УДК 004.056
DOI: 10.33764/2618-981X-2019-6-2-99-104

ОБЗОР СИСТЕМ И МЕТОДОВ КОНТРОЛЯ ДАННЫХ НА ПРИБОРОСТРОИТЕЛЬНОМ ПРЕДПРИЯТИИ

Денис Александрович Штепа
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант, тел. (913)376-35-88, e-mail: denis.shtepa@ngs.ru

Владимир Васильевич Чен-Шан
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант, тел. (953)788-87-00, e-mail: rf.cmex@gmail.com

Иван Андреевич Антонов
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант, тел. (960)786-74-33, e-mail: romeo00717437@mail.ru

Евгений Владимирович Грицкевич
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, кандидат технических наук, доцент кафедры информационной безопасности, тел. (383)343-91-11, e-mail: gricew@mail.ru

В статье анализируется ситуация, связанная с соблюдением режима сохранения целостности информации, циркулирующей в автоматизированной информационной системе, контроля требуемого уровня защиты информации, размещенной в базах данных этой системы, а также корректности функционирования применяемых при обработке алгоритмов. Рассматривается ситуация, характерная, прежде всего, для приборостроительного предприятия, на котором уже эксплуатируется или планируется к внедрению подобная система. Даны рекомендации по повышению ее информационной защищенности, намечены перспективные пути научной проработки возникающих при этом проблем.

Ключевые слова: информация, система, защита, безопасность, модель, целостность, нарушитель, угроза, управление.

OVERVIEW OF DATA CONTROL SYSTEMS AND METHODS AT DEVICE ENGINEERING ENTERPRISE

Denis A. Shtepa
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, phone: (913)376-35-88, e-mail: denis.shtepa@ngs.ru

Vladimir V. Chen-Shan
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, phone: (953)788-87-00, e-mail: rf.cmex@gmail.com

Ivan A. Antonov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, phone: (960)786-74-33, e-mail: romeo00717437@mail.ru

Evgenij V. Gritskevich
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Ph. D., Associate Professor, Department of Information Security, phone: (383)343-91-11, e-mail: gricew@mail.ru

The article analyzes the situation related to compliance of regime of preservation the integrity of information circulating in automated information system, control of required information protection level in system databases, as well as the correctness of functioning of algorithms used in processing. A situation is considered that is characteristic, first of all, for a device engineering enterprise, in which a similar system is already in operation or is planned to be introduced. Recommendations are given to improve its information security, promising ways of scientific study of arising problems are outlined.

Key words: information, system, protection, security, model, integrity, intruder, threat, control.

Введение

Режим сохранения целостности информации обеспечивает информационную защиту предприятия. Необходимо принимать во внимание, что в условиях современного высокотехнологичного производства практически вся используемая в производственном процессе информация размещается в базах данных (БД), входящих в состав автоматизированных информационных систем (АИС). Сохранение целостности означает и постоянный контроль корректности алгоритмов, обрабатывающих данные, необходимые для решения технологических задач. Для части производственных информационных систем главным аспектом является защита от несанкционированного внесения изменений [1–3]. Важнейшим условием обеспечения информационной безопасности АИС является гарантия отсутствия нарушения целостности программных технологий, обеспечивающих защиту информационных ресурсов.

Необходимо пояснить, в чем состоят особенности современного приборостроительного предприятия с точки зрения обеспечения его информационной безопасности. Для крупных производственных объектов, например, предприятий обрабатывающего цикла, проблемы такой безопасности решаются на государственном уровне [4]. Кроме того, движение информационных потоков как внутри предприятия, так и вне его нередко совпадает с движением материальных ресурсов, участвующих в производственном процессе. При этом номенклатура как информационных, так и материальных потоков является ограниченной по своему составу, что предопределяет эффективность мероприятий по защите целостности циркулирующей информации.

Иная ситуация характерна для приборостроительного предприятия. Во-первых, номенклатура выпуска производимых изделий является достаточно разнообразной и часто изменяемой. Во-вторых, при изготовлении выпускаемой продукции используется большое количество комплектующих элементов, что предопределяет разнообразие структурных компонентов баз данных, используемых при производстве конечной продукции, а также разветвленную сеть информационно-телекоммуникационных связей с экономическими партнерами,

в том числе и зарубежными. В-третьих, частая замена комплектующих изделий, например, из-за необходимости постоянной поддержки современного научно-технологического уровня производства, требует постоянной модификации соответствующих информационных ресурсов и изменения внешних информационных потоков за счет перемены поставщиков (смежников). В-четвертых, любое приборостроительное предприятие обладает высокой степенью эксклюзивности, что создает проблемы для применения стандартных подходов и требует адаптации последних к конкретным условиям производства, а также тщательной подстройки используемых в производстве информационных технологий.

Вышеперечисленные факторы объясняют актуальность темы данной работы.

Цель и задачи исследования

Целью работы является обзор систем и методов контроля данных на приборостроительном предприятии. Выбор архитектуры информационной системы, разработка и модификация управляющих программных технологий, обеспечивающих ее функционирование, являются ключевыми моментами поддержания требуемого уровня защищенности информации. Решение этих задач нуждается в соответствующей научной поддержке.

Общераспространенной практикой эксплуатации АИС является ситуация, когда используемые в АИС системы управления базами данных (СУБД) получены в виде готовых программных продуктов от внешнего контрагента, не имеющего никакого отношения к самой АИС [3]. Часто таким контрагентом выступает иностранный производитель, который не только не контролируется государственными органами, относящимися к сфере информационной безопасности, но и практически недоступен (или, по крайней мере, малодоступен) создателям АИС с точки зрения возможности получения оперативной информации по особенностям практического использования применяемой СУБД.

Наибольшие затруднения вызывает отсутствие у разработчиков АИС исходного программного кода СУБД промышленного уровня иностранного производства. Поэтому информация АИС хранится и обрабатывается с помощью алгоритмов, которые выполнены в программных модулях с закрытым кодом. Это несет высокий риск, так как в таком коде могут быть оставлены, по ошибке его создателей или сознательно, скрытые возможности по отключению средств защиты, что, в свою очередь, ставит под угрозу информационную безопасность организации. Решением проблемы является дополнение АИС системой обеспечения целостности (СОЦ).

Структура автоматизированных информационных систем

Структура применяемой или разрабатываемой АИС должна предусматривать целостность программных модулей серверной части БД, целостность информационных потоков при их транзакциях между клиентской и серверной частями, а также целостность программ, относящихся к клиентской части [5, 6].

Программными модулями могут являться автоматически генерируемые отчетные рапорты и формуляры, а также служебные библиотеки, подключаемые по мере необходимости в процессе функционирования АИС. Эти модули входят в состав операционной системы (ОС) клиентской части. Структура АИС может быть двухзвенной или трехзвенной. В первом случае пользователи находятся в клиентской части АИС [5, 7]. Во втором случае клиентская часть реализуется с помощью дополнительного (промежуточного) звена, называемого сервером приложений. На рис. 1 изображена обобщенная структура защищаемых АИС [3].

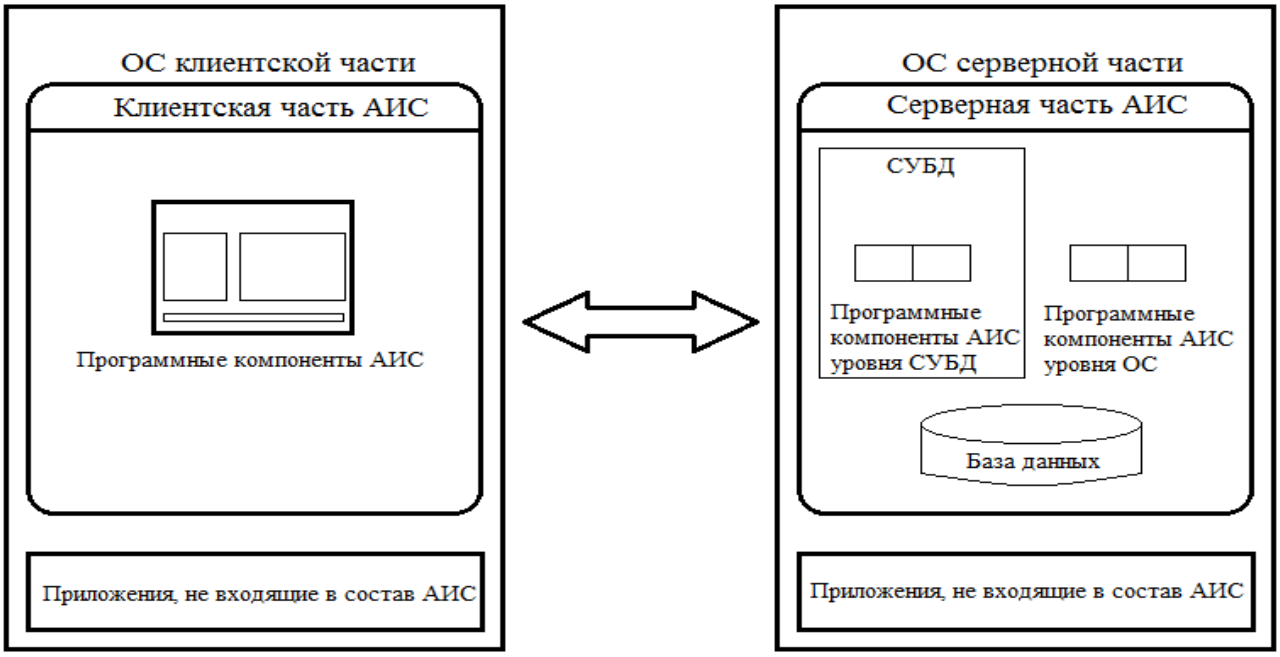

Рис. 1. Обобщенная структура АИС с СУБД

В данный момент наиболее часто применяемой моделью информационной безопасности является субъектно-ориентированная модель (СО-модель) защиты информации в АИС. Такая модель использует понятие изолированной программной среды (ИПС) [2, 8]. ИПС является набором программных модулей, в котором любой активный программный модуль не оказывает влияния на другой программный модуль и на данные, которые необходимы для работы иного алгоритма (программного компонента). Любая программа использует только для нее предназначенные данные. Активными могут стать только те программные компоненты, целостность которых протестирована и не вызывает сомнения [9, 10]. При этом возникает необходимость расширения ИПС до доверенной вычислительной среды (ДВС), поскольку в качестве программного компонента потенциальный злоумышленник может использовать программу, не входящую в состав АИС, или преднамеренно измененный программный код легального модуля.

При расположении компонента безопасности находится за пределами ДВС, необходимо наличие компонента, обеспечивающего возможность контролирования и, в случае необходимости, вмешательства в процессы функционирования ДВС при детектировании режимов работы, не предусмотренных протоколом. Подобный компонент должен являться резидентным объектом [8, 11], входящим в состав АИС. Он так и называется: резидентный компонент безопасности (РКБ). Элементом РКБ, реализуемом на физическом уровне, является аппаратная часть СОЦ, которая выполнена в виде электронной печатной платы, либо имеющей порт USB, либо монтируемой в блоке сервера СУБД АИС. Блочная структура СОЦ показана на рис. 2.

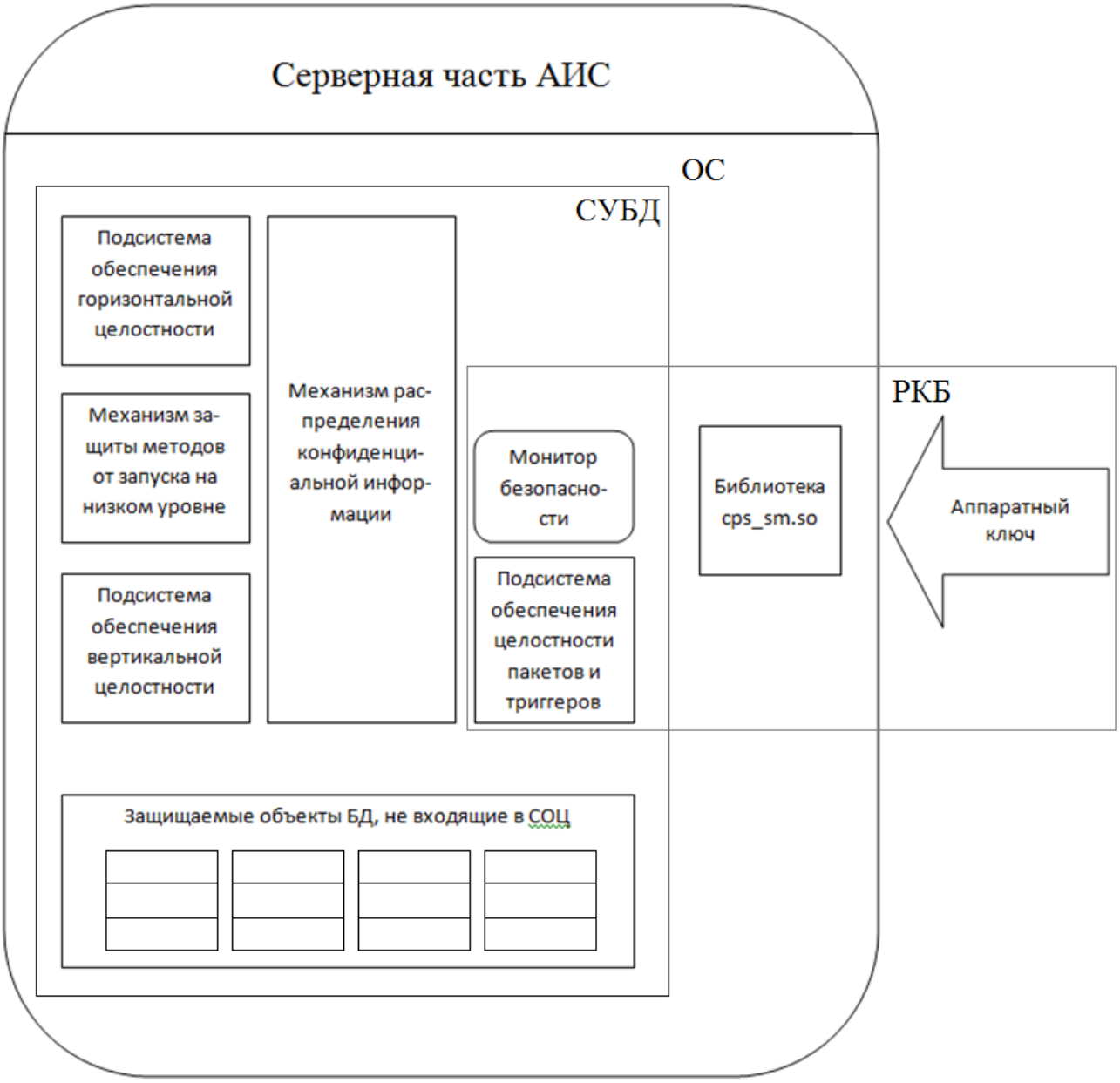

Рис. 2. Блочная структура СОЦ

Блочная структура СОЦ обеспечивает ее модифицируемость, адаптируемость и практическую настраиваемость к конкретным особенностям применяемой АИС.

Заключение

Очевидно, что РКБ является ядром СОЦ. РКБ должен включать в себя программные компоненты, находящиеся во взаимодействии и размещающиеся в разных уровнях. Модульный подход к архитектурным принципам построения АИС создает потенциальные возможности для их успешного применения в условиях современного приборостроительного предприятия.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Positive research 2015. Сборник исследований по практической безопасности [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/upload/corporate/ru-ru/download/PT_Positive_Research_2015_RU_web.pdf.
2. Громов Ю. Ю., Драчев В. О., Иванова О. Г. Информационная безопасность и защита информации : учеб. пособие. – Старый Оскол : ТНТ, 2010. – 384 с.
3. Рыжко А. Л., Рыбников А. И., Рыжко Н. А. Информационные системы управления производственной компанией : учебник для академического бакалавриата. – Люберцы : Юрайт, 2016. – 354 с.
4. В «Норникеле» оценили перспективы развития информационной безопасности [Электронный ресурс]. – Режим доступа: https://lenta.ru/news/2019/04/10/kyber/.
5. Ворона В. А., Тихонов В. А. Системы контроля и управления доступом. – М. : Горячая линия Телеком, 2010. – 272 с.
6. Указ Президента Российской Федерации «О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» от 9 мая 2017 г. № 203 [Электронный ресурс]. – Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_216363/.
7. Выявление угроз информационной безопасности в реальном времени / Пархоменко Н. Г., Боташев Н. М., Колбанов П. М., Григоренко Е. С. // Известия ЮФУ. Технические науки. – 2016. – № 4. – С. 325–326.
8. Ярочкин В. И. Информационная безопасность : учебник для студентов вузов. – 3-е изд. – М. : Академический проект : Гаудеамус, 2004. – 544 с.
9. Безопасность критической информационной инфраструктуры РФ: коротко о главном [Электронный ресурс]. – Режим доступа: http://iteco.vestifinance.ru/bezopasnost_kriticheskojj_inform.
10. Петраков А. В. Основы практической защиты информации. – М. : СОЛОН-Пресс, 2005. – 384 с.
11. Зегжда Д. П., Ивашко А.М. Основы безопасности информационных систем. – М. : Горячая линия Телеком, 2000. – 452 с.