Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

3. Турчин, В. Ф. Феномен науки: Кибернетический подход к эволюции / В. Ф. Турчин. – М.: ЭТС. – Изд. 2-е – 2000. – 368 с.

ПОДХОД К ОЦЕНКЕ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННЫХ ОБЪЕКТОВ В УСЛОВИЯХ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

Ю.Е. КУЛЕШОВ

Белорусский государственный университет информатики и радиоэлектроники

В настоящее время в отечественных и зарубежных военно-аналитических публикациях [1-4] значительное внимание уделяется рассмотрению вопросов борьбы в информационной сфере. По мере расширения информатизации вооруженных сил появились новые возможности информационного воздействия на систему управления войсками и оружием.

Однако, с научно-методологической (теоретической) и практической (организационной) точки зрения следует отметить, что до настоящего времени математически не формализован процесс информационного противоборства, не разработана методология и механизм влияния информационного противоборства на эффективность боевых действий. Большинство военно-научных публикаций по данной проблематике носят поверхностный, описательный характер.

Поэтому актуальной научной проблемой в военной науке является необходимость развития теории и математических моделей информационного противоборства, позволяющих оценить влияние информационной составляющей на эффективность боевых действий.

Можно с уверенностью констатировать как очевидный факт, что процесс информационного противоборства является сложноформализуемым. От того насколько правильно и своевременно проведен прогноз тенденций поведения исследуемого процесса, насколько точно составлена оценка состояния данного процесса для i-х условий обстановки в итоге зависит успех всех планируемых действий. Это положение справедливо для различных видов деятельности, в которых состояние исследуемого процесса подчиняется известным законам развития. В равной степени к такому виду деятельности можно отнести и информационное противоборство.

Задача рационального планирования военных действий и на его основе выбора оптимальных для определенных условий способов действий, немыслима без оценки их ожидаемой эффективности. В противном случае действия будут выполняться вслепую, или же основываться лишь на интуиции лица, управляющего ими, что не обязательно приведет к желаемому результату.

Вопросам оценки эффективности боевых действий посвящено большое количество исследований. Однако, несмотря на это, даже в достаточно хорошо изученных предметных областях вопросы оценки эффективности военных действий остаются достаточно сложными в постановке и реализации. В частности, наибольшие противоречия возникают при определении цели действий, в некорректности выбора показателей эффективности, недостаточной адекватности моделей оценки эффективности.

Анализ различных моделей оценки эффективности позволил прийти к выводу и констатировать тот факт, что для ряда систем военного назначения задача оценки эффективности их функционирования является трудно формализуемой (в смысле разработки моделей действий и оценки степени достижения поставленных целей).

Исследование систем военного назначения и процессов их функционирования показало, что наиболее сложно формализовать целевые функции таких систем, как информационного противоборства и некоторых других [5].

Предлагается методический подход к формализации процесса информационного противоборства и формированию методики оценки эффективности функционирования системы информационного противоборства.

Для начала сформулируем общее правило: «Эффективным может считаться только то действие, затраты на совершение которого ставятся в соответствие с полученным эффектом и в результате такого сопоставления не превосходят его».

Следовательно, оперирующая сторона так должна организовать и провести информационное противоборство, чтобы «обмен» ресурсов С, Т на целевой эффект $R_{рез}$ был для нее предельно выгодным. С точки зрения эффективности информационного противоборства – это не просто способность системы информационного противоборства сформировать целевой эффект $R_{рез}$, а скорее действенность такой способности, т. е. результативность, соотнесенная с затратами всех видов ресурсов С (ресурсоемкостью мероприятий информационного противоборства) и времени Т (оперативностью решения задач информационного противоборства).

Корректно оценить и математически достоверно сопоставить затраты оперирующей стороны и полученный результат возможно только в том случае, если показатели затрат и результата выражаются в одних физических единицах, например, в единицах стоимости.

Однако на практике очень редко удается представить в одних физических единицах затраты на боевые действия и результаты боевых действий, что можно отнести и к информационному противоборству.

В том случае, если удалось сопоставить в одних единицах затраты и результаты информационного противоборства, выбор стратегии информационной операции сводится к определению стратегии, максимизирующей разность результата и затрат:

$$\mathrm{s}^{*}: \underset{(\mathrm{s})}{R_{\text{рез}}(\mathrm{s},\mathrm{v}) - C(\mathrm{s},\mathrm{v}) \to \max}, \tag{1}$$

где s – стратегия исследуемого процесса информационного противоборства, $\mathrm{s}^{*} \in \{\mathrm{s}\}$;

v – нормированные к результатам затраты на проведение s-й стратегии.

В случае невозможности сопоставления в одних единицах затрат и результатов информационного противоборства, целесообразно в критерии эффективности учитывать все условия, виды ресурсов и требования к комплексному показателю эффективности *W* или целевому эффекту $R_{рез}$.

В дальнейшем условия (в виде ограничений) целесообразно наложить на каждый показатель, тогда каждое такое условие будет являться самостоятельным критерием, а задача выбора становится многокритериальной.

Для информационного противоборства целесообразно многокритериальный выбор осуществлять в виде задачи распределения ограниченных материальных и временных ресурсов с максимальной выгодой:

$$\begin{aligned} &\underset{(\mathbf{s})}{W(\mathbf{s},\mathbf{v}) \to max} \\ &C(\mathbf{s},\mathbf{v}) < C\text{тр}, \\ &T(\mathbf{s},\mathbf{v}) < T\text{тр}, \end{aligned} \tag{2}$$

или задачи минимизации затрат:

$$\begin{aligned} & C(\mathbf{s},\mathbf{v}) \to min \\ & \qquad (\mathbf{s}) \\ & W(\mathbf{s},\mathbf{v}) > W\text{тр}, \\ & T(\mathbf{s},\mathbf{v}) < T\text{тр}. \end{aligned} \qquad (3)$$

Главной целью информационного противоборства является обеспечение необходимой степени собственной информационной безопасности и максимальное снижение уровня информационной безопасности противостоящей стороны и достигается решением ряда задач, основные из которых – поражение объектов информационной среды противостоящей стороны информационным оружием и защита собственной информации

Поэтому для описания системы информационного противоборства целесообразно в первую очередь разработать формализованную комплексную модель оценки уязвимостей информационных объектов. Данная модель, представленная на рисунке, позволит пояснить процесс нанесения ущерба информационным объектам воздействием информационного оружия вследствие реализации всех возможных априорно известных угроз через оцениваемую уязвимость информационных объектов (элементов), влияние различных факторов на этот процесс и позволит оценить множество рисков нанесения ущерба $R_1^{\bullet} = \left\{ r_{c_1}^{\bullet} = \langle y_i, v_{k^{\otimes}}, a_j \rangle \right\}, i = \overline{1,I}$, $k^{\otimes} = \mathbf{k}^{\otimes}, j = \overline{1J}$ и непосредственно множество ущербов, причиненных информационным объектам $U_1^{\bullet} = \left\{ u_{c_1}^{\bullet} \right\} = \left\{ r_{c_1}^{\bullet} \; s_{c_1} \right\}, c_1 = \overline{1,C_1}$, которые могут быть получены в результате реализации угрозы, где $\mathbf{k}^{\otimes}$ – оцениваемая уязвимость.

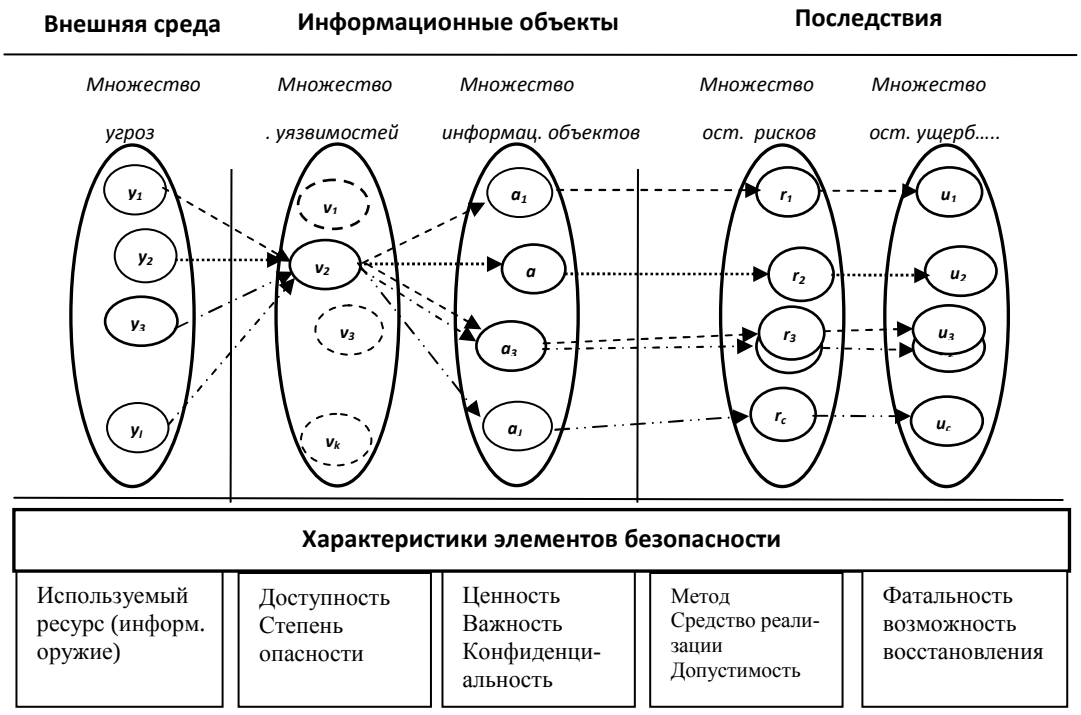

Рис. 1 – Комплексная модель уязвимости информационных объектов

Для данной комплексной модели уязвимости информационных объектов справедливо выполнение условия:

$$\exists\left(v_{k^{\otimes}} \in V^{\otimes}\right)\ \exists\left(Y=\{y_i\}\right)\left(R_1^{\bullet}=\left\{r_{c_1}^{\bullet}=\langle y_i, v_{k^{\otimes}}, a_j\rangle\right\}, \mathbf{r}_{\mathbf{c_1}}^{\otimes}=\left(\mathbf{y_i}\ \mathbf{v_{k^{\otimes}}}\mathbf{a_j}\right)\neq \mathbf{0}\right),\ i=\overline{1,I}, j=\overline{1J}.$$

Таким образом, задача формализации процесса информационного противоборства может быть решена. С целью развития теоретических основ информационного противоборства методика ее решения может корректироваться в рамках предложенного подхода, а предложенная комплексная модель уязвимости информационных объектов может быть использована для проведения оценки и ранжирования уязвимостей информационных объектов, определения степени их опасности в статическом режиме, разработки комплексного показателя, характеризующего уязвимость информационных объектов как элемент безопасности.

Список литературы

1. Гриняев, С. Н. Информационная война в ходе агрессии США, Великобритании и их союзников против Ирака. / С. Н. Гриняев. // Аналитический доклад. Центр стратегических оценок и прогноза. – М., 2010. – 118 с.

2. Гриняев, С. Н. Поле битвы – киберпространство: теория, приемы, средства, методы и системы ведения информационной войны / С. Н. Гриняев. – Минск: Харвест, 2004. – 448 с.

3. Гриняев, С. Н. Война в четвертой сфере / С. Н. Гриняев. // Независимое воен. обозрение. – №42. – 2000.

4. Рудаков, А. Б. Стратегия информационной войны / А. Б. Рудаков. // АТЕНЕЙ. – М.: 2003. – 145 с.

5. Горевич, Б. Н, Эльяс, В. П. Проблема оценки эффективности функционирования сложноформализуемых систем военного назначения. / Б. Н Горевич, В. П. Эльяс. // С-Пб.: ВМИРЭ им. А.С. Попова. Прикладные вопросы военно-морской радиоэлектроники. 2008.

ДОВЕРЕННАЯ ТРЕТЬЯ СТОРОНА: РЕАЛИИ И ПЕРСПЕКТИВЫ РАЗВИТИЯ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Д.В. МОСКАЛЕВ

Республиканское унитарное предприятие «Национальный центр электронных услуг»

Современный мир стремится к взаимодействию в электронном виде. В различных областях жизнедеятельности общества – будь то здравоохранение, образование или бизнес, банковская или социальная сфера – для информационного взаимодействия применяются электронные документы, подлинность и целостность которых подтверждается электронной цифровой подписью (далее – ЭЦП). ЭЦП позволяет создавать электронные документы, имеющие юридическую силу на территории определенного государства.

Вместе с тем в основе применяемых электронных цифровых подписей различных государств лежит несколько существенных отличий:

различные криптографические алгоритмы,

различия в законодательстве,

различные подходы к защите информации,

различные системы сертификации (экспертизы) средств криптографической защиты информации.