УДК 004.056

Профессор Я.Е. Львович, аспирант Д.С. Яковлев
(Воронеж. инст. высоких технол.) кафедра информационных систем и технологий.
тел. (473) 2-205-605
E-mail: office@vivt.ru

Professor Ia.E. L'vovich, graduate D.S. Iakovlev
(Voronezh institute of high technologies) Department of information systems and technologies. phone (473) 2-205-605
E-mail: office@vivt.ru

Оптимизация проектирования систем защиты информации в автоматизированных информационных системах промышленных предприятий

Optimizing the design of the systems of information protection in automated informational systems of industrial enterprises

Реферат. В настоящее время для повышения показателей эффективности и работоспособности сложных систем применяют средства автоматизации. Отмечена возрастающая роль информации, которая стала универсальным товаром для взаимоотношений между различными структурами. Наиболее актуальным становится вопрос ее защиты. Особое значение отводится оптимальному проектированию при построении систем защиты, позволяющему с наибольшей вероятностью выбирать наилучшие решения на множестве альтернатив. В настоящее время это становится актуальным для большинства промышленных предприятий, поскольку правильно спроектированная и внедренная система защиты будет являться залогом успешного функционирования и конкурентоспособности всей организации. Представлены этапы работ по построению системы информационной безопасности промышленного предприятия. Акцентировано внимание на одном из наиболее важных подходов к реализации оптимального проектирования – многоальтернативной оптимизации. В статье рассмотрена структура построения системы защиты с точки зрения различных моделей, каждая из которых дает представление об особенностях проектирования системы в целом. Особое внимание уделено проблеме построения системы информационной безопасности, поскольку она имеет наиболее сложную структуру. Обозначены задачи для процессов автоматизации каждого из этапов проектирования системы защиты информации промышленных предприятий. Дано представление о каждом из этапов работ при проектировании системы защиты, что позволяет наилучшим образом понять внутреннюю структуру построения системы защиты. Следовательно, дается возможность наглядного представления необходимых требований к построению надежного комплекса защиты информации промышленного предприятия. Тем самым дается возможность нивелирования рисков на ранних стадиях проектирования систем защиты, организации и определения необходимых типов программно-аппаратных комплексов для будущей системы.

Summary. Now to increase of indicators of efficiency and operability of difficult systems apply an automation equipment. The increasing role of information which became universal goods for relationship between various structures is noted. The question of its protection becomes the most actual. Special value is allocated for optimum design at creation of systems of the protection, allowing with the greatest probability to choose the best decisions on a set of alternatives. Now it becomes actual for the majority of the industrial enterprises as correctly designed and introduced system of protection will be pledge of successful functioning and competitiveness of all organization. Stages of works on creation of an information security system of the industrial enterprise are presented. The attention is focused on one of the most important approaches to realization of optimum design – multialternative optimization. In article the structure of creation of system of protection from the point of view of various models is considered, each of which gives an idea of features of design of system as a whole. The special attention is paid to a problem of creation of an information security system as it has the most difficult structure. Tasks for processes of automation of each of design stages of system of information security of the industrial enterprises are designated. Idea of each of stages of works is given at design of system of protection that allows to understand in the best way internal structure of creation of system of protection. Therefore, it is given the chance of evident submission of necessary requirements to creation of a reliable complex of information security of the industrial enterprise. Thereby it is given the chance of leveling of risks at early design stages of systems of protection, the organization and definition of necessary types of hardware-software complexes for future system.

Ключевые слова: оптимизация, защита информации, информационные системы промышленных предприятий.

Keywords: optimization, information security, information systems of industrial enterprises

Средства автоматизации проектирования широко используются для повышения эффективности разработки сложных систем.

Прогресс в этом направлении достигается при переходе к оптимальному проектированию, позволяющему интегрировать процесс синтеза проектных вариантов с автоматическим или автоматизированным выбором наилучшего варианта на множестве альтернатив. Одним из таких подходов к реализации оптимального проектирования является многоальтернативная оптимизация. В этом случае происходит естественное объединение объектно-ориентированных методов САПР и инвариантных методов выбора рационального проектного решения.

Одной из систем, где при проектировании эффективно совмещаются объектно-ориентированные и инвариантные методы, является система защиты информации. При этом отечественные и зарубежные исследования в большей мере посвящены инвариантным средствам оптимального проектирования, что в полной мере касается и многоальтернативной оптимизации.

Проблема построения оптимальной системы защиты информации в настоящее время является наиболее актуальной и востребованной для большинства промышленных предприятий. Цель любой системы защиты определяется возможностью устойчивого функционирования системы в целом, определения и нейтрализации угроз безопасности, предотвращения утечки информации по различным каналам. Одной из главных задач становится оптимизации проектирования системы защиты.

Сегодня для промышленных предприятий информация представляет собой основной товар для коммерции. С развитием информационных технологий и доступа к рынкам появляется потребность в ее защите для обеспечения ее конфиденциальности, целостности и доступности. Для многих промышленных предприятий внедрение систем защиты является необходимым этапом на пути к успешному развитию, т. к. каждая из них имеет свою критическую информацию, утрата и/или утечка которой может свести к минимуму конкурентоспособность и шансы на успешное развитие на рынке. Распространение такой информации может привести к потере репутации и нанести материальный ущерб.

Следует отметить, что активное внедрение автоматизированных информационных систем обусловливает возникновение проблем, связанных с информационной безопасностью. Решение данных проблем может быть реализовано с применением специальных автоматизированных программно-технических средств.

Рассмотрим структуру построения системы защиты с точки зрения моделей систем автоматизированного проектирования. Различают функциональную, информационную, поведенческую и структурную модели.

Функциональная модель представлена совокупностью функций, выполняемых системой защиты:

- Предупреждение условий, порождающих дестабилизирующие факторы.
- Предупреждение проявлений дестабилизирующих факторов.
- Обнаружение проявившихся дестабилизирующих факторов.
- Предупреждение воздействия дестабилизирующих факторов на информацию.
- Локализация и ликвидация последствий проявления дестабилизирующих факторов.

Обобщенная информационная модель системы защиты отражает ее состав и взаимосвязи в ней.

Поведенческая модель системы защиты информации характеризуется переходом из нормального состояния в активное, т.е. при обнаружении каких-либо внешних/внутренних воздействий, которые угрожают или могут дестабилизировать функционирование информационной системы, система защиты ликвидирует или минимизирует угрозы безопасности, таким образом, поддерживая целостность и работоспособность системы.

Структурная модель защиты информации характеризует морфологию системы защиты – состав подсистем, их взаимосвязи.

Содержанием последующих этапов нисходящего проектирования являются уточнение перечней приобретаемого оборудования и готовых программных продуктов, построение системной среды, проектирование баз данных и их первоначальное наполнение, разработка собственного оригинального программного обеспечения, которое, в свою очередь, делится на ряд этапов нисходящего проектирования. После этого следуют закупка и инсталляция программно-аппаратных средств, внедрение и опытная эксплуатация системы.

Таким образом, среди проектных задач особое место занимает разработка системы защиты информации, поскольку ее техническое обеспечение имеет сетевую структуру. Необхо-

дим осознанный выбор типов коммутационного оборудования, серверов, сетевых программных продуктов, определение способов защиты передаваемых данных. Возникающие при этом проблемы напрямую связаны с детальным проектированием системы защиты информации.

Следовательно, процесс автоматизации системы защиты информации должен решать две задачи:

1. Оценка существующей системы защиты информации (в случае, если данная система уже внедрена в организации):

- проверка соответствия системы поставленным задачам;
- проверка на соответствие нормативным требованиям;
- апробация системы защиты путем тестирования.

2. Проектирование и внедрение новой системы защиты информации.

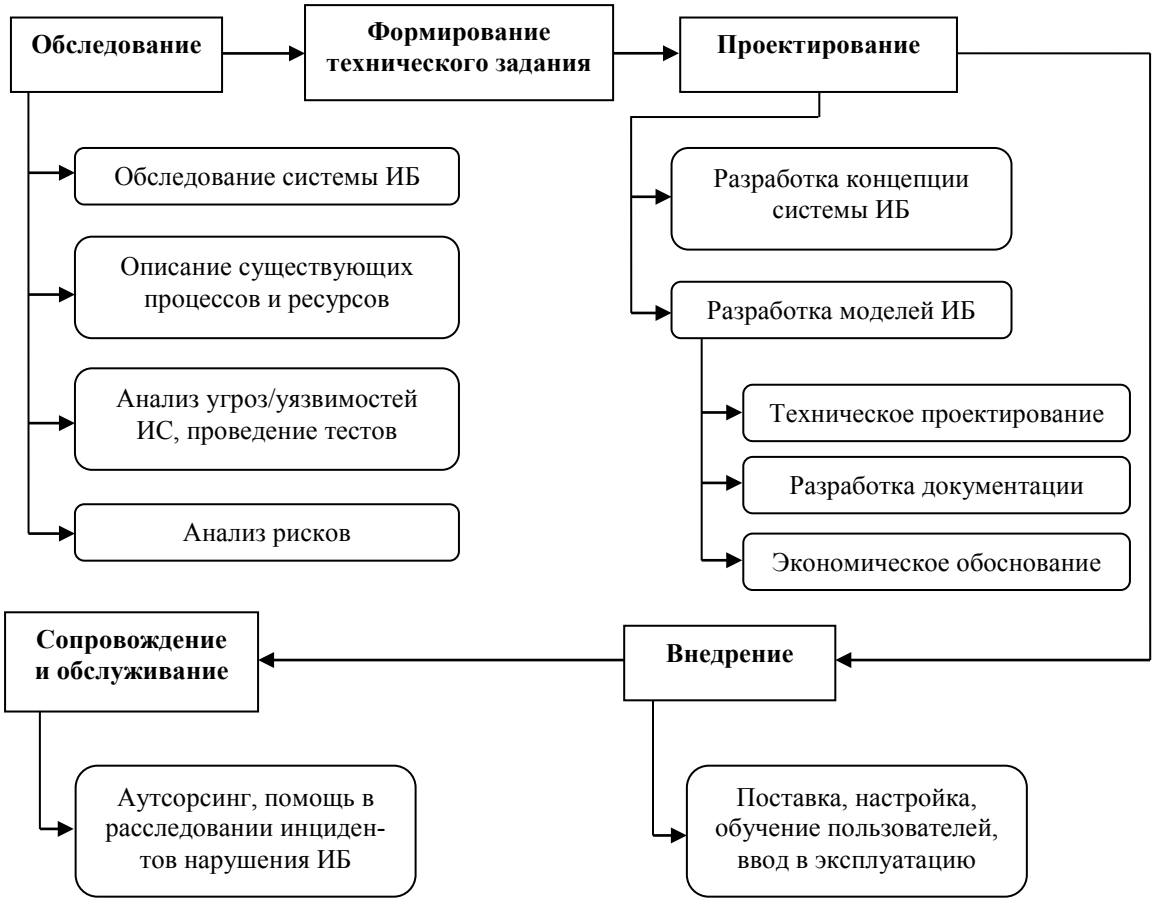

Рисунок 1 - Общая схема этапов работ по построению системы ИБ промышленного предприятия

Общая схема этапов работ по построению системы информационной безопасности включает (рисунок 1) обследование, проектирование, внедрение, сопровождение и обслуживание. Рассмотрим более детально каждый из этапов. На первом этапе происходит:

- анализ информационной системы и ресурсов, входящих в ее состав;
- анализ внешних и внутренних угроз;
- составление перечня защищаемых объектов;
- анализ существующей системы защиты (в случае ее наличия);
- анализ рисков;
- определение критичности информации.

Данный этап позволяет собрать необходимую информацию для построения комплексного подхода к проектированию системы защиты информации. Автоматизировать данный этап представляется возможным благодаря использованию различных программных продуктов, которые содержат описание и градацию угроз безопасности ИС, дают оценку критично-

сти ресурсов и информации, дают наглядное представление ИС в графическом виде, позволяют оценить эффективность выбранной меры защиты для конкретного ресурса.

На втором этапе на основе полученных данных реализуется разработка концепции безопасности (расположение средств защиты согласно проведенному анализу), разработка документации, проведение испытаний. Проведение тестовых испытаний определяет наиболее уязвимые места в спроектированной системе защиты, что позволяет принять превентивные меры по изменению механизмов защиты, логической и функциональной схем.

Автоматизировать данный этап можно с помощью использования программного обеспечения, предназначенного для моделирования помещения, в котором будет установлена система защиты, места расположения и установки ее компонентов, проведение анализа на оптимальное соотношение выбранных средств по критерию «цена-качество», предоставление предварительного проектного решения в наглядном виде.

На третьем этапе происходит внедрение спроектированной системы, ее настройка, обучение персонала и ввод в эксплуатацию.

Заключительный этап представляет собой сопровождение и обслуживание внедренной системы безопасности. Неотъемлемой частью является поддержание системы защиты в актуальном состоянии на основе анализа возможных модификаций существующих и выявления новых видов угроз безопасности ИС.

Таким образом, представленные в наглядном виде этапы проектирования применительно к системе защиты информации дают возможность для детального рассмотрения и учета необходимых требований к построению надежного комплекса защиты информации промышленного предприятия. Заметим, что такие этапы как «обследование» и «проектирование» требуют более глубокого исследования ввиду их многокритериальности.

ЛИТЕРАТУРА

1 Львович Я.Е., Михель А.А. Оптимизационное моделирование ресурсоэффективности системы высшего образования по результатам мониторинго-рейтингового оценивания // Экономика и менеджмент систем управления. 2014. Т. 11. № 1.1. С. 144-149.

2 Львович Я.Е., Сахаров Ю.С., Яковлев Д.С. Принятие решений в условиях дестабилизации системы // Вестник Воронежского Института Высоких Технологий. 2013. №11. С. 114-115.

3 Дерканосова А.А., Коротаева А.А. Особенности российского рынка комбикормов и перспективы его развития // Экономика. Инновации. Управление качеством. 2013. № 3 (4). С. 107а-107б.

4. Анализ инновационной привлекательности использования вегетативной массы растений в комбикормах / Шевцов А.А. [и др.] // Вестник Воронежского университета инженерных технологий. 2013. №1. С. 224-226

5 Роль биомодифицированных кормов в повышении качества продукции перепеловодства /Черемушкина И.В. [и др.] // Вестник Воронежской государственной технологической академии. Серия: пищевая биотехнология. 2010. Т. 45. № 3. С. 82-84.

6 Развитие малого инновационного предпринимательства в АПК на основе использования методики форсайта / Василенко В.Н. [и др.] // Вестник Воронежского государственного университета инженерных технологий. 2013. № 2. С. 223-226.

7Использование системного подхода для повышения экономической эффективности комбикормовой промышленности [Текст] / Василенко В.Н. [и др.] // Финансы Экономика Стратегия. 2010. № 5. С. 50-53.

REFERENCES

1 L'vovich Ya.E., Mixel A.A. Optimization modeling resource efficiency of higher education based on the results of monitoring and evaluation rating. *Ekonomika i menedzhment sistem upravleniya.* [Economics and management control systems], 2014, vol. 11. no.1.1, pp. 144-149. (In Russ.).

2 L'vovich Ja.E., Saharov Ju.S., Jakovlev D.S. Decision-making in terms of destabilizing the system. *Vestnik Voronezhskogo Instituta Vysokih Tehnologij.* [Herald of the Voronezh Institute of High Technologies], 2013. no. 11. pp. 114-115

3 Derkanosova A.A., Korotaeva A.A. Features of the Russian compound feed market and its prospects. *Jekonomika. Innovacii. Upravlenie*

kachestvom. [Economy. Innovation. Quality management], 2013, no. 3 (4), pp. 107a-107б. (In Russ.).

4 Shevtsov A.A., Drannikov A.V., Derkanosova A.A., Korotaeva A.A. Analysis of innovation attractiveness of plants vegetative growth in compound feed. *Vestnik Voronezhskogo universiteta inzhenernyh tehnologij*. [Herald of the Voronezh State University of Engineering Technologies], 2013, no. 1 (55), pp. 224-226. (In Russ.).

5 Cheremushkina I.V., Chigirina N.A., Anohina E.P., Korneeva O.S. Role of the biomodified forages in improvement of quality of production of poultry farming. *Vestnik Voronezhskoj gosudarstvennoj tehnologicheskoj akademii. Serija: pishhevaja biotehnologija.* [Herald of the Voronezh State Technological Academy. Series: Food biotechnology], 2010, vol. 45.no. 3. pp. 82-84. (In Russ.).

6 Vasilenko V.N., Bautin V.M., Frolova L.N., Dragan I.V. The development of small innovative enterprises in agriculture based on the use of foresight methods. *Vestnik Voronezhskogo universiteta inzhenernyh tehnologij*. [Herald of the Voronezh State University of Engineering Technologies], 2013, no. 2 (56), pp. 223-226. (In Russ.).

7 Vasilenko V.N., Ostrikov A.N., Frolova L.N., Tatarenkov E.A., Osipov I.P. Using a systematic approach to improve the economic efficiency of the compound feed industry. *Finansy. Jekonomika. Strategija.* [Finance Economy Strategy], 2010, no. 5, pp. 50-53. (In Russ.).