ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

НАУЧНЫЙ ЖУРНАЛ №2(24) 2020

ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКИЙ ВЕСТНИК

Подписано в печать 17.06.2020
Формат В5
Печать офсетная. Усл.печ.л. 11,6
Тираж 500 экз.
Заказ № 82-11
Отпечатано в типографии
ООО «Научный консультант»
г. Москва
Хорошевское шоссе, 35, корп.2

УДК 004.85

Основы оценки интегральной эффективности ведения информационной безопасности и радиоэлектронной борьбы

В.Н. Соляной, кандидат военных наук, доцент, старший научный сотрудник,
заведующий кафедрой «Информационной безопасности»,
Государственное бюджетное образовательное учреждение
высшего образования Московской области
«Технологический университет», г. Королев, Московская область

Бурный рост «цифровой» экономики в современном мире обуславливает необходимость постоянного совершенствования перспективных технологий в области обеспечения информационной безопасности. Развитие мобильных информационных технологий, которые базируются на широком использовании подвижных радиоэлектронных компонентах, приводит к целесообразности создания интегральных (единых) комплексных систем информационной безопасности и радиоэлектронной борьбы. В этих условиях проблематичным является осуществление как общей, так и частных оценок эффективности их использования. В настоящее время процесс развития и постоянной модернизации этого нового направления по совместному обеспечению безопасности критической информационной инфраструктуры представляет научный и практический интерес.

«Цифровая» экономика, информационная безопасность, радиоэлектронная борьба (защита), интегральная эффективность.

The basics of assessing the integral effectiveness of information security and electronic warfare

V.N. Solyanoy, Associate Professor, S.N.S., Head of the Department
of Information Security,
State Educational Institution of Higher Education
Moscow Region «University of technology», Korolev, Moscow region

The rapid growth of the digital economy in today's world necessitates the continuous improvement of advanced technologies in the field of information security. The development of mobile information technologies, which are based on the widespread use of mobile electronic components, leads to the feasibility of creating integrated (single) integrated systems of information security and electronic warfare. In these circumstances, both general and private assessments of their effectiveness are problematic. At present, the process of developing and constantly modernizing this new area of critical information infrastructure security together is of scientific and practical interest.

«Digital» economy, information security, electronic warfare (protection), integral efficiency.

Постоянно возникающие информационные конфликты в условиях цифровизации современной экономики обостряют и усложняют процессы, связанные с разрешением появляющихся проблем по обеспечению информационной безопасности (ИБ) критической информационной инфраструктуры (КИИ) важнейших объектов промышленности и обороны страны. Быстро меняющаяся информационная обстановка в таких конфликтах разного масштаба обуславливает необходимость использования высокомобильных сил по обеспечению ИБ в различных удаленных районах и регионах страны с широким применением наземных, морских, воздушных и космических радиоэлектронных средств (связи и управления, разведки, навигации, радиолокации и т.п.) [4, с.14].

Данная постановка задачи предопределяет изыскание новых практических взглядов и научных подходов по осуществлению интегральной оценки эффективности совместных действий привлекаемых сил и средств как ИБ, так и РЭБ и, в частности, мер по радиоэлектронной защите (РЭЗ) используемых радиоэлектронных систем и комплексов (РЭС и К).

В рамках самостоятельных областей по ИБ [8, с.56] и по РЭБ [9, с.284] вопросы, связанные с оценкой эффективности нашли достаточно широкий обзор в указанной выше научно-практической литературе. В то же время слияние отдельных задач по оценки эффективности ИБ и РЭБ в единые целевые установки и реализуемые, как техническими, так и технологическими процессами, не нашли своего должного отражения в существующей литературе.

В этих условиях возникает проблема необходимости осуществлении оценки комплексного обеспечения безопасности функционирования КИИ силами и средствами интегральной системы (ИБ и РЭБ) в условиях протекания радиоэлектронно-информационных конфликтах. Данная проблема особенно ярко проявляется применительно к космической сфере существования конфликтных ситуаций различного масштаба [7, с.168]. Следовательно, целью исследования, представленных в данной статье является разработка общих основ по оценке эффективности интегрального введения ИБ и РЭБ, прежде всего, в интересах безопасности функционирования критической информационной инфраструктуры (КИИ) важнейших объектов промышленности и обороны страны.

В основе разрешения рассмотренной проблемы лежат рекомендуемые базовые положения по моделированию разрозненных отдельных подсистем ИБ и РЭБ в интегральной системе ведения информационного противоборства [1, с.53]. Такую предлагаемую интегральную систему, в общем виде, можно представить как некое К-мерное пространство. В такой системе определяется результат совместной деятельности по безопасности функционирования КИИ. Данный суммарный показатель ($F_{\sum}$) является суммой частных показателей (F_i), которые характеризуют отдельные составляющие общего показателя (1)

$$F\sum = \sum_{i=1}^{k} F_i. \qquad (1)$$

Данные показатели искомой оценки эффективности отражают вероятностные события и имеют следующие ограничения:

$$F_i = |F_i| \leq 1;$$

$$F_\Sigma = |F_\Sigma| \leq 1.$$

Применительно к выше изложенным подсистемам ИБ и РЭБ, которые являются определяющими[5, с.87 и с.133] в системе информационного противоборства (ИПБ), их общая эффективность можно оценивать по формуле (2).

$$F_{ИПБ} = F_{ИБ} + F_{РЭБ}, \qquad (2)$$

где $F_{ИБ}$ – оценка функциональной эффективности подсистемы ИБ и которая определяется по формуле (3).

$$F_{ИБ} = F_{ФЗ} + F_{ТЗ} + F_{ПАЗИ} + F_{УПР.\ ИБ} \qquad (3)$$

где $F_{ФЗ}$; $F_{ТЗ}$; $F_{ПАЗИ}$; $F_{УПР.\ ИБ}$ – соответственно, эффективности подсистем: физической защиты; технической защиты; программно-аппаратной защиты информации; управление ИБ.

$F_{РЭБ}$ – оценка функциональной эффективности подсистемы РЭБ, которая определяется по формуле (4).

$$F_{РЭБ} = F_{РЭР} + F_{РЭП} + F_{РЭЗ} + F_{УПР.\ РЭБ}, \qquad (4)$$

где $F_{РЭР}$; $F_{РЭП}$; $F_{РЭЗ}$; $F_{УПР.РЭБ}$ – соответственно, эффективности подсистем: радиоэлектронной разведки; радиоэлектронного подавления; радиоэлектронной защиты; управления РЭБ.

В зависимости от условий (внутренних и внешних факторов – μ_j) протекания информационно-радиоэлектронного конфликта соответствующий частный показатель эффективности (F_i) можно вычислить по формуле (5).

$$F_i^j = \mu_j * F_i, \qquad (5)$$

где μ_j – вероятностный показатель, учитывающий внутренние и внешние условия функционирования оцениваемых систем.

При этом показатель (μ_j) зависит как от обеспеченности исследуемого процесса (подсистемы) – вероятность функционирования (P), так и от времени (T) его протекания или реализации (6).

$$\mu_j = f(P,T) \qquad (6)$$
$$(0 \leq \mu_j \leq 1)$$

В целом, разрешение изложенной проблемы по определению методологических аспектов моделирования оценок интегральной эффективности ИБ КИИ во взаимодействии с системой РЭБ в современных информационно-радиоэлектронных конфликтах непростое, так как зависит от большого числа факторов и условий. В таких случаях целесообразно рассматриваемый подход

реализовывать на основе компьютерного моделирования [6, с.4] с использованием методов математической статистики при анализе опасностей [10, с.283].

В основе компьютерного моделирования для решения поставленной задачи предлагается использовать методологический подход изложенной в литературе [3, с.189]. Данная модель позволяет оценивать как отдельные процессы, объекты и подсистемы ИБ, так и в комплексе в виде комплексной системы ИБ (как совокупность различных подсистем ИБ). Вопросы, связанные с оценкой эффективности применения мер по РЭБ, в явном виде, в данном источнике не рассматривались.

Структура упруженной предложенной комплексной модели представлена на рисунке в виде таблицы 1 и состоит из совокупности анализируемых систем ИБ и взаимодействующей подсистемы РЭБ.

В каждые свободные ячейки для каждой подсистемы вносятся исходные вероятностные экспертные данные, которые характеризуют эффективность отдельных оцениваемых процессов, реализуемых по исследуемым этапам.

Частные оценки проставляются в итоговых ячейках соответствующих строк и столбцов таблицы рассчитываются как среднеарифметические значения оценок эффективности каждого этапа (по строкам) и каждого процесса всех отдельных подсистем, в целом, за все этапы.

Применительно к излагаемой проблеме и вышеизложенной идеи ее разрешения была разработана компьютерная технология (модель) оценки эффективности интегральной системы ИБ КИИ во взаимодействии с мерами по радиоэлектронной защите (РЭБ). Данная модель ориентирована, прежде всего, для телекоммуникационных сетей, имеющие в своей структуре радиоканалы [2, с.51].

В предложенном подходе целевая функция моделирования исследуемой защиты КИИ представляет собой эффективность проводимых мер по ИБ и РЭБ информационно-радиоэлектронных объектов как по частным показателям (применительно к отдельным подсистема, процессам, этапам ИБ и РЭБ), а также по обобщенному показателю эффективности в целом.

Общий вид целевой функции представляет собой среднеарифметическое значение входных экспертных оценок (7).

$$\overline{W}_{\Sigma} = \frac{\sum_{j=1}^{m} a_j * b_j}{m} \qquad (7)$$

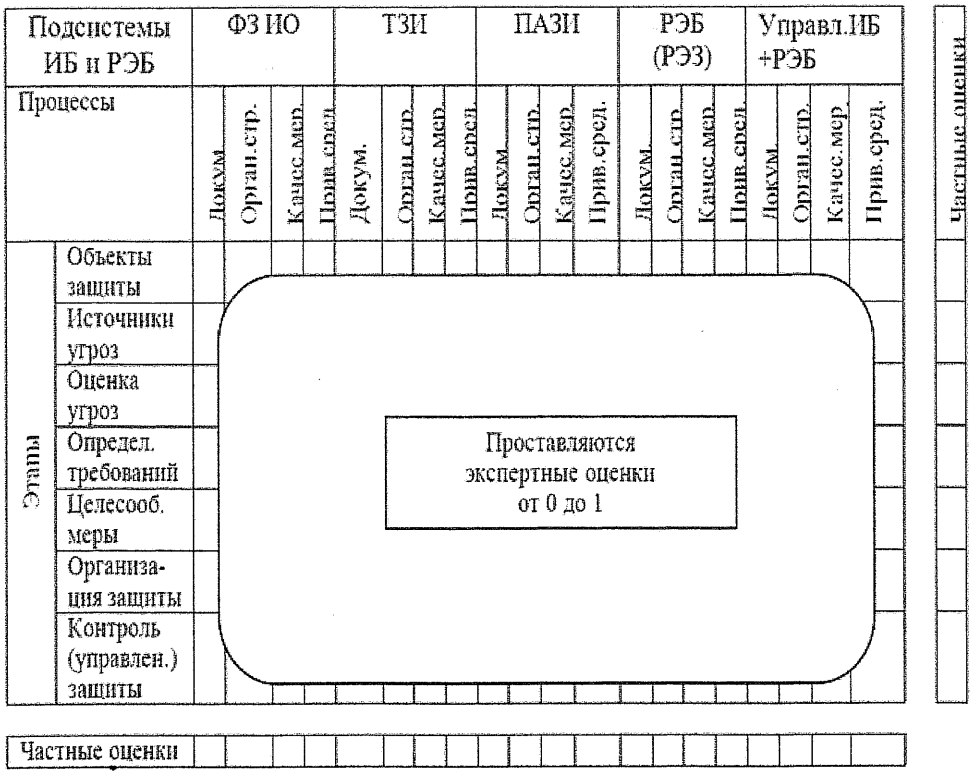
$$0 \le \overline{W}_{\Sigma} \le 1$$

где a_j – коэффициенты важности (значимости) оцениваемых параметров $(0 \le a_j \le 1)$;

b_j – количественные (вероятностные) значения оцениваемых параметров $(0 \le b_j \le 1)$;

m – количество оцениваемых параметров.

Таблица 1 – Структура и исходные данные компьютерной модели интегрального обеспечения ИБ и РЭБ КИИ



С учетом выше изложенного обобщенная комплексная оценка эффективности проводимых мер по ИБ и РЭБ исследуемых КИИ в предлагаемой модели представляется в табличной форме. Пример представления итоговых результатов моделирования анализируемой эффективности для каждой подсистемы и в целом для всей системы показан в таблице 2.

Таблица 2 – Интегральные общее и частные оценки эффективности исследуемых подсистем ИБ и РЭБ (пример)

Наименование обобщенного количествен. показателя	Оцениваемые подсистемы ИБ и РЭБ					Количеств. значения обобщен. показателя
	ФЗ	ТЗИ	ПАЗИ	**РЭБ (РЭЗ)**	Интегр. СУ	
Вероятность защиты КИИ	0,71	0,79	0,72	**0,67**	0,72	0,71

Анализируя приведенный пример интегральной оценки эффективности ИБ и РЭБ КИИ можно утверждать, что наиболее слабой (уязвимой) подсистемой следует рассматривать подсистему радиоэлектронной защиты, так как ее значение оценки показателя эффективности наименьшее.

В рассмотренной модели оценки эффективности ИБ и РЭБ имеется воз-

можность представления результатов расчетов также и в графическом виде.

Таким образом, рассмотренный методологический подход оценки эффективности обеспечение ИБ КИИ во взаимодействии с мероприятиями по РЭБ (РЭЗ) в информационно-радиоэлектронном конфликте можно рассматривать как приемлемым для его дальнейшего практического использования.

Данный изложенный подход, в настоящее время, используется в учебном процессе и в научных исследованиях Технологического университета (г. Королев) на кафедре информационной безопасности.

В заключении можно утверждать, что изложенные результаты приведенных исследований заслуживают особого внимания, так как обладает рядом положительных сторон. К таким чертам предложенного подхода можно отнести: универсальность, наглядность, простота представления результатов исследования, возможность маневра располагаемыми силами и средствами ИБ и РЭБ, и, в целом позволяет анализировать эффективность исследуемой комплексной (интегральной) системы ИБ и РЭБ для разных ситуаций реальной и прогнозируемой информационно-радиоэлектронной обстановки.

В качестве предложений по направлению дальнейших исследований по данной тематики следует отметить целесообразность их проведения в более широкой сфере деятельности, т.е. в области ведения информационного противоборства различного масштаба. В данной перспективной и значимой сфере, изложенные в данной статье подходы по интегральной оценке эффективности ИБ и РЭБ должны занять достаточно важное место.

Авторы выражают признательность коллегам кафедры информационной безопасности Технологического университета за помощь в разработке и апробации данного подхода в учебной и научно-исследовательской работе.

Литература

1. Ворона В.А. и др. Концептуальные основы создания и применения системы защиты объектов // М.: Горячая линия-Телеком. 2012. 196 с.
2. Гольдштейн Б.С. Инфокоммуникационные сети и системы // СПб.: БХВ-Петербург. 2019. 208 с.
3. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты // К.: ТИД ДИА Софт. 2002. 490 с.
4. Конфликтно-устойчивые радиоэлектронные системы. Методы анализа и синтеза / Под ред. С.В. Ягольникова // М.: Радиотехника. 2015 г. 312 с.
5. Козьминых С.И. Обеспечение комплексной защиты объектов информатизации // М.: ЮНИТИ-ДАНА. 2020. 543 с.
6. Кузьмин В.А. Общая характеристика и методы анализа экспериментальных исследований радиоэлектронных систем // М.: ИНФРА-М. 2019. 80 с.
7. Куприянов А.И. и др. Радиоэлектронные системы космических комплексов // М.: Вузовская книга. 2017. 268 с.
8. Курилов А.П. и др. Обеспечение информационной безопасности и бизнеса // М.: БДЦ-пресс. 2005. 512 с.
9. Куприянов А.И. Радиоэлектронная борьба // М.: Вузовская книга. 2016. 260 с.
10. Переездчиков И.В. Анализ опасностей промышленных систем человек-машина-среда и основы защиты // М.: КНОРУС. 2011. 784 с.