Модели функционирования критической информационной инфраструктуры в условиях кибернетического противоборства

Models of functioning of critical information infrastructure in the conditions of a cybernetic counter-fight

Саенко / Saenko I.
Игорь Борисович
(ibsaen@mail.ru)
доктор технических наук, профессор.
ФГКВОУ ВО «Военная академия связи имени Маршала Советского Союза С. М. Буденного» МО РФ,
профессор.
г. Санкт-Петербург

Захарченко / Zakharchenko R.
Роман Иванович
(romanzakharchenko@yandex.ru)
кандидат технических наук.
ФГКВОУ ВО «Краснодарское высшее военное училище им. генерала армии С. М. Штеменко» МО РФ,
докторант.
г. Краснодар

Ясинский / Yasinsky S.
Сергей Александрович
(yasinsky777@mail.ru)
доктор технических наук, доцент.
ЗАО «Институт телекоммуникаций»,
ведущий специалист.
г. Санкт-Петербург

Грязев / Gryazev A.
Андрей Николаевич
(agryazev@zniis.ru)
кандидат технических наук.
ФГУП «Центральный научно-исследовательский институт связи»,
генеральный директор.
г. Москва

Ключевые слова: критическая информационная инфраструктура – critical information infrastructure; информационная безопасность – information security; информационное противоборство – information warfare; устойчивость – resistance.

Рассматриваются концептуальная, вероятностно-статистическая и информационно-динамическая модели функционирования критической информационной инфраструктуры в условиях кибернетического противоборства. Формируются и анализируются временные зависимости показателей функционирования критической информационной инфраструктуры. Обосновываются гипотезы о возможности обеспечения устойчивого функционировании критической информационной инфраструктуры в условиях кибернетического противоборства.

Conceptual, probable and statistical, and information and dynamic models of functioning of critical information infrastructure in the conditions of a cybernetic counter-fight are considered. Temporal dependences of indices of functioning of critical information infrastructure are created and analyzed. Hypotheses of a possibility of support steady functioning of critical information infrastructure in the conditions of a cybernetic counter-fight are justified.

Введение

В настоящее время информационные системы, информационно-телекоммуникационные сети (ИТКС) и автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской деятельности, промышленности, а также в оборонной области и в государственном управлении, в соответствии с Федеральным Законом от 26.07.2017 № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" формируют критическую информационную инфраструктуру (КИИ) государства. Доступность КИИ через киберпространство, формируемое сетями общего пользования (Интернетом), сетями мобильной связи, социальными сетями и т. д., ставит проблему обеспечения национальной безопасности в зависимость от степени защищенности КИИ. При этом защищенность КИИ напрямую зависит от возможностей средств кибернетического воздействия (кибероружия), степени его эффективности, методов использования и средств защиты от него [1, 2]. Таким образом, функционирование КИИ происходит в условиях проведения непрерывного кибернетического противоборства [3, 4]. Разработка моделей функционирования КИИ в условиях этого противоборства является основной целью статьи.

2-2018.indd 46 04.07.2018 14:25:18

Концептуальная модель функционирования КИИ в условиях кибернетического противоборства. *Кибернетическое противоборство* представляет собой процесс антагонистического взаимодействия как минимум двух сторон, осуществляемое при совместном использовании общего ресурса – глобального информационного пространства (ГИП). Нарушение устойчивости функционирования объектов КИИ в результате противоборства в ГИП может привести к различным эффектам – от временной потери управления этими объектами до их физического разрушения. По оценке зарубежных экспертов, эффект целевого применения кибероружия на объекты КИИ сравним с эффектом применения оружия массового поражения [4].

Таким образом, функционирование КИИ в условиях кибернетического противоборства порождает новые уязвимости и угрозы ее безопасности, что требует разработки новых моделей, позволяющих принимать эффективные контрмеры по обеспечению требуемой защищенности КИИ.

Предлагаемая концептуальная модель функционирования КИИ в условиях кибернетического противоборства представлена на рис. 1, который отражает компьютерное противоборство двух сторон, одной из которых является КИИ (представленная в границах отдельного ведомства). Управление этим противоборством должно рассматриваться как целенаправленное воздействие двух подсистем управления, стремящихся распространить управляющие воздействия друг на друга. Одной из таких подсистем является система управления (СУ) деструктивными информационными воздействиями (ДИВ) противника, которая управляет применением кибероружия. Вторая подсистема – это СУ устойчивостью функционирования (УФ) КИИ, которая вырабатывает управляющие информационные воздействия (УИВ). Процесс взаимодействия этих подсистем рассматривается как информационный конфликт с пассивным поведением одной из противоборствующих сторон СУ УФ [5, 6]. Причиной возникновения подобного конфликта является наличие у противоборствующих сторон антагонистических целей. СУ ДИВ стремится нарушить устойчивость функционирования, а СУ УФ, наоборот, стремится обеспечить требуемую устойчивость функционирования КИИ.

Исследование устойчивости функционирования КИИ необходимо рассматривать в контексте целей ее функционирования. Обобщенная структура целей для КИИ представляет собой иерархию, в которой на верхнем уровне расположена единая глобальная цель, а на нижнем – локальные цели. Эта иерархия соответствует иерархии уровней построения самой КИИ, в которой выделяются следующие уровни: КИИ; «Ствол КИИ»; «Кластер объектов КИИ»; «Отдельный объект КИИ». Следует подчеркнуть, что достижение локальных целей не является обязательным условием для достижения глобальной цели.

Наличие автоматизированных систем управления в каждом объекте КИИ позволяет им осуществлять выбор траектории достижения цели в пределах некоторой области допустимых изменений локальных параметров функционирования. Данная особенность относит объекты КИИ к классу активных технических объектов. Однако выработка эффективной стратегии достижения поставленных целей объектами КИИ, являющимися активными техническими объектами, весьма затруднена вследствие несогласованности и противоречи-

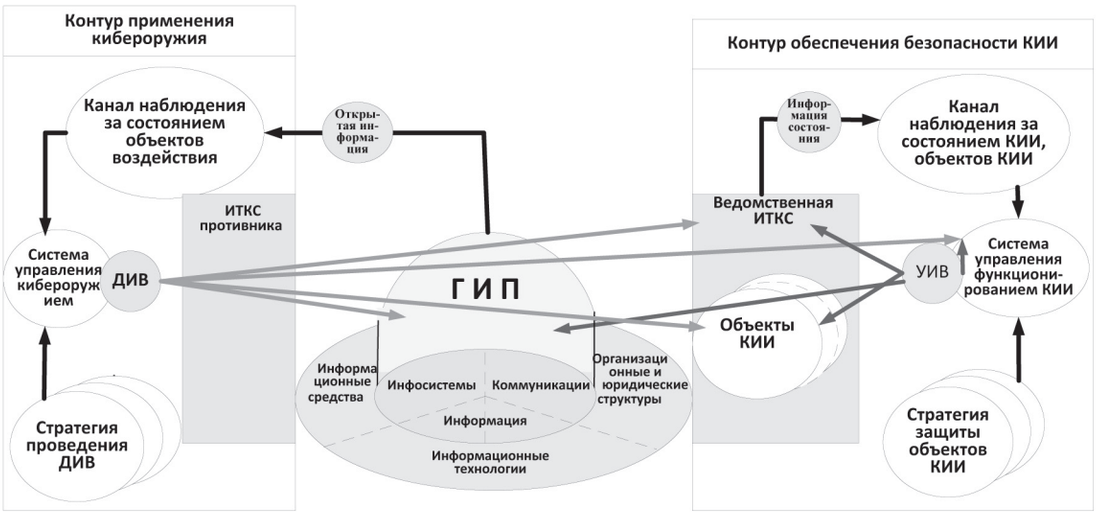

Рис. 1. Концептуальная модель функционирования КИИ в условиях кибернетического противоборства

2-2018.indd 47 04.07.2018 14:25:18

вости и высокой динамики изменения параметров их функционирования (степени готовности, уровня опасности и т.д.) с учетом текущих решаемых задач [7, 8].

Для активных технических систем принципиальное отсутствие возможности точного предсказания будущего поведения самой системы и ее элементов становится их основной особенностью [7]. Это свойство определяется тем, что подобные системы, взаимодействуя со средой функционирования, то есть с киберпространством, принимают участие в «бифуркационных» событиях, исход которых не может быть заранее однозначно предсказан [8]. Каждому бифуркационному событию соответствует не один, а несколько возможных исходов, характеризующихся вероятностью реализации после свершения события. Эти исходы образуют множество возможных результатов данного события. Если событие произошло, то из всего множества возможных исходов реализуется один, а дальнейшее развитие процесса происходит лишь по одному из возможных сценариев до тех пор, пока не произойдет новое событие с несколькими возможными исходами.

Вопросы принятия решений в условиях, когда влияющие факторы принимают случайные значения, обладают высокой сложностью. Это придает особую актуальность рассмотрению вопросов принятия решений в условиях целенаправленных деструктивных информационных воздействий. Обоснованный выбор конкретной стратегии, наиболее соответствующей текущей ситуации, требует моделирования поведения противоборствующих сторон. Рассмотрим следующие возможные подходы к такому моделированию: вероятностно-статистический и информационный.

Вероятностно-статистический подход к моделированию кибернетического противоборства. Примем в качестве показателя, наиболее полно отражающего суть конфликтного взаимодействия СУ УФ КИИ и СУ ДИВ, вероятность пребывания противоборствующих сторон в состоянии выигрыша в течение времени t. Для СУ УФ таким показателем является вероятность $P_у(t)$ обеспечения устойчивого функционирования на заданном интервале $[0; t]$, определяемая выражением:

$$P_у(t) = \int_0^t f_{ув}(\tau)\left[1 - \int_0^\tau f_{дв}(x)dx\right]d\tau, \qquad (1)$$

где $f_{ув}(\tau)$ – плотность распределения вероятности реализации УИВ системой СУ УФ КИИ, приводящей к устойчивому функционированию объекта КИИ; $f_{дв}(x)$ – плотность распределения вероятности реализации ДИВ системой СУ ДИВ противника, нарушающей устойчивое функционирование КИИ.

Рассматривая информационный конфликт с позиции СУ УФ КИИ, можно сделать вывод, что задачей последней в условиях кибернетического конфликта является синтез такой стратегии обеспечения устойчивого функционирования, которая для некоторой фиксированной оценки поведения нарушителя $f_{дв}^*(t)$, полученной на основе априорных данных и предыдущего опыта взаимодействия с СУ ДИВ, максимизирует значение целевого показателя $P_у(t)$. Этот критерий можно записать следующим образом:

$$P_у(t) = \left(\int_0^t f_{ув}(\tau)d\tau - \int_0^t f_{ув}(\tau)\int_0^\tau f_{дв}^*(x)dxd\tau\right) \xrightarrow[\{f_{ув}(\tau)\}]{} 1, \qquad (2)$$

где $\{f_{ув}(\tau)\}$ – множество возможных законов распределения времени обеспечения устойчивого функционирования, соответствующих множеству возможных стратегий СУ УФ.

Значение выражения (2) максимально и равно единице при выполнении хотя бы одного из следующих условий:

1) воздействия нарушителя отсутствуют, $f_{дв}^*(x) = 0$ на всем интервале $[0; \tau]$;

2) система СУ УФ КИИ на всем интервале функционирования $[0; t]$ обеспечивает бесконфликтное взаимодействие с СУ ДИВ противника, что может быть представлено следующим равенством:

$$\int_0^t f_{ув}(\tau)P_{дв}(\tau)d\tau = 0\ , \qquad (3)$$

где $P_{дв}(\tau)$ – функция распределения времени нарушения противником устойчивости функционирования КИИ за период $[0; \tau]$, ортонормальная по отношению к функции $f_{ув}(\tau)$.

Рассмотрим интерпретацию показателя целевой функции системы СУ УФ КИИ, определяемого выражением (1), задав функции $f_{ув}(\tau)$ и $f_{дв}(x)$ в виде нормального закона распределения. В этом случае выражение (1) примет следующий вид:

$$P_у(t) = \frac{1}{2\pi h_1 h_2}\int_0^t \exp\left(-\frac{(\tau-\tau_1)^2}{2h_1^2}\right)\times$$
$$\times\left[1 - \int_0^\tau \exp\left(-\frac{(x-x_2)^2}{2h_2^2}\right)dx\right]d\tau, \qquad (4)$$

где τ_1, h_1, x_2, h_2 – параметры распределений, характеризующие среднее время и разброс времени реализации стратегий обеспечения (τ_1 и h_1) и нарушения (x_2 и h_2) устойчивости функционирования, соответственно.

Учитывая, что при адаптивном управлении основой процесса обеспечения устойчивости функционирования КИИ выступает оценка способности выполнять целевую функцию объектом КИИ, можно предположить, что данная способность СУ УФ обеспечивается на основе параметрической адаптации идентификации состояния объекта КИИ, параметрической, структурной и функциональной адаптации системы, а также параметрической адаптации комплекса средств

2-2018.indd 48 04.07.2018 14:25:19

системы защиты информации. Физически это означает, что в зависимости от вида и значений параметров наблюдаемого воздействия осуществляется поиск таких значений параметров функционирования КИИ, которые обеспечивают минимальное время реализации выбранной стратегии обеспечения устойчивого функционирования или максимальное время реализации стратегии воздействия.

Параметры h_1 и h_2, в свою очередь, могут рассматриваться как характеристика концентрации или распределения ресурсов, используемых для обеспечения устойчивого функционирования. В данном случае можно предположить, что в зависимости от полученной оценки защищенности КИИ должна быть обеспечена необходимая адаптация КИИ к ДИВ. Физически это означает поиск такого варианта применения ресурсов КИИ, при котором обеспечивается максимум целевого показателя $P_у(t)$.

Информационный подход к моделированию кибернетического противоборства. Для выявления закономерностей взаимодействия противоборствующих сторон в условиях кибернетического противоборства будем полагать, что в процессе взаимодействия систем СУ УФ КИИ и СУ ДИВ происходит накопление информации каждой из противоборствующих сторон, условно обозначенных как S и U соответственно [9]. В этом случае модель противоборства будет иметь вид, показанный на рис. 2.

Имеющееся к некоторому моменту времени у СУ ДИВ количество информации о стратегиях обеспечения устойчивого функционирования $I(U, S)$ и стратегиях проведения ДИВ $I(U, S)$ будет определять сложность преодоления СУ УФ КИИ и сложность защиты от ДИВ. Для количественной оценки последних могут быть использованы значения условной энтропии $H[S|I(U, S)]$ и $H[S|I(U, S)]$. Соотношение этих значений на определенном этапе взаимодействия СУ УФ и СУ ДИВ будет определять исход информационного конфликта в пользу одной из противоборствующих сторон.

Рассматривая временную динамику конфликта, можно выделить следующие противоречия. Увеличение времени конфликта приводит к увеличению количества информации о СУ ДИВ $I(S, U)$, повышению вероятности правильной идентификации ДИВ $P_{пи}(t)$ и, следовательно, повышению устойчивости функционирования КИИ. Вместе с тем излишне продолжительная идентификация воздействий уменьшает своевременность реализации стратегии обеспечения устойчивого функционирования $P_у(t < t_{дв})$. Это, в свою очередь, позволяет системе СУ ДИВ накопить большее

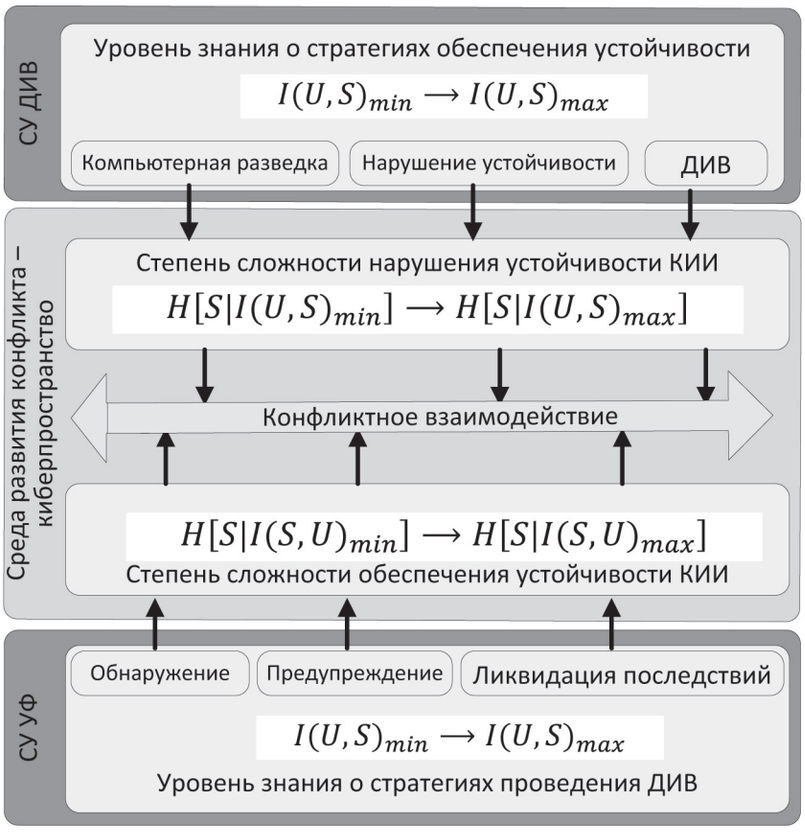

Рис. 2. Модель противоборства СУ УФ КИИ и СУ ДИВ при информационном подходе

2-2018.indd 49 04.07.2018 14:25:20

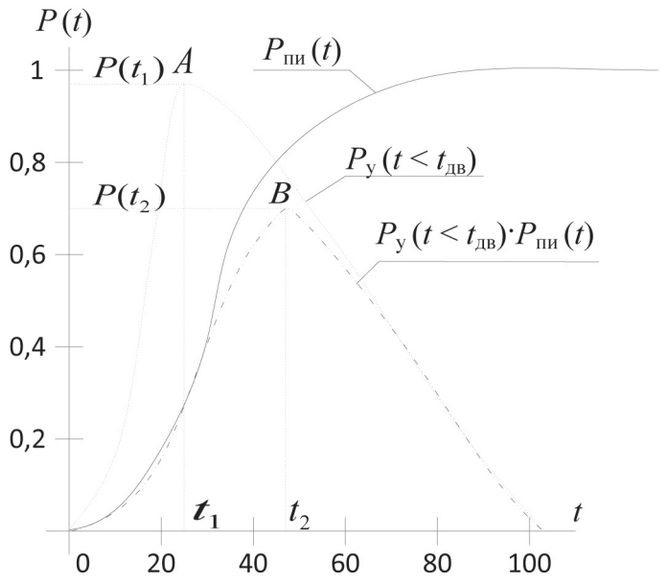

Рис. 3. Пример динамики изменения зависимостей показателей своевременности, достоверности и эффективности обеспечения устойчивого функционирования КИИ в условиях кибернетического противоборства

количество информации о СУ УФ I (U, S) и выбрать более эффективную стратегию воздействия на КИИ.

Пример динамики изменения значений своевременности $P_у$ ($t < t_{дв}$), достоверности $P_{пи}$ (t) и эффективности $P_у$ ($t < t_{дв}$)·$P_{пи}$ (t) обеспечения устойчивого функционирования КИИ в условиях кибернетического противоборства, полученной при информационном подходе, приведен на рис. 3.

На рис. 3 точка A соответствует максимальному значению $P_у$ ($t < t_{дв}$), достигаемому к моменту времени t_1. В точке B эффективность обеспечения устойчивого функционирования КИИ, выражаемая через произведение значений показателей $P_у$ ($t < t_{ну}$) и $P_{пи}$ (t), достигаемых в момент времени t_2, является максимальной. Это соответствует компромиссу между своевременностью реализации стратегии обеспечения устойчивого функционирования КИИ и достоверностью результатов идентификации ДИВ. Существование подобного компромисса позволяет предположить возможность информационной адаптации СУ УФ КИИ, заключающейся в выборе оптимального уровня информированности о наблюдаемом воздействии для принятия решения о стратегии обеспечения устойчивого функционирования КИИ.

Заключение

Таким образом, предложенные модели функционирования КИИ в условиях кибернетического противоборства и проведенный с их помощью анализ процесса взаимодействия СУ УФ КИИ и СУ ДИВ противника позволяют сделать следующие выводы, касающиеся возможности обеспечения устойчивого функционировании КИИ в условиях кибернетического противоборства:

1) существуют стратегии упреждения и затягивания воздействий нарушителя, а также имеется возможность их реализации на основе адаптации идентификации состояний КИИ в условиях целенаправленных ДИВ;

2) имеются стратегии концентрации и распределения ресурсов КИИ и существует возможность их реализации на основе структурной, параметрической и функциональной адаптации КИИ в условиях целенаправленных ДИВ;

3) существует компромисс между достоверностью идентификации ДИВ и своевременностью реализации стратегии управления устойчивостью функционирования и имеется возможность его нахождения на основе информационной адаптации СУ УФ КИИ.

Дальнейшие исследования планируется направить на разработку методик, позволяющих реализовать эти гипотезы для различных вариантов функционирования КИИ в условиях кибернетического противоборства.

Работа выполнена при поддержке РФФИ (проект 18-07-01369).

Литература

1. Котенко, И. В. Аналитический обзор докладов международного семинара «Научный анализ и поддержка политик безопасности в киберпространстве» (SA&PS4CS 2010) / И.В. Котенко, И.Б. Саенко, Р.М. Юсупов // Труды СПИИРАН. – 2010. – № 2 (13). – С. 226–248.

2. Управление доступом к ресурсам ведомственных информационных систем на основе информационных профилей поль-

2-2018.indd 50 04.07.2018 14:25:20

зователей / И.Б. Саенко [и др.] // Информация и Космос. – 2017. – № 4. – С. 119–125.

3. Глобальная безопасность в цифровую эпоху: стратагемы для России / под общ. ред. А.И. Смирнова. – М. : ВНИИ геосистем, 2014. – 394 с.

4. Бедрицкий, А. В. Информационная война: концепции и их реализация в США / А.В. Бедрицкий ; под ред. Е.М. Кожокина. – М.: РИСИ, 2008. – 187 с.

5. Губарев, В. А. Концептуальная модель конфликта в информационной борьбе / В.А. Губарев, П.П. Крутских // Радиотехника. – 1998. – № 6. – С. 29–31.

6. Кузнецов, А. С. Синтез гипотез поведения систем в радиоэлектронном конфликте / А.С. Кузнецов, М.Ю. Сохен // Радиотехника. – 1997. – № 6. – С. 3–8.

7. Щербатов, И. А. Сложные слабоформализуемые многокомпонентные технические системы / И.А. Щербатов, О.М. Проталинский // Управление большими системами: сборник трудов. – 2013. – № 45. – С. 30–46.

8. Малинецкий, Г. Г. Современные проблемы нелинейной динамики / Г.Г. Малинецкий, А.Б. Потапов. – М.: Эдиториал УРСС, 2000. – 336 с.

9. Курбацкий, А. Н. Информационный метод анализа и оптимизации в системах поддержки принятия решений / А.Н. Курбацкий, В.А. Чеушев. – Мн.: Институт технической кибернетики НАН Беларуси, 1999. – 220 с.

2-2018.indd 51 04.07.2018 14:25:20