

В. А. Ворона
В. А. Тихонов

Комплексные (интегрированные) системы обеспечения безопасности

Москва
Горячая линия – Телеком
2013

УДК 699.81:654.924

ББК 38.96

В83

Серия «Обеспечение безопасности объектов»; Выпуск 7.

Редакционная коллегия серии:

академик РАН *В. К. Левин (председатель редколлегии);*

доктор воен. наук, профессор *В. П. Лось;* канд. техн. наук, доцент *А. А. Торокин;*

доктор техн. наук, профессор *В. А. Ворона;* канд. техн. наук, профессор *В. А. Тихонов,*

доктор техн. наук, профессор *В. В. Саморуков,* канд. техн. наук, доцент *Д. М. Платонов*

Ворона В. А., Тихонов В. А.

В83 Комплексные (интегрированные) системы обеспечения безопасности. – М.: Горячая линия–Телеком, 2013. – 160 с.: ил.

ISBN 978-5-9912-0238-1.

В книге приведены характеристики комплексных (интегрированных) систем безопасности (КСОБ, ИСБ). Значительное внимание уделено концепции «интеллектуального здания» (ИЗ). Рассмотрены практические проекты реализации ИСБ, КСОБ, ИЗ. Приведенные сведения могут быть использованы при организации работ по защите предприятий, вычислительных центров, узлов связи, банков, офисов, коммерческих объектов, жилых домов и транспортных средств.

Для специалистов в области создания и эксплуатации средств инженерно-технической защиты объектов, руководителей и сотрудников служб безопасности (охраны) предприятий, студентов вузов и слушателей курсов повышения квалификации, обучающихся по специальностям обеспечения интегральной безопасности объектов (в том числе объектов информатизации) и личности.

ББК 38.96

Адрес издательства в Интернет WWW.TECHBOOK.RU

Справочное издание

Ворона Владимир Андреевич

Тихонов Виктор Алексеевич

Комплексные (интегрированные) системы обеспечения безопасности

Редактор **И. Н. Андреева**

Обложка художника **В. Г. Ситникова**

Компьютерная верстка **Ю. Н. Чернышова**

Подписано в печать 07.11.2012. Формат 60×90/16. Уч.-изд. л. 10. Тираж 500 экз. (1-й завод 100 экз.) Изд. № 12238.

ООО «Научно-техническое издательство «Горячая линия – Телеком»

ISBN 978-5-9912-0238-1

© В. А. Ворона, В. А. Тихонов, 2012

© Издательство «Горячая линия–Телеком», 2012

ВВЕДЕНИЕ

Термины КСОВ (комплексная система обеспечения безопасности), ИСВ (интегрированная система безопасности) и ИЗ (интеллектуальное здание) возникли сравнительно недавно (1994 г.) в связи с решением обеспечения безопасности крупных объектов*.

К этому времени уже широко использовались отдельные системы для обеспечения безопасности объектов:

- охранно-пожарная система (ОПС);
- система контроля и управления доступом (СКУД);
- система охранного телевидения (СОТ);
- система жизнеобеспечения.

Поэтому первым шагом при создании ИСВ было объединение существующих систем в одну под общим управлением. Позже пришло понимание того, что, кроме обеспечения безопасности, такие системы должны также обеспечивать решение задачи противодействия широкому спектру угроз, носящих различный характер и исходящих от разного рода нарушителей. Подобные системы получили название комплексные системы обеспечения безопасности (КСОВ).

Таким образом, по характеру решаемых задач и целям понятие КСОВ является более широким, чем понятие ИСВ.

Понятие «Интеллектуальное здание» (ИЗ) в России появилось позднее, уже на следующем этапе в обеспечении безопасности крупных объектов.

Основные характеристики ИЗ:

- оптимальная структура объекта;
- оптимальная структура и набор необходимых систем жизнеобеспечения;
- оптимальная структура службы безопасности;
- оптимальное управление всеми элементами объекта и взаимоотношениями между элементами.

* Под крупным объектом будем понимать объект, состоящий из 20–200 самостоятельных помещений, которые необходимо ставить или снимать с охраны.

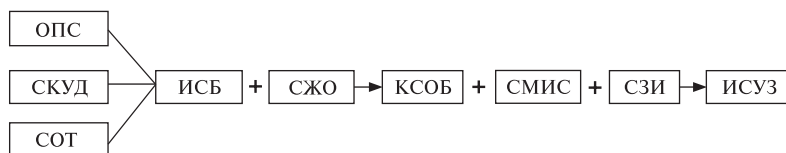


Рис. В.1. Этапы превращения ИСБ в КСОВ и ИСУЗ

Затем пришло понимание того, что все системы обеспечения безопасности (СОВ) должны использоваться не только по своему прямому назначению, но и в интересах других сфер деятельности защищаемого объекта. В этом случае ИСБ, КСОВ, ИЗ должны фактически становиться системами контроля бизнеса, т. е. они органично встраиваются в общую систему управления бизнесом без нарушения существующей организационной структуры предприятия и без больших затрат [18].

Однако с точки зрения нормативной документации дать определение ИСБ, КСОВ, ИЗ не так просто. Последние 15 лет у нас обсуждается данная тема [1, 18, 30, 52, 53, 55, 57, 58, 65, 66, 69, 78], но пока общепринятые нормы в этой сфере не разработаны. Пока все эксперты только сходятся на одной мысли, что применение ИСБ является достаточно эффективным.

Поэтому, пока не будет создана единая нормативная база, будем считать, что ИСБ в основном состоит из подсистем: ОПС, СКУД, СОТ. Если к этому набору подсистем добавить систему жизнеобеспечения (СЖО), то получим КСОВ. Если добавить к КСОВ систему мониторинга и управления инженерными системами (СМИС) и систему защиты информации (СЗИ), то получим ИСУЗ (интеллектуальная система управления зданием). Этот процесс превращения ИСБ в КСОВ и ИСУЗ показан на рис. В.1.

Таким образом, СОВ позволяет оптимизировать распределение целей, задач, обязанностей, ответственности, как отдельных сотрудников, так и подразделений объекта.

На рис. В.2 приведены преимущества в деятельности предприятия, применяющего комплексную СОВ, эти преимущества заключаются в следующем:

- направленность на предупреждение процессов возникновения и развития угроз;
- многопараметрический анализ в текущем режиме времени;
- снижение неопределённости в оценке развития событий;
- итерационное планирование на основе данных индикаторов безопасности;

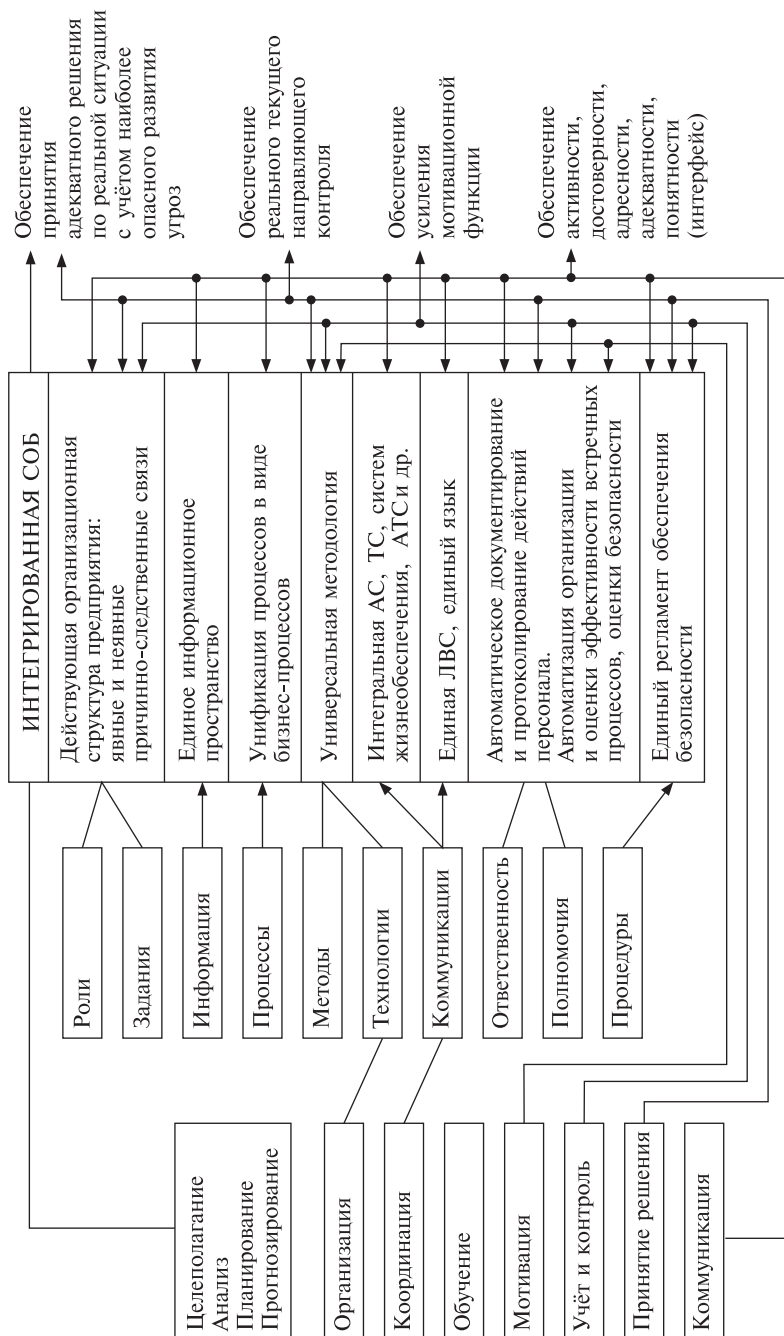


Рис. В.2. Преимущества КСОБ

- повышение эффективности в работе организации;
- усиление мотивации персонала;
- обучение персонала на реальных ситуациях «собственного» объекта;
- эффективный контроль деятельности предприятия;
- обеспечение адекватности и устойчивости коммуникаций;
- снижение риска при принятии решения и т. д.

В настоящее время на большинстве предприятий уже существуют отдельные подсистемы обеспечения безопасности: ОПС, СКУД, СОТ, АТС, ИС и др. При создании комплексных СОБ одна из них может послужить *базовой*.

Хорошие результаты достигаются, если ИСБ строятся либо на единой элементной базе, либо на единой программной платформе.

Выше мы уже говорили, что одной из проблем, сдерживающих широкое внедрение КСОБ и ИСУЗ, является отсутствие нормативно-правовой базы.

В соответствии с ФЗ № 184 «О техническом регулировании» должны быть разработаны технические регламенты (ТР). На начало 2012 г. большая часть технических регламентов в ИБ еще не принята.

В настоящее время в стадии разработки находятся:

Общий технический регламент (ОТР) «О безопасной эксплуатации зданий, строений и безопасном использовании прилегающих к ним территорий».

ОТР «Общие требования пожарной безопасности».

Специальный технический регламент (СТР) «О технических требованиях к системам антитеррористической и антикриминалистической защиты объектов».

СТР «О технических требованиях к системам противокриминалистической защиты имущества».

С учетом того, что по Федеральному закону № 65 от 01.05.2007 г., внесшему ряд существенных изменений в Закон № 184 «О техническом регулировании», деление регламентов на общие и специальные (ОТР и СТР) отменено, в разрабатываемые ТР будут внесены соответствующие коррективы.

К числу действующих нормативных актов следует отнести:

ГОСТ Р 22.1.12-2005 «Безопасность в ЧС. Структурирования система мониторинга и управления инженерными системами зданий и сооружений. Общие требования».

ОГЛАВЛЕНИЕ

Введение	3
1. Интегрированные системы безопасности.....	8
1.1. Этапы разработки ИСБ	13
1.2. Структура ИСБ	15
1.3. Тенденции в развитии ИСБ	20
1.4. Примеры ИСБ.....	21
2. Комплексные системы обеспечения безопасности	60
2.1. Стандарты и протоколы КСОВ (СКОВ)	62
2.2. Структура КСОВ (СКОВ)	66
2.3. Примеры КСОВ	70
3. Интеллектуальное здание	86
3.1. Нормативная база	91
3.2. Структура интеллектуального здания	103
3.3. Тенденции в развитии ИЗ	106
3.4. Примеры ИЗ.....	107
4. Методы оценки защищенности объекта	117
Приложение 1. Перспективная программа развития национальных стандартов	122
Приложение 2. Вариант ТЗ на разработку ИСБ.....	139
Приложение 3. Перечень компаний производящих компоненты и системы безопасности (ИСБ, КСОВ, СУИЗ (ИЗ)	141
Приложение 4. Фрагмент документа МГСН 4.19-260-Г	142
Приложение 5. Сравнение открытых и закрытых систем	151
Список сокращений.....	152
Литература	155