УДК 621.96:681.327.8

Модель подсистемы безопасности и защиты информации системы связи и управления критически важного объекта

Жидко Е. А., Разиньков С. Н.

Постановка задачи. *Неуклонное совершенствование средств и способов информационного противоборства требует от разработчиков систем связи и управления адекватных решений по повышению их конфликтной устойчивости и надежности функционирования. Основные сложности обеспечения безопасности и защиты информации обусловлены наличием интеллектуальных компонентов в современных средствах информационно-технических воздействий, позволяющих адаптивно изменять структурные признаки и корректировать цели воздействия. Меры по защите информации выбираются из условий минимизации времени обнаружения элемента с деструктивными функциями и достижения требуемого качества управления ресурсами, выделяемыми для его нейтрализации, в течение времени реализации конфликта. Задача выбора таких мер, а также обоснования порядка и последовательности их реализации может быть решена на основе моделирования подсистемы безопасности и защиты информации системы связи и управления и исследования ее свойств при наличии конфликтного компонента.* ***Цель работы*** *– построение модели подсистемы безопасности и защиты информации системы связи и управления критически важного объекта.* ***Используемые методы.*** *Модель подсистемы безопасности и защиты информации системы связи и управления в условиях вредоносных информационно-технических воздействий построена с использованием методов теории конфликта, теории графов и математической статистики. Технологический цикл управления ресурсами для выявления и нейтрализации деструктивных элементов обоснован с применением методов теории идентификации и принятия решений в условиях априорной неопределенности ситуации.* ***Результат.*** *Разработана модель подсистемы безопасности и защиты информации критически важного объекта, по результатам испытаний которой определены фазы технологического цикла управления ресурсами для борьбы с деструктивным информационно-техническим воздействием.* ***Практическая значимость.*** *Обоснованы пути реализации и характеристики средств защиты информации, способы адаптивного управления параметрами операционной среды при конфликтном взаимодействии системы связи и управления со средствами информационно-технических воздействий.*

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

Актуальность темы исследования

Одной из основных задач информационного противоборства является нарушение нормальной устойчивой работы критически важных объектов, обеспечивающих потребности и создающих условия развития общества и государства, изменение регламента и прекращение функционирования которых приводит к потере управления административно-территориальной единицей, дестабилизации ее деятельности на длительный период времени [1]. Перечень таких объектов включает в себя топливно-энергетические и горнодобывающие комплексы,

Библиографическая ссылка на статью:
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. URL: http://sccs.intelgr.com/archive/2018-01/06-Zhidko.pdf

Reference for citation:
Zhidko E. A., Razinkov S. N. Model of security and information protection subsystem of a communication and control system of a critical object. *Systems of Control, Communication and Security*, 2018, no. 1, pp. 122-135. Available at: http://sccs.intelgr.com/archive/2018-01/06-Zhidko.pdf (in Russian).

предприятия ядерной, нефтехимической и металлургической промышленности, морские порты, аэродромы и авиабазы [1-3].

Возможной причиной сбоев и отказов в их работе является преднамеренное деструктивное информационно-техническое воздействие (ИТВ) на системы связи и управления [4-7].

Для выявления аспектов ИТВ взаимодействие систем связи и управления со средствами, вносящими конфликтный компонент, необходимо рассматривать в форме информационного конфликта (ИК).

С позиций информационного противоборства [1, 8] сущность конфликта заключается в создании средствами ИТВ угроз нарушения безопасности информации в системах связи и управления и адекватной реакции систем на угрозы [9-11]. Для противодействия ИТВ в системе связи и управления организуется целенаправленная деятельность аппаратных и программных устройств, образующих подсистему безопасности и защиты информации (ПБЗИ), с целью обнаружения и нейтрализации элементов с деструктивными функциями при допустимой степени снижения эффективности передачи-приема информации [4].

Исход ИК в условиях ограниченных информационных ресурсов средств ИТВ и ПБЗИ существенным образом зависит от качества их управления [12, 13]. Поэтому для обоснования рациональных стратегий поведения конфликтующих сторон, порядка и последовательности выполнения мероприятий в соответствии с целевыми функциями необходимо выявить закономерности поведения ПБЗИ систем связи и управления и средств ИТВ в условиях адаптивного управления при защите информационного ресурса и воздействии на информационный ресурс противоборствующей стороны [1, 3].

Основные сложности построения и организации работы ПБЗИ обусловлены наличием в средствах ИТВ интеллектуальных компонентов, позволяющих адаптивно изменять структурные признаки и корректировать цели воздействия [2, 12]. В складывающихся условиях меры по обеспечению информационной безопасности экологически опасного критически важного объекта должны выбираться в соответствии с критерием минимизации времени обнаружения элемента с деструктивными функциями и достижения требуемого качества управления ресурсами, выделяемыми для его нейтрализации, в течение времени ИК.

Для определения перечня, порядка и последовательности реализации таких мер актуальной является разработка модели ПБЗИ системы связи и управления.

Постановка задачи исследования

Согласно [14-16], при моделировании ПБЗИ системы связи и управления необходимо рассматривать как эргатическую систему с активным управлением.

Цель предлагаемой работы – разработка модели ПБЗИ для формализованного описания процессов взаимодействия программных и технических средств системы связи и управления между собой и со средствами ИТВ в процессе обнаружения и нейтрализации деструктивных элементов, а также обоснования технологического цикла управления ресурсами для борьбы с ИТВ.

В модели воспроизводятся адаптивные механизмы управления компонентами ПБЗИ и средств ИТВ с активными обратными связями [12, 14] для опре-

деления ресурсов сторон, требуемых для защиты и нарушения нормального устойчивого функционировании системы связи и управления. Выбор мер по организации и преодолению защиты на основе адаптивного управления элементами системы связи и управления в процессе ИК позволяет исследовать закономерности и обосновать рациональные стратегии функционирования ПБЗИ и средств ИТВ в соответствии с целевыми функциями.

Построение модели и анализ адаптивной подсистемы безопасности и защиты информации системы связи и управления

Будем полагать, что система связи и управления в процессе функционирования проходит ряд промежуточных состояний b_k, k=0, 1, 2, …, в каждом из которых уровень защищенности информации о критически важном объекте характеризуется n-мерным вектором

$$\bar{p}_z^k = p_z^k(\nu_1, \nu_2, \ldots, \nu_n), \quad (1)$$

где ν_j – количественная мера j-го свойств защищаемого компонента в текущий момент времени, j=1,…, k. В качестве вероятностно-временной характеристики $\bar{p}_z^k$, k=0, 1, 2, …, может использоваться вероятность достижения соответствующей степени защищенности информации в системе P_k, k=0, 1, 2, …, в состоянии b_k, k=0, 1, 2, … [5, 14].

Переход системы из состояния b_k в состояние b_{k+1}, k=0, 1, 2, …, совершается в результате включения комплекта средств защиты S_k, k=0, 1, 2, …, по соответствующим управляющим командам. Состояние системы определяется не только количеством средств защиты S_k, но и ее состоянием в предыдущий момент времени b_{k-1}, а уровень защищенности информации характеризуется функциональной зависимостью

$$\bar{p}_z^{k+1} = F(\bar{p}_z^k, S_k). \quad (2)$$

Степень защиты системы связи и управления в состоянии b_k, k=0,1,2,…, также может определяться на основе предъявления запросов и анализа реакции на них. Она характеризуется показателем соответствия информации о состоянии защищенности системы, содержащейся в ответе на k – й запрос, эталонному описанию защищенного объекта

$$\bar{p}_z^k = F(X_k, X'_k), \quad (3)$$

где X_k и X'_k – ответ на запрос и эталонная информация о состоянии защищаемого объекта соответственно.

При формировании ответов на запросы, которые можно представить в виде дискретных операций, степень защиты характеризуется оценкой $\hat{P}_k$ вероятности реализации целевой функции P_k, k=0, 1, 2, …, определяемой по правилу

$$\hat{P}_k = m/N, \quad (4)$$

где m – число положительных ответов, N – количество запросов kn($N \le kn$).

Содержание запросов зависит от уровня иерархии системы. В тривиальном случае защищаемый объект может ответить на запрос положительно или отрицательно и $\hat{P}_k$, k=0, 1, 2, …, принимает значение «0» или «1» соответственно.

При рассмотрении абстрактной совокупности объектов с тождественными свойствами величина P_k, k=0, 1, 2, …, представляет собой вероятность того, что какой-либо объект даст положительный ответ на k-й запрос; она будет определяться как относительное число объектов, давших положительный ответ на k-й запрос.

Определение вероятности достижения объектом требуемого уровня защищенности имеет вид [3]

$$P_k(t)=1-n_0(t)/N, \quad (5)$$

где $n_0(t)$ – число отрицательных ответов, выданных за время $t \in (t_k, t_{k+1})$ на N запросов, t_k – время перехода объекта в состояние b_k, k=0, 1, 2, …

Кроме того, в качестве одного из вариантов оценки уровня защищенности можно использовать систему баллов [3, 6]. Для этого необходимо установить ранг каждого запроса и в соответствии с ним анализировать ответы.

Оценка вероятности того, что объект имеет требуемый уровень защиты, вычисляется следующим образом

$$\hat{P}_k = l/N, \quad (6)$$

где l – количество баллов, набранных объектом, по N – балльной системе.

Базовыми компонентами модели динамического управления ПБЗИ системы связи и управления являются блоки имитации защищаемого объекта и управляющей системы, охваченные линиями обратной связи. Структурная схема модели приведена на рис. 1.

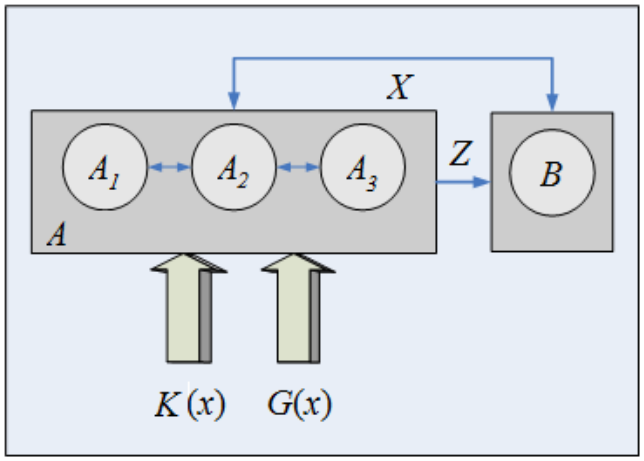

Рис. 1. Структурная схема модели динамического управления ПБЗИ системы связи и управления

В ней приняты следующие обозначения: A – управляющая система, A_1 – информационно-логическое устройство для обработки ответов на запросы и передачи результатов на решающее устройство, A_2 – решающее устройство, обрабатывающее информацию по защите объекта, A_3 – источник управляющей информации (запросов), B – защищаемый объект, $K(x)$ – закон классификации каждого ответа по признакам идентификации [17-19], $G(x)$ – функция, определяющая стратегию поведения управляющей системы в зависимости от ответов на запросы, x – переменная, характеризующая структуру и содержание ответов. Решение, вырабатываемое устройством A_2, является основой для выдачи управ-

ляющего воздействия, определяющего состав средств защиты S_k, k=0, 1, 2, …

Действие управляющей системы A осуществляется следующим образом. В момент времени t_0 блок A_3 выдает управляющее воздействие Z_0 на объект, который переходит из состояния b_0 в состояние b_1. Степень защиты объекта определяется ответом x_0, сравниваемым с эталонным значением x_0^* в блоке контроля A_1. В дальнейшем управляющая система периодически вырабатывает запрос Z_k, k≥1. Объект B формирует ответы x_i на полученные запросы. Величина ошибки, содержащейся в ответе x, совместно с функциями $K(x)$ и $G(x)$ определяет уровень защищенности объекта и через блоки A_2 и A_3 формирует новое управляющее воздействие Z_k, k≥2.

Для синтеза устройств в виде конечных автоматов, выполняющих функции блоков A_1 и A_2, структура ПБЗИ может быть представлена в виде графа, узлами которого являются пункты управления защитой информации, оконечными вершинами – средства защиты, а дугами – логические каналы информационного взаимодействия средств защиты между собой и со средствами ИТВ, возникающие в процессе функционирования ПБЗИ и управления ее функционированием.

Каждое из средств защиты может находиться в двух устойчивых состояниях:

1) исправное состояние, в котором ПБЗИ сохраняет свою работоспособность, не имеет повреждений, дефектов, в работе системы связи и управления отсутствуют сбои и аварии, обусловленные ИТВ;
2) состояние отказа, характеризуемое нарушением работоспособности ПБЗИ в результате повреждения или несоответствия характеристик средств защиты установленным значениям).

Контроль ПБЗИ заключается в последовательном применении тестов по проверке отдельных функций средств защиты.

Процессы управления средствами защиты в ПБЗИ могут быть представлены в виде замкнутого технологического цикла, состоящего из связанных по целям и результатам фаз.

Модель технологического цикла управления ПБЗИ системы связи и управления представлена на рис. 2.

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

Цикл контроля объединяет фазы формирования первичной информации о состоянии средств защиты, ее передачи в центр управления безопасностью информации (ЦУБИ), обобщения и обработки, а принятия решения в условиях неполноты анализа и априорной неопределенности обстановки.

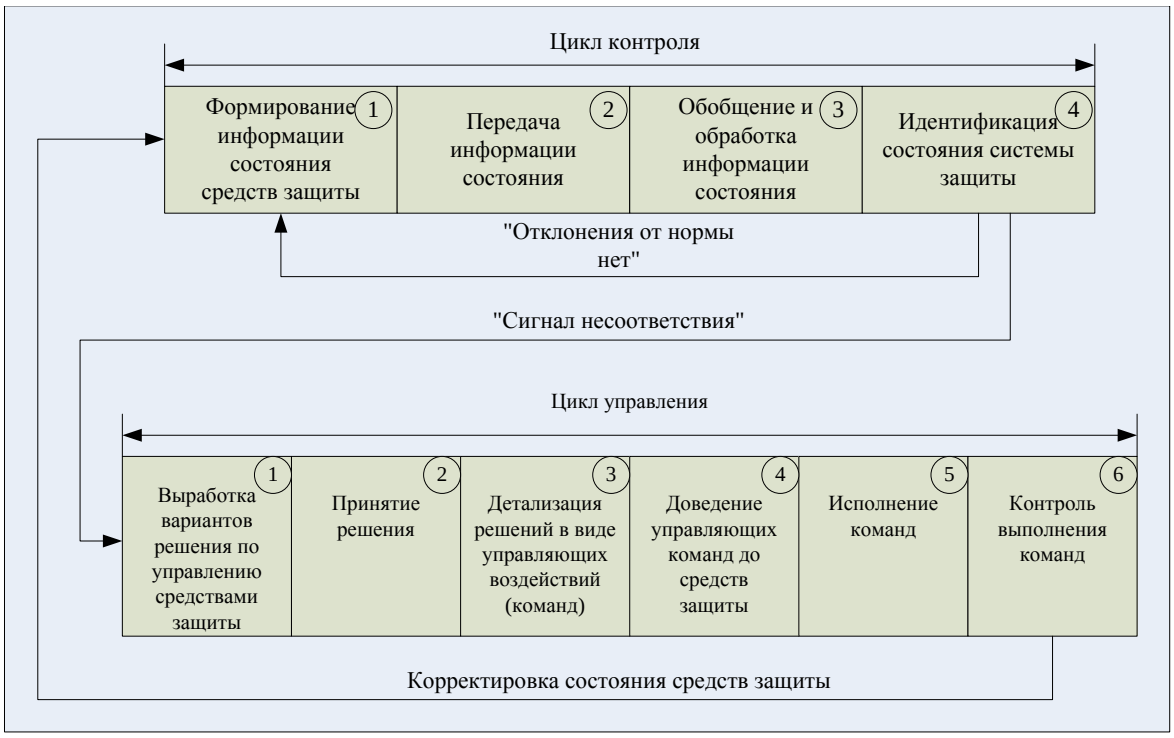

Рис. 2. Модель технологического цикла управления ПБЗИ системы связи и управления

Контроль состояния подсистемы безопасности и защиты информации системы связи и управления

Контроль состояния средств защиты проводится в целях проверки работоспособности ПБЗИ и выявления средств защиты в состоянии отказа.

Для комплексной проверки средств защиты и управления применяется глобальный зондовый тест ПБЗИ.

Процедура контроля средств, для которых зафиксировано событие нарушения работоспособного состояния, включает множество тестов. Исход теста считается успешным, если в проверяемом подмножестве средств защиты не обнаружено неисправных программно-аппаратных компонентов, обеспечивающих формирование сообщений с заранее определенной структурой и их выдачу в адрес ЦУБИ или соответствующих автоматизированных рабочих мест (АРМ) обеспечения безопасности информации (ОБИ).

Совокупность тестов, достаточных для выполнения процедуры контроля средств защиты, можно задать матрицей, строки которой соответствуют тестам контроля, а столбцы – средствам защиты.

Эффективность контроля ПБЗИ достигается при условии превышения вероятностью $P_b(\Delta R, \Delta t)$ того, что существенные отклонения показателей защищенности ΔR не останутся не выявленными в течение интервала времени Δt, заданного значения P'_b при минимальных расходах C_k, k=0, 1, 2,…, на организацию контроля:

$$P_b(\Delta R, \Delta t) \geq P'_b;\ C_k \rightarrow \min,\ k=0, 1, 2,\ldots \qquad (7)$$

Если по каким-либо причинам ресурсы на организацию контроля средств защиты ограничены значением C'_k, k=0, 1, 2,…, то суть решения поставленной

задачи заключается в разработке процедуры проверки средств защиты с использованием тестов, при которой

$$C_k \le C'_k,\ k=0, 1, 2,\ldots,\ P_b(\Delta R, \Delta t) \to \max. \quad (8)$$

При таком подходе сущность контроля состояния средств защиты с использованием глобального зондового теста заключается в образовании замкнутых маршрутов, покрывающих все вершины графа и проходящих через вершину, являющуюся генератором зондов. Зондовым тестом является пилотное сообщение, передающееся по сети через определенные интервалы времени по замкнутому маршруту, который заканчивается в узле-генераторе тестов.

Реализация безадресного зондирования обеспечивает полноту контроля состояния ПБЗИ. Такая технология контроля позволяет узлам, через которые проходят тестовые зонды, отслеживать состояние той части ПБЗИ, информация о которой записана в проходящих зондах.

Наиболее сложной в цикле контроля является фаза идентификации состояния ПБЗИ системы связи и управления [17, 18]. Результатом идентификации является определение необходимости корректировки мер защиты на основе данных о текущих значениях показателей защищенности информации в системе.

Таким образом, пункт управления безопасностью (ЦУБИ или АРМ ОБИ) и датчики состояния средств защиты работают постоянно, а информация об их состоянии передается через определенные кванты времени или при изменении состояния до пределов допустимого [5, 19].

Состояние ПБЗИ классифицируется по областям значений, которые принимает функция безопасности информации R с аргументами в виде показателей защищенности информации в n элементах K_i, $i=1,\ldots, n$.

Сигнал $q(R)$, характеризующий несоответствие состояния ПБЗИ требуемому, определяется условиями:

- $q(R)=0$, если результаты контроля состояния ПБЗИ K_i, $i=1,\ldots, n$, соответствуют заданным требованиям;
- $q(R)=1$, если указанное соответствие не установлено.

При определении значений сигнала несоответствия $q(R)$ требуемые параметры состояния средств защиты характеризуются интервальными значениями

$$K_{1i} \le K_i \le K_{2i}, \quad (9)$$

где $K_{1i}=K_i(1-\Delta_{i1})$, $K_{2i}=K_i(1+\Delta_{i2})$, $\Delta_{i1[2]}$ – интервалы допустимых значений, $i=1,\ldots, n$.

При принадлежности параметра состояния K_i, $i=1,\ldots, n$, диапазону значений $[K_{1i}; K_{2i}]$ требования по безопасности информации выполняются полностью, т.е. $q(R)=0$. При нахождении параметра состояния в допустимом диапазоне безопасности информации считается, что уровень защищенности снизился, но сигнал тревоги не вырабатывается, т.е. по-прежнему $q(R)=0$. Значение $q(R)=1$ вырабатывается только при выходе K_i, $i=1,\ldots, n$, за пределы допустимого диапазона. С помощью величин $\Delta_{i1[2]}$, $i=1,\ldots, n$, можно регулировать скорость реакции пункта управления безопасностью на изменения в обстановке. По мере уменьшения интервалов допустимых значений $\Delta_{i1[2]}$, $i=1,\ldots, n$, повышается точность сведений о поведении параметров состояния [15].

Схема формирования сигнала $q(R)$ приведена на рис. 3. На ней выделены три зоны, характеризующие состояние объекта защиты:

- норма;
- критическое состояние;
- тревога.

Сигнал $q(R)$ формируется как разность двух составляющих, характеризующих принадлежность K_i, $i=1,\ldots,n$, требуемому q_0 и допустимому q_1 диапазонам. Его выработка инициирует выполнение цикла управления, в котором осуществляется корректировка состояния средств защиты информации.

Цикл управления безопасностью информации включает шесть фаз:

1) выработка вариантов решения по управлению средствами защиты информации;
2) принятие решения по управлению ПБЗИ для предотвращения утечки информации или минимизации возможного ущерба из-за обнаруженного факта несанкционированного доступа к ресурсам защищаемого объекта;
3) детализация решения в виде последовательности команд, направленных на изменение режимов работы средств зашиты;
4) доведение команд управления до средств защиты;
5) исполнение команд управления;
6) контроль выполнения команд управления.

Функция безопасности R связана с параметрами состояния средств защиты цикла контроля.

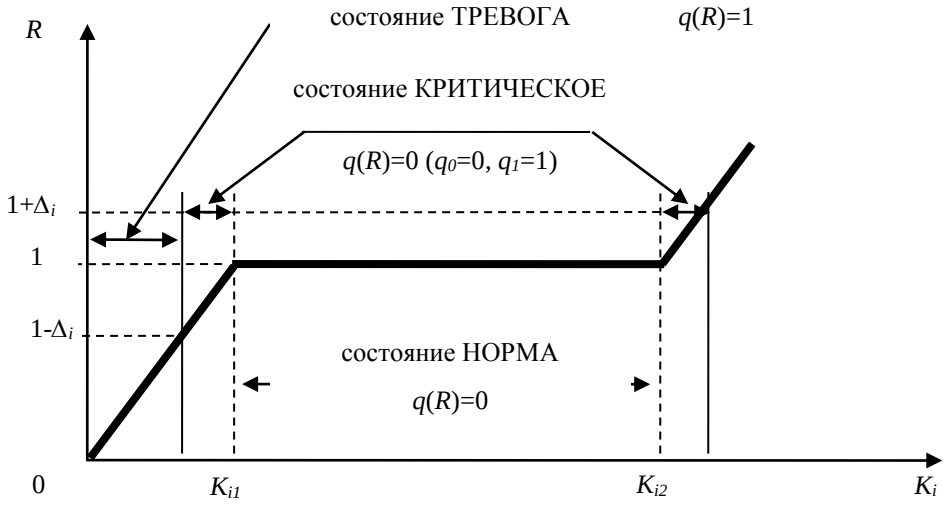

Рис. 3. Схема формирования сигнала $q(R)$
в ПБЗИ системы связи и управления

Ситуация становится критической, если значения параметров состояния средств защиты приближаются к границе интервала $[K_{1i}; K_{2i}]$, $i=1,\ldots,n$. В ситуации, когда значение хотя бы одного показателя K_i, $i=1,\ldots,n$, выходит за пределы допустимого диапазона, то формируется сигнал «тревога».

Ввиду того, что каждый показатель K_i, i=1,…, n, ограничен собственным диапазоном допустимых значений, его можно привести к нормализованному виду

$$K_i''=\frac{2\left|K_i-K_i^m\right|}{K_{1i}\left(1-\Delta_{i1}\right)+K_{2i}\left(1+\Delta_{i2}\right)},\ i=1,\ldots,n, \qquad (10)$$

где

$$K_i^m=\frac{K_{1i}\left(1-\Delta_{i1}\right)+K_{2i}\left(1+\Delta_{i2}\right)}{2},\ i=1,\ldots,n.$$

Показатель K_i'', i=1,…, n, определен на интервале значений [0; 1], его можно рассматривать как величину относительных потерь безопасности.

Показатель K_i, i=1,…, n, не может принимать значения $K_{1i}(1-\Delta_{i1})$ и $K_{2i}(1+\Delta_{i2})$, поэтому ситуация $2|K_i-K_i^m|=K_{1i}(1-\Delta_{i1})+K_{2i}(1+\Delta_{i2})$, невозможна, следовательно, диапазон изменения K_i, i=1,…, n, открыт справа.

Согласно [20], выбор варианта управления средствами защиты можно осуществить на основе меры близости относительных потерь безопасности к предельным значениям.

При этом в ситуации, когда $K_i''\to 1$, i=1,…, n, необходимо минимизировать величину $(1-K_i'')^{-1}$ только для фиксированного порядкового номера параметра состояния системы, что эквивалентно минимаксным моделям. Если относительные потери значительно меньше единицы, то данная модель будет эквивалентна модели интегральной оптимизации [3].

Минимизация выбранного решения для ПБЗИ системы связи и управления критически важного объекта должна осуществляться автоматически в виде последовательности команд управления [1]. Каждая команда включает управляющую часть и служебную информацию, в которых содержатся сведения о режимах работы средств защиты, подлежащих реализации при получении команды [3, 12].

Фазы доведения команд до средств защиты, исполнения команд и контроля полученного результата выполняются по аналогии с соответствующими фазами типовых циклов управления технических устройств [5, 6, 14].

Выводы

С использованием методов теории конфликта, теории графов и математической статистики разработана модель ПБЗИ системы связи и управления критически важного объекта. В модели воспроизводятся адаптивные механизмы управления компонентами ПБЗИ и средств ИТВ с активными обратными связями для определения ресурсов сторон, требуемых для защиты и нарушения нормального устойчивого функционировании системы связи и управления. Анализ процессов взаимодействия программных и технических средств системы связи и управления между собой и со средствами ИТВ позволяет обосновать рациональные стратегии функционирования ПБЗИ и средств ИТВ в соответствии с целевыми функциями.

Процессы управления средствами защиты в ПБЗИ могут быть представлены в виде замкнутого технологического цикла, состоящего из взаимосвязанных циклов контроля средств защиты и управления ими. Цикл контроля средств защиты включает в себя фазы выработки вариантов и принятия решения по управлению средствами защиты, детализации решений в виде управляющих воздействий (команд) и доведения этих команд до средств защиты; цикл управления отводится для исполнения команд и контроля их исполнения.

Контроль состояния средств защиты проводится в целях проверки работоспособности ПБЗИ и выявления средств защиты в состоянии отказа с применением глобального безадресного зондового теста ее структуры.

Наиболее сложной в цикле контроля является задача идентификации состояния ПБЗИ системы связи и управления, по результатам решения которой определяется необходимость корректировки мер защиты на основе данных о текущих значениях показателей защищенности информации.

Выбор рационального варианта управления средствами защиты требуется осуществить на основе меры близости относительных потерь безопасности к предельным значениям. При малых потерях информации модель адаптивного управления средствами защиты системы связи и управления эквивалентна модели интегральной оптимизации ее ПБЗИ.

Литература

1. Макаренко С. И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. – СПб.: Наукоемкие технологии, 2017. – 546 с.

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. Логико-вероятностно-информационный подход к моделированию информационной безопасности объектов защиты. – Воронеж: Воронежский государственный архитектурно-строительный университет, 2016. - 123 с.

4. Максимов Р. В., Павловский А. В., Стародубцев Ю. И. Защита информации от технических средств разведки в системах связи и автоматизации. – СПб.: ВАС, 2007. – 88 с.

5. Хорошко В. А. Методы и средства защиты информации. – М.: Юниор, 2003. – 504 с.

6. Жидко Е. А. Научно-обоснованный подход к классификации угроз информационной безопасности // Информационные системы и технологии. 2015. № 1 (87). С. 132-139.

7. Жидко Е. А., Попова Л. Г. Информационная безопасность модернизируемой России: постановка задачи // Информация и безопасность. 2011. Т. 14. № 2. С. 181-190.

8. Современная радиоэлектронная борьба. Вопросы методологии / Под ред. В.Г. Радзиевского – М.: Радиотехника, 2006. – 424 с.

9. Жидко Е. А., Попова Л. Г. Информационная и интеллектуальная поддержка управления развитием социально-экономических систем // Вестник Иркутского государственного технического университета. 2014. № 10 (93). С. 12-19.

10. Жидко Е. А., Попова Л. Г. Человеческий фактор как аргумент информационной безопасности компании // Информация и безопасность. 2012. Т. 15. № 2. С. 265-268.

11. Жидко Е. А. Методические основы системного моделирования информационной безопасности // Интернет-журнал «Науковедение». 2014. № 3. – URL: http://naukovedenie.ru/PDF/68TVN314.pdf (дата обращения 27.01.2016).

12. Антипов О. И., Неганов В. А, Потапов А. А. Детерминированный хаос и фракталы в дискретно-нелинейных системах. – М.: Радиотехника, 2009. – 235 с.

13. Жидко Е. А. Логико-вероятностно-информационный подход к формированию единого алгоритма исследований информационной безопасности объектов защиты // Системы управления, связи и безопасности. 2016. № 1. С. 262-277.

14. 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.

15. Лебедев Б. К. Методы поисковой адаптации для решения оптимизационных задач // Прикладные информационные технологии и интеллектуальные системы. 2003. № 3. С. 24-30.

16. Сазонова С. А. Оценка надежности работы сетевых объектов // Вестник Воронежского института высоких технологий. 2016. № 1 (16). С. 40-42.

17. Разиньков С. Н., Решетняк Е. А. Многоальтернативное отождествление объектов с оценкой максимального правдоподобия однотипных параметров // Физика волновых процессов и радиотехнические системы. 2014. Т. 17. № 3. С. 67-73.

18. Разиньков С. Н., Решетняк Е. А. Оптимальное и квазиоптимальное отождествление объектов при структурно-системном мониторинге обстановки // Физика волновых процессов и радиотехнические системы. 2015. Т. 18. № 3. С. 42-47.

19. Железняк В. К. Защита информации от утечки по техническим каналам. – СПб: Государственный университет аэрокосмического приборостроения, 2006. – 188 с.

20. Валдайцев С. В. Антикризисное управление на основе инноваций: учебное пособие. – СПб.: Изд-во С.-Петерб. ун-та, 2001. – 232 с.

References

1. Makarenko S. I. *Informacionnoe protivoborstvo i radioelektronnaya bor'ba v setecentrischteskich voyinach naschtala XXI veka* [Information confrontation and radio-electronic fight in network-centric wars of the beginning of the XXI st century]. Saint-Petersburg, Naukoemkie tekhnologii, 2017. 546 p. (in Russian).

2. Davydov A. E., Maksimov R. V., Savickiy O. K. *Zaschita i bezopasnost' vedomstvennych integrirovannych infokommunikacionnych system* [Protection and safety of the departmental integrated information and communication systems]. Moscow, Voentelecom, 2017. 536 p. (in Russian).

3. Zhidko E. A. *Logiko veroyatnostno-informacionnyj podhod k modelirovaniyu informacionnoj bezopasnosti ob'ektov zashchity* [Logical probability-information approach to modeling information security of protection objects]. Voronezh, Voronezh State University of Architecture and Civil Engineering Publ., 2016. 123 p. (in Russian).

4. Maksimov R. V., Pavlovskiy A. V., Starodubcev Yu. I. *Zaschita informacii ot tchnischteskich sredstv razvedki v sistemach svyazi i avtomatizacii* [Information security from technical means of investigation in communication systems and automation]. Saint-Petersburg, Military Academy of the Signal Corps, 2007. 88 p. (in Russian).

5. Horoschko V. A. *Metody i sredstva zaschity informacii* [Methods and means of information protection]. Moscow, Junior, 2003, 504 p. (in Russian).

6. Zhidko E. A. Research-based Approach to the Classification of Threats to Information Security. *Information systems and technologies*, 2015, vol. 87, no. 1, pp. 132-139 (in Russian).

7. Zhidko E. A., Popova L. G. Information security modernized Russia: problem formulation. *Information and security*, 2011, vol. 14, no. 2, pp. 181-190 (in Russian).

8. *Sovremennaja radiojelektronnaja bor'ba. Voprosy metodologii* [Modern electronic warfare. Issues of methodology]. Moscow, Radiotekhnika, 2006, 424 p. (in Russian).

9. Zhidko E. A., Popova L. G. Information and Intellectual Support of Management of Development of Socio-Economic Systems. *Bulletin of Irkutsk State Technical University*, 2014, vol. 93, no. 10, pp. 12-19 (in Russian).

10. Zhidko E. A., Popova L. G. The human factor as an argument information security company. *Information and security*, 2012, vol. 15, no. 2, pp. 265-268 (in Russian).

11. Zhidko E. A. Methodological foundations of systems modeling of information security. *Naukovedenie*, 2014, vol. 22, no. 3. Available at: http://naukovedenie.ru/PDF/68TVN314.pdf (accessed 27 January 2016) (in Russian).

12. Antipov O. I., Neganov V. A., Potapov A. A. *Determinirovannyj haos i fraktaly v diskretno-nelinejnyh sistemah* [Deterministic chaos and fractals in discrete-nonlinear systems]. Moscow, Radiotekhnika, 2009, 235 p. (in Russian).

13. Zhidko E. A. Logical-and-probabilistic-informational approach to the formation of a unified algorithm of research of information security protection. *Systems of Control, Communication and Security*, 2016, no. 1, pp. 262-277 (in Russian).

14. Tolstykh N. N., Pyatunin A. N., Mareychenko I. V., Pavlov V. A. A study of the conflict of information systems by methods of the theory of coordination *Information and security*, 2004, no. 1, pp. 84-85 (in Russian).

15. Lebedev B. K. Search methods adaptation for the solution of optimization problems and. *Applied information technologies and intellectual systems*, 2003, no. 3, pp. 24-30 (in Russian).

16. Sazonova S. A. Evaluation of the reliability of network objects *Vestnik Voronezhskogo instituta vysokikh tekhnologii*, 2016, no. 1 (16), pp. 40-42 (in Russian).

17. Razin'kov S. N., Reschetnyak E. A. Multi-alternative identification of objects with maximum likelihood estimation of homogeneous parameters. *Fizika volnovykh protsessov i radiotekhnicheskie sistemy*, 2014, vol. 17, no. 3, pp. 67-73 (in Russian).

18. Razin'kov S. N., Reschetnyak E. A. Optimal and quasi-optimal identification of objects in structural and system monitoring of the situation. *Fizika volnovykh protsessov i radiotekhnicheskie sistemy*, 2015, vol. 18, no. 3, pp. 42-47 (in Russian).

19. Zheleznyak V. K. *Zaschita informacii ot uteschtki po technischteskim kanalam* [Protection of information from leaks through technical channels]. Saint-Petersburg. State University of Space Instrument Making, 2006. 188 p. (in Russian).

20. Valdaytsev S. V. *Antikrizisnoye upravleniye na osnove innovaciy.* [Anti-crisis management through innovation]. Saint-Petersburg, Saint-Petersburg University Publ, 2001. 232 p. (in Russian).

Статья поступила 14 марта 2018 г.

Информация об авторах

Жидко Елена Александровна – кандидат технических наук, доцент. Профессор кафедры управления повседневной деятельностью подразделений. Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е Жуковского и Ю.А. Гагарина» (Воронеж). Область научных интересов: методы и средства обеспечения устойчивого развития, экологическая и информационная безопасность критически важных объектов. E–mail: lenag66@mail.ru

Разиньков Сергей Николаевич – доктор физико-математических наук, старший научный сотрудник. Ведущий научный сотрудник Научно-исследовательского испытательного института (радиоэлектронной борьбы). Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е Жуковского и Ю.А. Гагарина» (Воронеж). Область научных интересов: методы и средства информационного противоборства в сфере связи и управления, способы информационно-технических воздействий на информационно-управляющие системы. E–mail: razinkovsergey@rambler.ru

Адрес: 394052, г. Воронеж, ул. Старых Большевиков 54а.

Model of Security and Information Protection Subsystem of a Communication and Control System of a Critical Object

E. A. Zhidko, S. N. Razinkov

Formulation of the Problem. *The developers of communication and management systems have to improve means and methods of information confrontation for increasing their conflict stability and operational reliability. The main difficulties in ensuring the security and protection of information are due to the presence of intelligent components in modern means of information and technical influences that allow to change adaptively structural features and to adjust the targets of the impact. Measures to protect information are selected from the conditions of minimizing the time of detection of an element with destructive functions and achieving the required quality of resource management. The task of selecting such measures, can be solved on the basis of modeling the security subsystem and protecting the information of the communication and management system and investigating its properties in the presence of a conflict component.* ***The aim of the paper is*** *building a model of the security subsystem and protecting the information of the communication system and the management of a critical object.* ***Used Methods.*** *The model of the subsystem of security and information system of communication and management in the context of malicious information and technical influences is constructed by using the methods of conflict theory, graph theory and mathematical statistics. The technological cycle of resource management to identify and neutralize destructive elements is justified with using methods of the theory of identification and making decisions under conditions of a priori uncertainty of the situation.* ***Result.*** *A model of the security and information protection subsystem of a critical object is developed. According to the results the phases of the technological cycle of resource management of combating information and technical impact are determined.* ***Practical significance.*** *The ways of realization and characteristics of information protection means, methods of adaptive management of external surroundings parameters in case of conflict interaction of the communication and management system with malicious influences means are substantiated.*

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

Information about Authors

Elerna Aleksandrovna Zhidko – Ph.D. of Engineering Sciences, Docent. Professor at the Department of day-to-day activities of the departments. Military Educational and Scientific Center of the Air Force «The Air Force Academy named after Professor N.Ye. Zhukovsky and Yu.A. Gagarin» (Voronezh). Field of research: methods and means for ensuring sustainable development, environmental and information security, critical asset systems. E–mail: lenag66@mail.ru

Sergey Nikolaevich Razinkov – Dr. habil. of Physico-mathematical Sciences, Docent. Senior Research assistant of the Research test center of radio-electronic struggle. Military Educational and Scientific Center of the Air Force «The Air Force Academy named after Professor N.Ye. Zhukovsky and Yu.A. Gagarin» (Voronezh). Field of research: methods and means of information confrontation in the field of communication and management, ways of information and technical impacts on information management systems. E–mail: razinkovsergey@rambler.ru

Address: Russia, 394064, Voronezh, Starych Bolschevikov str. 54a.