УДК 681.3

РЕЗУЛЬТАТЫ АПРОБАЦИИ КОМПЛЕКСА ПРОГРАММ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ УПРАВЛЕНИИ БЕЗОПАСНОСТЬЮ ОБЪЕКТОВ СОЦИАЛЬНОГО НАЗНАЧЕНИЯ

© 2021 Д. Е. Орлова, Л. В. Россихина

Воронежский институт высоких технологий (Воронеж, Россия)

Приведены результаты апробации компьютерного комплекса программ поддержки принятия решений при управлении безопасностью объектов социального назначения. Апробация проводилась применительно к типовому учреждению уголовно-исполнительной системы при использовании ИСБ «Рубеж-08». Апробация осуществлялась методом компьютерного эксперимента с привлечением стандартных процедур экспертных оценок.

Ключевые слова: комплекс программных средств, апробация, экспертная оценка, объект уголовно-исполнительной системы.

Краткая характеристика комплекса программ. Комплекс предназначен для поддержки принятия решений в процессе управления комплексной безопасностью объектов социального назначения типа торговые и культурно развлекательные центры, транспортно-коммуникационные и логистические комплексы, учреждения уголовно-исполнительной системы. Он позволяет в интерактивном режиме работы с пользователем решать следующие задачи:

- отображать текущие показатели по всем аспектам безопасности объекта, включая безопасность режима и охраны, пожарную безопасность, информационную безопасность и безопасность жизнедеятельности;

- идентифицировать ситуации безопасности по классам «критическая», «угрожающая» и «штатная»;

- осуществлять оптимизацию процессов управления безопасностью в критических, угрожающих и штатных ситуациях по критерию минимума отклонения от предъявляемых требований;

- оценивать устойчивость управленческих решений, принимаемых при управлении процессом обеспечения.

В основу разработки комплекса положены следующие принципы:

- *интерактивности*, согласно которому диалог между пользователем и компьютером инициируется как пользователем, так и самим комплексом, причем общение ведется на языке, понятном пользователю, неподготовленному в компьютерном отношении, то есть не являющемуся программистом;

- *обучаемости*, предполагающему пополнение и модификацию как исходных данных, необходимых для работы комплекса, так его выходного интерфейса и алгоритмов проведения вычислений, без перепрограммирования его компонентов;

- *соответствия* алгоритму управления процессом обеспечения безопасности, устанавливающему генеральный порядок активации блоков и модулей комплекса;

- *иерархичности и модульности*, согласно которому комплекс строится в виде иерархической совокупности относительно самостоятельных, но тесно взаимодействующих друг с другом модулей и блоков;

- *унификации*, в соответствии с которым комплекс разрабатывается с применением единого программного обеспечения и на базе единой операционной системы;

- *адаптации и развития,* в соответствии с которым программная структура комплекса может подстраиваться под требования конкретного пользователя, сохраняя при этом возможность наращивания своего состава;

- *информационного единства*, т. е. во всех компонентах программного обеспечения используются единые термины, символы, обозначения и способы представления;

- *совместимости* – язык, символы, коды и средства программного обеспечения согласованы, обеспечивают совместное функционирование всех его подсистем и сохраняют открытой структуру системы в целом;

Россихина Лариса Витальевна – Воронежский институт высоких технологий, профессор, доктор техн. наук, rossihina_lv@mail.ru.

Орлова Дарья Евгеньевна – Воронежский институт высоких технологий, аспирант, dasha_scorobogat@mail.ru.

- *инвариантности* – предопределяет, что компоненты программного обеспечения инвариантны к обрабатываемой информации, являются универсальными или типовыми;

- *стандартизации*, в соответствие с которым комплекс строится с соблюдением действующих стандартов по обеспечению качества программных продуктов (имеются в виду стандарты ISO 12207: 1995; ISO 9000-3:1997; MIL-STD-498, DO-179B).

Блок-схема комплекса приведена на рисунке 1.

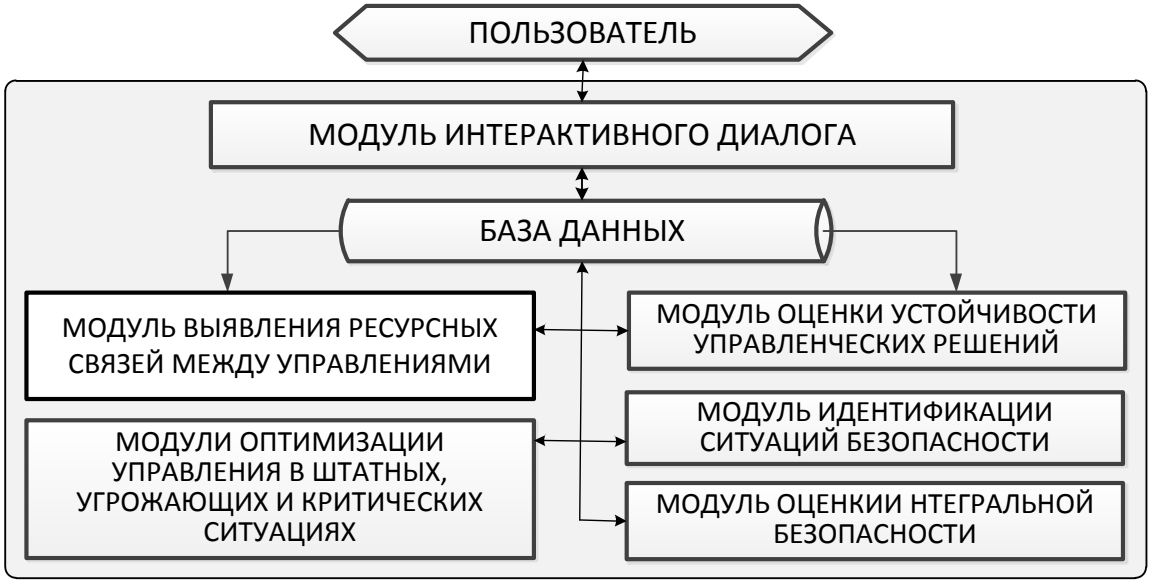

Рисунок 1. Блок-схема комплекса программ поддержки принятия решений при управлении комплексной безопасностью объектов социального назначения

Комплекс исполнен в среде TURBO PASCAL с применением процедур и функций VISUAL BAISIC, DELPHI и C++, ориентированных на создание приложений в среде Windows 7(10).

Апробация комплекса проводилась на примере оценки безопасности типового учреждения УИС при использовании на ее объектах интегрированной системы безопасности (ИСБ) «Рубеж-08» [1,2].

Краткая характеристика ИСБ «Рубеж-08». Интегрированная система безопасности «Рубеж-08» представляет собой аппаратно-программный комплекс, предназначенный для создания систем комплексной безопасности различных объектов: жилых домов, магазинов, офисов, банков, учреждений, предприятий, в том числе и объектов особой важности и повышенной опасности. Аппаратной основой ИСБ «Рубеж-08» являются: блок центральный процессорный (БЦП) и адресные сетевые устройства (СУ) различного типа и функционального назначения. СУ подключаются к БЦП по адресной линии связи с интерфейсом RS-485. В состав СУ входит номенклатура контроллеров, приборов и блоков, необходимых для защиты объектов любой сложности и любого масштаба. Программное обеспечение системы «Рубеж» включает в себя:

- ПО Р-08 – специализированный комплекс программ, обеспечивающих поддержку оборудования ИСБ «Рубеж-08» аппаратно-программной платформы Р-8;
- RM-3 – универсальная программная интеграционная платформа, предназначенная для создания единого верхнего уровня ИСБ, обеспечивающая поддержку оборудования ИСБ «Рубеж» аппаратной платформы Р-08 и широкие возможности интеграции оборудования и систем других производителей;
- СПО «ИНДИГИРКА» – кроссплатформенное решение, ориентированное на работу с защищенными ОС российского производства типа МСВС и *Astra Linux*, полностью удовлетворяет требованиям 188-ФЗ о едином реестре российских программ.

Оценка локальных показателей безопасности учреждения УИС при использовании ИСБ «Рубеж-08» осуществлялась с использованием стандартной экспертной методики [3]. Результаты представлены в таблице 1.

Таблица 1

Результаты экспертной оценки локальных показателей безопасности учреждения УИС при использовании ИСБ «Рубеж-08»

Тип	Наименование показателя	Оценка	
		без ИСБ	с ИСБ
Показатели безопасности режима и охраны	q_{11} – уровень охраны территорий и помещений от несанкционированного проникновения, в том числе с использованием ДПЛА;	*0,45*	*0,60*
	q_{12} – уровень личной безопасности сотрудников объекта, включая сотрудников службы безопасности;	*0,75*	*0,80*
	q_{13} – уровень контроля режима секретности и допуска;	*0,88*	*0,88*
	q_{14} – уровень контроля радиочастотного спектра в зоне объекта и возможность пресечения несанкционированной работы мобильных средств связи;	*0,56*	*0,56.*
	q_{15} – своевременность реагирования и пресечения нарушений режима и охраны.	*0,70.*	*0,95*
Показатели Пожарной безопасности	q_{21} – уровень защиты от возгорания заранее припасенными средствами и средствами, находившимися на месте поджога;	*0,60*	*0,90*
	q_{22} – уровень защиты от поджогов с помощью технических приспособлений дистанционного действия;	*0,80*	*0,80*
	q_{23} – уровень защищенности от самовозгорающихся средств;	*0,80*	*0,90*
	q_{24} – уровень защиты от распространения пожара на примыкающие территории;	*0,85*	*0,85*
	q_{25} – уровень организации и управления пожарной безопасностью;	*0,70*	*0,90*
	q_{26} – уровень подготовки личного состава действиям на пожаре;	*0,90*	*0,95*
	q_{27} – своевременность выявления и ликвидации пожаров.	*0,70*	*0,90*
Показатели информационной безопасности	q_{31} – уровень защищенности СУБД;	*0,60*	*0,90*
	q_{32} – уровень защищенности операционных систем;	*0,50*	*0,90*
	q_{33} – уровень защищенности сетевого программного обеспечения;	*0,70*	*0,95*
	q_{34} – уровень криптозащиты информации;	*0,90*	*0,94*
	q_{35} – уровень надежности разграничения доступа;	*0,50*	*0,80*
	q_{36} – уровень защищенности объектов от средств криминальной технической разведки;	*0,70*	*0,85*
	q_{37} – своевременность выявления кибератак и ликвидации их последствий.	*0,60*	*0,90*
Показатели безопасности жизнедеятельности	q_{41} – уровень защищенности личного состава от применения химических отравляющих веществ и средств ошеломляющего действия;	*0,70*	*0,90*
	q_{42} – уровень защищенности инженерных сооружений;	*0,60*	*0,90*
	q_{43} – уровень организации медицинской помощи в случае возникновения критических ситуаций;	*0,50*	*0,50*
	q_{44} – уровень организации мероприятий по эвакуации личного состава;	*0,60*	*0,70.*
	q_{45} – своевременность выявления и ликвидации критических ситуаций, связанных с опасностью жизнедеятельности.	*0,70*	*0,90*

Оценка интегральной безопасности учреждения УИС при использовании ИСБ «Рубеж-08» осуществлялась с использованием метода аддитивной свертки применительно к критической ситуации при одинаковой важности всех локальных показателей безопасности. При этом оценка проводились для двух вариантов: с оптимизацией управления и без оптимизации. Результаты оценки приведены в таблице 2.

Таблица 2

Результаты оценки интегральной безопасности учреждения УИС при использовании ИСБ «Рубеж-08»

Уровни безопасности	Оценка			
	без оптимизации		с оптимизацией	
	без ИСБ «Рубеж-08»	с ИСБ «Рубеж-08»	без ИСБ «Рубеж-08»	с ИСБ «Рубеж-08»
Безопасность режима и охраны	*0,63*	*0,73*	*0,75*	*0,95*
Пожарная безопасность	*0,78*	*0,86*	*0,86*	*0,98*
Информационная безопасность	*0,64*	*0,88*	*0,78*	*0,96*
Безопасность жизнедеятельности	*0,62*	*0,78*	*0,78*	*0,86*
Интегральная безопасность	***0,67***	***0,82***	***0,80***	***0,93***

Анализ результатов оценки показал, что применение ИСБ «Рубеж-08» совместно с реализацией алгоритмов оптимизации управления позволяет примерно на 15 % повысить интегральную безопасность в учреждении УИС. При этом наибольший прирост безопасности обеспечивается за счет: а) совместного применения средств ИСБ «Рубеж-08» и алгоритмов оптимизации; б) повышения оперативности управления по всем аспектам безопасности, что достигается применением современных высокоавтоматизированных средств контроля и внутренней связи; б) повышения уровня информационной безопасности, что достигается применением СПО «ИНДИГИРКА», ориентированного на работу с защищенными ОС российского производства типа МСВС и *Astra Linux.*

Вместе с тем, применение ИСБ «Рубеж-08» даже с применением алгоритмов оптимизации и не решает проблем, связанных с защитой от проникновения дистанционно-пилотируемых летательных аппаратов (ДПЛА) на охраняемые территории и контроля радиочастотного спектра с целью пресечения несанкционированной работы мобильных средств связи. В этом плане необходимо создание специализированных групп в составе учреждения, оснащенных средствами борьбы с ДПЛА радиоэлектронными методами.

ЛИТЕРАТУРА

1. Интегрированные системы безопасности серии «Рубеж» для охраны объектов и учреждений ФСИН России / Н. С. Хохлов, О. В. Четкин, Д. Г. Зыбин. – Воронеж: Полиграфия, 2011. – 179 с.

2. Крахмалев А. К. Интегрированная система безопасности «Рубеж». Учебное пособие / А. К. Крахмалёв; под ред. А. Г. Зайцева. – М.: НПФ «СИГМА-ИС», 2007. – 244 с.

3. Литвак Б. Г. Экспертная информация: методы получения и анализа / Б. Г. Литвак. – М.: Радио и связь, 1982. – 184 с.

RESULTS OF APPROBATION OF A SET OF PROGRAMS TO SUPPORT DECISION-MAKING IN THE MANAGEMENT OF SECURITY OF SOCIAL FACILITIES

© 2021 D. E. Orlova, L. V. Rossikhina

Voronezh Institute of High Technologies (Voronezh, Russia)

The results of approbation of a computer complex of programs for decision-making support in the management of security of social facilities are presented. The approbation was carried out in relation to a standard institution of the penitentiary system using the HMB "Rubezh-08". The approbation was carried out by a computer experiment with the use of standard expert assessment procedures.

Keywords: software package, approbation, expert assessment, object of the penitentiary system.