Алексей Ю. Боровиков[1], Артем П. Карпов[2], Владимир Н. Пелин[3], Станислав Е. Кузнецов[4]
Пензенский филиал АО «Научно-технический центр «Атлас»,
пр–кт Победы, 69, Пенза, 440028, Россия
[1]e-mail: alexey_bau@mail.ru, https://orcid.org/0000-0002-3595-2533
[2]e-mail: atlas@atlas-pf.ru, https://orcid.org/0000-0002-3462-2153
[3]e-mail: atlas@atlas-pf.ru, https://orcid.org/0000-0003-4274-9047
[4]e-mail: atlas@atlas-pf.ru, https://orcid.org/0000-0003-0516-7806

СОЗДАНИЕ СПЕЦИАЛИЗИРОВАННОГО ДОВЕРЕННОГО УСТРОЙСТВА АНАЛИЗА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

DOI: http://dx.doi.org/10.26583/bit.2022.1.03

Аннотация. Целью работы является создание специализированного доверенного устройства анализа информации (СДУ АИ), предназначенного для контроля и фильтрации информации при управлении каналообразующими средствами в автоматизированной системе в защищенном исполнении, обрабатывающей информацию ограниченного доступа и имеющей возможность передачи информации по открытым (незащищенным от несанкционированного доступа) каналам связи. С развитием автоматизированных систем все большее значение приобретают автоматизация функций, в том числе управления каналообразующими средствами, безопасность обрабатываемой информации и оперативность выполняемых задач. При этом в автоматизированных системах в защищенном исполнении (АСЗИ) для организации оперативного автоматизированного управления каналообразующими средствами, как правило, требуется обеспечить взаимодействие сетей с различной степенью конфиденциальности обрабатываемой информации. Объектом исследования являются АСЗИ обрабатывающие информацию ограниченного доступа в одной сети и реализующие обмен информацией по открытым (незащищенным от несанкционированного доступа) каналам связи с другой сетью. Предметом исследования является оценка возможности применения СДУ АИ для обеспечения возможности сопряжения сетей с различной степенью конфиденциальности обрабатываемой информации, выполняющего функции контроля и фильтрации информации при управлении каналообразующими средствами. Разработана унифицированная архитектура СДУ АИ. Рассмотрены угрозы информационной безопасности, возникающие при реализации обмена информацией по открытым каналам связи. Предложен способ создания СДУ АИ на базе доверенной аппаратно-программной платформы, предназначенного для применения в АСЗИ для защиты от выявленных угроз информационной безопасности.

Ключевые слова: автоматизированная система в защищенном исполнении, доверенная аппаратно-программная платформа, каналообразующие средства, канал связи, защита информации, информационная безопасность, автоматизированное управление, фильтрация информации.

Для цитирования: БОРОВИКОВ, Алексей Ю. и др. СОЗДАНИЕ СПЕЦИАЛИЗИРОВАННОГО ДОВЕРЕННОГО УСТРОЙСТВА АНАЛИЗА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ. Безопасность информационных технологий, [S.l.], т. 29, № 1, с. 17–29, 2022. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1408. DOI: http://dx.doi.org/10.26583/bit.2022.1.03.

Alexey Y. Borovikov[1], Artem P. Karpov[2], Vladimir N. Pelin[3], Stanislav E. Kuznecov[4]
Penza Branch of Atlas Scientific and Technical Center JSC,
Pobedy Avenue, 69, Penza, 440028, Russia.
[1]e-mail: alexey_bau@mail.ru, https://orcid.org/0000-0002-3595-2533
[2]e-mail: atlas@atlas-pf.ru, https://orcid.org/0000-0002-3462-2153
[3]e-mail: atlas@atlas-pf.ru, https://orcid.org/0000-0003-4274-9047
[4]e-mail: atlas@atlas-pf.ru, https://orcid.org/0000-0003-0516-7806

Method for creating a specialized trusted device for analyzing information in protected operational system

DOI: http://dx.doi.org/10.26583/bit.2022.1.03

Abstract. This work aims to create a specialized trusted information analysis device (SDU AI) designed to control and filter information when controlling channel-forming means in an automated system in a secure design that processes restricted access information and can transmit information over open (unprotected from unauthorized access) communication channels. With the development of automated systems, automation of functions, including the control of channel-forming means, the security of processed information and the efficiency of tasks are becoming increasingly important. At the same time, in automated systems in protected execution (ASZI), for the organization of operational automated control of channel-forming means, as a rule, it must ensure the interaction of networks varying degrees of confidentiality of the processed information. The object of the study is ASZI processing restricted access information in one network and implementing the exchange of information through open (unprotected from unauthorized access) communication channels with another network. The subject of the study is to assess the possibility of using SDU AI to ensure the possibility of interfacing networks with varying degrees of confidentiality of processed information, performing the functions of monitoring and filtering information when managing channel-forming means. A unified architecture of the SDU AI has been developed. The threats to information security arising from the implementation of information exchange through open communication channels are considered. A method for creating a SDU AI based on trusted hardware and software platform designed for use in the ASZI to protect against identified threats to information security is proposed.

Keywords: automated system in secure execution, trusted hardware and software platform, channel-forming means, communication channel, information protection, information security, automated management, information filtering.

For citation: BOROVIKOV, Alexey Y. et al. Method for creating a specialized trusted device for analyzing information in protected operational system. IT Security (Russia), [S.l.], v. 29, no. 1, p. 17–29, 2022. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1408. DOI: http://dx.doi.org/10.26583/bit.2022.1.03.

Введение

В настоящее время военно-промышленный комплекс Российской Федерации характеризуется ростом различного рода автоматизированных систем, разрабатываемых в интересах МО РФ и предназначенных для обработки информации ограниченного доступа (АСЗИ). Разработка и совершенствование таких систем с целью соответствия их современным требованиям по оперативности взаимодействия, автоматизации управления и обеспечения безопасности обрабатываемой информации является важнейшей задачей обеспечения обороноспособности страны и суверенитета государства.

Рассматриваемые автоматизированные системы в общем случае включают в себя сеть обработки информации ограниченного доступа (информация для служебного пользования, информация, содержащая сведения, составляющие государственную тайну, и др.) (далее – защищенная сеть) и сеть обработки общедоступной информации, в том числе обеспечивающая возможность обмена информацией по открытым (незащищенным от несанкционированного доступа) каналам связи (далее – открытая сеть).

Для обмена информацией ограниченного доступа по открытым каналам связи в АСЗИ используются средства криптографической защиты информации (СКЗИ). При этом, разрабатываемая АСЗИ должна удовлетворять требованиям нормативных документов МО РФ, предъявляемым к программному обеспечению и автоматизированным системам, а также требованиям нормативных документов ФСБ России в части корректного применения СКЗИ и получения разрешения на его эксплуатацию в АСЗИ.

При проектировании данных АСЗИ разработчику требуется обеспечить сопряжение открытой и защищенной сети АСЗИ и организовать оперативное автоматизированное управление каналообразующими средствами.

В данной работе рассматривается создание СДУ АИ, предназначенного для применения в АСЗИ при организации автоматизированного управления каналообразующими средствами, обеспечивающего защиту от возникновения угроз информационной безопасности при использовании СКЗИ в АСЗИ.

Типовая архитектура АСЗИ представлена на рис. 1.

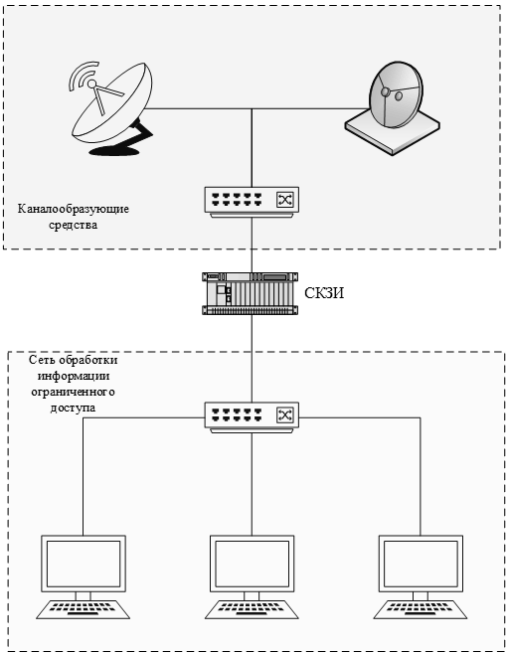

Рис. 1. Типовая архитектура АСЗИ
Fig. 1. Typical architecture of protected operational system

При типовой архитектуре построения АСЗИ требуется решение задач, связанных с необходимостью автоматизированного управления каналообразующими средствами: настройка технических средств (задание основных параметров работы, рабочей частоты, текущего времени и т.д.), сбор и централизованное хранение сведений о состоянии данных технических средств (включен, выключен, занят, в режиме ожидания и т.д.), прием и обработка инициативных сообщений (сообщения об ошибках, квитанции, сообщения об изменениях состояний и режимов работы и т.д.). Описание методов управления каналообразующими средствами в современных системах связи дано в [1], при этом в АСЗИ важным аспектом является обеспечение безопасной реализации данных методов.

Поскольку в рассматриваемой структуре построения АСЗИ все передаваемые из защищенной сети данные являются преобразованными с использованием СКЗИ, они не могут быть применены для управления каналообразующими средствами. Введение в состав открытой сети отдельного технического средства для выполнения функций управления каналообразующими средствами нецелесообразно по следующим причинам:

– технические средства (в частности – каналообразующие средства) из состава открытой сети АСЗИ, как правило, размещаются в условиях ограниченного пространства, в необслуживаемых и опломбированных помещениях (отсеках). Выделить в этих условиях

дополнительное автоматизированное рабочее место затруднительно, а иногда и невозможно;

– техническое средство из состава открытой сети не может взаимодействовать с защищенной сетью, следовательно, не может оперативно получать актуальные данные, необходимые для настройки каналообразующих средств (режим работы, рабочая частота и т.д.). Для обеспечения такого взаимодействия может быть использована внутренняя телефонная линия, но подобное взаимодействие не удовлетворяет требованиям оперативности, удобства использования и автоматизации, которым должны соответствовать современные автоматизированные системы [2].

Организация централизованного и автоматизированного управления каналообразующими средствам из защищенной сети является эффективным решением перечисленных проблем. Однако решение данной задачи осложняется появлением угроз безопасности информации, таких как попадание информации ограниченного доступа в открытые каналы связи и воздействие нарушителя по каналам связи с целью осуществления несанкционированного доступа к обрабатываемой информации.

Для предотвращения указанных угроз, при сопряжении сетей АСЗИ необходимо использовать специальные средства контроля и фильтрации информации. Такие средства не относятся ни к одной из рассматриваемых сетей, поскольку не обрабатывают информацию ограниченного доступа и не являются частью каналообразующих средств.

В настоящее время на российском рынке к изделиям, которые предназначены для сопряжения сетей разного уровня конфиденциальности, относятся межсетевые экраны и однонаправленные шлюзы.

Межсетевые экраны не могут быть применены для решения описываемой задачи, поскольку, в соответствии с действующими нормативными документами МО РФ и ФСБ России, использование данных технических средств для сопряжения защищенной сети с открытой сетью, имеющей подключение к открытым (незащищенным от несанкционированного доступа) каналам связи, не допускается.

Однонаправленные шлюзы в соответствии с действующими нормативными документами РФ могут применяться в составе АСЗИ, однако данные технические средства по определению не обеспечивают двунаправленное взаимодействие [3, 4] и, как следствие, не позволяют полноценно выполнять задачи по управлению и контролю состояния каналообразующих средств.

В связи с этим существующие в настоящее время изделия не могут быть использованы для реализации автоматизированного двунаправленного управления каналообразующими средствами в АСЗИ.

С целью реализации автоматизированного обмена информацией при управлении каналообразующими средствами в АСЗИ, учитывая архитектуру, протоколы информационного взаимодействия сетей, объемы передаваемой информации и ее содержание, предлагается разработать и применить СДУ АИ, в общем случае выполняющее следующие функции:

– контроль формата пакетов и значений в полях пакетов с управляющей информацией, между защищенной сетью и каналообразующими средствами открытой сети в соответствии с протоколом сетевого взаимодействия;

– возможность индивидуальной настройки (задания допустимых форматов и значений протокола взаимодействия) для каждой АСЗИ;

– защиту от передачи защищаемой информации из сети обработки информации ограниченного доступа;

– защиту от воздействий нарушителя по каналу связи с целью осуществления несанкционированного доступа к защищаемой информации.

1. Требования к математическому обеспечению СДУ АИ

Учитывая многообразие существующих и разрабатываемых АСЗИ, а также используемых в этих системах каналообразующих средств, разработка универсального устройства, обеспечивающего контроль и фильтрацию информации для всех существующих (и перспективных) сетевых и прикладных протоколов, невозможна. При этом, может быть определен и зафиксирован состав аппаратного обеспечения данного устройства, в то время как программное обеспечение, реализующее протокол межсетевого взаимодействия, должно предусматривать возможность конфигурации для каждой отдельно взятой АСЗИ, в которой используется СДУ АИ.

Ведущими специалистами ПФ АО «НТЦ «Атлас» был выполнен ряд инициативных работ, в рамках которых была создана унифицированная архитектура СДУ АИ, позволяющая, с одной стороны, реализовать целевые функции по фильтрации и контролю информации, а с другой – обеспечить возможность гибкой настройки и минимальной доработки программного обеспечения для применения СДУ АИ в конкретной АСЗИ.

СДУ АИ состоит из трех вычислительных модулей – абонентского (АВМ), канального (КВМ) и специального (СВМ), размещенных в едином конструктиве с учетом требований по стойкости к внешним воздействующим факторам. Абонентский и канальный модуль служат для сетевого взаимодействия с сопрягаемыми сетями АСЗИ и должны обеспечивать возможность настройки параметров межсетевого взаимодействия, а специальный вычислительный модуль выполняет основные функции защиты от попадания защищаемой информации в каналы связи и от воздействия нарушителя по каналам связи на технические средства АСЗИ. Такая архитектура позволяет унифицировать аппаратную часть устройства, обеспечить требуемый уровень защиты от угроз информационной безопасности за счет реализации основных мер защиты на специальном вычислительном модуле, а также обеспечить требуемую гибкость при проектировании СДУ АИ для различных АСЗИ. При встраивании СДУ АИ требуется доработка только программного обеспечения в соответствии с протоколом межсетевого взаимодействия АСЗИ.

Для применения СДУ АИ в конкретной АСЗИ необходимо тщательно проработать протокол взаимодействия сетей с учетом используемых каналообразующих средств. Данный протокол должен содержать полный перечень полей и значений управляющей информации и предусматривать возможность преобразования индивидуального формата управления каждым каналообразующим средством в универсальный формат межсетевого взаимодействия с СДУ АИ. Данные функции должны быть реализованы в программном обеспечении технических средств из состава АСЗИ.

При формировании универсального протокола межсетевого взаимодействия СДУ АИ и технических средств из состава АСЗИ необходимо руководствоваться следующими правилами:

– взаимодействие технических средств с СДУ АИ должно осуществляться по TCP или UDP-протоколу;

– поле данных в сетевых пакетах должно содержать ограниченный алфавит символов, который подлежит контролю на СДУ АИ. В качестве алфавита допускается использовать следующее множество: [a..z, 0..9, +,-,’ ’, !, ?, ., /,\, ^,%]. Мощность предложенного алфавита равна 46 и в соответствии с мерой Р. Хартли [5, 6] данный алфавит может быть закодирован $[\log_2(46)] + 1 = 6$ значащими битами. Таким образом, при

реализации злоумышленником описанных угроз информационной безопасности, стандартные символьные кодировки, требующие 8 бит (например, UTF-8, ASCII), 16 бит (например, UTF-16) и более, будут отбракованы на СДУ АИ;

– поле данных сетевых пакетов должно быть представлено в текстовом формате в виде «ключ-значение». Сетевые пакеты, которые содержат данные в бинарном формате или текстовую информацию в другом виде, будут отбракованы СДУ АИ. Таким образом, СДУ АИ будет блокировать потенциальные сетевые атаки нарушителя с использованием бинарных исполняемых файлов или текстовых программных скриптов. При этом представление «ключ-значение» является предпочтительным с точки зрения унификации протоколов управления разнообразных каналообразующих средств – для любого протокола можно определить исчерпывающий перечень ключей (команд) и соответствующий им перечень значений (параметров команд). В свободном доступе, в открытых исходных текстах содержится ряд библиотек для работы с подобными форматами (XML, JSON и т.д.). В связи с этим упрощается разработка программного обеспечения работы с управляющей информацией на технических средствах из состава АСЗИ для сопряжения с СДУ АИ [7, 8];

– поле данных сетевых пакетов должно содержать контрольную сумму, которая подлежит проверке на СДУ АИ. Контрольные суммы сформированных данных гарантируют их неизменность и защищают от случайного попадания информации ограниченного доступа в сетевые пакеты во время их доставки до СДУ АИ. В качестве контрольной суммы может быть использована одна из реализаций стандарта CRC32 [9, 10].

Формат пакета, сформированного в соответствии с рассмотренным протоколом взаимодействия, приведен на рис. 2.

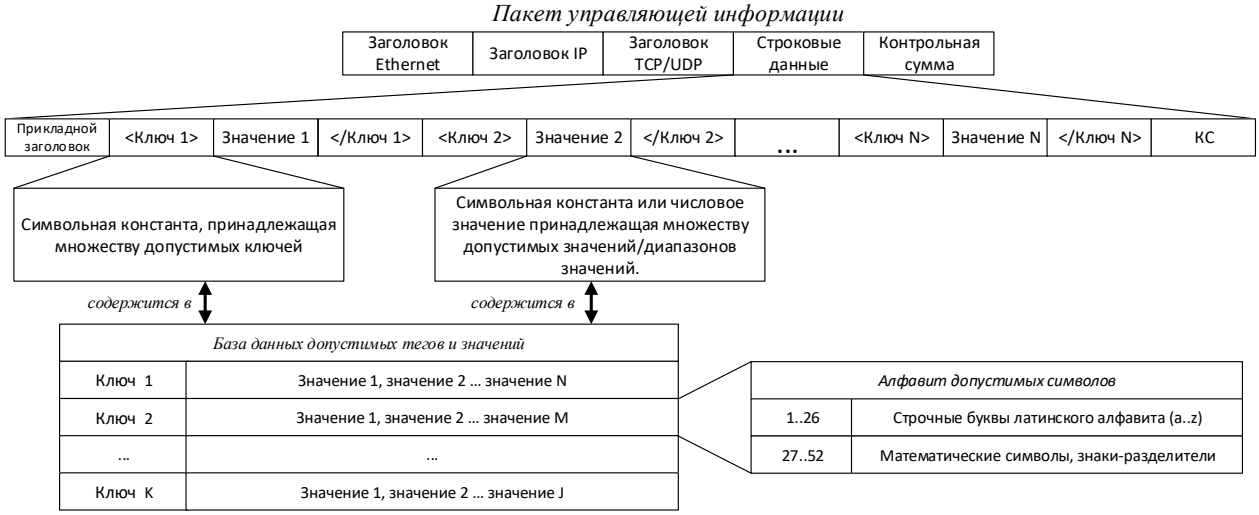

Рис. 2. Формат пакета управляющей информации
Fig. 2. Controlling information packet format

При реализации описанного протокола взаимодействия функции СДУ АИ можно свести к контролю соответствия передаваемых данных рассмотренному протоколу. В этом случае в АСЗИ защита от попадания информации в каналы связи и от воздействия нарушителем будет обеспечиваться за счет:

– контроля корректности адресной информации пакета с управляющей информацией;

– контроля корректности контрольной суммы пакета;

– контроля наличия в пакетах только данных в формате строк;

– контроля корректности контрольной суммы поля данных;

– контроля соответствия всех символов передаваемой строки допустимому алфавиту;

– контроля соответствия всех тегов и значений (диапазонов значений) передаваемых данных значениям, определенным в протоколе взаимодействия.

Пакеты с информацией ограниченного доступа, нештатно (за счет неисправностей, сбоев и ошибочных действий обслуживающего персонала) попадающие в СДУ АИ, будут отбракованы, равно как и пакеты с вредоносным программным обеспечением, которые могут быть сформированы и переданы нарушителем по каналам связи.

2. Требования к аппаратно-программному обеспечению СДУ АИ

Для обеспечения соответствия СДУ АИ и реализуемых им функций по защите информации уровню доверия, достаточному для сопряжения сетей АСЗИ, СДУ АИ должно удовлетворять следующим требованиям [11]:

– наличие конструкторской (схемы электрические принципиальные, схемы электрические подключений, габаритные и сборочные чертежи) и эксплуатационной документации (паспорт, руководство по эксплуатации) на аппаратную платформу;

– наличие исходного кода, программной документации и отсутствия опасных функциональных возможностей во встроенном программном обеспечении аппаратной платформы;

– применение сертифицированных по требованиям безопасности информации общесистемного, прикладного и специального программного обеспечения по соответствующему уровню контроля отсутствия недекларированных возможностей;

– применение сертифицированных аппаратно-программных или программных средств защиты информации для обеспечения невозможности работы несанкционированных пользователей и замкнутости программной среды.

– выполнение организационно-режимных и технических мер защиты информации от несанкционированного доступа.

Как показано в [12] при проектировании СДУ АИ выполнение указанных требований может быть обеспечено за счет:

– разработки на базе доверенной аппаратно-программной платформы отечественного производства, например, вычислительный блок БВ001 ЦИАТ.467444.251 (производитель ПФ АО «НТЦ «Атлас») на базе модуля процессора СРС1311 (производитель ЗАО «НПФ «Доломант») с загрузчиком операционных систем Горизонт ЦИАТ.00169-01 (ЗОС Горизонт), выполняющим функции ПО BIOS и реализующим механизмы защиты от несанкционированного доступа на этапе начального старта до загрузки операционной системы. Данный загрузчик реализует комплекс мер защиты от несанкционированного доступа к ПО, в том числе от атак на уровне базовой системы ввода/вывода и решает задачу построения доверенной вычислительной среды [13, 14]. В настоящее время с ЗОС Горизонт проводятся тематические исследования по требованиям нормативных документов ФСБ России;

– использования в качестве общесистемного программного обеспечения отечественной доверенной операционной системы реального времени ТрастОС КПДА.10966-01 (производитель ООО «СВД Встраиваемые Системы»). В настоящее время с ДОС РВ проводятся тематические исследования по требованиям нормативных документов ФСБ России;

– использования специального программного обеспечения, реализующего фильтрацию и преобразование информации в соответствии с протоколом взаимодействия и прошедшего тематические исследования по требованиям нормативных документов ФСБ России;

– обеспечения встроенными средствами операционной системы функций защиты от несанкционированного доступа и контроля целостности программного обеспечения СДУ АИ.

При этом разработчиком АСЗИ и эксплуатирующей организацией должно быть обеспечено выполнение организационно-режимных и технических мер защиты информации от несанкционированного доступа в АСЗИ [15].

Перед вводом в эксплуатацию СДУ АИ необходимо провести специальный инженерный анализ и расчет специальной надежности. При оценке допустимо руководствоваться методом расчета надежности, который учитывает актуальные для системы угрозы информационной безопасности [16, 17, 18]. При проведении анализа должна быть проверена оценка корректности реализации аппаратно-программного обеспечения устройства, принятого комплекса организационно-технических мер по его эксплуатации, проведены исследования, в том числе экспериментальные, подтверждающие соответствие заявленного алгоритма функционирования СДУ АИ фактическому.

Окончательные выводы о возможности применения СДУ АИ для каждой конкретной АСЗИ делает экспертная организация ФСБ России по результатам экспертизы материалов, отражающих реализацию требований по встраивании СКЗИ в АСЗИ и принятых мер по защите от возникновения угроз информационной безопасности в АСЗИ.

Унифицированная архитектура СДУ АИ, удовлетворяющая всем рассмотренным требованиям, приведена на рис. 3.

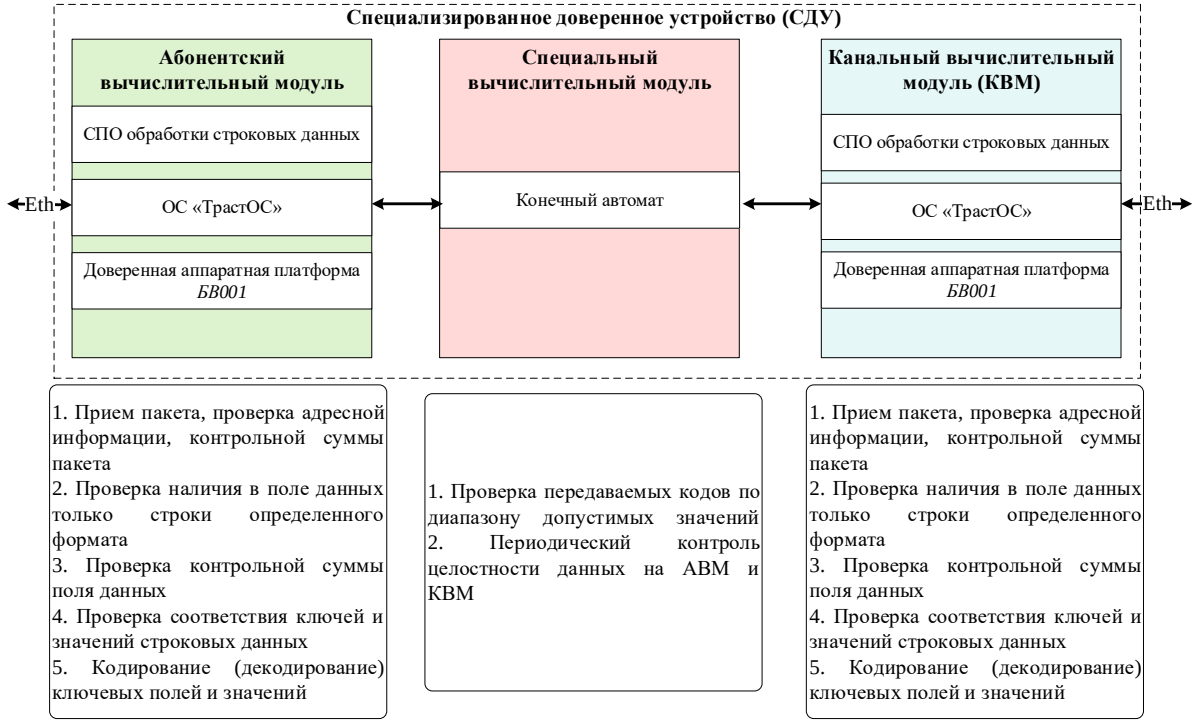

Рис. 3. Унифицированная архитектура СДУ АИ
Fig. 3. Unified architecture of the specialized trusted device for analyzing service information

3. Настройка СДУ АИ и обмен управляющей информацией

С целью возможности применения СДУ АИ в различных АСЗИ, для управления различными типами каналообразующих средств предлагается реализовать на абонентском и канальном вычислительных модулях программное обеспечения работы с базами данных управляющей информации и предусмотреть для данного изделия режим конфигурации. В данном режиме база данных, содержащая определенные по результатам анализа управляющей информации допустимые значения рассмотренного выше протокола взаимодействия, может быть записана на абонентский и канальный вычислительные модули СДУ АИ.

Схема работы СДУ АИ в режиме конфигурации приведена на рис. 4.

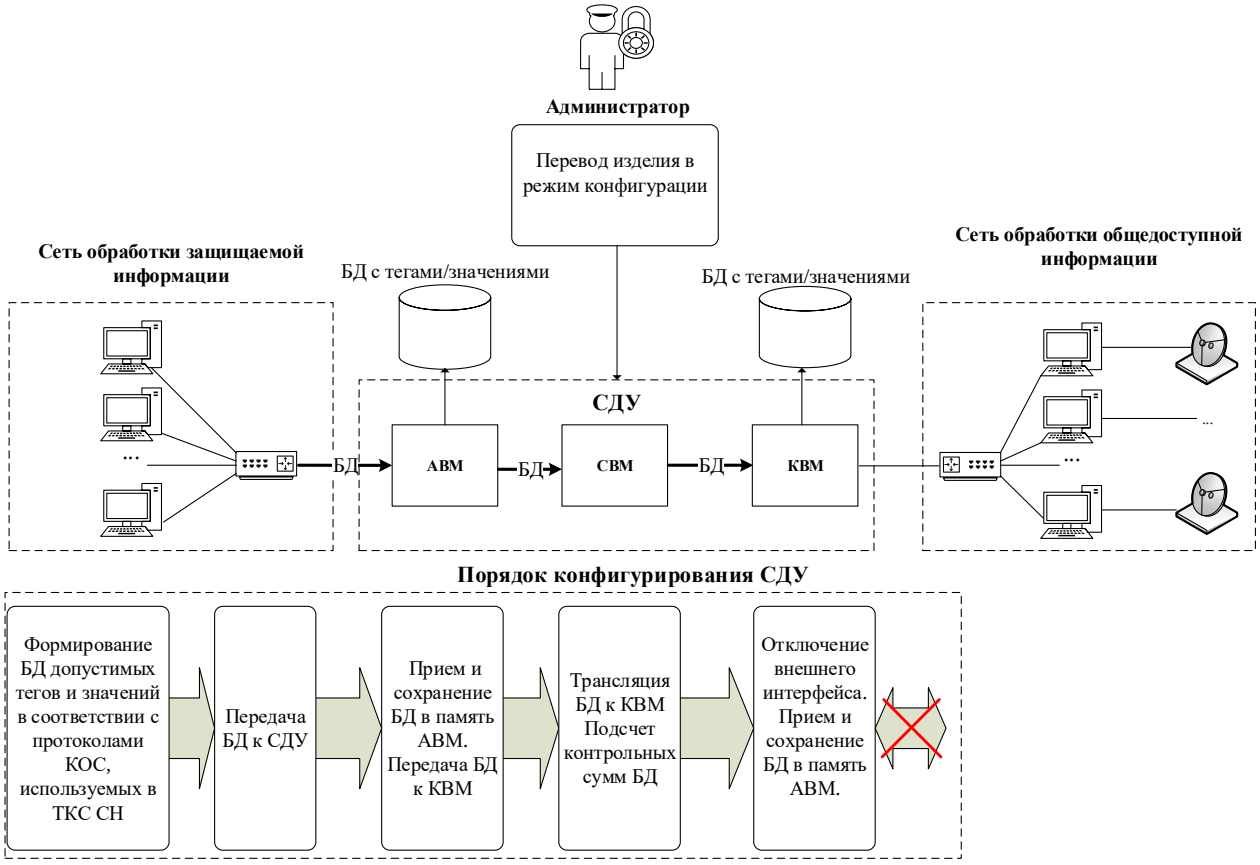

Рис. 4. Порядок конфигурирования СДУ АИ
Fig. 4. Configuration of the specialized trusted device for analyzing service information

Защита от попадания информации ограниченного доступа в каналы связи и от воздействия нарушителя по каналам связи будет обеспечиваться за счет следующих факторов:

– проверка (на АВМ и на КВМ) следующих данных:
  - адресной информации пакета;
  - контрольных сумм;
  - текстового формата и вида «ключ-значение» сообщения;
  - наличия в базе данных всех ключей и значений сообщения.

– преобразование и восстановление ключей и значений сообщения на АВМ и КВМ и невозможность «сквозного» обмена сообщениями между сетями;

– проверка соответствия значений диапазону допустимых значений на СВМ;

– периодический контроль целостности данных специального программного обеспечения и баз данных СДУ АИ;

– комплекс организационно-технических мер защиты информации от несанкционированного доступа, реализованный в АСЗИ.

Описанный порядок обработки управляющей информацией, циркулирующей в АСЗИ через СДУ АИ, приведен на рис. 5.

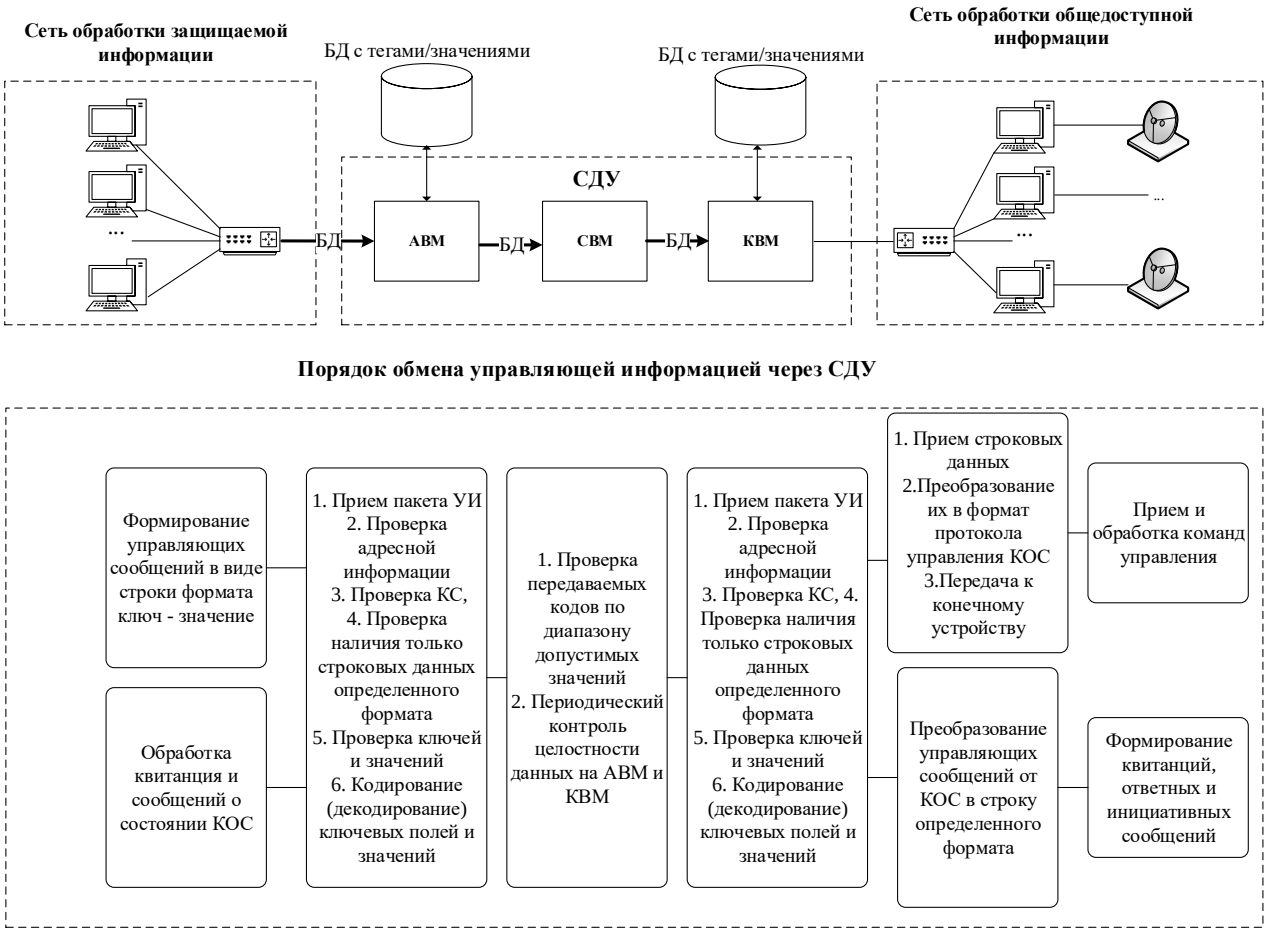

Рис. 5. Порядок обмена управляющей информацией через СДУ АИ
Fig. 5. The procedure for exchanging information through the specialized trusted device for analyzing service information

Таким образом, при условии корректной аппаратно-программной реализации механизмов контроля и фильтрации информации, выполнения комплекса технических мер защиты от несанкционированного доступа к аппаратно-программному обеспечению, а также реализации комплекса организационно-режимных мер при встраивании СДУ АИ в АСЗИ [19, 20], разработанных по результатам проведения специального инженерного анализа по требованиям нормативных документов ФСБ России, СДУ АИ может быть применено в АСЗИ для контроля и фильтрации информации при автоматизированном управлении каналообразующими средствами.

Заключение

В результате проведения работ получен способ создания специализированного доверенного устройства анализа информации на базе доверенной аппаратно-программной платформы. Предложенная архитектура построения СДУ АИ позволяет осуществлять контроль и фильтрацию информации в АСЗИ при управлении каналообразующими средствами и обеспечивает гибкую настройку и минимальную доработку программного обеспечения при встраивании СДУ АИ в конкретную АСЗИ. СДУ АИ обеспечивает защиту от возникновения угроз информационной безопасности при использовании СКЗИ в АСЗИ, в которой реализованы функций автоматизированного управления каналообразующими средствами.

СПИСОК ЛИТЕРАТУРЫ:

1. Чуднов А.М., Путилин А.Н., Попов А.И. Комплексное управление маршрутизацией пакетов и режимами работы радиосредств в неоднородной сети передачи данных. РТС. 2019, № 1 (33), с. 46–56. URL: https://cyberleninka.ru/article/n/kompleksnoe-upravlenie-marshrutizatsiey-paketov-i-rezhimami-raboty-radiosredstv-v-neodnorodnoy-seti-peredachi-dannyh (дата обращения: 16.01.2022).
2. Гутгарц Р.Д., Полякова П.М. Анализ особенностей формулирования функциональных требований к автоматизированной информационной системе. Программные продукты и системы. 2019, № 3, с. 358–367. URL: https://cyberleninka.ru/article/n/analiz-osobennostey-formulirovaniya-funktsionalnyh-trebovaniy-k-avtomatizirovannoy-informatsionnoy-sisteme (дата обращения: 26.02.2022).
3. Бирюков А. Устройства однонаправленной передачи данных. Системный администратор. 2018, № 1–2, с. 182–183. URL: http://samag.ru/archive/article/3579 (дата обращения: 16.01.2022).
4. Воронцов А.Г., Петунин С.А. Организация однонаправленных сетей передачи информации в условиях защищённой среды. Вопросы кибербезопасности. 2017, № 2 (20), с. 21–29. URL: https://cyberleninka.ru/article/n/organizatsiya-odnonapravlennyh-setey-peredachi-informatsii-v-usloviyah-zaschische-nnoy-sredy (дата обращения: 16.01.2022).
5. Авсентьев О.С., Рубцова И.О. Методика оценки аналогии математической модели показателя эффективности защиты информации в компьютерных системах. Вестник ВИ МВД России. 2018, № 2, с. 30–36. URL: https://cyberleninka.ru/article/n/metodika-otsenki-analogii-matematicheskoy-modeli-pokazatelya-effektivnosti-zaschity-informatsii-v-kompyuternyh-sistemah (дата обращения: 26.02.2022).
6. Майер Р.В. Автоматизированный метод оценки количества различных видов информации и ее сложности в физическом тексте с помощью ПЭВМ. Известия ВУЗов. Поволжский регион. Гуманитарные науки. 2014, № 3 (31), с. 200–209. URL: https://cyberleninka.ru/article/n/avtomatizirovannyy-metod-otsenki-kolichestva-razlichnyh-vidov-informatsii-i-ee-slozhnosti-v-fizicheskom-tekste-s-pomoschyu-pevm (дата обращения: 16.01.2022).
7. Беседина К.В. Особенности языка разметки xml. European research. 2016, № 8 (19), с. 51–52. URL: https://cyberleninka.ru/article/n/osobennosti-yazyka-razmetki-xml (дата обращения: 26.02.2022).
8. Шульман В.Д., Шабанов В.В., Сухов П.А., Чунихин А.О. Сравнительный анализ форматов сериализации и передачи данных JSON, XML, CBOR И GPB. StudNet. 2021. № 7, с. 1686–1696. URL: https://cyberleninka.ru/article/n/sravnitelnyy-analiz-formatov-serializatsii-i-peredachi-dannyh-json-xml-cbor-i-gpb (дата обращения: 26.02.2022).
9. Диченко С.А. Контроль и обеспечение целостности информации в системах хранения данных. Наукоемкие технологии в космических исследованиях Земли. 2019. № 1, с. 49–57. URL: https://cyberleninka.ru/article/n/kontrol-i-obespechenie-tselostnosti-informatsii-v-sistemah-hraneniya-dannyh (дата обращения: 26.02.2022).
10. Клименко С.В., Яковлев В.В., Благовещенская Е.А. Исследование реализаций алгоритмов контрольной суммы CRC32. Известия Петербургского университета путей сообщения. 2018, № 3, с. 471–477. URL: https://cyberleninka.ru/article/n/issledovanie-realizatsiy-algoritmov-kontrolnoy-summy-crc32 (дата обращения: 16.01.2022).
11. Боровиков А.Ю., Новиков К.Б., Маслов О.А. Описание подхода программной реализации модуля доверенной загрузки операционной системы. Наукоемкие технологии в космических исследованиях Земли. 2019, № 1, с. 43–48. URL: https://cyberleninka.ru/article/n/opisanie-podhoda-programmnoy-realizatsii-modulya-doverennoy-zagruzki-operatsionnoy-sistemy (дата обращения: 16.01.2022).
12. Боровиков А.Ю., Маслов О.А., Мордвинов С.А., Есафьев А.А. Повышение уровня доверия к аппаратно-программным платформам с целью предупреждения компьютерных атак из-за уязвимостей в ПО BIOS. Вопросы кибербезопасности. 2021, № 6 (46), с. 68–77.

URL: https://cyberleninka.ru/article/n/povyshenie-urovnya-doveriya-k-apparatno-programmnym-platformam-s-tselyu-preduprezhdeniya-kompyuternyh-atak-iz-za-uyazvimostey-v-po (дата обращения: 26.02.2022).
13. Гефнер И.С., Марков А.С. Механизмы реализации атак на уровне базовой системы ввода/вывода. Защита информации. Инсайд. 2017, № 5, с. 80–83. URL: https://www.elibrary.ru/item.asp?id=30268272 (дата обращения: 26.02.2022).
14. Чернов А.Ю., Коноплев А.С. Задача построения доверенной вычислительной среды на аппаратной платформе Intel. Проблемы информационной безопасности. Компьютерные системы. 2016, № 4, с. 36–41. URL: https://jisp.ru/article/zadacha-postroeniya-doverennoj-vychislitelnoj-sredy-na-apparatnoj-platforme-intel/ (дата обращения: 26.02.2022).
15. Авсентьев О.С., Вальде А.Г., Конкин Ю.В. Обеспечение защиты информации в процессе создания информационной системы объекта информатизации. Вестник ВИ МВД России. 2021, № 3, с. 36–48. URL: https://cyberleninka.ru/article/n/obespechenie-zaschity-informatsii-v-protsesse-sozdaniya-informatsionnoy-sistemy-obekta-informatizatsii (дата обращения: 26.02.2022).
16. Беззатеев С.В., Волошина Н.В., Санкин П.С. Методика расчета надежности сложных систем, учитывающая угрозы информационной безопасности. Информационно-управляющие системы. 2014, № 3 (70), с. 78–83. URL: https://cyberleninka.ru/article/n/metodika-rascheta-nadezhnosti-slozhnyh-sistem-uchityvayuschaya-ugrozy-informatsionnoy-bezopasnosti (дата обращения: 16.01.2022).
17. Удалов В.П. Эффективность метода экспертного оценивания модели надежности технической системы безопасности. Вестник ВИ МВД России. 2019, № 2, с. 113–122. URL: https://cyberleninka.ru/article/n/effektivnost-metoda-ekspertnogo-otsenivaniya-modeli-nadezhnosti-tehnicheskoy-sistemy-bezopasnosti (дата обращения: 26.02.2022).
18. Гаранин А.И. О функциональной надежности информационных систем. ИТНОУ: информационные технологии в науке, образовании и управлении. 2018, № 2 (6), с. 45–50. URL: https://cyberleninka.ru/article/n/o-funktsionalnoy-nadezhnosti-informatsionnyh-sistem (дата обращения: 26.02.2022).
19. Родионов А.С., Белянин В.И., Горбунов А.А. Совершенствование методов защиты информации от несанкционированного доступа. NBI-technologies. 2018, № 2, с. 39–43. URL: https://cyberleninka.ru/article/n/sovershenstvovanie-metodov-zaschity-informatsii-ot-nesanktsionirovannogo-dostupa (дата обращения: 26.02.2022).
20. Качаева Г.И., Попов А.Д., Рогозин Е.А. Показатели эффективности функционирования при разработке систем защиты информации от несанкционированного доступа в автоматизированных информационных системах. Вестник ДГТУ. Технические науки. 2018, № 1, с. 147–149. URL: https://cyberleninka.ru/article/n/pokazateli-effektivnosti-funktsionirovaniya-pri-razrabotke-sistem-zaschity-informatsii-ot-nesanktsionirovannogo-dostupa-v (дата обращения: 26.02.2022).

REFERENCES:

[1] Chudnov A.M., Putilin A.N., Popov A.I. Kompleksnoe upravlenie marshrutizaciej paketov i rezhimami raboty radiosredstv v neodnorodnoj seti peredachi dannyh. RTS. 2019, № 1 (33). URL: https://cyberleninka.ru/article/n/kompleksnoe-upravlenie-marshrutizatsiey-paketov-i-rezhimami-raboty-radiosredstv-v-neodnorodnoy-seti-peredachi-dannyh (accessed: 16.01.2022) (in Russian).
[2] Gutgarts R.D., Polyakova P.M. Analysis of the features of the formulation of functional requirements for an automated information system. Software products and systems. 2019, no. 3, p. 358–367. URL: https://cyberleninka.ru/article/n/analiz-osobennostey-formulirovaniya-funktsionalnyh-trebovaniy-k-avtomatizirovannoy-informatsionnoy-sisteme (accessed: 26.02.2022) (in Russian).
[3] Biryukov A. Ustrojstva odnonapravlennoj peredachi dannyh. Sistemnyj administrator. 2018, № 1–2, s. 182–183. URL: http://samag.ru/archive/article/3579 (accessed: 16.01.2022) (in Russian).
[4] Voroncov A.G., Petunin S.A. Organizaciya odnonapravlennyh setej peredachi informacii v usloviyah zashchishchënnoj sredy. Voprosy kiberbezopasnosti. 2017, № 2 (20), s. 21–29. URL: https://cyberleninka.ru/article/n/organizatsiya-odnonapravlennyh-setey-peredachi-informatsii-v-usloviyah-zaschische-nnoy-sredy (accessed: 16.01.2022) (in Russian).
[5] Avsentiev O.S., Rubtsova I.O. Methods for evaluating the analogy of the mathematical model of the indicator of the effectiveness of information protection in computer systems. Bulletin of the VI Ministry of Internal Affairs of Russia. 2018, no. 2, p. 30–36. URL: https://cyberleninka.ru/article/n/metodika-otsenki-analogii-matematicheskoy-modeli-pokazatelya-effektivnosti-zaschity-informatsii-v-kompyuternyh-sistemah (accessed: 26.02.2022) (in Russian).
[6] Majer R.V. Avtomatizirovannyj metod ocenki kolichestva razlichnyh vidov informacii i ee slozhnosti v fizicheskom tekste s pomoshch'yu PEVM. Izvestiya VUZov. Povolzhskij region. Gumanitarnye nauki. 2014, № 3 (31), s. 200-209. URL: https://cyberleninka.ru/article/n/avtomatizirovannyy-metod-otsenki-kolichestva-razlichnyh-vidov-informatsii-i-ee-slozhnosti-v-fizicheskom-tekste-s-pomoschyu-pevm (accessed: 16.01.2022) (in Russian).

[7] Besedina K.V. Osobennosti yazyka razmetki xml. European research. 2016, № 8 (19), s. 51–52. URL: https://cyberleninka.ru/article/n/osobennosti-yazyka-razmetki-xml (accessed: 16.01.2022) (in Russian).
[8] Shulman V.D., Shabanov V.V., Sukhov P.A., Chunikhin A.O. Comparative analysis of serialization and data transmission formats JSON, XML, CBOR and GPB. StudNet. 2021, no. 7, p. 1686–1696. URL: https://cyberleninka.ru/article/n/sravnitelnyy-analiz-formatov-serializatsii-i-peredachi-dannyh-json-xml-cbor-i-gpb (accessed: 26.02.2022) (in Russian).
[9] Dichenko S.A. Monitoring and ensuring the integrity of information in data storage systems. Science-intensive technologies in space research of the Earth. 2019, no. 1, p. 49–57. URL: https://cyberleninka.ru/article/n/kontrol-i-obespechenie-tselostnosti-informatsii-v-sistemah-hraneniya-dannyh (accessed: 26.02.2022) (in Russian).
[10] Klimenko S.V., YAkovlev V.V., Blagoveshchenskaya E.A. Issledovanie realizacij algoritmov kontrol'noj summy CRC32. Izvestiya Peterburgskogo universiteta putej soobshcheniya. 2018, № 3, s. 471–477. URL: https://cyberleninka.ru/article/n/issledovanie-realizatsiy-algoritmov-kontrolnoy-summy-crc32 (accessed: 16.01.2022) (in Russian).
[11] Borovikov A.Y., Novikov K.B., Maslov O.A. Opisanie podhoda programmnoj realizacii modulya doverennoj zagruzki operacionnoj sistemy. Naukoemkie tekhnologii v kosmicheskih issledovaniyah Zemli. 2019, № 1, s. 43–48. URL: https://cyberleninka.ru/article/n/opisanie-podhoda-programmnoy-realizatsii-modulya-doverennoy-zagruzki-operatsionnoy-sistemy (accessed: 16.01.2022) (in Russian).
[12] Borovikov A.Y., Maslov O.A., Mordvinov S.A., Esafiev A.A. Increasing the level of trust in hardware and software platforms in order to prevent computer attacks due to vulnerabilities in BIOS software. Cybersecurity Issues. 2021, no. 6 (46), p. 68–77. URL: https://cyberleninka.ru/article/n/povyshenie-urovnya-doveriya-k-apparatno-programmnym-platformam-s-tselyu-preduprezhdeniya-kompyuternyh-atak-iz-za-uyazvimostey-v-po (accessed: 26.02.2022) (in Russian).
[13] Gefner I.S., Markov A.S. Mechanisms for Implementing Attacks at the Level of the Basic Input/Output System. Information Security. Inside. 2017, no. 5, p. 80–83. URL: https://www.elibrary.ru/item.asp?id=30268272 (accessed: 26.02.2022) (in Russian).
[14] Chernov A.Yu., Konoplev A.S. The task of building a trusted computing environment on the Intel hardware platform. Problems of information security. Computer systems. 2016, no. 4, p. 36–41. URL: https://jisp.ru/article/zadacha-postroeniya-doverennoj-vychislitelnoj-sredy-na-apparatnoj-platforme-intel/ (accessed: 26.02.2022) (in Russian).
[15] Avsentiev O.S., Valde A.G., Konkin Yu.V. Ensuring the protection of information in the process of creating an information system of an informatization object. Bulletin of the VI Ministry of Internal Affairs of Russia. 2021, no. 3, p. 36–48. URL: https://cyberleninka.ru/article/n/obespechenie-zaschity-informatsii-v-protsesse-sozdaniya-informatsionnoy-sistemy-obekta-informatizatsii (accessed: 26.02.2022) (in Russian).
[16] Bezzateev S.V., Voloshina N.V., Sankin P.S. Metodika rascheta nadezhnosti slozhnyh sistem, uchityvayushchaya ugrozy informacionnoj bezopasnosti. Informacionno-upravlyayushchie sistemy. 2014, № 3 (70), s. 78–83. URL: https://cyberleninka.ru/article/n/metodika-rascheta-nadezhnosti-slozhnyh-sistem-uchityvayuschaya-ugrozy-informatsionnoy-bezopasnosti (accessed: 16.01.2022) (in Russian).
[17] Udalov V.P. Efficiency of the method of expert evaluation of the reliability model of a technical security system. Bulletin of the VI Ministry of Internal Affairs of Russia. 2019, no. 2, p. 113–122. URL: https://cyberleninka.ru/article/n/effektivnost-metoda-ekspertnogo-otsenivaniya-modeli-nadezhnosti-tehnicheskoy-sistemy-bezopasnosti (accessed: 26.02.2022) (in Russian).
[18] Garanin A.I. On the functional reliability of information systems. ITNOU: information technologies in science, education and management. 2018, no. 2 (6), p. 45–50. URL: https://cyberleninka.ru/article/n/o-funktsionalnoy-nadezhnosti-informatsionnyh-sistem (accessed: 26.02.2022) (in Russian).
[19] Rodionov A.S., Belyanin V.I., Gorbunov A.A. Improving methods of protecting information from unauthorized access. NBI-technologies. 2018, no. 2, p. 39–43. URL: https://cyberleninka.ru/article/n/sovershenstvovanie-metodov-zaschity-informatsii-ot-nesanktsionirovannogo-dostupa (accessed: 26.02.2022) (in Russian).
[20] Kachaeva G.I., Popov A.D., Rogozin E.A. Performance indicators in the development of information protection systems from unauthorized access in automated information systems. Bulletin of the DSTU. Technical science. 2018, no. 1, p. 147–149. URL: https://cyberleninka.ru/article/n/pokazateli-effektivnosti-funktsionirovaniya-pri-razrabotke-sistem-zaschity-informatsii-ot-nesanktsionirovannogo-dostupa-v (accessed: 26.02.2022) (in Russian).

Поступила в редакцию - 18 октября 2021 г. Окончательный вариант – 28 февраля 2022 г.
Received – October 18, 2021. The final version – February 28, 2022.