УДК 004.684: 621.381

Владимир Алексеевич Хорошко,
Наталья Борисовна Дахно

ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ИНФОРМАЦИИ

Введение

При создании систем обработки и хранения информации, информационно-вычислительных сетей различного назначения одной из основных задач является обеспечение безопасности информации. При этом под безопасностью информации понимают такое состояние хранимой, обрабатываемой и передаваемой информации, при которой невозможно их случайное преднамеренное раскрытие, изменение или уничтожение [1; 2]. Безопасность информации обеспечивается и поддерживается комплексом программно-аппаратных средств защиты, которые выполняют свои функции в тесном взаимодействии с основными компонентами систем обработки и хранения информации (СОХИ). Совокупность этих средств образует систему защиты информации (СЗИ), с одной стороны, средства защиты являются общественными ресурсами СОХИ, а с другой стороны, в силу специфики решаемых задач СЗИ может быть представлена в виде самостоятельной внутрисистемной структурой, которая нуждается в собственном управлении. При этом основным назначением подсистемы управления средствами защиты является координация всех процессов, выполняющихся в СОХИ в интересах обеспечения безопасности информации.

Цель статьи — определить принципы построения системы управления безопасностью информации. ***Задачи*** статьи: 1) определить основные направления управления комплексом средств обеспечения безопасности информации; 2) привести формализованное описание правил защиты информации от несанкционированного доступа; 3) рассмотреть назначение и функциональную схему центра управления безопасностью, а также абстрактный граф алгоритма принятия решения.

Задачи управления можно разбить на два класса взаимосвязанных частных задач. К первому классу относится компенсация нарушений функционирования системы защиты, которые возникают в результате отказа каких либо элементов системы или при воздействии на систему злоумышленника. Здесь необходимо учитывать возможность преднамеренного нарушения целостности и непротиворечивости распределенной между элементами системы служебной информации, нарушения безопасности ключей и паролей [3], что связано с определением допустимого времени их использования, а также возможность потери или частичного искажения служебной информации в результате отказов аппаратных или программных средств элементов системы защиты. Кроме того, необходимо учитывать изменения уровней (вплоть до полной потери) работоспособности отдельных элементов системы защиты или нарушение связей между ними.

Основная часть

Рассматриваемые нарушения могут быть разделены по виду на внешние и внутренние. Внешние являются следствием целенаправленной деятельности злоумышленника с целью получения несанкционированного доступа к защищенной информации или изменения режимов работы системы защиты. При рассмотрении нарушений этого вида можно говорить о живучести системы защиты [4]. Внутренние нарушения являются следствием скрытых дефектов элементов системы защиты или связей между ними и проявляются случайным образом в процессе эксплуатации. К задачам второго класса относятся координация временных и точностных условий функционирования элементов системы защиты, синхронизация на основе значения ключей и паролей, синхронизация и управление последовательностью операций по контролю доступа и ресурса СОХИ и контроля их использования, изме-

нения состава используемых и текущих моментов времени элементов системы за счет включения резервных и отключения отказавших, изменения режимов функционирования элементов системы при изменении условий применения СОХИ.

Реализация рассмотренных задач возможна лишь при наличии единой системы управления, охватывающей все функциональные элементы системы защиты. При этом основные функции системы управления выполняются центром управления опасностью информации в СОХИ, который может размещаться на территории центра управления системой.

Рассмотрим как совокупность абонентских систем, объединенных сетью передачи информации, работает. Абонентские системы представляют собой ПЭВМ, выполняющие функции обработки или хранения информации. Каждая абонентская система может быть представлена в виде множества информационных вычислительных ресурсов и множества прикладных процессов, причем прикладные процессы являются абонентами СОХИ и для выполнения функций используют распределение в сети ресурсы. Ресурсом может быть любая сервисная функция, устройство, включенное к абонентской системе, база данных или любой файл в базе, а также любой процесс, выполняющийся в абонентской системе. При этом все ресурсы могут быть разделены на активные, которые для выполнения собственных функций используют другие ресурсы СОХИ, и пассивные (объекты), которые участвуют в выполнении каких-либо функций под управлением активных ресурсов. Необходимо отметить, что объект может быть пассивным в один момент времени и активным в другой. Абонентские системы подключаются к сети передачи информации через абсолютные комплекты, которые обычно реализуют функции противодействия нижних пяти уровней эталонной модели взаимодействия открытых систем [5].

Средства обеспечения безопасности информации можно разделить на два основных класса: локальные средства, являющиеся принадлежностью абонентских систем, и сетевые средства защиты, выполняющие свои функции в тесном взаимодействии с протоколами уравнения передачей информации в сети. Локальные средства защиты выполняют проверку возможности доступа абонента к запрашиваемому ресурсу, а сетевые обеспечивают управление потоками защищенной информации в сети.

Формализовать традиционные подходы возможно следующим образом. Пусть X — вектор угроз

$$X = (x_1,\ x_2,\ \ldots,\ x_n) \qquad (1)$$

где n — число угроз.

Для обеспечения защиты формируется вектор Y, который отражает реализуемый комплекс защитных мер.

$$Y = (y_1,\ y_2,\ \ldots,\ y_n) \qquad (2)$$

Для каждой угрозы и соответствующей защитной меры формируется функция $f_i(x_i,\ y_i)$. Определим, что $f_i(x_i,\ y_i) \le 0$, если защитные меры нейтрализуют i-тую угрозу, и $f_i(x_i,\ y_i) > 0$ — в противном случае. Система считается защищенной, если для каждой угрозы $f_i(x_i,\ y_i) \le 0$.

Отметим, что данная модель является весьма упрощенной и приведена для оценки существующих подходов к обеспечению информационной безопасности СОХИ. Более развитые модели учитывают вероятность появления той или иной угрозы, влияние применяемой защитной меры на нейтрализацию двух и более угроз и т.п.

Приведенная модель позволяет продемонстрировать следующие ограничения традиционных подходов к обеспечению безопасности СОХИ.

Во-первых, задание перечня угроз для конкретной системы является достаточно нетривиальной задачей. С одной стороны, при сокращенном перечне угроз сокращается перечень защитных мер, что приводит к ослаблению защиты системы. С другой стороны, увеличение перечня угроз может привести к нерациональным затратам. Выходом из создавшейся ситуации могла бы быть некая оптимальная модель, но применительно к защите государственных секретов такой подход отвергался принципиально.

Во-первых, если следовать принципу невозможности создания абсолютной системы защиты, даже по выделенному перечню угроз можно говорить только об относительной защищенности. [6].

Практическая реализация изложенного подхода приводит к тому, что для каждой угрозы задается коэффициент “опасности”. В этом случае вектор X может быть представлен как

$$X = (a_1 x_1,\ a_2 x_2,\ \ldots,\ a_n x_n)$$

где a_i — коэффициент “опасности” i-той группы.

Введение указанных коэффициентов позволяет сформировать перечень актуальных угроз и в определенной мере решить оптимизационную задачу по соотношению защищенности системы и затрат на ее обеспечение.

Обобщая приведенные рассуждения, можно утверждать, что традиционные подходы к обеспечению информационной безопасности СОХИ основываются на определенной формализации и обобщении экспертных знаний. Если перечень закрытых

мер перекрывает перечень угроз из модели, считается, что система имеет удовлетворительный уровень защиты. Несмотря на слабое теоретическое обоснование, защиту большинства систем можно считать удовлетворительной. Вместе с тем данный подход к обеспечению информационной безопасности приводит к тому, что оценка защищенности для одной и той же СОХИ может иметь "колебательный" характер: при выявлении новой уязвимости система становится незащищенной, после выхода и применения обновления система снова считается защищенной. В результате, если совсем утрировать, то чем меньше у нас знаний о том, как можно "сломать" систему, тем больше она считается защищенной. В результате понятие защищенность начинает носить субъективный характер.

В результате приведенных рассуждений приходим к выводу, что обеспечение информационной безопасности СОХИ на основе реализации установленного перечня требований является удовлетворительным решением только в условиях незначительно изменяющегося перечня угроз на основе традиционных подходов достаточно трудно не только оценить текущую защищенность системы, но и спрогнозировать ее на ближайшую перспективу.

Для решения указанных противоречий предлагается подход к обеспечению информационной безопасности СОХИ, основанный на контроле качества управления безопасность, реализуемого в СОХИ. Возможность применения подобного подхода основывается на том, что любая СОХИ, в том числе требующая обеспечения информационной безопасности, является элементом системы управления безопасностью информации, реализующим функциональную задачу.

Введение в СОХИ систему управления безопасностью информации (СУБИ) приводит к появлению звена с передаточной функцией $W_{\text{сохи}}(S)$. Реализация различного угроз применительно к СОХИ в контуре управления приводит к тому, что передаточная функция изменяется на $W_{\text{сохи}}(S)^*$. Это в свою очередь приводит к тому, что полезный сигнал $S^*(t)$ на выходе системы отличается отличается от сигнала при отсутствии угроз.

Таким образом, реализация угроз информационной безопасности может быть описана как особого рода помехи по управлению, что дает возможность использовать развитый аппарат теории автоматического управления.

Преимущества данного подхода — возможность использования интегрального показателя защищенности, носящего комплексный характер, а также развитого математического аппарата.

Разрешить эти противоречия можно только в случае если рассматривать защищенность СОХИ как функцию от времени. Обозначим ее как $D(t)$. Тогда если сравнивать качество управления СОХИ СУБИ в моменты времени t_1 и t_2, при штатных мерах по защите от угроз раскрытия параметров СУБИ и нарушения конфиденциальности, можно определить, ли эти меры лостаточными на интервале времени (t_1, t_2).

Необходимость образования отдельного функционального элемента системы управления безопасностью, который выполняет основные функции распределения ресурсов системы защиты регистрации абонентов СОХИ, генерации и рассылки служебной информации (паролей, ключей и т.д), контроля работы отдельных элементов и подсистем обеспечения безопасности, прежде всего обусловлена тем, что с увеличением числа элементов защиты, которые могут формировать и распространять служебную информацию, существенно увеличивается вероятность компроментации этой информации и соответственно снижается надежность всей системы защиты в целом [7]. Таким образом, основным элементом управления системой является ЦУБ, который оснащается комплексом специальных технологических и программных средств. Для реализации возложенных на ЦУБ функций в его состав должны входить средства вычислительной техники с достаточным объемом внешней и оперативной памяти и высоким быстродействием и автоматизированное рабочее место администратора службы обеспечения безопасности СОХИ. ЦУБ должна подключаться к сети передачи информации и взаимодействия с удаленными локальными и сетевыми элементами системы защиты.

В последнее время системы управления сложными распределенными системами, к которым с полным основанием может быть отнесена и система защиты информации в СОХИ, создаются с помощью методов и средств искусственного интеллекта [8].

Основным содержанием концепции построения интеллектуальных систем управления является использование введенных в систему и пополняемых в ходе функционирования знаний. Применение методов искусственного интеллекта позволяет существенно повысить эффективность управления такими объектами, как сети передачи информации [9]. Целесообразность использования искусственного интеллекта в ЦУБ обусловлена тем, что при отказе или нарушении работы каких-либо элементов системы защиты может возникнуть возможность

утечки информации, что недопустимо. Предотвращение утечки обеспечивается оперативным блокированием утечки СОХИ, которая содержит неисправный элемент системы защиты. Следовательно, ЦУБ должен постоянно проводить контроль функционирования элементов системы защиты, анализировать результаты этого контроля и оперативно реагировать на возникновение различного рода сбойных ситуаций независимо от природы их возникновения (случайных или преднамеренно создаваемых злоумышленником). Включение в контур управления оператора ЦУБ в качестве лица, принимающего решение по предоставляемой ему информации контроля, не позволяет достичь достаточной оперативности реакции на возможные нарушения. Таким образом, необходимо оснастить ЦУБ специализированной экспертной системой, которая выполняет функции оперативного управления системой защиты. Оператор ЦУБ в этом случае может влиять на процесс управления на любом этапе, введя операторные директивы с собственного терминала.

При функционировании средств защиты информации можно выделить быстропротекающие процессы, к которым можно отнести образование и рассасывание очередей в случайных базах информации при проверке атрибутов доступа к ресурсам СОХИ, медленные процессы измерения интенсивности потока запросов на реализацию защитных функций, а также очень медленные процессы старения ключевой и парольной информации [10]. Отслеживание и анализ протекания этих процессов также являются функциями экспертной системы.

Структура системы принятия решений по управлению средствами обеспечения безопасности информации (рис. 1) содержит множество функциональных компонентов, что позволяет максимально автоматизировать и ускорить процесс выработки управляющих воздействий при изменении ситуации в СОХИ.

Подсистема функционального контроля средств защиты информации предназначена для формирования и выдачи в СОХИ тестовых команд (запросов), направленных на проверку правильности работы тех или иных средств защиты. Результаты проверок собираются этой же подсистемой в реальном масштабе времени, что обеспечивает возможность оперативного реагирования на возникающие нарушения и атаки. Подсистема контроля является активной стороной при проведении проверок. Поступающая из СОХИ информация о результатах контроля используется для обновления знаний о текущем состоянии системы защиты и в совокупности с ретроспективными знаниями служат основой для выработки необходимых управляющих воздействий.

Блок интерпретации результатов контроля предназначен для преобразования

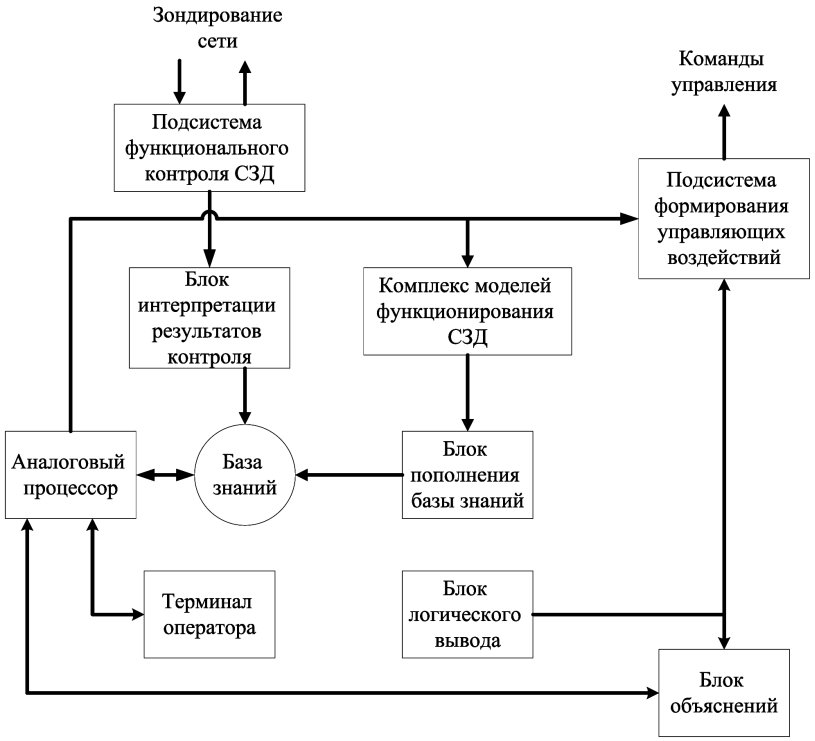

Рис. 1 Структура системы поддержки принятия решений по управлению средствами обеспечения безопасности информации в СОХИ

поступающей информации в форму представления в базе знаний и формирования исходной информации для моделирования работы системы защиты.

Комплекс моделей функционирования системы защиты информации на основании результатов контроля определяет текущее состояние СОХИ с точки зрения обеспечения безопасности и является средством контроля соответствия состояния СОХИ принятым правилам предотвращения несанкционированного доступа к защищаемой информации.

Результаты моделирования используются блоком пополнения базы знаний для внесения изменений в информацию, характеризующей различные ситуации в СОХИ и связанные с процессами обеспечения безопасности.

Блок логического вывода предназначен для определения типа управляющего воздействия и элементов СОХИ, в том числе и средств защиты, с помощью которых можно предотвратить и компенсировать возникающие нештатные ситуации. При выявлении ситуации, которая может привести к утечке информации в СОХИ, могут использоваться различные методы на основе теории вероятностей. Однако значительная неопределенность, связанная с отсутствием априорных данных о возможностях злоумышленника, времени и месте попыток несанкционированного доступа, обуславливает появление неполной и неточной информацией. В этих условиях для обнаружения и локализации места попыток несанкционированного доступа или возникновения каналов утечки информации может использоваться теория нечетных множеств [9], получившая достаточное распространение за последние годы. Методы интерпретации различных видов нечетностей в существующей информации с целью получения конкретных рекомендаций по управлению системой защиты должны быть положены в основу принципов построения блока логического вывода.

Блок объяснений служит для предоставления оператору комментариев в процессе управления системой обеспечения безопасности. Поскольку оператор должен нести персональную ответственность за предотвращение утечки информации, то ему дается право вмешиваться в процесс управления на любом этапе и ввести управляющие директивы с операторного терминала. Однако все действия оператора в этом случае будут регистрироваться и анализироваться с использованием базы знаний.

Рассмотренная структура позволяет в общих чертах определить значение СОХИ и принципы использования искусственного интеллекта для управления системой обеспечения безопасности информации СОХИ.

Рассмотрим более подробно, как работает система поддержки принятия решения. Причем, принятие решений в большинстве случаев заключается в генерации возможных альтернатив решений их оценки и выборе лучшей альтернативы. Принять правильное решение — значит выбрать такую альтернативу из числа возможных, которая в максимальной степени будет способствовать достижению поставленной цели.

При выборе альтернатив приходится учитывать большое число противоречивых требований и, следовательно, оценивать варианты решений по многим критериям. Противоречивость требований, неоднозначность оценки ситуаций, ошибки в выборе приоритетов сильно усложняют принятие решений.

Другой необъемлемой особенностью принятия решений являются неопределенности, которые делятся на три класса [8]: неопределенности, связанные с неполнотой значений; неточное понимание своих целей оператором; неопределенность при учете реакции окружающей среды. Эти неопределенности не позволяют точно сформулировать цели принятия решения. Единственно возможным способом решения этих неопределенностей является субъективная оценка оператора. Процесс принятия решений (ПР) удобно рассматривать с операционной и логико-психологической точки зрения [8; 9].

Операционное описание позволяет рассматривать процесс ПР в виде композиции трех множеств

$$H = H_1 \times H_2 \times H_3 \qquad (1)$$

где множество H_1 характеризует совокупность операций информационной подготовки ПР; H_2 — этап выбора решения; H_3 — действия, ведущие к его реализации.

Информационная подготовка ПР складывается из внешнего и внутреннего информационного обеспечения [11]. При внешнем — решается вопрос отбора необходимой информации и выбора способов ее оптимального представления. Этап внутренней подготовки включает в себя процедуры классификации и обобщения информации о текущих ситуациях, построение оперативных моделей деятельности. Следовательно, внешнее информационное обеспечение производится при априорной подготовке ПР, внутреннее — при решении конкретных оперативных задач.

Выбор решения состоит из формирования рабочих гипотез, сопоставления их с концептуальными моделями текущих ситуаций, корректировки сформированных моделей, оценки соотношения гипотез и

достигаемых результатов, выбора наилучших гипотез и последовательности действий для решения в соответствии с выбранной гипотезой.

Общую логико-психологическую структуру процесса ПР можно представить в виде ориентированного графа, $\Gamma(H, \omega)$, где H — множество элементов или действий принятия решения; ω — множество соответствующих отображений, $\omega > H > H_j$ $i, j = 1, 2, ..., i \neq j$ (отсутствие петель в графе). В соответствии с [12, 13] множество Н целесообразно представить в виде трех подмножеств $H = H_1 \cup H_2 \cup H_3$; H_1, H_2, $H_3 \neq \varnothing$. Очевидно, желаемым результатом анализа процесса ПР является выполнение условий $H_1 \cup H_2 = 0$, $H_1 \cup H_3 = 0$, $H_2 \cup H_3 = 0$. Вместе с тем получить такие непересекающиеся множества практически невозможно, поскольку мыслительная деятельность имеет многоуровневый характер, обобщающий психофизиологический, психологический, гносеологический и программный уровни со сложными взаимосвязями [13]. Поэтому все синтезируемые структуры ПР являются приближенными. Граф алгоритма принятие решения приведен на рис. 2.

Содержание этапов ПР поясняет табл. 1.

Условно выделено 10 действий по ПР. Действия 1—6 относятся к этапу информационной подготовки H_1; 7 — к выбору решения H_2; 8—10 — к реализации решения H_3. Считается, что действия 7 оператора по выбору решения H_2 принципиально не формализуемы. На этом этапе оператор использует в ручном режиме три основные формы мыслительной деятельности: эмпирическую, аксиномантическую и диалектическую.

Представленный граф является абстрактным, однако позволяет описать последовательность ПР и моделировать процесс ПР. В частности, из него следует, что для автоматизации информационного обеспечения ПР необходимо возложить выполнение действий 1—6, 9, 10 на технические средства, т.е. автоматизировать функции распознавания ситуаций, управления информационной моделью с целью отбора необходимой для ПР информации и оптимизации условий восприятия, планирования решений и накопления опыта.

Поддержка принятия решения заключается в помощи оператору в процессе принятия решения. Она включает [8]:

- помощь оператору при анализе и оценке ситуации и ограничений, накладываемых внешней средой;
- ранжирование приоритетов при принятии решений;
- генерацию возможных решений, т.е. формирование списка альтернатив;
- оценку возможных альтернатив исходя из предпочтений оператора и ограничений накладываемых внешней средой;
- анализ последствий принимаемых решений;
- выбор лучшего варианта.

Суть компьютерной поддержки принятия решений заключается в формализации

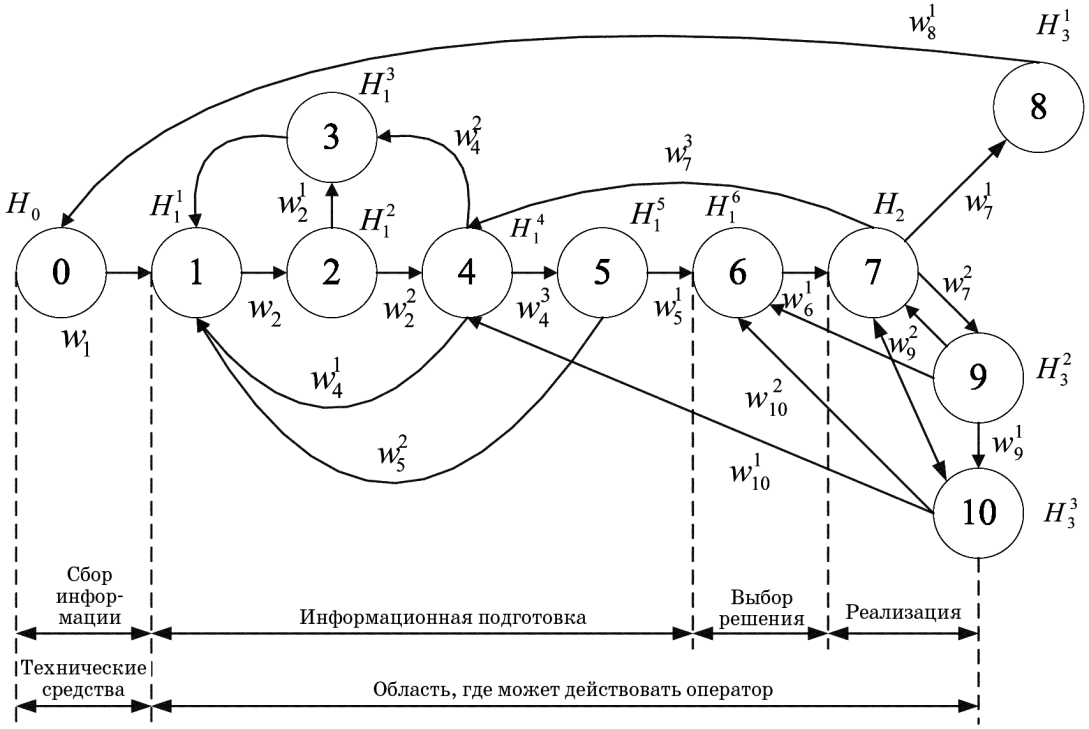

Рис. 2. Абстрактный граф алгоритма принятия решений

Таблица 1

Этап принятия решения	Формальное представление	Содержание этапа
H_0	$\omega_0: H_0 \to H_1^1$	Формирование ИМ
	$\omega_1: H_1^1 \to H_1^2$	Восприятие ИМ
	$\omega_2^1: H_1^2 \to H_1^3$	Управление ИМ для улучшения условий восприятия
	$\omega_3: H_1^3 \to H_1^1$	Реализация отдельных операций по управлениям
H_1	$\omega_2^2: H_1^2 \to H_1^4$	Распознавание ситуаций
	$\omega_4^1: H_1^4 \to H_1^1$	Контроль обстановки
	$\omega_4^2: H_1^4 \to H_1^3$	Корректировка ИМ для детализации информации
	$\omega_4^3: H_1^4 \to H_1^5$	Формирование концептуальных моделей обстановки
	$\omega_5^1: H_1^5 \to H_1^6$	Переход к ПР
	$\omega_5^2: H_1^5 \to H_1^1$	Возвращение к контролю обстановки
	$\omega_5^1: H_1^6 \to H_2$	Определение целей и критериев ПР
H_2	$\omega_7^1: H_2 \to H_1^3$	Утверждение решения и переход к его реализации
	$\omega_7^2: H_2 \to H_3^2$	Генерирование альтернатив и оценка результатов решений
	$\omega_7^3: H_2 \to H_1^4$	Дополнительное прогнозирование состояний системы при затруднениях в выборе решения
H_3	$\omega_8: H_3^1 \to H_1^1$	Реализация ПР в переход к анализу обстановки
	$\omega_9^1: H_3^2 \to H_3^3$	Оценка результатов ПР и запоминание их (накопление опыта)
	$\omega_9^2: H_3^2 \to H_2$	Переход к повторному ПР при неудовлетворительных результатах
	$w_{11}: H_3^3 \to H_1^4, H_1^6, H_2$	Взаимосвязь составляющих процесса ПР с использованием памяти и мышления оператора

описания процессов обработки исходной информации и выработке решения, а также алгоритмизации этих процессов.

Выводы

Проведенный анализ задач управления системой обеспечения безопасности информации в СОХИ позволил сформулировать основные принципы построения единой системы управления, охватывающей все функциональные элементы защиты. Функционирование системы управления основывается на формальной модели обеспечения безопасности данных в СОХИ с учетом существования двух классов средств защиты — локальных и сетевых [14]. При этом основным элементом системы управления является ЦУБ, который для реализации связей функции использует специализированную экспертную систему, постоянно контролирующую правильность работы системы обеспечения безопасности информации.

Однако сложность проблемы управления безопасностью информации в СОХИ требует проведения дополнительных исследований для оценки эффективности предлагаемых методов, конкретизации функций и принципов построения элементов систем управления и поддержки принятия решения, а также для оценки влияния средств контроля функционирования системы защиты на загрузку сети. Кроме того, самостоятельной проблемой является разработка методологии функционального контроля системы защиты при использовании централизованной схемы генерации последовательностей контрольных команд.

Литература

1. Ленков С. В. Методы и средства защиты информации : В 2 т. / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко / Под ред. В. А. Хорошко. — К. : Арий, 2008. **2. Хорошко В. А.** Методы и средства защиты информации / В. А. Хорошко, А. А. Чекатов. — К. : Юниор, 2003. — 504 с. **3. Соколов А. В.** Защита информации в распределенных корпоративных сетях и системах / А. В. Соколов, В. Ф. Шаньгин. — М. : ДМК Пресс, 2002. — 656 с. **4. Гурина С. А.** Живучесть систем защиты информации в условиях внешних воздействий / С. А. Гурина, Ф. И. Егоров, В. А. Хорошко // Захист інформації. — 2008. — № 2. — С. 69—73. **5. Стенг Д.** Секреты безопасности сетей / Д. Стенг, С. Мун. — К. : Диагностика, 1995. — 544 с. **6. Кобзева А. А.** Модель системы защиты информации, основанная на принципах естественной ситемы управления / А. А. Кобзева, В. А. Хорошко // Захист інформації. — 2007. — Спец. вип. — С. 56—72. **7. Домарев В. В.** Защита информации и безопасность компьютерных систем / В. В. Домарев — К. : Диа-Софт, 1999. — 480 с. **8. Герасимов Б. М.** Системы поддержки принятия решений: проектирование, применение, оценка эфективности /

Б. М. Герасимов, М. М. Давидинюк, Н. Ю. Субач — Севастополь : Изд. центр СНИЯЭиП, 2004. — 320 с. **9. Тарасов В. А.** Интелектуальные системы поддержки принятия решений: теория, синтез, эффективность / В. А. Тарасов, Б. М. Герасимов, Н. А. Левин, В. А. Корнейчук. — К. : МАКНС, 2007. — 336 с. **10. Капустян М. В.** Модели передачи информации с учетом обнаружения, недопущения и устранения тупиковых ситуаций / М. В. Капустян, Т. И. Олешко, В. А. Хорошко // Вісн. ДУІКТ. — 2006. — № 4 (3). — С. 156—162. **11. Кобзева А. А.** Методика оценки адекватности системы защиты информации / А. А. Кобзева, В. А. Хорошко // Вісник ДУІКТ. — 2007. — № 5 (3). — С. 328—334. **12. Кобзева А. А.** Использование взвешеного графа при моделировании террористической сети / А. А. Кобзева, В. А. Хорошко // Інформаційні технології та комп'ютерна інженерія. — 2007. — № 3 (10). — С. 61—67. **13. Кобзева А. А.** Использование теории графов для анализа структурі террористических сетей / А. А. Кобзева, В. А. Хорошко // Захист інформації. — 2008. — № 1. — С. 22—31. **14. Бабак И. И.** Количественная оценка значимости произвольного средства защиты информации для функционирования информацыонно-технологической системы / И. И. Бабак, А. А. Кобозева, В. А. Хорошко // Вісн. ДУІКТ. — 2008. — № 6 (1). — С. 33—45.

У статті надано визначення основних задач управління космплексом засобів забезпечення безпеки інформації, наведено формалізований опис правил захисту інформації від несанкціонованого доступу й розглянуто призначення й функціональна схема центра управління безпеки, а також абстрактний граф алгоритма прийняття рішення.

Ключові слова: управління космплексом засобів забезпечення безпеки інформації, захист інформації, несанкціонований доступ, абстрактний граф алгоритма прийняття рішення.