ЭМВ в бою дают эффект, являющийся частным случаем эффекта КА в различных вариантах их применения.

Методика обоснования требований к защищенности ВВТ ВФ от КА

Рассмотренные выше результаты исследования аналитической модели современного боя свидетельствуют о необходимости обеспечения защиты образцов ВВТ ВФ от КА ввиду значительного влияния этого относительно нового вида ИТВ на соотношение БП ВФ.

При планировании боя рассчитывается максимально допустимый уровень доли остаточной численности своего ВФ $\mathfrak{M}_{\text{нач}}$. Например, при планировании наступления тактического ВФ $\mathfrak{M}_{\text{нач}}$ = 75…80% [25]. В то же время существует пороговое значение остаточной доли численности ВФ (т.н. «А-правило») или соотношения численностей ВФ (т.н. «Р-правило»), по достижении которого ВФ отказывается от дальнейшего сопротивления $\mathfrak{M}_{\text{пор}}$. У ВФ разных стран и тем более незаконных вооруженных формирований значения $\mathfrak{M}_{\text{пор}}$ могут существенно различаться (например, по «А-правилу» в обороне это значение может составлять 5-10% [26]). То есть в наиболее общем случае для нарушения замысла противника нужно его начальную численность сократить не менее чем на $\mathfrak{M}_{\text{нач}} - \mathfrak{M}_{\text{пор}}$. Из этого следует критерий, к выполнению которого необходимо стремиться при проведении мероприятий по защите ВВТ ВФ от КА:

$$\Delta N^{*}_{\text{син}} \le \mathfrak{M}_{\text{нач}} - \mathfrak{M}_{\text{пор}}\Big|_{\xi_{\text{защ}} \le \xi_{\text{доп}}}, \qquad (7)$$

где: $\Delta N^{*}_{\text{син}}$ – остаточная численность ВФ, которое противостоит ВФ с образцами ВВТ, в отношении которых произведены мероприятия по защите от КА; $\xi_{\text{защ}}$ и $\xi_{\text{доп}}$ – требуемая и допустимая стоимость мероприятий по обеспечению защиты ВВТ ВФ от КА, соответственно.

Рассмотрим условия, при которых возможно определить, смогут ли меры по защите ВВТ ВФ от КА обеспечить выполнение критерия (7).

Существуют три типовых вида общевойскового боя [25]: встречный бой, бой с неподготовленными позициями обороны и бой с подготовленными позициями обороны. Широко известны классические критерии исходного соотношения численностей ВФ, по которым в наиболее общем случае принимается решение: для встречного боя – 1,5:1; для неподготовленных позиций обороны – 3:1; для подготовленных позиций обороны – 6:1. Если органом управления наступающей стороны принято решение атаковать противника в заданных условиях, то это означает, что указанный критерий по его расчетам выполнен, а неизменная ограниченность ресурсов в наиболее общем случае будет способствовать тому, чтобы расчетные соотношения исходных численностей ВФ не отклонялись от этих критериев. При этом реальное значение соотношения исходных численностей противоборствующих ВФ может варьироваться в соответствии с возможностями сторон по воздействию на противника и с состоянием обороняемых позиций, определяемым показателем ослабления ущерба обороняемым позициям U (для наступающей стороны он равен 1).

Оценить значение показателя U предлагается следующим образом. Сначала следует задать указанные в таблице 1 параметры возможностей сторон при типовом соотношении численностей для заданных боевых условий (например, для неподготовленных позиций обороны $N_{син} : N_{кр} = 3:1$) и $P_{ИТВ}=0$. Далее следует определить такое значение U, при котором наступающие теряют $\mathfrak{M}_{нач}$ своей численности. После этого следует уменьшить значение $N_{син}$ так, чтобы для реального значения $P_{ИТВ}$ при оцененном значении U Синие теряли $\mathfrak{M}_{нач}$ своей численности. Полученное таким образом исходное соотношение численностей ВФ будет учитывать возможности КА и особенности обороняемых позиций.

ВФ, которое противостоит ВФ с защищаемыми от КА образцами ВВТ может быть любым, но рационально соизмеримым с защищаемым ВФ в диапазоне 6:1…1,5:1. Оптимальным с точки зрения минимизации исходных данных является вариант, когда защищаемое ВФ ведет бой само с собой (несколькими такими же ВФ) и одна из сторон дополнительно включает подсистему КА.

С учетом изложенного предлагается следующая методика обоснования требований к защищенности образцов ВВТ ВФ от КА.

Шаг 1. Определение значения показателя ослабления ущерба обороняемым позициям U, при котором остаточная доля численности ВФ, противостоящего защищаемому ВФ, равна $\mathfrak{M}_{нач}$. Для этого моделируется бой, в котором защищаемое ВФ противостоит такому ВФ, характеристики подсистем которого аналогичны защищаемому ВФ, а исходное соотношение численности средств ОП сторон определяется заданным видом боя (то есть 1,5:1, 3:1 или 6:1).

Шаг 2. Определение действительного исходного соотношения численности средств ОП защищаемого ВФ и противостоящего ему ВФ. Для этого моделируется бой, в котором при определенном на шаге 1 значении показателя U защищаемому ВФ противостоит ВФ, характеристики подсистем которого аналогичны защищаемому ВФ, с дополнительно приданной ему подсистемой КА. В ходе моделирования определяется такая исходная численность средств ОП противостоящего ВФ сторон, при которой остаточная доля его численности равна $\mathfrak{M}_{нач}$.

Шаг 3. Определение такой вероятности успешной реализации КА, при которой выполняется критерий (7). Блок-схема алгоритма, реализующего этот шаг, приведена в [26]. При невозможности выполнения обоих критериев стоимостный критерий является приоритетным, а остаточная доля численности стремится у противостоящего ВФ к минимуму, а у защищаемого ВФ к максимуму (с его приоритетом).

Примеры применения методики для встречного боя одинаковых ВФ при значении $\mathfrak{M}_{\text{нач}}$, стремящемся к максимуму, и $\mathfrak{M}_{\text{пор}} = 66{,}7\%$ без рассмотрения вопросов стоимости мероприятий по защите образцов ВВТ от КА приведены выше в ходе анализа процесса применения КА в современном бою.

В интересах повышения оперативности применения предложенной методики в ходе анализа рассмотренной модели современного боя при различных вариантах применения ИТВ выявлена универсальная аналитическая зависимость остаточной доли численности ВФ от вероятности реализации ИТВ во встречном бою одинаковых ВФ, одно из которых дополнено подсистемой ИТВ:

$$\Delta N^{*}_{\text{син}} = a \cdot \Delta^{b}\left(1-\left(d \cdot P_{\text{ИТВ}}\right)^{c}\right), \qquad (8)$$

где: a – коэффициент, зависящий от временных характеристик функционирования подсистем в результате ИТВ; b и c – коэффициенты, зависящие от вероятностных и временных характеристик функционирования подсистем в результате ИТВ; d – коэффициент, учитываемый при ИТВ на подсистему связи ВФ.

Фактически формула (8) является формулой оценки защищенности ВФ от ИТВ. В ходе исследований проведен регрессионный анализ результатов использования модели [12] и с применением метода наименьших квадратов получены формулы для расчета значений коэффициентов в формуле (8) применительно к КА, как наиболее эффективному виду ИТВ в общевойсковом бою. Эти формулы приведены в таблице 2 для вариантов тотального воздействия КА на все подсистемы и выборочного воздействия КА на подсистему связи, управления, разведки или ОП.

Таблица 2 – Коэффициенты в формуле оценки защищенности ВФ от ИТВ

Условия боя	Аналитические выражения для расчета коэффициентов	Примечание
1. Тотальные КА или скрытное поражение ЭМИ	$a=1;\ b=\left(\Delta^{1,88}s^{2,05}+k^{2,04}\right)^{-1};\ s=3{,}55-0{,}02\cdot\ln n;$ $k=1{,}21+0{,}84\cdot T_{\text{бц}}^{-0{,}06}n^{-1};\ c=\Delta^{2,34}k^{2,56}+k^{1,29};\ d=1$	$T_{\text{бц}}$ – время с момента обнаружения цели до первого выстрела по ней
2. КА, скрытное поражение ЭМИ или РЭП подсистемы связи	$a=1{,}04-\left(8\cdot10^{-4}\cdot T_{\text{св}}+0{,}03\right)\cdot\ln T_{\text{бц}}+6\cdot10^{-3}\cdot T_{\text{св}};$ $b=0{,}0147\cdot e^{-0{,}027\cdot T_{\text{св}}}\cdot T_{\text{бц}}+2\cdot10^{-4}\cdot T_{\text{св}}^{2}-0{,}015\cdot T_{\text{св}}+$ $+1{,}144+1{,}1\cdot T_{\text{св}}^{-1{,}04}\cdot\ln n;$ $c=63{,}1\cdot T_{\text{бц}}^{-1{,}19}\cdot T_{\text{св}}^{1-4{,}43\cdot T_{\text{бц}}^{-0{,}4}}-5\cdot10^{-5}\cdot T_{\text{бц}}+0{,}014;\ d=P_{\text{гар}}^{-1}$	$T_{\text{бц}}$ – аналогично условиям тотального КА
3. КА или скрытное	$a=1+0{,}64e^{0{,}0366T_{\text{бц}}}T_{\text{упр}}^{-1{,}2313e^{0{,}0022T_{\text{бц}}}}+0{,}0626e^{0{,}0357\cdot T_{\text{бц}}}T_{\text{упр}}^{-0{,}782e^{0{,}0044T_{\text{бц}}}};$	$T_{\text{бц}}$ не включает $T_{\text{св}}$

Условия боя	Аналитические выражения для расчета коэффициентов	Примечание
поражение ЭМИ подсистемы управления	$b = 1,283 + 0,2358 \cdot T_{\text{упр}}^{-0,842} \cdot T_{\text{бц}} - 0,0013 \cdot T_{\text{упр}} - 0,018 \cdot \ln T_{\text{упр}}$; $c = 1,39 + \left(0,0386 \cdot \ln T_{\text{бц}} + 0,059\right) \cdot \ln T_{\text{упр}} - -0,4093 \cdot \ln T_{\text{бц}} + 0,0175 \cdot e^{-0,003 \cdot T_{\text{бц}}}$; $d = 1$	
4. КА или скрытное поражение ЭМИ подсистемы разведки / огневого поражения	$a = 1 + 0,045 \cdot T_{\text{бц}}^{-0,228} \cdot T_{\text{р}}^{k}$ $k = 0,24 - 10^{-6} \cdot T_{\text{бц}}^2 + 5 \cdot 10^{-4} \cdot T_{\text{бц}}$; $b = 0,555 + \left(0,0744 - 2 \cdot 10^{-4} \cdot T_{\text{р}}\right) \cdot \ln T_{\text{бц}} - -5,59 \cdot T_{\text{р}}^{-0,665} \cdot n^{-8,98 \cdot T_{\text{р}}^{-0,628}}$; $c = 0,7784 + \left(0,012 - 0,0274 \cdot \ln T_{\text{р}}\right) \cdot \ln T_{\text{бц}} + +0,2176 \cdot \ln T_{\text{р}} + 2 \cdot n^{-1,66}$; $d = 1$	$T_{\text{бц}}$ не включает $T_{\text{р}}$.
Примечание: Для всех условий рассматриваемого боя $n = \left\lceil \ln\left(1 - P_{\text{гар}}\right) / \ln\left(1 - P \cdot_{\text{р}} P_{\text{1бп}}\right) \right\rceil$.		

Точность формул в таблице 2 характеризуется соответствующими диаграммами максимальных абсолютных отклонений численных значений, полученных с применением формулы оценки защищенности ВФ от ИТВ, от результатов вычислений, полученных с применением рассматриваемой в настоящей работе аналитической модели боя. Эти диаграммы для различных условий боя показаны на рис. 24-28.

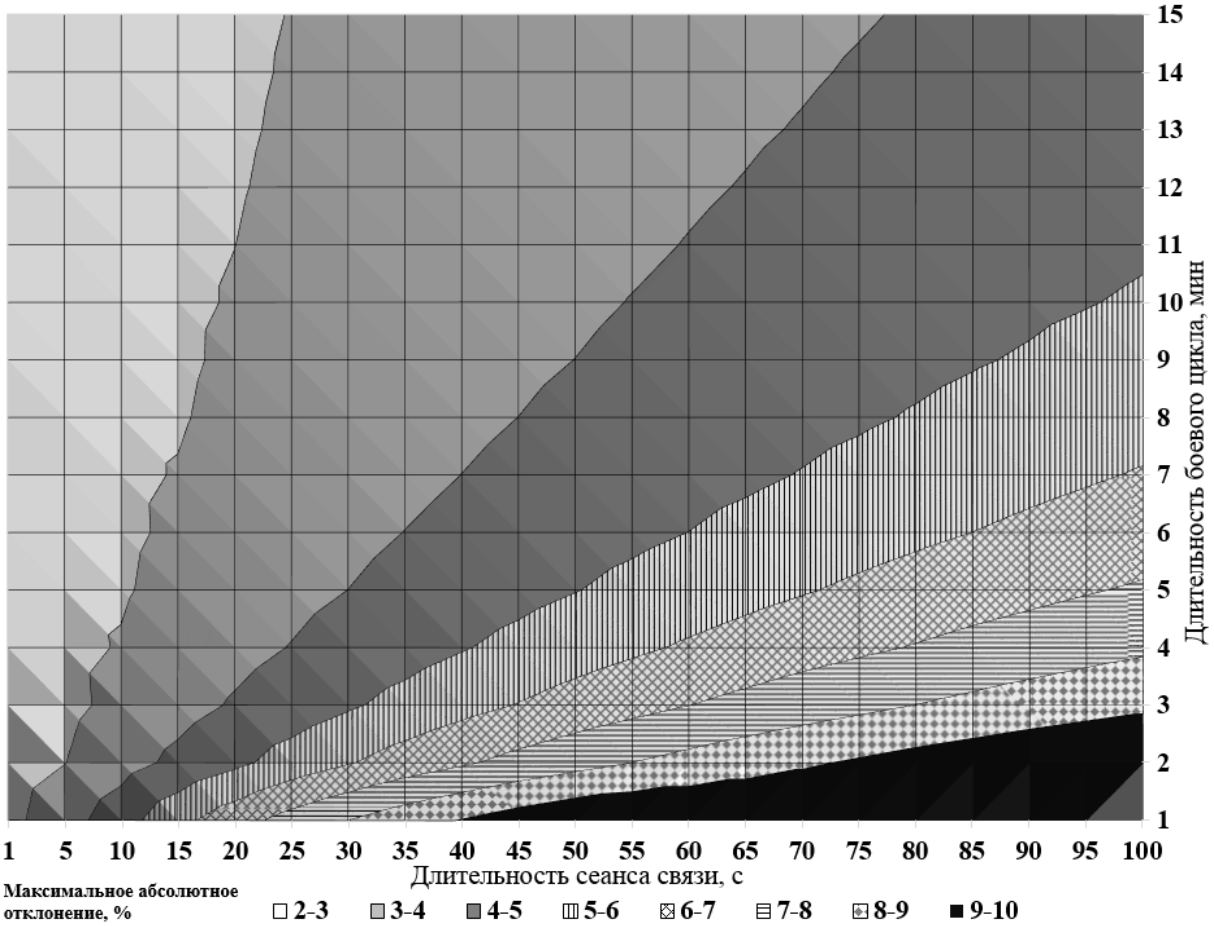


Рис. 24. Диаграмма для тотальных КА или скрытного поражения ЭМИ

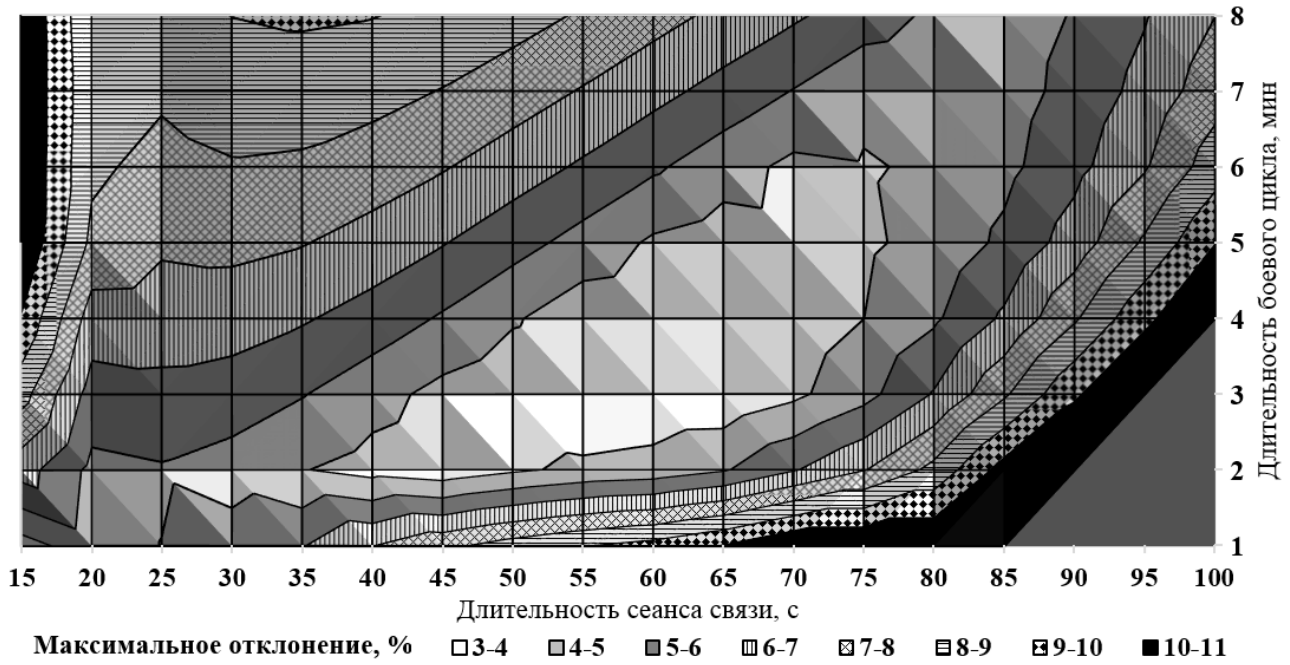


Рис. 25. Диаграмма для КА, скрытного поражения ЭМИ или РЭП применительно к подсистеме связи

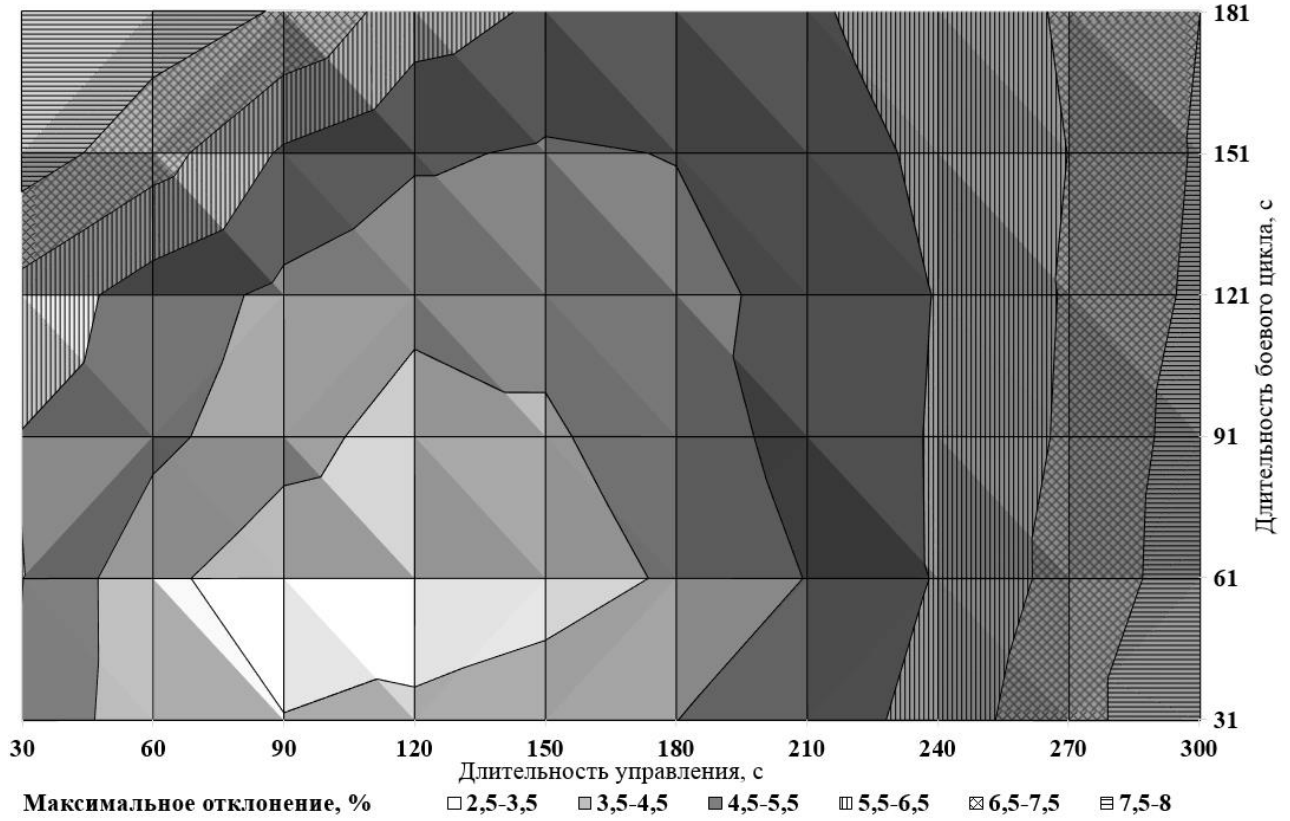


Рис. 26. Диаграмма для КА или скрытного поражения ЭМИ подсистемы управления при стрельбе с закрытых позиций с применением обычных средств огневого поражения ($P_{оп}$=0,1…0,6)

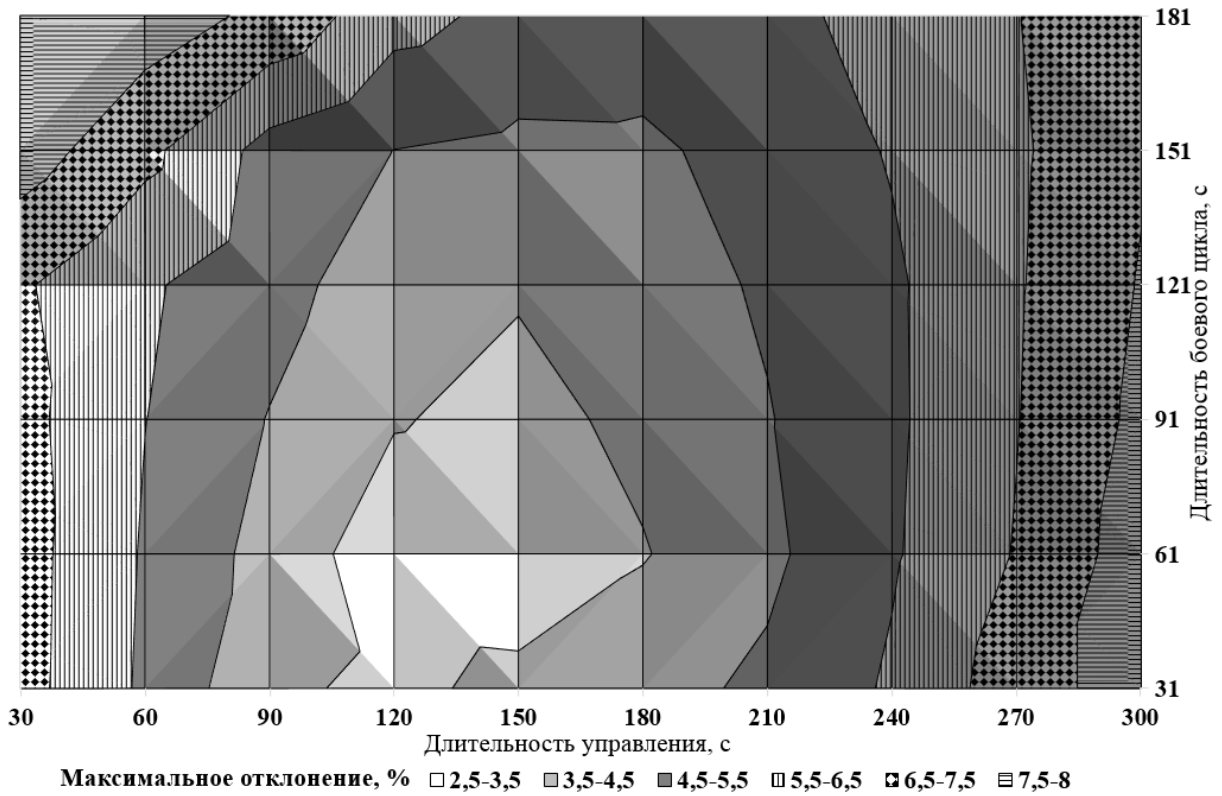


Рис. 27. Диаграмма для КА или скрытного поражения ЭМИ подсистемы управления при стрельбе прямой наводкой и с закрытых позиций с применением высокоточных средств ОП ($P_{оп}$=0,6...0,9)

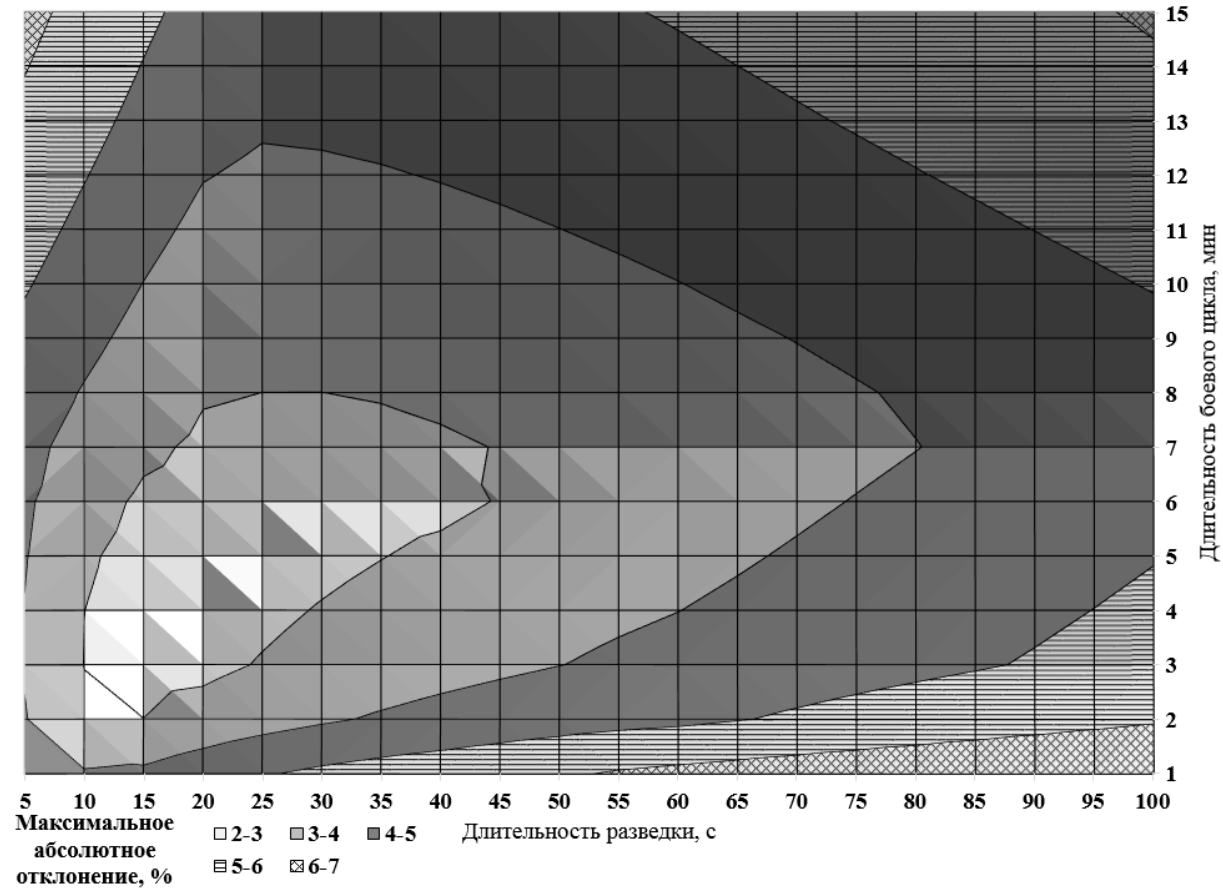


Рис. 28. Диаграмма максимальных абсолютных отклонений для КА или скрытного поражения ЭМИ подсистемы разведки / огневого поражения

Область применения результатов решения задачи

Предложенная методика может найти применение при разработке перспективных и модернизации существующих образцов ВВТ в части обоснования требований к конфликтной устойчивости их информационно-технических средств в условиях КА противника.

Дальнейшей проработки в рамках этого направления исследований требуют вопросы уточнения рассмотренных в настоящей статье эмпирических формул для вычисления значений коэффициентов в формуле оценки защищенности ВФ от ИТВ, а также разработки таких формул для других вариантов применения ИТВ в боевых условиях. Эту задачу наиболее качественно представляется возможным решить с применением высокопроизводительных вычислительных платформ.

Заключение

Таким образом, в настоящей работе исследована аналитическая модель современного боя, позволяющая оценить эффект от системного влияния огневого поражения, электромагнитного воздействия и кибератак на временные и вероятностные характеристики подсистем разведки, связи, управления и огневого поражения, функционирующих в рамках единого боевого цикла воинского формирования, а также разработана методика обоснования требований к защищенности образцов вооружения и военной техники от кибератак.

В интересах повышения оперативности применения предложенной методики выявлена универсальная аналитическая зависимость остаточной доли численности воинского формирования от вероятности реализации кибератак во встречном бою двух одинаковых воинских формирований, одно из которых дополнено подсистемой информационно-технических воздействий. Для этой закономерности предложены формулы оценки коэффициентов при тотальном воздействии кибератак на все подсистемы и выборочном воздействии на подсистему связи, управления, разведки или огневого поражения. Приведены диаграммы максимальных абсолютных отклонений значений, полученных с применением предложенных формул, от результатов моделирования. Показаны примеры обоснования требований к обеспечению конфликтной устойчивости воинских формирований при различных вариантах реализации кибератак.

Предложенная методика может найти применение при обосновании требований к конфликтной устойчивости информационно-технических средств существующих и перспективных образцов вооружения и военной техники в условиях кибератак противника.

Литература

1. Бойко А. А., Дьякова А. В. Способ разработки тестовых удаленных информационно-технических воздействий на пространственно распределенные системы информационно-технических средств // Информационно-управляющие системы. 2014. № 3. С. 84-92.

2. Бойко А. А., Храмов В. Ю. Модель информационного конфликта информационно-технических и специальных программных средств в

вооруженном противоборстве группировок со статичными характеристиками // Радиотехника. 2013. № 7. С. 5-10.

3. Бойко А. А. Способ стратифицированного аналитического описания процесса функционирования информационно-технических средств // Информационные технологии. 2015. № 1. С. 35-42.

4. Бойко А. А., Будников С. А. Модель информационного конфликта специального программного средства и подсистемы защиты информации информационно-технического средства // Радиотехника. 2015. № 4. С. 136-141.

5. Бойко А. А. Способ аналитического моделирования процесса распространения вирусов в компьютерных сетях различной структуры // Труды СПИИРАН. 2015. № 5. С. 196-211.

6. Бойко А. А. О защищенности информации воинских формирований в современном вооруженном противоборстве // Военная Мысль. 2016. № 4. С. 38-51.

7. Бойко А. А., Дегтярев И. С. Метод оценки весовых коэффициентов элементов организационно-технических систем // Системы управления, связи и безопасности. 2018. № 2. С. 245-266.

8. Бойко А. А. Способ оценки уровня информатизации образцов вооружения // Системы управления, связи и безопасности. 2019. № 1. С. 264-275. DOI: 1024411/2410-9916-2019-10116.

9. Бойко А. А. Способ аналитического моделирования боевых действий // Системы управления, связи и безопасности. 2019. № 2. С. 1-27. DOI: 10.24411/2410-9916-2019-10201.

10. Бойко А. А. Метод разработки иерархических многоуровневых моделей для аналитической оценки соотношения сил воинских формирований // Военная Мысль. 2019. № 7. С. 104-113.

11. Бойко А. А., Иванников К. С., Кузнецов Д. А. Методика построения графоаналитической модели позиционной динамики боя на основе вероятностно-временной синхронизации действий элементов боевых порядков воинских формирований // Системы управления, связи и безопасности. 2020. № 2. С. 24-48. DOI: 10.24411/2410-9916-2020-10202.

12. Бойко А. А. Боевая эффективность кибератак: аналитическое моделирование современного боя // Системы управления, связи и безопасности. 2020. № 4. С. 101-133. DOI: 10.24411/2410-9916-2020-10404.

13. Дроботун Е. Б. Теоретические основы построения систем защиты от компьютерных атак для автоматизированных систем управления. – СПб.: Наукоемкие технологии, 2017. – 120 с.

14. Мунтяну А. А. Методика оценки информационно-программных рисков функционирования автоматизированных информационно-управляющих систем военного назначения // Информационные войны. 2014. № 4(32). С.40-45.

15. Скиба В. А. Синтез информационно-коммуникационного пространства эргатических систем военного назначения // Военная Мысль. 2018. № 11. С. 39-48.

16. Мистров Л. Е., Павлов В. А., Шерстяных Е. С. Устойчивость информационных систем в конфликтном взаимодействии организационно-технических систем // Стратегическая стабильность. 2017. № 2(79). С. 43-49.

17. Антонов С. Г., Зорин Э. Ф., Рыжов Б. С., Якименко В. М. Оценка защищенности средств информатизации автоматизированной системы военного назначения, функционирующей в условиях информационно-технических воздействий // Стратегическая стабильность. 2017. № 2(79). С. 43-49.

18. Стародубцев Ю. И., Бречко А. А. Моделирование сетей связи, функционирующих в условиях деструктивных программных воздействий // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2019. № 1-2(127-128). С. 21-28.

19. Шостак Р. К., Лепешкин О. М., Новиков П. А., Худайназаров Ю. К. Модель сетевого контроля защищенности узлов связи сети передачи данных от деструктивных программно-аппаратных воздействий, разработанная в среде радикалов // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2018. № 11-12(125-126). С. 61-70.

20. Коцыняк М. А., Лаута О. С., Иванов Д. А., Лукина О. М. Методика оценки эффективности защиты информационно-телекоммуникационной сети в условиях таргетированных кибернетических атак // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2018. № 11-12(125-126). С. 71-79.

21. Зорин Э. Ф., Антонов С. Г., Рыжов Б. С., Бубенщиков Ю. Н. Оценка рисков снижения качества функционирования информационно-телекоммуникационных систем в условиях информационно-технических воздействий // Информационные войны. 2017. № 3 (43) С. 70-75.

22. Карганов В. В., Пилявец О. Г., Шевченко А. А. К вопросу предупреждения и обеспечения требуемого уровня информационной безопасности информационно-вычислительной сети специального назначения от несанкционированных воздействий // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2018. № 1-2(115-116). С. 78-85.

23. Белый А. Ф. Метод регулирования рисков проектируемых комплексов средств автоматизации для условий компьютерных атак // Стратегическая стабильность. 2011. № 3(56). С. 26-27.

24. Захарченко Р. И., Королев И. Д. Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры, функционирующей в киберпространстве // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 2. С. 52-61. DOI: 10.24411/2409-5419-2018-10041.

25. Дорохов В. Н., Ищук В. А. Боевые потенциалы подразделений как интегральный критерий оценки боевых возможностей воинских формирований и боевой эффективности вооружения, военной и специальной техники // Известия РАРАН. 2017. № 4. С. 27-36.

26. Jaiswal N. K. Military operations research: quantitative decision making. – N. Y.: Kluwer Academic Publishers, 1997. – 388 p. DOI: 10.1007/978-1-4615-6275-7.

27. Бойко А. А., Будников С. А. Обеспечение конфликтной устойчивости программной реализации алгоритмов управления радиоэлектронной аппаратурой пространственно распределенных организационно-технических систем // Системы управления, связи и безопасности. 2019. № 4. С. 100-139. DOI: 1024411/2410-9916-2019-10404.

References

1. Boyko A. A., Djakova A. V. The Method of Developing Test Remote Information-Technical Impacts on Spatially Distributed Systems of Information-Technical Tools. *Information and Control Systems*, 2014, no. 3, pp. 84-92 (in Russian).

2. Boyko A. A., Hramov V. Yu. The Model of Information Conflict between Information-Technical Means and Special Software in Armed Confrontation of Groups with Static Characteristics. *Radiotekhnika*, 2013, no. 7, pp. 5-10 (in Russian).

3. Boyko A. A. Sposob stratificirovannogo analiticheskogo opisaniya processa funkcionirovaniya informacionno-technicheskih sredstv [The Stratified Analytical Description Method of the Functioning Process of Information-Technical Tools]. *Informacionnye Tehnologii*, 2015, no. 1, pp. 35-42 (in Russian).

4. Boyko A. A., Budnikov S. A. The Model of Information Conflict between Special Software and Information Security Subsystem of Information-Technical Tool. *Radiotekhnika*, 2015, no. 4, pp. 136-141 (in Russian).

5. Boyko A. A. The Analytical Modeling Method of the Virus Propagation Process in Computer Various Structures Networks. *SPIIRAS Proceedings*, 2015, no. 5, pp. 196-211 (in Russian).

6. Boyko A. A. O zashishennosti informacii voinskih formirovaniy v sovremennom vooruzhennom protivoborstve [About the Information Security of Military Formations in the Modern Armed Confrontation]. *Military Thought*, 2016, no. 4, pp. 38-51 (in Russian).

7. Boyko A. A., Degtyarev I. S. The Weight Coefficient Estimation Method of Elements in Organizational and Technical Systems. *Systems of Control, Communication and Security*, 2018, no. 2, pp. 245-266 (in Russian).

8. Boyko A. A. Evaluation method of armament samples informatization level. Systems of Control, Communication and Security, 2019, no. 1, pp. 264-275. (in Russian). DOI: 1024411/2410-9916-2019-10116.

9. Boyko A. A. Warfare Analytical Modeling Method. *Systems of Control, Communication and Security*, 2019, no. 2, pp. 1-27. (in Russian). DOI: 10.24411/2410-9916-2019-10201.

10. Boyko A. A. The Method of Developing Hierarchic Multilevel Models for Analytical Assessment of the Correlation of Forces in Military Formations. *Military Thought*, 2019, no. 7, pp. 104-113 (in Russian).

11. Boyko A. A., Ivannikov K. S., Kuznetsov D. A. Constructing graphoanalytic combat positional dynamics model based on military formations combat orders elements actions probability-temporal synchronization. *Systems of Control, Communication and Security*, 2020, no. 2, pp. 24-25. (in Russian). DOI: 10.24411/2410-9916-2020-10202.

12. Boyko A. A. Combat Effectiveness of Cyber-attacks: Analytical Modeling of Modern Warfare. *Systems of Control, Communication and Security*, 2020, no. 4, pp. 101-133. (in Russian). DOI: 10.24411/2410-9916-2020-10404.

13. Drobotun E. B. *Teoreticheskie osnovy postroenija sistem zashhity ot komp'juternyh atak dlja avtomatizirovannyh sistem upravlenija* [Theoretical Bases of Construction of Systems of Protection Against Computer Attacks for Automated Control Systems]. Saint-Petersburg, Naukoemkie tekhnologii Publ., 2018. 120 p. (in Russian).

14. Muntjanu A. A. Metodika ocenki informacionno-programmnyh riskov funkcionirovanija avtomatizirovannyh informacionno-upravljajushhih sistem voennogo naznachenija [Methodic Evaluation Information and Program Risks Functioning of the Automated Information Management Systems of Military]. *Informsionatnye voiny*, 2014, no. 4(32), pp. 40-45. (in Russian).

15. Skiba V. A. Sintez informacionno-kommunikacionnogo prostranstva jergaticheskih sistem voennogo naznachenija [Synthesis of Information-and-Communication Space of Ergatic Military Systems]. *Military Thought*, 2018, no. 11, pp. 39-48 (in Russian).

16. Mistrov L. E., Pavlov V. A., Sherstjanyh E. S. Ustojchivost' informacionnyh sistem v konfliktnom vzaimodejstvii organizacionno-tehnicheskih system [Stability of Information Systems in Conflict Interaction of Organization and Technical Systems]. *Strategic Stability*, 2017, no. 2 (79), pp. 43-49 (in Russian).

17. Antonov S. G., Zorin Je. F., Ryzhov B. S., Jakimenko V. M. Ocenka zashhishhennosti sredstv informatizacii avtomatizirovannoj sistemy voennogo naznachenija, funkcionirujushhej v uslovijah informacionno-tehnicheskih vozdejstvij [Assessment of information security technology tools of an automated military system operating under information-technical impacts]. *Strategic Stability*, 2012, no. 2 (59), pp. 2-6 (in Russian).

18. Starodubcev Ju. I., Brechko A. A. Modelirovanie setej svjazi, funkcionirujushhih v uslovijah destruktivnyh programmnyh vozdejstvij // Voprosy oboronnoj tehniki [Simulation of Networks and its Operating with Cyber-Attacks Conditions]. *Enginery Problems. Series16. Anti-Terrorist Engineering Means*, 2019, no. 1-2 (127-128), pp. 21-28 (in Russian).

19. Shostak R. K., Lepeshkin O. M., Novikov P. A., Hudajnazarov Ju. K. Model' setevogo kontrolja zashhishhennosti uzlov svjazi seti peredachi dannyh ot destruktivnyh programmno-apparatnyh vozdejstvij, razrabotannaja v srede radikalov [Model of Network Control of Data Transmission Network Communication Nodes Protection From Destructive Software and Hardware Influences, Developed in the Environment of Radicals]. *Enginery Problems. Series 16. Anti-Terrorist Engineering Means*, 2018, no. 11-12 (125-126), pp. 61-70 (in Russian).

20. Kocynjak M. A., Lauta O. S., Ivanov D. A., Lukina O. M. Metodika ocenki jeffektivnosti zashhity informacionno-telekommunikacionnoj seti v uslovijah targetirovannyh kiberneticheskih atak [Methodology for Evaluating the Effectiveness of Information-Telecommunications Network Protection in the Context of Targeted Cyber Attacks]. *Enginery Problems. Series 16. Anti-Terrorist Engineering Means*, 2018, no. 11-12 (125-126), pp. 71-79 (in Russian).

21. Zorin Je. F., Antonov S. G., Ryzhov B. S., Bubenshhikov Ju. N. Ocenka riskov snizhenija kachestva funkcionirovanija informacionno-telekommunikacionnyh sistem v uslovijah informacionno-tehnicheskih vozdejstvij [Assessment of Risks of Reducing the Quality of Information-telecommunications systems Functioning in the Context of Information-Technical Impacts]. *Informsionatnye Voiny*, 2017, no. 3 (43), pp. 70-75 (in Russian).

22. Karganov V. V., Piljavec O. G., Shevchenko A. A. K voprosu preduprezhdenija i obespechenija trebuemogo urovnja informacionnoj bezopasnosti informacionno-vychislitel'noj seti special'nogo naznachenija ot nesankcionirovannyh vozdejstvij [To the Issue of Prevention and Ensuring the Required Level of Information Security of a Special-Purpose Information and Computer Network from Unauthorized Impacts]. *Enginery Problems. Series16. Anti-Terrorist Engineering Means*, 2018, no. 1-2 (115-116), pp. 78-85 (in Russian).

23. Belyj A. F. Metod regulirovanija riskov proektiruemyh kompleksov sredstv avtomatizacii dlja uslovij komp'juternyh atak [A Method of Risk Management Design of Automation Systems for the Conditions of Cyber Attacks]. *Strategic Stability*, 2011, no. 3 (56), pp. 26-27 (in Russian).

24. Zaharchenko R. I., Korolev I. D. Metodika ocenki ustojchivosti funkcionirovanija ob#ektov kriticheskoj informacionnoj infrastruktury, funkcionirujushhej v kiberprostranstve [Methodology for Assessing the Stability of Critical Information Infrastructure Functioning in Cyberspace]. *H&ES Research*, 2018, vol. 10, no 2, pp. 52-61. (in Russian). DOI: 10.24411/2409-5419-2018-10041.

25. Dorohov V. N., Ishhuk V. A. Boevye potencialy podrazdelenij kak integral'nyj kriterij ocenki boevyh vozmozhnostej voinskih formirovanij i boevoj jeffektivnosti vooruzhenija, voennoj i special'noj tehniki [Combat Potential of Units, as Integral Criterion of Estimation of Military Formations, Combat Effectiveness of Armament and Military Equipment Operational Capability]. *Izvestiya Rossijskoj akademii raketnyh i artillerijskih nauk*, 2017, no. 4, pp. 27-36 (in Russian).

26. Jaiswal N. K. *Military operations research: quantitative decision making*. New York, Kluwer Academic Publ., 1997. 388 p. DOI: 10.1007/978-1-4615-6275-7.

27. Boyko A. A., Budnikov S. A. Conflict Resistance Ensuring of Software Implementation of Control Algorithms of Radioelectronic Equipment of Spatially Distributed Organization and Technical Systems. *Systems of Control, Communication and Security*, 2019, no. 4, pp. 100-139. (in Russian). DOI: 1024411/2410-9916-2019-10404.

Статья поступила 20 ноября 2020 г.

Информация об авторе

Бойко Алексей Александрович – кандидат технических наук, доцент. Докторант. Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж). Область научных интересов: защита информации, моделирование сложных систем. E–mail: albo@list.ru

Адрес: 394064, Россия, г. Воронеж, ул. Ст. Большевиков, д. 54А.

Combat Effectiveness of Cyber-Attacks: Practical Aspects

A. A. Boyko

Problem Statement. *In modern warfare and armed conflicts, information-technical impacts are widely used. They include electromagnetic impacts (radio-electronic suppression and electromagnetic radiation damage) at the physical level of the OSI model and cyber-attacks at higher levels of this model. Issues of protection from electromagnetic impacts are traditionally given close attention. At the same time, no less important issues of protecting these objects from cyber-attacks in combat conditions are poorly studied and therefore remain without the required understanding by military and technical specialists. This article is the second part of the materials that consider the methodological basis for assessing the combat effectiveness of cyber-attacks at the level of the military formations combat potentials ratio. In the first part, a temporal approach to analytical warfare modeling is proposed, which allows to assess the effect of the systemic influence of fire destruction, electromagnetic impacts, and cyber-attacks on the time and probability characteristics of intelligence, communications, control, and fire destruction subsystems operating within a single military formation combat cycle.* ***Aim of the paper*** *is to research an analytical model of modern warfare and development a technique that justify the requirements for the weapons and military equipment protection from cyber-attacks.* ***The idea*** *of the technique is to:* 1) *modeling the combat of two identical military formations with protected weapons and military equipment samples, one of which is additionally assigned a cyber-attack subsystem; 2*) *assessment of the combat potentials ratio;* 3) *determination of requirements for the weapons and military equipment samples protection from cyber-attacks based on such an acceptable probability of successful implementation of cyber-attacks, in which the combat potentials ratio does not exceed the required value and the cost of eliminating vulnerabilities is not higher than the maximum allowed.* ***Novelty.*** *The novelty consists in obtaining the ability to quantify the impact of cyber-attacks on the combat potentials ratio of opposing military formations.* ***Result.*** *It is shown that electromagnetic impacts in combat produce an effect that is a special case of the effect of cyber-attacks in various applications. In order to increase the proposed technique application speed, a universal analytical dependence of the share of the remaining number of military formations on the probability of cyber-attacks in combat of two identical military formations, one of which is supplemented by a subsystem of information-technical impacts, is revealed. For this dependence proposed the formulas for estimating coefficients for the total impact of cyber-attacks on all subsystems and selective impact on communication, control, intelligence, or fire destruction subsystem. Diagrams of the maximum absolute deviations of the values obtained using the proposed formulas from the modeling results are presented. Examples of justifying the requirements for ensuring the conflict stability of military formations in various variants of cyber-attacks are shown.* ***Practical relevance.*** *The solution can be used to justify the requirements for the conflict stability of information-technical tools of existing and future weapons and military equipment samples in combat with cyber-attacks.*

Keywords: *analytical warfare model, cyber-attack, combat potentials ratio, military formation, combat cycle*

Information about Author

Aleksey Aleksandrovich Boyko – Ph.D. of Engineering Sciences, Associate Professor. Doctoral Candidate. Zhukovsky and Gagarin Military Aviation Academy. Field of research: methods and systems of information protection, methods of assessing the effectiveness of complex systems. E–mail: albo@list.ru

Address: Russia, 394064, Voronezh, Old Bolsheviks Street, 54A.