14. Шумилова Г.П. Прогнозирование электрических нагрузок с применением методов искусственного интеллекта / Г.П. Шумилова, Н.Э. Готман, Т.Б. Старцева. – URL:http://www.energy.komisc.ru/seminar/StShum1.pdf. (дата обращения 12.12.2015).
15. Hippert H.S. Neural networks for short-term load forecasting: a rewiew and evaluation / H.S. Hippert, C.E. Pedreira, R.C. Souza // IEEE Trans. PAS. – 2001. – Vol. 16, no.1.
16. Paoletti S. Load forecasting for active distribution networks / S. Paoletti, M. Casini, A. Giannitrapani, A. Facchini, A. Garulli, A. Vicino // 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies (ISGT Europe). – 2011. – P. 1–6.
17. Ghods L. Different Methods of Long-Term Electric Load Demand Forecasting; A Comprehensive Review / L. Ghods, M. Kalantar // Iranian Journal of Electrical & Electronic Engineering. – 2011. – Vol. 7. – P. 249–259.
18. Christiaanse W.R. Short-Term Load Forecasting Using General Exponential Smoothing // Power Apparatus and Systems, IEEE Transactions on, V. PAS-90. – 1971. – no.2. – P. 900-911. DOI: 10.1109/TPAS.1971.293123.
19. Rabiner L.R. A tutorial on hidden Markov models and selected applications in speech recognition. - Proc. IEEE, vol.77, No.2, pp.257 – 286, 1989.
20. Taylor J.W. Short-Term Load Forecasting with Exponentially Weihted Methods / J.W.Taylor // IEEE Transactions on Power Systems.-2012.-27(1). – С.458–464.
21. Goel A. Regression Based Forecast of Electricity Demand of New Delhi / A.Goel // International Journal of Scientific and Research Publications.-2014. – Vol.4, Issue 9. – P.9.

Ссылка для цитирования:
О. Б. Урумбаева, Т. А. Шалаев, О. М. Шикульская. Концепция интеллектуального управления энергосетью // Инженерно-строительный вестник Прикаспия : научно-технический журнал / Астраханский государственный архитектурно-строительный университет. Астрахань : ГАОУ АО ВО «АГАСУ», 2020. № 3 (33). С. 69–74.

УДК 621.96:681.327.8
DOI: 10.35108/isvp20203(33)74-78

АДАПТИВНОЕ УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМ РЕСУРСОМ В СИСТЕМЕ СВЯЗИ КРИТИЧЕСКИ ВАЖНОГО ОБЪЕКТА

Е. А. Жидко[1], А. Б. Власов[2]
[1]Воронежский государственный технический университет, г. Воронеж, Россия
[2]Военно-воздушная академия имени профессора Н. Е. Жуковского и Ю.А. Гагарина, г. Воронеж, Россия

Эффективное функционирование системы управления критически важных объектов в современных условиях может быть достигнуто только при широком внедрении информационных технологий в повседневную деятельность органов их управления с существенным повышением уровня информационной поддержки процессов управления. Вместе с тем, сложность структуры и многообразие функций информационно-телекоммуникационной системы приводят к увеличению числа уязвимых элементов и, как следствие, путей информационно-технических воздействий. В частности, за счет воздействий на подсистемы управления системами связи могут изменяться условия протекания процессов передачи-приема информации. При этом нарушается целостность, полнота и оперативность доведения информации. Указанные обстоятельства определяют необходимость совершенствования защиты информационно-телекоммуникационной системы в условиях информационного противоборства в условиях ограничения ресурса, выделяемого для выявления и нейтрализации угроз.

***Ключевые слова**: информационная безопасность, система связи и управления, адаптивная подсистема безопасности, защита информации, качество управления информационными ресурсами.*

ADAPTIVE MANAGEMENT OF INFORMATION RESOURCE IN THE COMMUNICATION SYSTEM OF CRITICAL IMPORTANT OBJECT

E. A. Zhidko[1], A.B. Vlasov[2]
[1]Voronezh State Technical University, Voronezh, Russia
[2]The Air Force Academy named after Professor N.Ye. Zhukovsky and Yu.A. Gagarin, Voronezh, Russia

The effective functioning of the critical facilities management system in modern conditions can be achieved only with the widespread introduction of information technologies in the daily activities of their management bodies with a significant increase in the level of information support for management processes. At the same time, the complexity of the structure and the variety of functions of the information and telecommunication system lead to an increase in the number of vulnerable elements and, as a result, the ways of information and technical impacts. In particular, due to the impact on the control subsystems of communication systems, the conditions for the flow of information transmission and reception processes can change. At the same time, the integrity, completeness and efficiency of communicating information is violated. These circumstances determine the need to improve the protection of ITS in the context of information warfare in the face of limited resources allocated to identify and neutralize threats.

***Keywords:** information security, communication and control system, adaptive security subsystem, information protection, quality of information resources management.*

Введение

К критически важным относятся объекты (КВО), на которые возлагаются первостепенные функции выполнения повседневных задач и при прекращении деятельности которых возникает угроза срыва выполнения задач высокого уровня. К таким объектам относятся энергетические, транспортные, коммуникационные, строительные, промышленные, горнодобывающие, оборонные комплексы. Среди них можно выделить

предприятия топливно-энергетиче-ского комплекса (ТЭЦ, АЭС, объекты, связанные с эксплуатацией ядерных установок, объекты нефтехимической промышленности), металлургической промышленности, уникальные инженерные сооружения (плотины, эстакады, нефтегазохранилища), опасные объекты оборонного комплекса (крупные склады обычных и химических вооружений, военные аэродромы, парки со специальной техникой, склады горюче-смазочных материалов, ракетно-космические и самолетные системы с ядерными и обычными зарядами), а также отрасли, связанные с добычей и обогащением урановой и ториевой руд, производством ядерного топлива, с эксплуатацией радиационных источников, транспортированием по трубопроводам газа, нефти и предприятия в области цветной металлургии, обогащения железных руд и др. [1].

Система связи и управления, являющаяся ключевым компонентом технической основы КВО, представляет собой совокупность информационных и телекоммуникационных устройств и ресурсов, взаимодействующих в едином информационном пространстве. Ее главная задача заключается в своевременной передаче информации в системе управления и команд управления исполнительным элементам с требуемой достоверностью и точностью.

Сложность структуры и многообразие функций ИТС приводят к увеличению числа уязвимых элементов и, как следствие, путей ИТВ. В частности, через подсистемы управления автоматизированными системами связи КВО возможно изменять условия протекания процессов передачи-приема информации. Наличие информационных входов через радиоканалы создает предпосылки для внесения несанкционированных изменений в алгоритмы управления. Единая информационная платформа (форматы обмена и протоколов взаимодействия) позволяет через отдельные, наименее защищенные элементы влиять на состояние ИТС в целом, нарушать целостность, полноту и оперативность доведения информации, а также навязывать дезинформацию [2].

Поэтому необходимо совершенствование защиты систем связи КВО, которое направлено на своевременное распознавание угроз безопасности и минимизацию рисков нарушения регламентированных состояний при допустимых потерях целевых функций средств передачи-приема и обработки информации [3-5].

Постановка задачи исследования

Согласно [6–8], процесс информационного обмена в условиях конкурентной борьбы на внешних и внутренних рынках необходимо рассматривать в рамках информационного конфликта (ИК) ИТС со средствами ИТВ, в котором каждая из сторон стремится достичь максимальной реализации функциональных возможностей при минимизации функций противостоящей стороны [9, 10].

ИК ИТС со средствами ИТВ представляет собой специфическое взаимодействие, при котором хотя бы один компонент их целевых функций направлен на уменьшение вероятности реализации целевых функций противостоящей стороны.

Снижение эффективности передачи-приема и обработки информации при реализации мер по защите достигается за счет организации подсистемы безопасности и защиты информации (ПБЗИ). ПБЗИ КВО представляет собой стохастическую человеко-машинную (эргатическую) систему, нуждающуюся в активном управлении. Ее задачей является минимизация различия возмущенной и исходной (невозмущенной) целевых функций ИТС за счет реализации в системе внутреннего управления, направленного на сохранение заданного уровня вероятности реализации целевой функции [11–13].

Процессы управления средствами защиты в ПБЗИ КВО могут быть представлены в виде замкнутого технологического цикла, состоящего из связанных по целям и результатам фаз. Модель технологического цикла управления ПБЗИ КВО представлена на рис. 1 [11].

Первые четыре фазы определяют цикл контроля средств защиты, а остальные – цикл управления.

Защита ИТС состоит в исключении (затруднении) добывания противоборствующей стороной охраняемой информации и создания ИТВ на процессы информационного обмена. Она считается эффективной при выполнении условий надежности для всех элементов ИТС, подверженных угрозам. Стратегия защиты системы является рациональной, если ее применение обеспечивает требуемую защищенность содержания и инфраструктуры для сбора, передачи, хранения и обработки информации при всех возможных стратегиях ИТВ в условиях ограничения ресурса, выделяемого для выявления и нейтрализации угроз.

Для обеспечения конфликтной устойчивости ИТС при многократных угрозах, характерных для состояния ИПБ, необходимо использовать методы активного противодействия компонентам ИТВ в целях их полной или частичной нейтрализации в течение ИК.

Наиболее перспективными для исследования путей построения ПБЗИ являются методы, основанные на математическом (имитационном) моделировании ИТС в условиях ИК. В имитационных моделях воспроизводятся динамические состояния функциональных элементов и процессы передачи-приема и обработки информации при воздействии различных видов угроз. По результатам анализа реак-

ций на ИТВ и закономерностей изменения регламентированных состояний ИТС разрабатываются способы, формируются состав и структура упорядоченных компонентов, задействованных в мероприятиях по защите.

В работах П.И. Антоновича, Ю.Е. Донскова, В.И. Борисова, В.И. Владимирова, В.И. Кузнецова, В.В. Сысоева представлены иерархические модели ИТС в условиях ИК и способы защиты информации на основе распределения ресурсов из условий выполнения целевых функций и текущей опасности угроз.

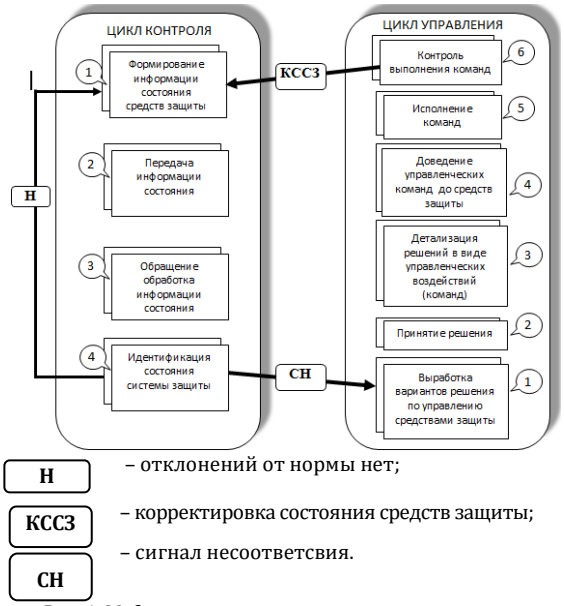

Рис. 1. Модель технологического цикла управления ПБЗИ КВО

Вместе с тем указанными авторами ИК представляется в виде активных помеховых воздействий на компоненты ИТС и реакций ИТС, направленных на предотвращение или минимизацию последствий наносимого информационного ущерба.

Однако при поражении инфраструктуры КВО, например военных аэродромов, деструктивным воздействиям подвергаются не только телекоммуникационные сети, но и информационные (информационно-вычислительные) комплексы. Конфликтные компоненты реализуются как в пространстве сигналов, так и в киберпространстве. Поэтому в имитационной модели ИТС требуется воспроизводить процессы передачи-приема и обработки информации на сигнальном, семантическом и прагматическом уровнях. На сигнальном уровне целевая функция системы определяется выборкой сигналов при реализации команд управления и обработке данных, на семантическом уровне – комплексом алгоритмов (формализованных правил) синтеза базы данных при обработке потока запросов и реакций, на прагматическом уровне – последовательностью команд управления с учетом связей между взаимодействующими объектами.

В трудах А.П. Колданова, О.С. Авсентьева, В.Г. Карташевского, А.Г. Остапенко, В.А. Павлова, Е.П. Петрова, Н.Н. Толстых построены модели ИТС с управляемыми структурами и синтезированы алгоритмы адаптивного управления в интересах защиты от ИТВ. Разработаны способы:

– пространственно-энергетической адаптации на основе регулирования мощностей передатчиков и применения адаптивных приемопередающих антенн;

– частотно-временной адаптации, базирующейся на использовании псевдослучайной перестройки рабочей частоты или нескольких частот информационных сигналов, а также передаче сообщений на фоне маскирующих излучений, которые не содержат информации, но затрудняют обнаружение полезных сигналов;

– структурной адаптации, реализуемой путем формирования кодовых групп импульсов и рационального выбора маршрутов для их передачи.

Процессы адаптации радиосистем исследованы с учетом статистической зависимости между векторами входных воздействий и реакций компонентов, алгоритмы определяют пути перевода систем в состояния с минимальными потерями информации за минимально возможное время. Защищенность ИТС оценивается по интегральным показателям скрытности информационного обмена, характеризуемой вероятностью обнаружения сигналов средствами радиоразведки противника, и помехоустойчивости, определяемой вероятностью безошибочного приема сообщений в условиях ИТВ.

Однако при этом анализу подвергаются только конфликтные взаимодействия элементов и только для установленного уровня иерархии. Адаптация, в основном, осуществляется на сигнальном уровне путем изменения условий приема и первичной обработки сообщений при идентификации в них конфликтного компонента.

Ввиду возможности проявления деструктивных факторов на различных уровнях иерархии, наличия в системах связи и управления элементов, способных к взаимодействию с компонентами ИТВ по схемам содействия, в рамках данного подхода, как правило, не удается реализовать оптимальную стратегию ПБЗИ, гарантирующую безопасность при допустимых потерях целевых функций ИТС.

На этапе безопасного входа конфликтного компонента в информационную область системы наиболее эффективным является метод адаптивного управления, поскольку он за счет перестройки структуры системы или изменения значений ее параметров воспрепятствует проникновению компонента в систему.

Принцип адаптивного управления ИТС заключается в выработке правил приспособлений характеристик аппаратных и программных средств к изменяющимся условиям обстановки для реализации целевых функций системы.

Адаптивное управление информационно-телекоммуникационной системой заключается в формировании механизмов воздействия на ее компоненты и средства ИТВ с активными обратными связями.

Адаптивное управление информационными ресурсами информационно-телекоммуникационной системы КВО

За счет распределения информационного ресурса применительно к складывающейся обстановке открываются возможности определения областей устойчивой адаптации ИТС, в которых время выявления деструктивных воздействий существенно меньше постоянной времени, характеризующей изменения обстановки.

Адаптация управления имитируется путем задания механизмов воздействия на компоненты ПБЗИ и ИТВ с активными обратными связями. Процессы взаимодействия компонентов ИТС и ИТВ представляются в виде последовательности состояний системы более высокого уровня, построенной на базе противодействия и содействия элементов различных уровней иерархии с различными целевыми функциями.

Эффективность адаптивного управления, оцениваемая по критерию обеспечения требуемого уровня защиты при рациональном распределении информационных ресурсов и сохранении требуемого качества передачи-приема и обработки информации, определяется возможностями изменения структуры и параметров ИТС или их отдельных элементов в складывающейся обстановке. В адаптивных системах управления информация об объекте и внешних воздействиях собирается и обрабатывается в процессе функционирования, что позволяет вырабатывать управляющие воздействия, актуальные для текущих состояний среды функционирования.

Основными видами адаптации систем связи КВО, позволяющими минимизировать информационные потери от деструктивных ИТВ, являются эволюция, привыкание, обучение и самообучение, организация и самоорганизация.

Адаптация охватывает процессы управления путем реализации и поддержания состояний системы или ее элементов в наиболее полной степени соответствия целям и задачам функционирования, а также непосредственно процессы функционирования за счет создания максимально благоприятных условий для ИТС. По характеру изменения объекта адаптация подразделяется на параметрическую, суть которой заключается в изменении его параметров объекта с сохранением структуры и взаимосвязей между элементами, и структурную, при которой изменяется структура объекта и перераспределяются функциональные взаимосвязи между элементами [13, 14].

Исходя из типовых условий и задач поражения военного аэродрома, функционирование системы связи, РТО и автоматизации управления рассматривается как процесс взаимной опережающей многоуровневой адаптации компонентов ИТС и ИТВ друг к другу и их совместной адаптации к внешней среде. Объект адаптации представляется в виде системы с вероятностной реакцией на изменение обстановки и условий функционирования. Количественная мера защищенности информации ИТС в последовательно изменяемых состояниях характеризуется вектором, компонентами которого являются количественные меры свойства защищаемых элементов в текущий момент времени.

Состояние системы, изменяемое в результате включения средств защиты по соответствующим управляющим командам, определяется не только количеством средств защиты, но и ее состоянием в предыдущий момент времени. Степень защиты системы характеризуется вероятностью реализацией ее целевой функции, устанавливающей меру соответствия состояния защищенности эталонному описанию.

Наибольшая эффективность адаптивного управления информационным ресурсом обеспечивается за счет перевода ИТС в состояние с минимальными потерями информации путем выявления компонентов, способных в текущий момент времени к содействию, и исключения резервирования информационного ресурса на их защиту. За счет распределения ресурса в складывающейся обстановке открываются возможности определения областей устойчивой адаптации ПБЗИ, в которых время обработки информации и выявления деструктивных воздействий существенно меньше постоянной времени, характеризующей изменения обстановки.

Структурная схема выработки управляющих воздействий при адаптивном управлении информационным ресурсом ИТС представлена на рисунке 3 [15].

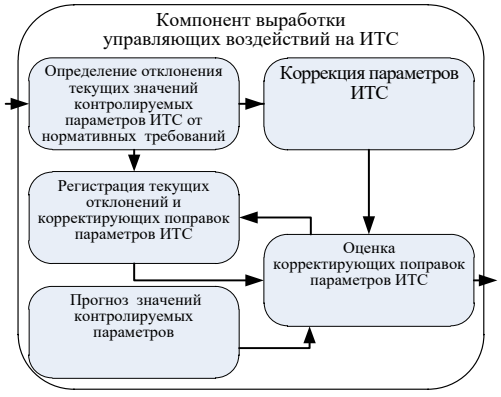

Рис. 3. Структурная схема выработки управляющих воздействий при адаптивном управлении ПБЗИ

Выводы

Известные подходы основываются на переводе объектов защиты, подверженных ИТВ, в состояния с минимальными потерями информации за минимально возможное время.

Адаптивное управление ПБЗИ, рассмотренное в работе, базируется на выборе рациональных условий функционирования ИТС за счет поддержания ее компонентов в состояниях, обеспечивающих наилучшие условия реализации целевой функции при требуемой степени безопасности информации или максимизации эффективности мер защиты при выполнении функциональных задач.

Эффективность адаптивного управления определяется временными характеристиками управляющих воздействий, вероятностными показателями изменения структуры и параметров ИТС и степенью их соответствия требованиям по безопасности и защите в складывающейся обстановке. Адаптивное управление информационными ресурсами необходимо рассматривать как процесс взаимной опережающей многоуровневой адаптации компонентов ИТС и ИТВ друг к другу и их совместной адаптации к внешней среде. Информационный ресурс, требуемый для выполнения целевых функций компонентов ИТС на конкретном уровне иерархии и этапе функционирования, определяется в соответствии с базовым соотношением Кобба – Дугласа [16]. Параметры управляющих воздействий находятся по результатам оптимизации критериальной функции ИК, которая наиболее эффективно выполняется с применением градиентных методов.

Устойчивость адаптации ИТС к изменяющимся условиям достигается за счет нахождения областей определения управляющих воздействий, при которых время выявления деструктивных факторов существенно меньше постоянной времени, характеризующей изменения параметров обстановки. Области устойчивой адаптации находятся на основе решения уравнений динамического баланса вероятностей реализации целевых функций ИТС и средств ИТВ.

Наибольшая эффективность адаптивного управления обеспечивается за счет перевода ИТС в состояния с минимальными потерями информации путем выявления компонентов, способных в текущий момент времени к бесконфликтному взаимодействию, и исключения резервирования информационных ресурсов на их защиту.

На основе анализа вариантов адаптивного управления при наличии и отсутствии модели текущего состояния системы, а также параметрической и структурной адаптации установлено, что для рационального распределения информационного ресурса, обеспечивающего достижение наиболее высокого уровня защиты, целесообразно применять метод поисковой структурной адаптации [15, 16].

Список литературы

1. Леонов П.М., Жидко Е.А. Определение технического состояния сложных военных объектов // ФЭС: Финансы. Экономика. 2015. № 5. С. 64-67.
2. Давыдов А. Е., Максимов Р. В., Савицкий О. К. Защита и безопасность ведомственных интегрированных инфокоммуникационных систем. – М.: Воентелеком, 2017. 536 с.
3. Жидко Е.А., Попова Л.Г. Принципы системного математического моделирования информационной безопасности // Интернет-журнал Науковедение. 2014. № 2 (21). С.34.[Электронный ресурс].
4. Жидко Е.А. Попова Л.Г. Методологические основы обеспечения информационной безопасности инновационных объектов // Информация и безопасность, 2012. Т. 15. № 3. С. 369-376.
5. Жидко Е.А., Попова Л.Г. Парадигма информационной безопасности компании // Вестник Иркутского государственного технического университета, 2016. № 1 (108). С. 25-35.
6. Павлов В.А., Павлов Р.В., Толстых Н.Н. Обобщенная модель процесса функционирования автоматизированных систем в режиме информационного конфликта // Информация и безопасность, 1999. №1. С.56-66.
7. Толстых Н. Н., Пятунин А. Н., Марейченко И. В., Павлов В. А. Исследование конфликта информационных систем методами теории координации // Информация и безопасность. 2004. № 1. С. 84-85.
8. Агафонов А. А., Афанасьев В. И., Разиньков С. Н. и др. Современная радиоэлектронная борьба. Вопросы методологии. – М.: Радиотехника, 2006. – 424 с.
9. Толстых Н.Н. Пятунин А.Н., Марейченко И.В., Слепов Ю.И., Павлов В.А. Принципы раннего обнаружения признаков конфликтного режима взаимодействия автоматизированных телекоммуникационных комплексов // Теория и техника радиосвязи. 2004. № 2. С.95-99.
10. Михайлов Р.Л. Радиоэлектронная борьба в вооруженных силах США: Монография. – СПб.: Наукоемкие технологии, 2018. – 131 с.
11. Жидко Е.А., Разиньков С.Н. Модель подсистемы безопасности и защиты информации системы связи и управления критически важного объекта // Системы управления, связи и безопасности. 2018. № 1. С. 122-135.
12. Антипов О.И., Неганов В.А. Анализ и прогнозирование поведения временных рядов: бифуркации, катастрофы, синергетика, фракталы и нейронные сети. – М.: Радиотехника, 2011. – 350 с.
13. Нестерук Г. Ф., Осовецкий Л. Г., Нестерук Ф. Г. Адаптивная модель нейросетевых систем информационной безопасности // Перспективные информационные технологии и интеллектуальные системы. 2003, №3 (15). С55-62.
14. Хорошко В.А. Методы и средства защиты информации. – М.: Юниор, 2003. – 504 с.
15. Жидко Е.А., Леонов П.М., Попова Е.С. Разработка модели идентификации конфликтного компонента и метода ситуационного управления информационными ресурсами информационно-телекоммуникационной системы критически важного объекта в условиях информационного противоборства. ВУНЦ ВВС «ВВА» им. профессора Н.Е. Жуковского и Ю.А. Гагарина" (г. Воронеж) - Воронеж, 2019. - 117 с.
16. Лебедев Б. К. Методы поисковой адаптации для решения оптимизационных задач // Прикладные информационные технологии и интеллектуальные системы. 2003. № 3. С. 24-30.

Ссылка для цитирования:
Е. А. Жидко, А. Б. Власов. Адаптивное управление информационным ресурсом в системе связи критически важного объекта // Инженерно-строительный вестник Прикаспия : научно-технический журнал / Астраханский государственный архитектурно-строительный университет. Астрахань : ГАОУ АО ВО «АГАСУ», 2020. № 3 (33). С. 74–78.