АЛГОРИТМЫ СИТУАЦИОННОГО УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЙ

Е.Н. Надеждин
Россия, Москва

В.А. Шептуховский
Россия, г. Шуя

Закономерным следствием интеграции информационно-вычислительных сетей (ИВС) образовательных учреждений и формирования единой информационной образовательной среды (ИОС) с выходом в Интернет-пространство явилось обострение проблемы обеспечения требований информационной безопасности (ИБ) [1, 3]. Традиционное использование стандартного набора аппаратно-программных средств защиты информации только расширило возможности несанкционированного доступа к ресурсам и сервисам распределенной ИОС. В этих условиях одним из перспективных направлений обеспечения ИБ является создание системы интегрированной защиты сетевых ресурсов, обладающей эффективными инструментами оптимального выбора и настройки механизмов интегрированной защиты (МИЗ) [2].

Общепринятая концепция интегрированной защиты ресурсов ИВС предполагает выделение специализированного сервера для осуществления основных функций управления рисками ИБ. Однако, в условиях использования распределенных баз данных и программного обеспечения, построенного на различных программно-аппаратных платформах, интересам ИБ ИОС, безусловно, будет отвечать гибкая стратегия управления ИБ. Ее осуществление предполагает разумную децентрализация функций управления и защиты сетевых ресурсов и адаптивную настройку МИЗ. Таким образом, в распределенной ИОС актуализируется задача выбора оптимального (в смысле

критерия «стоимость/эффективность») МИЗ, адекватного характеристикам информационных угроз и предусматривающего синхронизацию работы средств безопасности на всех уровнях ИОС.

Для формализации процесса управления МИЗ в настоящее время разработана стратегия адаптивного ситуационного управления информационными рисками [2]. Имеются многочисленные публикации, отражающие отдельные аспекты принятия решений в контуре ситуационного управления динамическими объектами. Однако вопросы практической реализации принципов адаптивного ситуационного управления в условиях специфических задач управления рисками ИБ требуют дополнительных исследований. В качестве сдерживающих факторов здесь выступают сложность оперативного сбора и аналитической обработки данных о состоянии сетевых ресурсов и выявленных угрозах, а необходимость адекватного выбора алгоритма ситуационного управления рисками ИБ в реальном масштабе времени.

Задачам интегрированной защиты сетевых ресурсов ИОС в наибольшей степени соответствует трехуровневая процессно-сервисная модель системы управления информационной безопасностью (СУИБ) [2], которая в общем случае включает: а) процессы стратегического уровня – управление рисками, обеспечение целостности сетевых ресурсов, корректировку политики ИБ верхнего уровня; б) процессы тактического уровня – разработку и настройку процедур защиты, развитие архитектуры системы ИБ, классификацию и анализ состояния ИТ-ресурсов, мониторинг и управление инцидентами; в) процессы операционного уровня – разграничение прав доступа, управление сетевой безопасностью, проверка соответствия ИБ установленным стандартам.

Рассмотрим общую математическую постановку задачи синтеза алгоритмов управления рисками ИБ [1,2].

Пусть модель обеспечения ИБ на заданном интервале времени $t \in T$ формально представлена функционалом приведенного ущерба $H = \Phi(E, M, U, Q)$,

отражающим результат воздействия информационных угроз на ресурсы E распределенной ИОС. Предположим также, что априорно известны:

$M = \{m_1, m_2, ..., m_r\}$ – возможные варианты исполнения МИЗ;

$U = \{u_1, u_2, ..., u_m\}$ – реализованные способы управления МИЗ;

$Q = R(W)$ – критериальная функция; $F = \{f_1, f_2, ..., f_k\}$ – функции, выполняемые МИЗ;

$W = (w_1, w_2, ..., w_p)$ – векторный показатель эффективности МИЗ;

В свою очередь, частные показатели эффективности – компоненты вектора W – зависят от архитектуры объектов защиты, характеристик угроз χ, конкретных механизмов защиты M и способов управления ими U: $W = C(\chi, M, U)$. С учетом введенных обозначений математическая модель задачи синтеза СУИБ может быть представлена в виде следующей экстремальной задачи.

Требуется найти:

$$H^* = \min \Phi\ (E, M^*, U^*, Q) \qquad (1)$$

при условиях $M^* \in M$, $U^* \in U$, которым соответствует $W^* \in W_Д$, где M^* и U^* – соответственно подмножества оптимальных вариантов механизмов защиты и алгоритмов управления ими, $W_Д$ – множество допустимых значений показателей эффективности МИЗ, определяемых требованиями политики ИБ. Иначе, на основе анализа полученной информации о проблемной ситуации в результате численного решения экстремальной задачи необходимо выбрать такие механизмы и способы управления системой защиты, при которых достигается минимум главного показателя $H = \Phi(E, M, U, Q)$ и выполняются ограничения на другие частные показатели эффективности.

На основе декомпозиции общей модели (1) получают модели частных задач управления ИБ: идентификации состояния ресурсов, направленного выбора и активизации механизмов защиты информации в КСЗИ. Наибольшие трудности при этом возникают при оценке защищенности распределенных ресурсов, при выборе оптимального иерархически организованного МИЗ и при

переходе от задачи оптимизации (1) к задаче управления МИЗ в режиме, близком к реальному времени.

Продуктивное решение задачи (1) в условиях реальных временных ограничений, неполноты и нечеткости исходной информации может быть получено на основе параллельных алгоритмов целочисленной оптимизации [4].

Ситуационное управление ИБ представляет собой целенаправленный процесс выработки и реализации управляющих воздействий, соответствующих состоянию объекта и окружающей среды и направленных на приведение объекта в заданное состояние. В рассматриваемом случае объектом управления является состояние защищенности сетевых ресурсов, а управляемой величиной – риски ИБ. Их стабилизация достигается за счет выбора и настройки изменяемых параметров в моделях МИЗ. В интересах автоматизации процесса управления ИБ необходимо выделить и формально описать в цикле управления совокупность типовых задач: оценки состояния защищаемого объекта, формирования управляющего воздействия (в соответствии с принятым законом управления) и реализацией данного воздействия.

Пусть известна сетевая многоальтернативная модель МИЗ в виде обратного ориентированного графа $G = (S, V, W)$, где $S = (S_0, S_1, ..., S_m, S_{m+1})$ – расширенное множество вершин, отражающих варианты исполнения механизмов защиты на каждом уровне, $V = (v_{i,j},\ \ i, j = \overline{1, m})$ – множество дуг, нагруженных набором показателей из множества W. Эффективность работы каждого частного алгоритма защиты оценивается вероятностью преодоления злоумышленником данного контура защиты. Пусть целевая функция является сепарабельной. Тогда выбор оптимального МИЗ формально может быть сведен к задаче поиска кратчайшего пути в графе $G = (S, V, W)$ по критерию минимума затрат при ограничениях на полную вероятность преодоления системы интегрированной защиты злоумышленником. Здесь могут быть использованы хорошо апробированные на практике методы теории сетевого анализа и управления. Особенности сопряжения и синхронизации параметров отдельных МИЗ при этом отражаются путем введения матрицы весовых коэффициентов.

Учитывая специфику архитектуры сети и особенности многопользовательского режима работы, можно утверждать, что требованиям гибкости и устойчивости функционирования в наибольшей степени будет отвечать концепция адаптивного ситуационного управления ИБ, которая реализуется по базовой схеме «ситуация - стратегия управления - действие» [2]. Ключевым моментом здесь является разработка методики дискретной адаптации МИЗ. В нашем исследовании предложены алгоритмы решения целочисленной линейной задачи (1), допускающие распараллеливание вычислений. Учитывая высокую размерность экстремальной задачи (1) в качестве базовой модели выбран известный метод построения последовательности планов, использующий модификацию канонической схемы метода ветвей и границ.

Разработанные авторами алгоритмы и программные средства решения задач выбора структуры и параметрических настроек МИЗ (в классической и сетевой постановках) обладают достаточной для практики вычислительной устойчивостью и могут быть использованы в контуре СУИБ для осуществления принятой стратегии ситуационного управления.

Литература

1. Надеждин Е.Н., Шептуховский В.А., Максин И.С. Проблемные вопросы создания защищенной корпоративной информационной образовательной среды // Информационная среда образования и науки». 2011. Вып. 5. URL: http://www.iiorao.ru/iio/pages/izdat/ison/publication/ison_2011/num_5_2011/

2. Надеждин Е.Н. Ситуационное управление рисками информационной безопасности инновационного образовательного учреждения с распределенной инфраструктурой // Материалы международной научно-практической конференции «Инновационные информационные технологии» / под ред. С.У. Увайсова; отв. за вып. И.А. Иванов и др. М.: ИМИЭМ, 2012. С. 578-580.

3. Надеждин Е.Н. Проблемные вопросы управления рисками информационной безопасности в сфере образования // Научный поиск. Специальный выпуск «Материалы V научной конференции «Шуйская сессия студентов, аспирантов, молодых ученых». 2012. №2. С.50-56.

4. Хохлюк В.И. Параллельные алгоритмы целочисленной оптимизации. М.: Радио и связь, 1987. 224 с.