

УДК 004.896.021

В. А. Куделькин
 Консорциум «Интегра-С», г. Самара
 И. М. Янников
 ИжГТУ имени М. Т. Калашникова

**АЛГОРИТМ ФУНКЦИОНИРОВАНИЯ РАСПРЕДЕЛЕННОЙ РАЗНОУРОВНЕВОЙ
 ИНТЕЛЛЕКТУАЛЬНОЙ ИНТЕГРИРОВАННОЙ СИСТЕМЫ БЕЗОПАСНОСТИ
 ПОТЕНЦИАЛЬНО ОПАСНЫХ ОБЪЕКТОВ**

Описан алгоритм функционирования распределенной разноуровневой интеллектуальной интегрированной системы безопасности потенциально опасных объектов. Рассмотрены преимущества, которые дает интегрированная система безопасности независимо от количества объектов и их географического расположения.

Ключевые слова: контроль физической защищенности, многоуровневое принятие решений, комплексное описание состояния защищенности объекта, интеграция данных.

Быстрое развитие современных технологий в области управления безопасностью позволяет рассматривать эту область не только как комплекс отдельных процессов, процедур и оборудования, направленных на охрану объектов или баз данных против несанкционированного доступа или использования, но и как всеохватывающую и более программно ориентированную систему [1, 2].

Разработанная авторами распределенная интеллектуальная интегрированная система безопасности (далее ИИСБ) содержит несколько ИИСБ низкого уровня и не менее одной ИИСБ высокого уровня, соединенной с ИИСБ низкого уровня (рис. 1) [3].

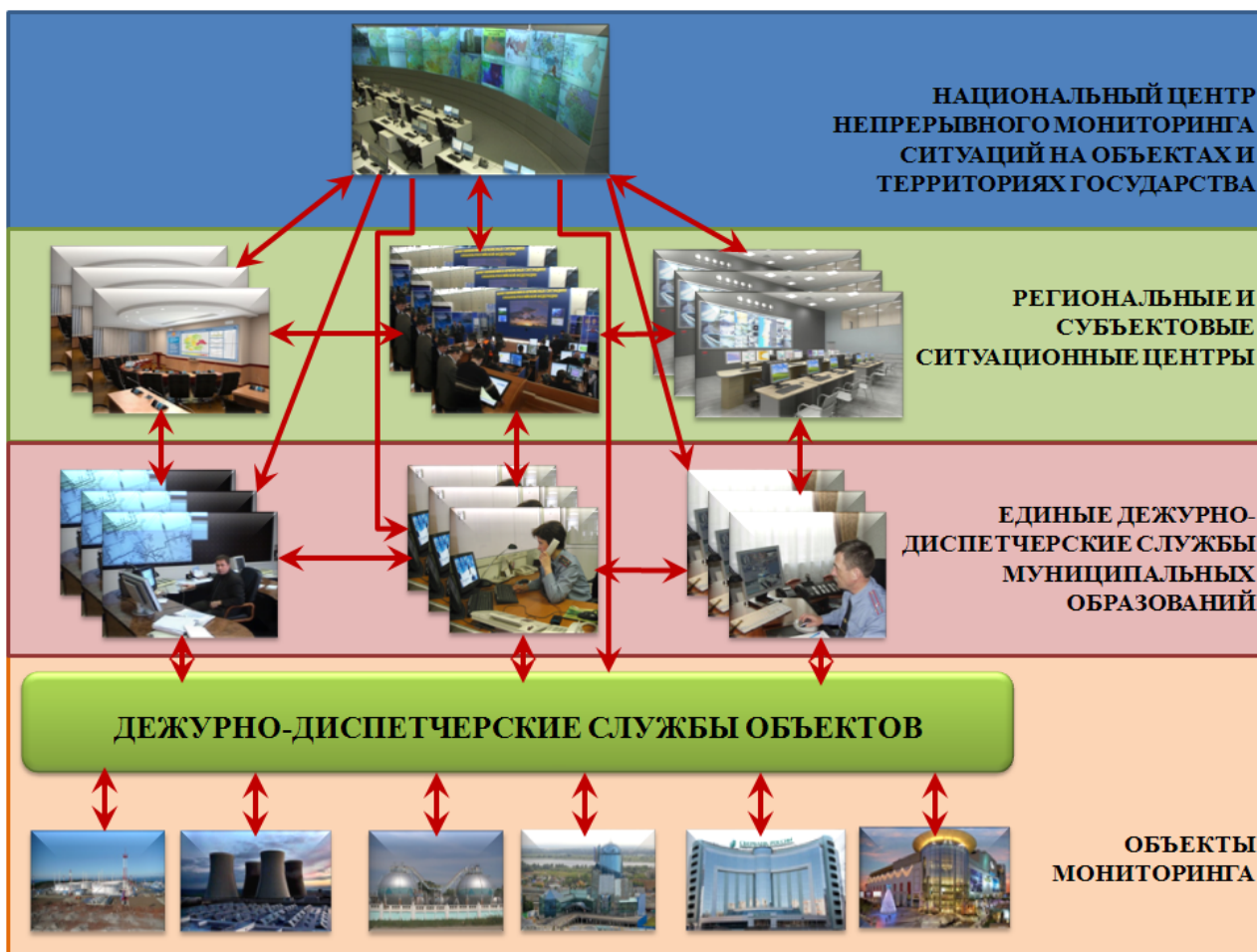


Рис. 1. Иерархическая схема организации контроля защищенности объектов

Алгоритм работы распределенной ИИСБ приведен на рис. 2. Результаты контроля физической защищенности объекта отображаются на видеомониторе и одновременно поступают на хранение в базу данных. В случае отклонения параметров защиты

в соответствии с правилами включается в действие автоматическая система.

Принятие оперативных решений, в том числе с использованием видеоданных, проводится в соответствии с инструкциями.

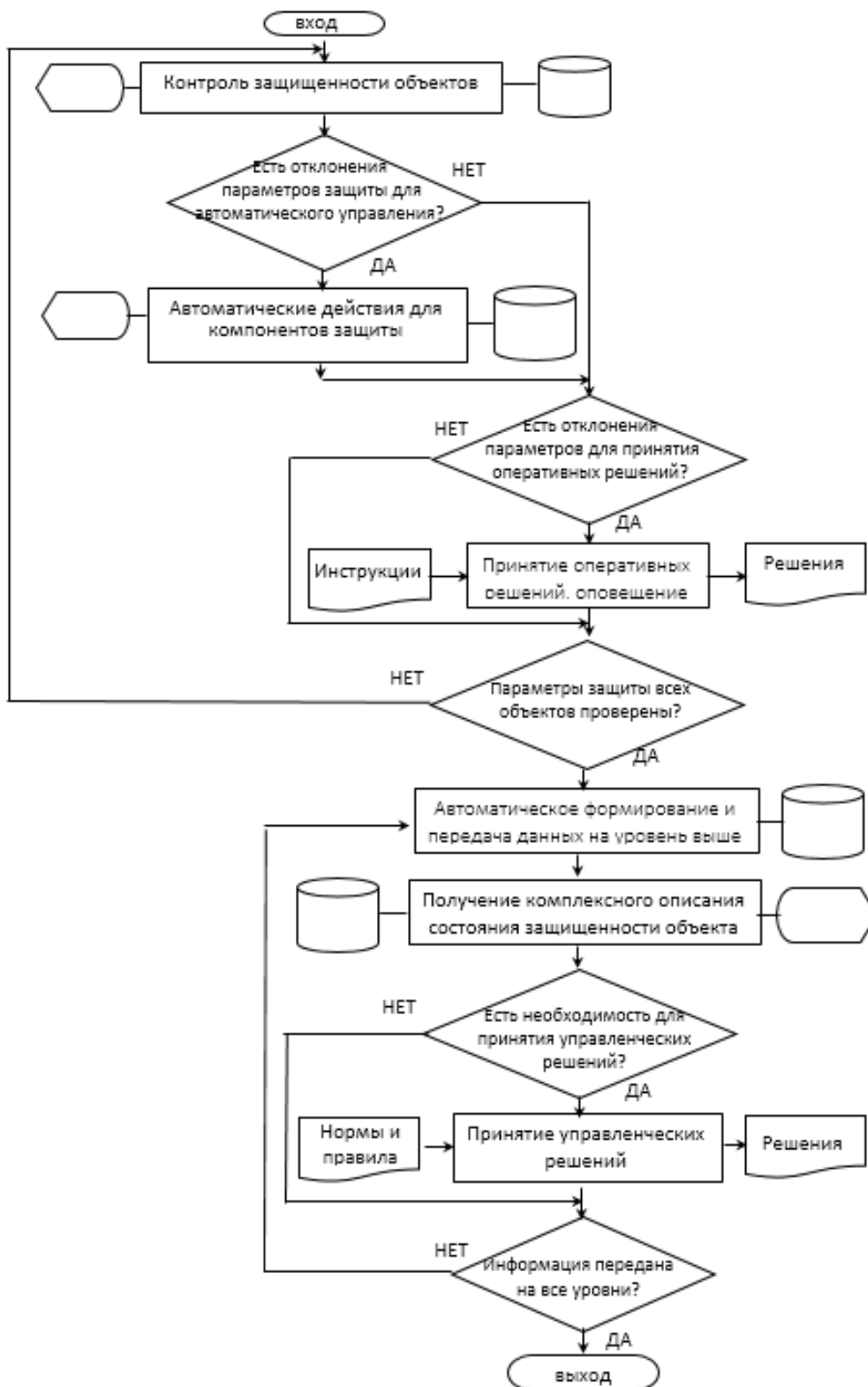


Рис. 2. Алгоритм работы распределенной ИИСБ

Независимо от автоматических действия компонентов защиты данные анализируются на наличие отклонений для принятия оперативных решений.

Решения поступают на объект управления и на вышестоящий уровень управления объектом. Анализ отклонений производится непрерывно, пока будет необходима физическая защита объекта.

Формирование отчетов и их отправка на более высокий уровень производится автоматически. До этого в алгоритме рассматривался контроль данных с объекта, на этом этапе данные поступают со всех контролируемых объектов. По результатам поступившей информации формируется комплексное описание состояния защищенности объекта, в том числе с числовыми оценками состояния и отображением данных на цифровой карте и в режиме 3Д и 4Д [4].

При необходимости принимаются управленческие решения, направленные на изменение состава и характеристик компонентов физической защиты, периодичности и состава поступающих данных, правил для автоматического управления системой защиты, а также инструкций и правил для принятия оперативных решений. Все решения на любом уровне должны соответствовать установленным законами нормативным документам.

Если данные поступили не на все вышестоящие уровни, проводится дальнейшая передача данных и формирование комплексного описания состояния кластеров объектов или доменов, позволяя объединить тысячи объектов федерального значения в единую систему непрерывного мониторинга ситуаций на объектах и территориях. Такая распределенная ИИСБ используется для обеспечения безопасности стратегически важных объектов государства: вокзалов, мостов, гидросооружений, портов, тоннелей и др.

Разработанный алгоритм работы распределенной ИИСБ обеспечит интеграцию локальных систем мониторинга безопасности и жизнеобеспечения и создание структур любой сложности с подключением неограниченного числа пользователей, объектов, подсистем безопасности и жизнеобеспечения.

Многоуровневость интеллектуальных интегрированных систем достигается:

- установкой ИИСБ низкого уровня – на частях объекта, а ИИСБ высокого уровня – на объекте;
- установкой ИИСБ низкого уровня – на объектах, ИИСБ более высокого уровня – в центре системы высокого уровня;
- соединением нескольких ИИСБ с глобальной ИИСБ через любую информационную сеть, в том числе Интернет, телефонную сеть или спутниковую связь.

Комплексные системы управления могут быть установлены как при строительстве новых зданий, так и в качестве надстройки к уже функционирующим системам. Конечная цель состоит в том, чтобы связать все сети и системы жизнеобеспечения здания единой IP-сетью.

Преимущества, которые дает интегрированная система безопасности при эксплуатации одного здания, относятся и к распределенному объекту, управ-

ляемому одной компанией, независимо от количества объектов и их географического расположения:

- повышение эффективности ведения бизнеса и управление системами безопасности без ограничения;
- контроль единым органом управления сетей, связанных воедино и подключенных к интегрированной системе безопасности;
- обеспечение гибкости в управлении, возможности перепрограммирования и расширенной функциональности;
- уменьшение сложности эксплуатации;
- снижение уровня первоначальных инвестиций, получение значительно более мощных решений в вопросах безопасности;
- повышение эффективности работы службы безопасности за счет совместной работы всех сетей здания и их возможности обмениваться данными и информацией;
- возможность руководителям служб безопасности благодаря единому интерфейсу менять режимы или уровни безопасности в одно мгновение или увеличивать объем данных, фиксируемых специальными системами.

Повышает безопасность людей, находящихся в здании, коллективное использование информации за счет более быстрого и четкого выявления проблемы и реакции на сигналы тревоги сотрудников служб безопасности.

За счет простой коммуникации всех систем, интегрированных в одну сеть, происходит улучшение информативности отчетов и более глубокое понимание сотрудниками текущего состояния по объекту (объектам).

Менеджеры по безопасности могут управлять интегрированными системами безопасности в соответствии с разработанным алгоритмом с различных устройств, в любое время, в любом месте, в том числе при дистанционном управлении для обеспечения доступа к системе с применением веб-страниц, карманных персональных компьютеров, сотовых телефонов и коммуникаторов. При необходимости эвакуации менеджеры по безопасности могут эвакуировать людей, находящихся в здании, и по-прежнему продолжать осуществлять контроль всех систем на объекте.

Разработанный алгоритм работы распределенной ИИСБ в совокупности со средствами связи дает возможность получать полную информацию с объектов в режиме онлайн, управлять установленными подсистемами безопасности и контролировать их техническое состояние. Реализованная система оснащена шифрацией каналов связи и имеет соответствующие сертификаты ФСБ России, а также обеспечивает доступ посредством электронной подписи.

Библиографические ссылки

1. Телегина М. В., Янников И. М., Габричидзе Т. Г. Методы и алгоритмы оценки воздействия потенциально опасных объектов на окружающую среду : монография. – Самара : Изд-во Самар. НЦ РАН, 2011. – 200 с.

2. Янников И. М., Габричидзе Т. Г., Янников И. М. Основы организации системы многоступенчатого экологического мониторинга и ее сопряжение с АИУС РСЧС // Промышленная и экологическая безопасность. – 2007. – № 5 (7). – С. 13–18.

3. Куделькин В. А., Денисов В. Ф. Архитектура интегрированных распределенных систем мониторинга и объектов

безопасности организационно-технических систем и территорий // МОНИТОРИНГ. Наука и безопасность. – 2013. – № 4 (12). – С. 64–79.

4. Система непрерывного мониторинга ситуаций на объектах и территориях «Интегра 4D» // Консорциум «Интегра-С»: Интеллектуальные системы безопасности. – Самара, 2014. – 30 с.

* * *

Kudelkin V. A., Consortium "Integra-S"
Yannikov I. M., Kalashnikov ISTU

Operation algorithm of distributed multi-level intellectual integrated security systems for potentially hazardous objects

The paper describes the operation algorithm of a distributed multi-level intelligent integrated security system for potentially dangerous objects. The paper also considers the advantages offered by the integrated security system regardless of the number of objects and their geographical location.

Keywords: physical security control, multi-level decision-making, comprehensive description of the object protection, data integration.

Получено: 18.09.15