Д. А. Мельников, В. Р. Петров, Е. В. Дириенко, А. А. Абрамов, И. А. Корсаков, С. С. Кузьминов

СПОСОБ ПАРИРОВАНИЯ АТАК НА СИСТЕМУ СЕТЕВОЙ СИНХРОНИЗАЦИИ, РЕАЛИЗОВАННЫЙ В СОДС «МАРШ! 3.0»[1]

Основным предназначением программно-аппаратного комплекса (средства) обеспечения доверенного сеанса связи СОДС «МАРШ! 3.0» (СОДС «МАРШ! 3.0») является обеспечение надежного с точки зрения обеспечения информационной безопасности (ИБ) и доверенного сеанса связи между взаимодействующими субъектами/объектами. Сеанс связи (или процедура информационного обмена, ПИнО), как правило, будет проводиться при решении различного рода задач ИБ, включая процедуры аутентификации (идентификации), управления доступом (УД), обеспечения неотказуемости, конфиденциальности, целостности и управления криптографическими ключами, а также аудиторских проверок.

1. Методика парирования атак на системы синхронизации

Методика парирования атак на систему сетевого времени (синхронизации) основана на целевой функции системы обеспечения ИБ и принципах функционирования СОДС «МАРШ! 3.0» с точки зрения обеспечения ИБ ПИнО.

1.1. Цель и частные задачи обеспечения безопасности ИТС

Цель обеспечения безопасности информационно-технологической сети или системы (ИТС) заключается в следующем: предоставить организации (частному лицу) возможность решать все свои экономические задачи и добиваться определенных результатов в своей основной деятельности с помощью внедрения ИТС в точном соответствии с рисками для организации (частного лица), связанными с использованием ИТС и взаимодействием со своими партнерами и потребителями.

Цель обеспечения ИБ может быть достигнута путем решения следующих частных задач обеспечения ИБ (рис. 1) [1, 2].

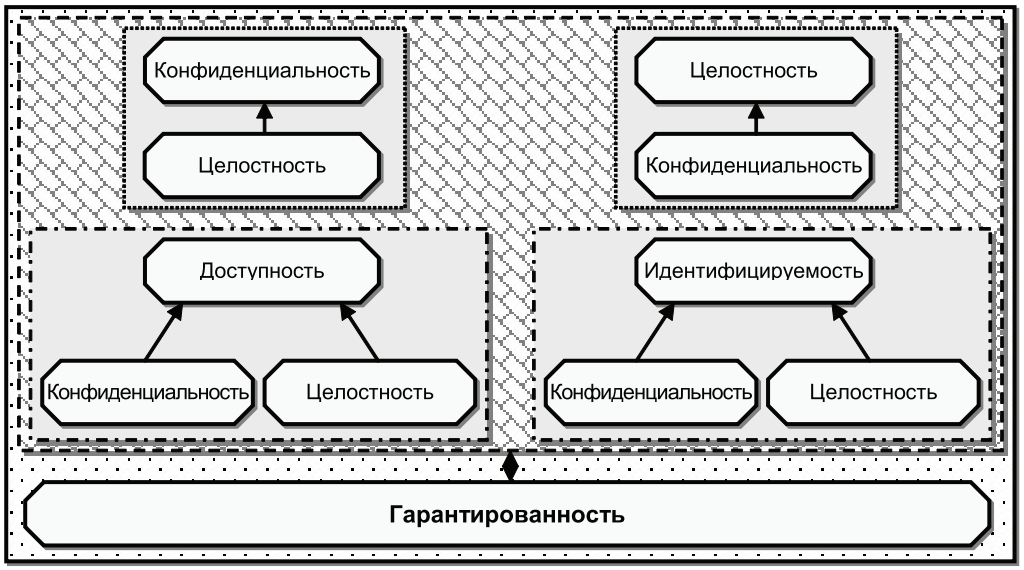

Рис. 1. Взаимозависимость задач обеспечения ИБ

[1] Данная работа выполнена в НИЯУ МИФИ при финансовой поддержке Министерства образования и науки Российской Федерации в рамках проекта «Создание инженерно-технических решений для высокотехнологичного производства инновационных программно-аппаратных средств защиты информации на базе перспективных высокоскоростных интерфейсов информационного взаимодействия», выполняемого совместно с ООО «ОКБ САПР» по договору № 02.G25.31.0050.

Доступность (систем и данных только для их использования по предназначению) представляет собой требование, предназначенное для обеспечения гарантий того, что система функционирует без задержек и для авторизованных пользователей не будет отказов в обслуживании.

Целостность (системы и данных) имеет два аспекта:

1) целостность данных (свойство, при котором данные не могут изменяться противоправным способом при их хранении, обработке и передаче);

2) целостность системы (качественная характеристика, при реализации которой система в период своего функционирования в штатном (неизмененном) режиме свободна от всякого рода противоправных манипуляций).

Конфиденциальность (данных и системной информации) представляет собой требование, в соответствии с которым частная и конфиденциальная информация должна быть не раскрываемой для неавторизованных пользователей. Защита конфиденциальности применяется к данным в процессе их хранения, обработки и передачи.

Идентифицируемость (для отдельного уровня архитектуры безопасности) представляет собой требование, в соответствии с которым все действия субъекта могут быть однозначно отслежены и зафиксированы для данного субъекта.

Гарантированность (того, что все предшествующие четыре задачи решаются (или решены) адекватно) является основой уверенности в том, что средства обеспечения безопасности (и технические, и эксплуатационные) работают по своему прямому предназначению, то есть защищают систему и реализуемые в ней процессы обработки информации.

Считается, что предыдущие четыре задачи (целостность, доступность, конфиденциальность и идентифицируемость) решаются (или решены) адекватно, когда:

1) обеспечена необходимая функциональность и она корректно реализуется;

2) имеет место эффективная защита от непреднамеренных ошибок и сбоев;

3) имеет место эффективная система нейтрализации преднамеренного преодоления защиты или ее обхода.

Гарантированность является очень важной задачей, без решения которой не могут быть решены другие задачи обеспечения ИБ. Уровень гарантированности зависит от исходных требований, предъявляемых к системе обеспечения ИБ.

На рис. 2 [1, 2] представлены службы, которые решают задачу обеспечения гарантий. С точки зрения конкретных служб обеспечения ИБ, гарантированность в большей степени зависит от тех служб, которые непосредственно определяют корректность функционирования и текущие параметры защищенности системы. В этом смысле характер и тип проводимых процедур аутентификации и уровень и объем требований при реализации принудительного режима управления доступом имеют первостепенное значение.

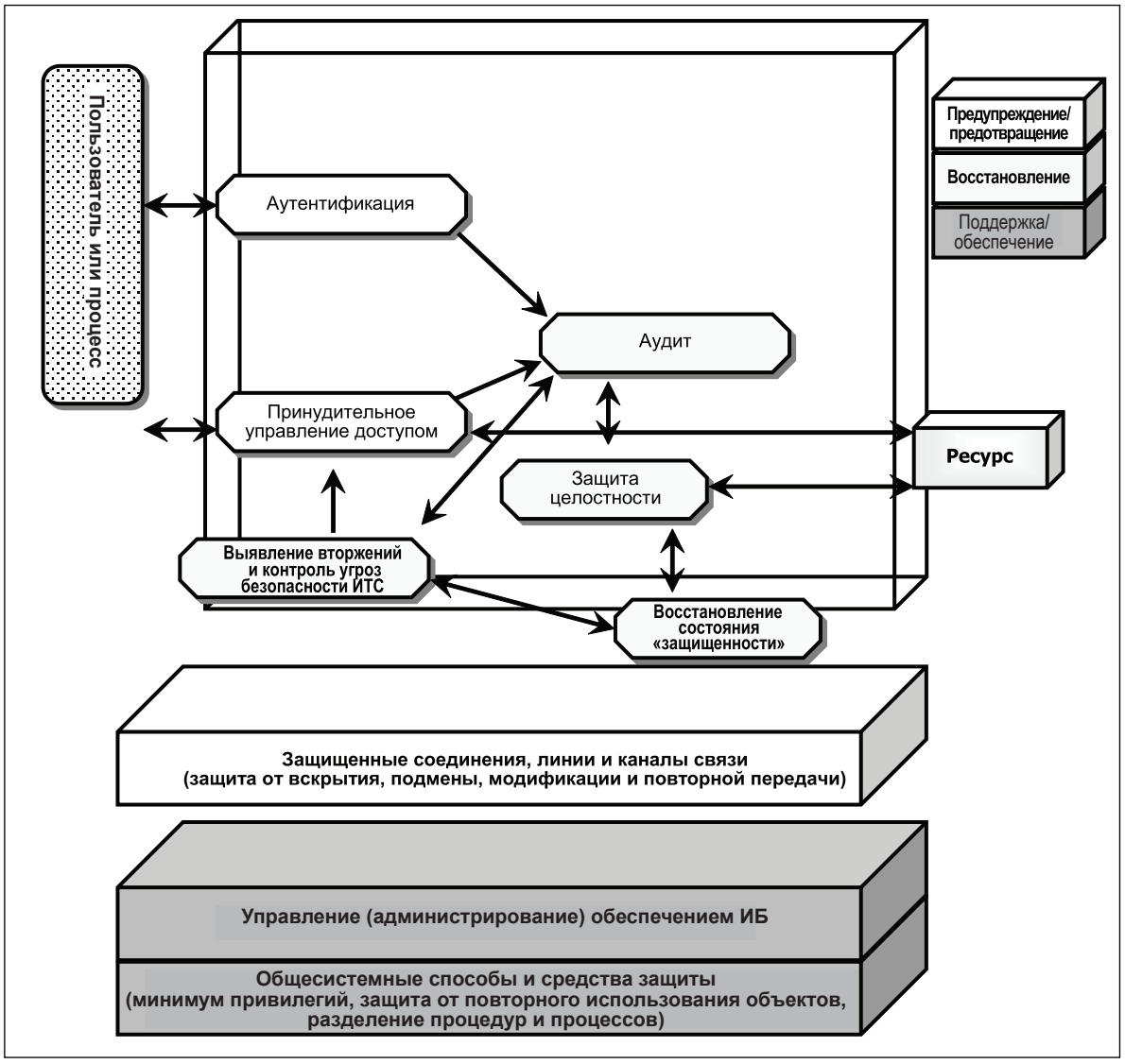

Рис. 2. Основополагающие службы, решающие задачу гарантированности

1.2. Принципы надежного и корректного функционирования СОДС «МАРШ! 3.0»

Первым и основным принципом надежного и корректного функционирования СОДС «МАРШ! 3.0» является наличие гарантий такого функционирования [2, 3]. Этот принцип подразумевает наличие доверенной операционной среды, предоставляющей определенные услуги по обеспечению ИБ, а также других программных компонентов (модулей), обеспечивающих работу СОДС «МАРШ! 3.0» и предоставление указанных услуг.

Второй принцип — создание внутреннего и независимого источника времени, который должен функционировать в автономном режиме. Этот принцип подразумевает, что источник времени должен получать исходный сигнал, формируемый системным процессом доверенной операционной системы.

Третий принцип — все преобразования входного сигнала должны осуществляться только самим источником времени. Любые вмешательства в работу источника времени недопустимы, так как любое воздействие может повлиять на его надежность.

Четвертый принцип — при необходимости (возникновении нештатных событий) любая корректировка источника времени должна осуществляться только по команде владельца СОДС

«МАРШ! 3.0» и только в ручном режиме через графический интерфейс, отображаемый на экране ПЭВМ. Этот принцип подразумевает передачу специализированного запроса на получение заверенной и защищенной метки времени от доверенного источника времени, определяемого соответствующей политикой безопасности.

Пятый принцип — начало функционирования источника времени должно осуществляться только по команде самого владельца СОДС «МАРШ! 3.0» и только один раз: в начале работы с СОДС «МАРШ! 3.0» после инициализации последнего. Этот принцип подразумевает, что в период инициализации работы СОДС «МАРШ! 3.0» в алгоритме работы последнего может быть предусмотрена автоматическая передача запроса на получение защищенной метки времени от доверенного источника времени. В противном случае начальное (текущее) значение времени должно вводиться пользователем.

Шестой принцип — двухмодульное построение источника времени в составе: основной счетчик времени и счетчик-дублер. При этом основной счетчик времени должен функционировать без каких бы то ни было прерываний или остановок.

Строгое выполнение указанных принципов позволит предотвратить любые преднамеренные и случайные действия по модификации и/или фальсификации меток времени.

2. Способ парирования атак компьютерного шпионажа системы сетевого времени

Предлагаемый способ фактически является отражением методики парирования атак на систему сетевого времени (синхронизации). В основе предлагаемого способа лежит использование автономного источника времени, встроенного в СОДС «МАРШ! 3.0» (рис. 3а и 3б).

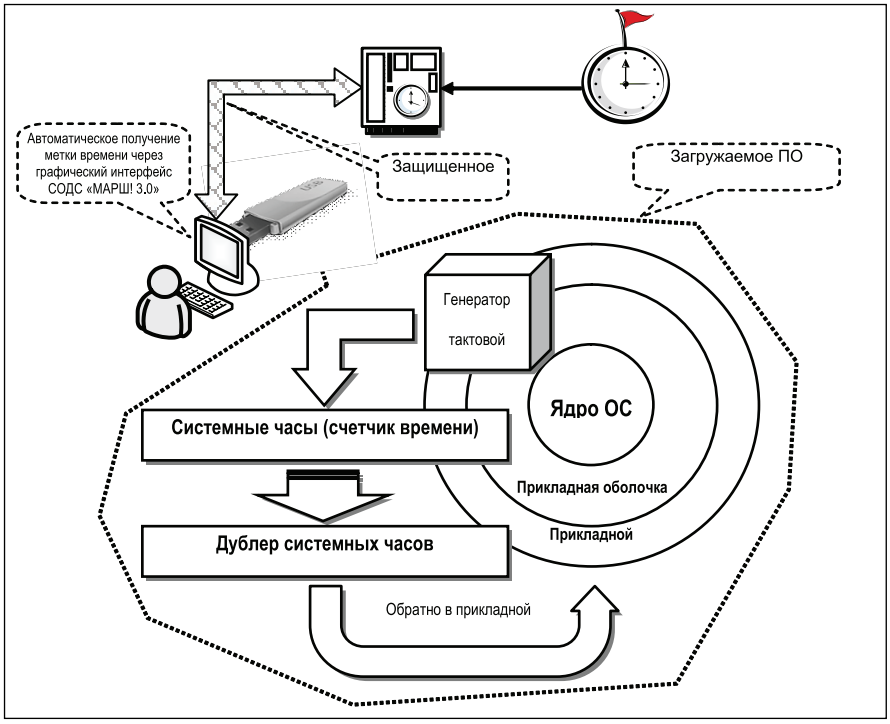

Рис. 3а. Способ парирования криптоаналитических атак на систему сетевого времени (автоматический режим установки начального времени)

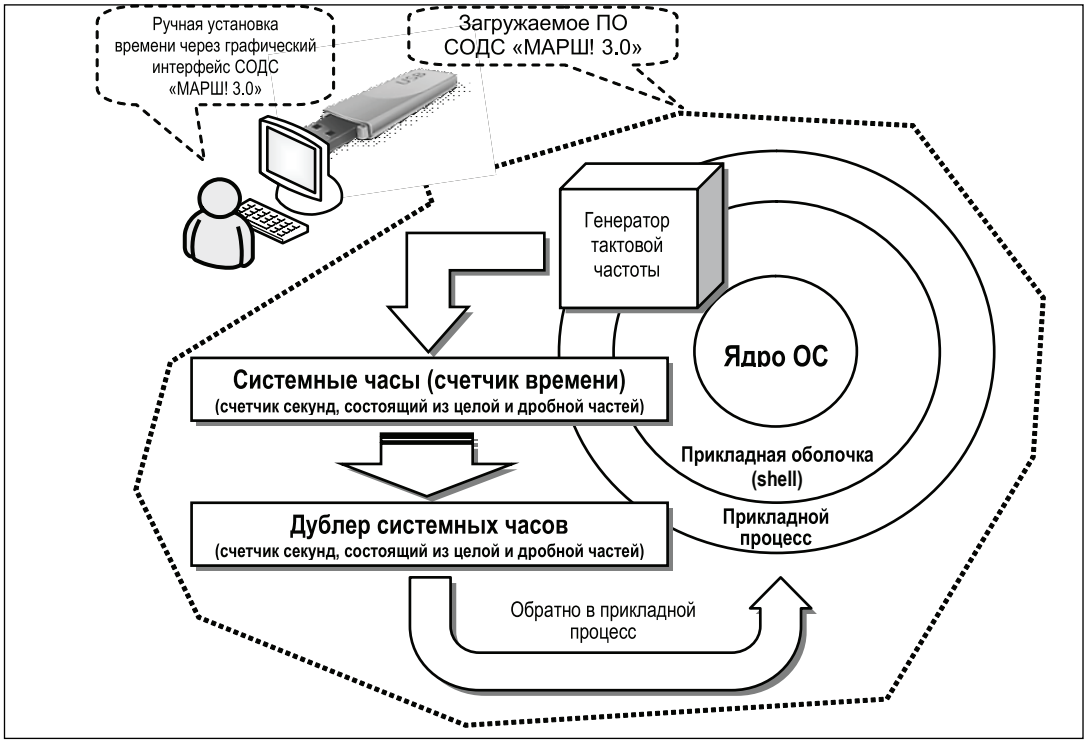

Рис. 3б. Способ парирования криптоаналитических атак на систему сетевого времени (ручной режим установки начального времени)

Сущность способа заключается в том, что использование внутреннего источника меток времени позволяет исключить любую возможность их фальсификации, что, в свою очередь, позволит значительно (более чем в два раза) усложнить задачу криптоанализа на основе подбора открытого текста, решаемую потенциальным нарушителем [1, 4, 5].

3. Реализационные аспекты способа парирования атак компьютерного шпионажа системы сетевого времени (синхронизации)

К особенностям реализации рассмотренного способа парирования атак КШ системы сетевого времени (синхронизации) относятся:

– размещение источника времени «внутри» СОДС «МАРШ! 3.0»;

– использование внутреннего генератора тактовой частоты (ГТЧ);

– в противном случае, ГТЧ является обязательным составным элементом источника времени, а синхронизация (цепь питания) ГТЧ осуществляется по цепи синхронизации элементов сигнала (моментов передачи битов) USB-интерфейса;

– источник времени конструктивно должен исполняться по двухрегистровой схеме (рис. 3а и 3б);

– счетчик времени должен начинать свою работу с момента начала доверенного сеанса связи;

– счетчик времени должен заканчивать свою работу в момент завершения доверенного сеанса связи.

На рис. 4 представлен алгоритм функционирования ПАК, обеспечивающего с высокой вероятностью парирование атак на систему сетевого времени (синхронизации).

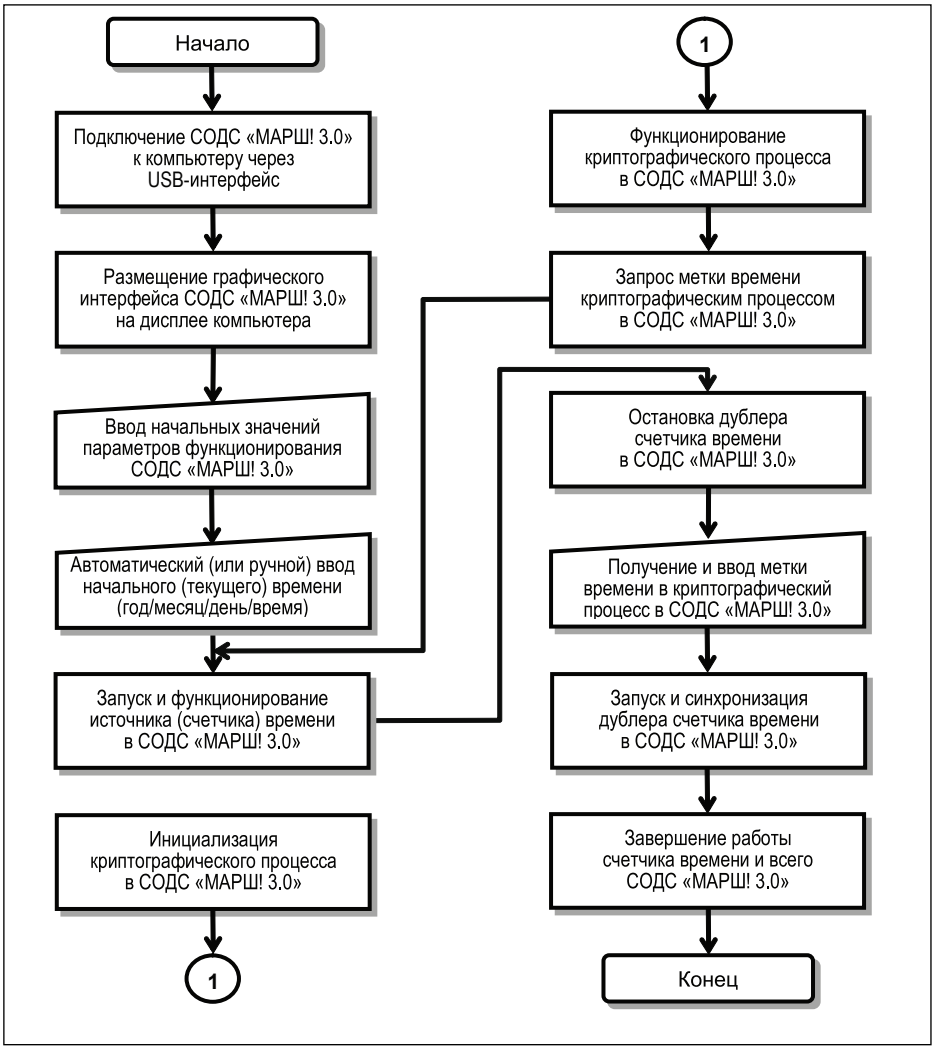

Рис. 4. Алгоритм функционирования источника времени в составе СОДС «МАРШ! 3.0»

Выводы

Гарантированность является важнейшей задачей, без решения которой не могут быть решены другие задачи обеспечения ИБ, возложенные на СОДС «МАРШ! 3.0». Представленные в статье методика, способ и реализационные аспекты подтверждают возможность создания «автономного» источника времени, способного генерировать надежные метки времени, и последующего формирования на их основе уникальных (конфиденциальных) данных.

СПИСОК ЛИТЕРАТУРЫ:

1. *Мельников Д. А.* Организация и обеспечение безопасности информационно-технологических сетей и систем: Учебник. М.: Университетская книга, 2012.
2. U.S. Department of Commerce. Underlying Technical Models for Information Technology Security. National Institute of Standards Special Publication, December 2001.
3. *Мельников Д. А.* Информационная безопасность открытых систем: Учебник. М.: ФЛИНТА, Наука, 2013.
4. *Melnikov D., Jones A.* 'Masquerade' Attacks and a Process for Their Detection // Proceedings of the 3rd European Conference on Information Warfare and Security. Royal Holloway University of London, UK. 28–29 June 2004. P. 269.
5. *McNamara J.* Secrets of Computer Espionage: Tactics and Countermeasures. New York: John Wiley & Sons, Inc., 2003.