Научная статья
УДК 004.451.5
https://doi.org/10.24143/2072-9502-2025-4-23-32
EDN DRDLLF

Программно-аппаратный комплекс диспетчеризации данных при работе с внешними носителями

Валентина Юрьевна Кузнецова[1]✉, Ирина Юрьевна Квятковская[2], Елена Прокофьевна Карлина[3], Даниил Александрович Сапельников[4]

[1–3]Астраханский государственный технический университет, Астрахань, Россия, arhelia@bk.ru✉

[4]Астраханский государственный университет имени В. Н. Татищева, Астрахань, Россия

Аннотация. Рассматривается проблема диспетчеризации данных при взаимодействии с внешними носителями информации, такими как USB-носители, широко используемых организациями и частными лицами. Важность темы обусловлена высокими рисками нарушения информационной безопасности, связанными с переносом конфиденциальных данных вне контролируемой среды. Приводятся статистические данные исследований и аналитические отчеты, согласно которым наиболее распространенным способом утечки корпоративных данных являются именно съемные накопители. Описаны существующие подходы к решению проблемы управления потоками данных, включая организацию однонаправленных каналов передачи информации и специализированные программно-аппаратные комплексы. Рассматриваются методы защиты, применяемые в современных системах, такие как аутентификация пользователей и контроль доступа к устройствам. Отмечается недостаток удобства и эффективности большинства существующих решений, приводятся конкретные недостатки коммерческих продуктов. Приводится сравнительная характеристика рыночных аналогов, демонстрирующая недостаточную поддержку необходимых функций современными промышленными образцами. Детально изложено программное обеспечение комплекса, расписаны процедуры передачи и фильтрации данных, принципы аутентификации и протоколы обмена информацией. Обосновывается необходимость разработки универсального программно-аппаратного комплекса, способного эффективно управлять передачей данных с внешнего носителя на защищенные рабочие места с обеспечением максимальной защиты от несанкционированного доступа и утечек данных. Особое внимание уделено архитектуре комплекса, включающей клиентскую и серверную части, подробно рассмотрены их функции и алгоритмы работы. Представлена подробная структура предлагаемого комплекса, указаны ключевые компоненты, такие как модули фильтрации, аутентификации и аудита. Подчеркиваются преимущества разработанной архитектуры, позволяющие обеспечить надежную и удобную работу с данными даже в крупных организациях. Исследуется функциональность клиентской и серверной сторон, предложены способы интеграции системы в современные ИТ-инфраструктуры.

Ключевые слова: управление потоками данных, съемные носители, диспетчеризация данных, программно-аппаратный комплекс

Для цитирования: *Кузнецова В. Ю., Квятковская И. Ю., Карлина Е. П., Сапельников Д. А.* Программно-аппаратный комплекс диспетчеризации данных при работе с внешними носителями // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2025. № 4. С. 23–32. https://doi.org/10.24143/2072-9502-2025-4-23-32. EDN DRDLLF.

Original article

Hardware and software complex for dispatching data when working with external media

Valentina Yu. Kuznetsova[1]✉, Irina Yu. Kvyatkovskaya[2], Elena P. Karlina[3], Daniil A. Sapelnikov[4]

[1-3]Astrakhan State Technical University, Astrakhan, Russia, arhelia@bk.ru✉

[4]Astrakhan Tatishchev State University, Astrakhan, Russia

Abstract. This article examines the urgent problem of data dispatching when interacting with external storage media, such as USB flash drives, which are widely used by organizations and individuals. The importance of the topic is due to the high risks of information security breaches associated with the transfer of confidential data outside a controlled environment. The author cites statistical data from a SearchInform study, according to which removable drives are the most common way to leak corporate data. The existing approaches to solving the problem of data flow management, including the organization of unidirectional information transmission channels and specialized hardware and software complexes, are being investigated. The security methods used in modern systems, such as user authentication and device access control, are considered. The lack of convenience and efficiency of most existing solutions is noted, and specific disadvantages of commercial products are given. The authors substantiate the need to develop a new universal software and hardware complex capable of effectively managing data transfer from external media to secure workstations, providing maximum protection against unauthorized access and data leaks. Special attention is paid to the architecture of the complex, which includes client and server parts, and their functions and algorithms are discussed in detail. The detailed structure of the proposed complex is presented, and key components such as filtering, authentication, and auditing modules are indicated. The advantages of the developed architecture are emphasized, which make it possible to ensure reliable and convenient work with data even in large organizations. The functionality of the client and server sides is investigated, and ways of integrating the system into modern IT infrastructures are proposed. A comparative table of market analogues is provided, demonstrating the insufficient support of the necessary functions by modern industrial designs. Further, the software of the complex is described in detail, procedures for data transmission and filtering, principles of authentication and protocols for information exchange are described. The article ends with the conclusions of the authors, emphasizing the importance of introducing new approaches to data management, especially in the face of growing digital threats. The list of functional features of the proposed complex is given, proving its advantage over existing analogues. Finally, recommendations are given for the implementation of the complex in any environment that provides increased requirements for information security.

Keywords: data flow management, removable media, data dispatching, hardware and software system

For citation: Kuznetsova V. Yu., Kvyatkovskaya I. Yu., Karlina E. P., Sapelnikov D. A. Hardware and software complex for dispatching data when working with external media. *Vestnik of Astrakhan State Technical University. Series: Management, computer science and informatics*. 2025;4:23-32. (In Russ.). https://doi.org/10.24143/2072-9502-2025-4-23-32. EDN DRDLLF.

Введение

В современном мире цифровизации хранение и передача данных становятся важнейшими аспектами информационной деятельности организаций и частных лиц. Одним из наиболее распространенных инструментов хранения и обработки информации являются USB-флеш-накопители, обладающие удобством, компактностью и доступностью. Однако именно эта простота обращения нередко становится причиной серьезных угроз информационной безопасности. Еще в 2020 г. исследование компании SearchInform показало, что самым распространенным каналом утечки корпоративной информации являются флэш-накопители – 68 % случаев от общего числа утечек данных ограниченного доступа, – что ставит под сомнение обеспечение качественной работы в области управления данными. Исследование основано на результатах анализа обезличенных данных за первое полугодие 2020 г. 50 компаний малого и среднего бизнеса [1, 2]. Такие высокие показатели обусловлены двумя предельно обобщенными проблемами: первая – на флэш-накопителях можно унести то, что не следует уносить, а вторая – на них можно принести то, что не следует приносить. Для обеих проблем разработчики программного обеспечения предлагают свои решения. Решения эти различны по качеству и базовым принципам, однако ни одно из них не обеспечивает возможности комфортной и в то же время безопасной работы в организации с USB-накопителями, ведь качественная нейтрализация угроз, связанных с использованием интерфейса USB, достигается посредством гибкого сочетания функций мониторинга и контроля доступа к устройствам, подключаемым через интерфейс USB, и управления потоками данных на стороне самого интерфейса.

Зачастую такие решения предполагают установку аппаратных идентификаторов на носителях, что ограничивает в целом возможность подключения устройства или, наоборот, разрешает: либо все подключения разрешены, либо запрещены, что противоречит смыслу диспетчеризации и существенно осложняет работу как обычным пользователям, так и администраторам систем. К тому же существуют некоторые сферы направленности работ компаний, где есть проблема передачи данных из незащищенной среды в полностью изолированный сегмент информационной системы посредством реализации односторонней передачи информации – исключительно со съемных носителей на автоматизированное рабочее место, с ограничением его взаимодействия с USB-накопителями в обратном направлении.

Литературный и технологический обзор

Проблема управления потоками данных в корпоративной предпринимательской среде в условиях активного становления и развития цифровой экономики, сопровождающегося ростом угроз в инфор-

мационном пространстве, имеет весьма высокую степень важности.

В статье А. Д. Ахметбекова и А. В. Доля предлагается для диспетчеризации данных при использовании съемных носителей применять однонаправленные каналы передачи данных. Благодаря этому исключается возможность обратной передачи данных, что обеспечивает надежное соединение сегментов информационных систем с разными уровнями хранения и обработки информации. Предложенное решение препятствует физическому перенаправлению сигнала и предотвращает изменение настроек безопасности или правил межсетевых экранов [3].

В исследовании С. Н. Гончарова, С. Ю. Соколова и В. Н. Фомченко [4] отмечается, что наилучшую защищенность автоматизированной системы обеспечивают системы на основе специализированных программно-аппаратных средств, которые поддерживают оригинальный протокол обмена информацией. В исследовании говорится, что для организации безопасной передачи данных между персональным компьютером и внешними объектами необходимо специальное согласующее устройство – модуль управления, и на такой модуль в общем случае должны быть возложены следующие функции:

– наличие гибкого, быстро адаптируемого алгоритма, позволяющего изменять функциональные возможности модуля в зависимости от предъявляемых требований;

– обеспечение совместно с персональным компьютером идентификации и аутентификации пользователей;

– ввод и хранение (совместно с внешними устройствами) необходимой ключевой информации и индикация требуемых параметров;

– обеспечение безопасности конфиденциальной информации, циркулирующей как внутри модуля, так и при передаче внешним устройствам;

– хранение результатов аудита совершаемых санкционированных и несанкционированных операций.

Статья А. В. Архангельской, В. Г. Архангельского и В. В. Калмыкова [5] посвящена изучению характеристик программного макета, моделирующего взаимодействие между участниками обмена данными через однонаправленный шлюз. Авторы отмечают, что на сегодняшний день существует сравнительно немного аналогичных решений, и ни одно из них не гарантирует надежную однонаправленную передачу значительных объемов данных в автоматическом режиме. Обычно, стремясь упростить реализацию и повысить скорость передачи, производители используют протокол UDP, который не требует предварительной установки соединений между участниками обмена. Потеря отдельных пакетов в таком сценарии не ведет к повторной передаче всего сообщения целиком – достаточно передать лишь недостающие фрагменты, что повышает эффективность использования доступной полосы пропускания. Тем не менее этот подход противоречит принципу строгой однонаправленности передачи данных через шлюз, создавая потенциальную угрозу формирования канала утечки информации [5].

Вопрос актуальности применения однонаправленных шлюзов передачи данных освещен в работе А. Г. Воронцова и С. А. Петунина [6]. Авторы утверждают, что применение устройств такого класса, как DataDiode, позволяет безопасно перемещать информацию из открытых источников без каких-либо маркеров защиты в закрытый сегмент сети, а также осуществлять несогласованное управление сервисами внутри закрытого сегмента, отдавая команды управления из открытого сегмента сети [6]. Однако отсутствие обратной связи порождает целый ряд технических трудностей: ключевой при этом становится проблема подтверждения подлинности полученных данных, которая зачастую играет решающую роль в обеспечении основных сервисов безопасности.

Анализ уже имеющихся на рынке решений однонаправленной передачи данных представлен в таблице.

Сравнительный анализ имеющихся на рынке решений

Comparative analysis of the solutions available on the market

Характеристика	Numa uGate	Altell КОП–USB	USB DataDiode
Скорость передачи данных	До 9 Мбит/с	До 480 Мбит/с	
Совместимость	Windows, Linux		Windows
Интерфейс передачи данных	USB		
Фильтрация	–	–	–
Аудит			
Программное конфигурирование			

Промышленные образцы имеют ряд недостатков, таких как невозможность фильтрации передаваемых данных, аудит передачи файлов, разграничение доступа, т. к. они предназначены для широкого круга организаций [7, 8].

По результатам анализа существующих промышленных образцов можно утверждать, что в настоящее время на рынке нет готовых решений,

удовлетворяющих требованиям руководящих документов в области защиты информации и организации информационного потока между доверенной средой и внешним источником информации с использованием шлюза безопасности. Промышленные образцы имеют эффективную аппаратную реализацию, но не обладают программными средствами защиты. Модификация существующих шлюзов невозможна, поскольку все механизмы передачи информации являются закрытыми [9].

Таким образом, становится актуальной разработка новой реализации шлюза защищенной однонаправленной передачи файлов, обладающего функциями аутентификации, разграничения доступа, фильтрации на основе анализа, аудита и логирования событий. Совокупность способов управления потоками данных, предлагаемых в качестве решения, позволит обеспечить необходимый уровень защиты информации, гарантируя соблюдение требований по ранению информации ограниченного доступа на объектах информатизации.

Аппаратная и программная реализация программно-аппаратного комплекса

На основе анализа существующих примеров шлюзов однонаправленной передачи файлов было принято решение сформировать требования к функционалу разрабатываемого программно-аппаратного комплекса (ПАК).

Предлагаемый ПАК должен быть кроссплатформенным и обладать клиент-серверной архитектурой, интерфейс должен быть простым и интуитивно понятным. Аппаратная часть при этом должна быть либо российского производства, либо из доступных рынков.

Согласно вышеперечисленным требованиям, структура АС (автоматизированной системы) и разрабатываемого ПАК должна иметь вид, представленный на рис. 1.

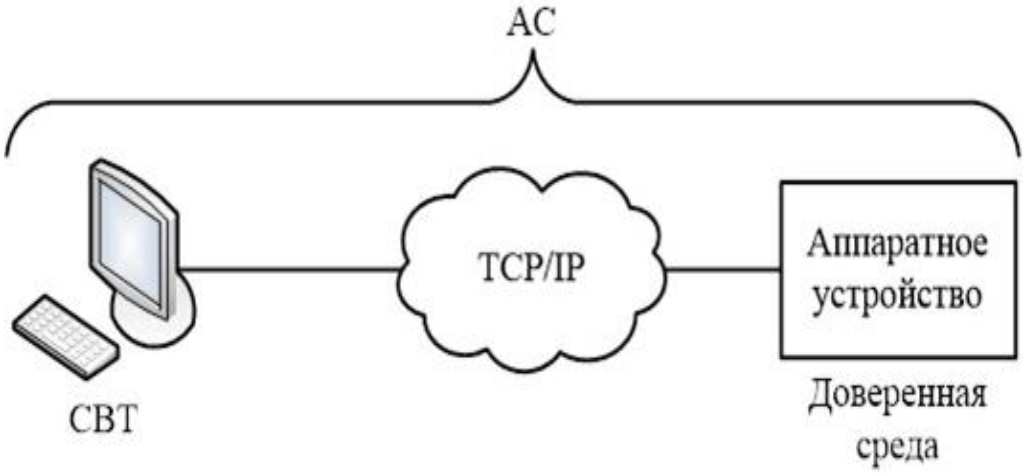

Рис. 1. Архитектура проектируемого программно-аппаратного комплекса:
СВТ – средство вычислительной техники; TCP/IP – протокол передачи данных

Fig. 1. Architecture of the projected hardware and software complex:
CBT – computer technology tool; TCP/IP – data transmission protocol

Аппаратное устройство представляет собой одноплатный миникомпьютер. Он должен обладать USB-интерфейсами для подключения носителей информации и сетевым интерфейсом типа Ethernet. На аппаратное устройство устанавливается серверная часть разрабатываемого ПАК, на которой будет реализован модуль фильтрации передаваемых файлов с использованием сигнатурного анализа. Кроме того, серверная часть должна включать в себя модуль мониторинга переданных файлов. На стороне аппаратного устройства реализуется модуль передачи данных и дерева файлов в сторону клиента. Серверная часть также отвечает за поддержание функций администратора.

Работа ПАК обеспечивается путем клиент-серверного взаимодействия через протокол TCP/IP. Серверная часть отвечает на поступающие запросы со стороны клиента. Для этого обеспечивается сетевое взаимодействие между клиентом и сервером посредством сетевого кабеля типа Ethernet (рис. 2).

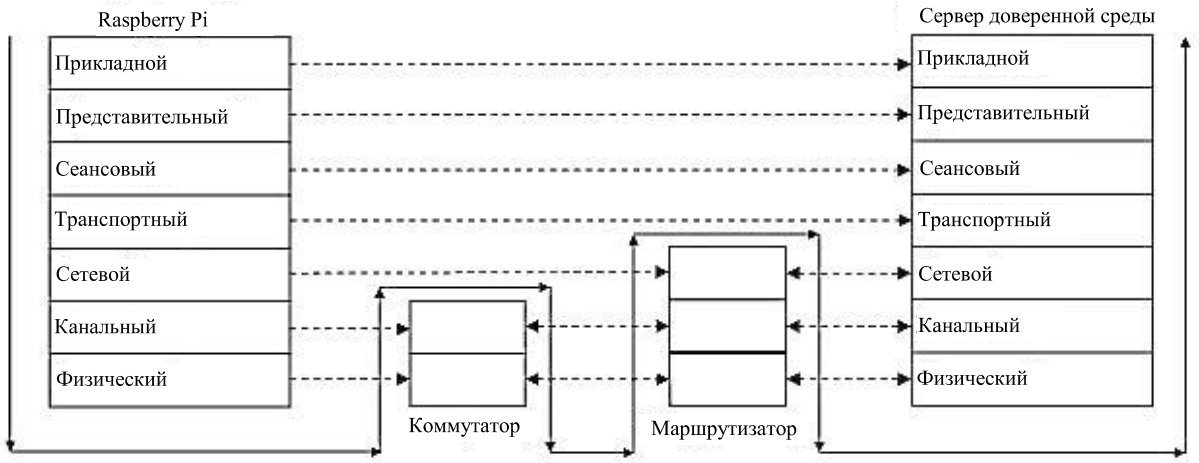

Рис. 2. Модель сетевого взаимодействия шлюза с доверенной средой

Fig. 2. The gateway's network interaction model with a trusted environment

Комплексный механизм защищенной однонаправленной передачи файлов состоит из двух частей программного обеспечения, одна (серверная) из них устанавливается на СВТ), а вторая (клиентская) – на аппаратную платформу шлюза безопасности. Каждая из частей имеет свои требования к разработке и функционалу.

Серверная часть должна:

– осуществлять передачу данных, сервер должен находиться в режиме прослушивания по протоколу User Datagram Protocol (UDP);

– обеспечивать правильную идентификацию запросов, принимаемых клиентом, соответственно, необходим единый Application Programming Interface (API);

– производить сигнатурный анализ и антивирусную проверку, помещая нелегитимные данные в карантин;

– обеспечивать разграничение доступа посредством анализа соответствия серийных номеров носителей информации и уникальных идентификаторов пользователей информационной системы.

Возможность фильтрации передаваемых данных реализуется следующим образом: для распознавания типа файла предлагается использовать сигнатурный анализ файлов. Сигнатурный является основным алгоритмом анализа файлов, используемых для выявления наличия вредоносного программного обеспечения, определения типа вирусной угрозы и способов ее устранения. Сигнатура представляет собой уникальный формализованный признак, характерный исключительно для конкретного типа файла или программы. Этот признак должен быть максимально специфичным, чтобы минимизировать вероятность ошибочного распознавания. Примером сигнатуры может служить последовательность байтов, такая как «E2 E3 BA C2 ? ? FF ? ?», или специальный маркер, определяемый условием, например, первый байт, выходящий за пределы таблицы символов ASCII, считается концом тестового файла. Типы файлов часто определяются по особенностям структуры их заголовков, например исполняемые файлы формата PE или графические файлы. В интерфейсе администратора фигурирует возможность выбора типа разрешенных файлов, доступ к которому обеспечивается путем аутентификации пользователя как администратора. Так, для аудита переданных с USB-носителей данных, а также разграничения доступа выявлены следующие функции: регистрация учетных записей сотрудников, регистрация эксплуатируемых ими съемных носителей информации, регистрация фактов передачи файлов. В совокупности данные функции должны фиксировать информацию о серийном номере съемного носителя, данные сотрудника, за кем зарегистрирован данный носитель, дату и время использования носителя, а также информацию, которая была передана.

Клиентская часть должна:

– поддерживать единый API с сервером;

– проверять наличие на съемный носитель информации (СМНИ), подключаемого к шлюзу безопасности, специального корневого раздела, содержащего файлы для передачи на СВТ;

– предоставлять доступ к функционалу системы по уникальным токенам (логин и пароль);

– принимать от сервера допущенные к передаче файлы.

Применение предлагаемой реализации программно-аппаратного механизма защищенной однонаправленной передачи файлов позволит обеспечить необходимый уровень разграничения потоков данных и гарантировать соблюдение требований по хранению информации на объектах информатизации, а процесс односторонней передачи таких данных с СМНИ на СВТ достигнет условия

максимальной безопасности. Также разработанный шлюз управления потоками данных несет в себе возможность масштабирования за счет использования сетевых технологий, что поможет расширить область применения данного средства.

Разработка алгоритма функционирования программно-аппаратного комплекса однонаправленной передачи данных

При разработке алгоритма функционирования программно-аппаратного шлюза защищенной однонаправленной передачи файлов с USB-носителя, подключаемого к СВТ, необходимо учитывать сформулированные требования к функциям данного комплекса. На основании вышеизложенного была разработана структурная схема ПАК (рис. 3).

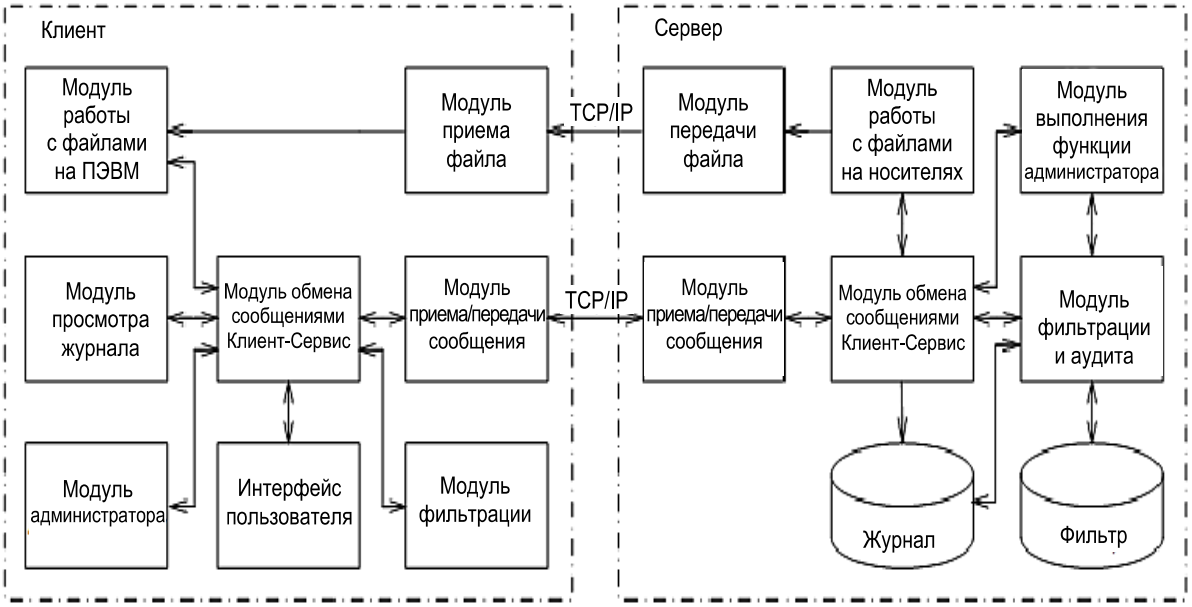

Рис. 3. Структурная схема программно-аппаратного комплекса

Fig. 3. Block diagram of the hardware and software complex

Клиентская часть устанавливается на компьютер и предназначена для приема файлов, передаваемых со стороны серверной части, просмотра журнала принятых файлов, а также управления функциями администратора модуля фильтрации, принимаемых файлов. Алгоритм работы ПО, устанавливаемого на персональный компьютер, представлен на рис. 4.

Клиентская часть является совокупностью следующих модулей:

– модуль работы с файлами на персональной ЭВМ предназначен для сохранения принятых файлов в директории ЭВМ;

– модуль приема файла предназначен для непосредственного приема обрабатываемой информации от сервера в сторону клиента;

– модуль просмотра журнала позволяет просматривать данные аудита. Журнал отображает список переданных файлов, время и дату передачи, а также размер переданного файла;

– модуль обмена сообщениями «Клиент – Сервер» предназначен для создания запросов с клиентской части и обработки ответов, принятых от серверной части;

– модуль администратора предназначен для администрирования панели фильтрации. Позволяет включать/отключать фильтрацию, выбирать список разрешенных сигнатур из предложенного списка;

– интерфейс пользователя предназначен для управления всеми функциями клиентской части и, соответственно, для их наглядного отображения;

– модуль приема/передачи сообщения предназначен для отправки запросов в сторону сервера и приема ответов, пришедших в сторону клиента от сервера.

Предназначением серверной части являются обработка получаемых от клиента сообщений, считывание и отправление затребованных файлов, ведение журнала переданных файлов, фильтрация передаваемых файлов в соответствии с настройками фильтра, проверка и выполнение функций администрирования фильтрации запрашиваемых файлов. Алгоритм работы ПО, устанавливаемого на компьютер, представлен на рис. 5.

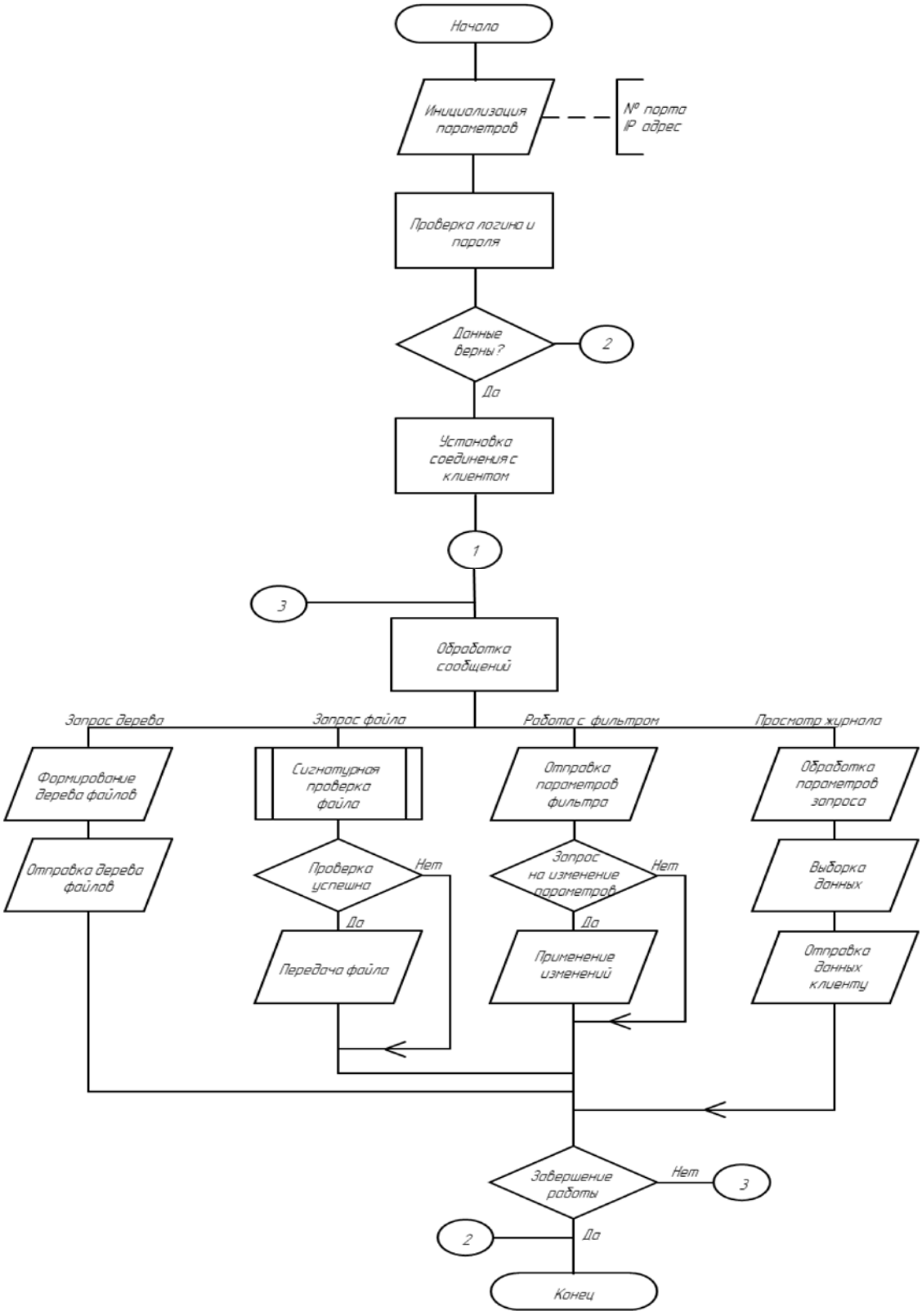

Рис. 4. Часть алгоритма работы клиентского ПО

Fig. 4. Part of the client software algorithm

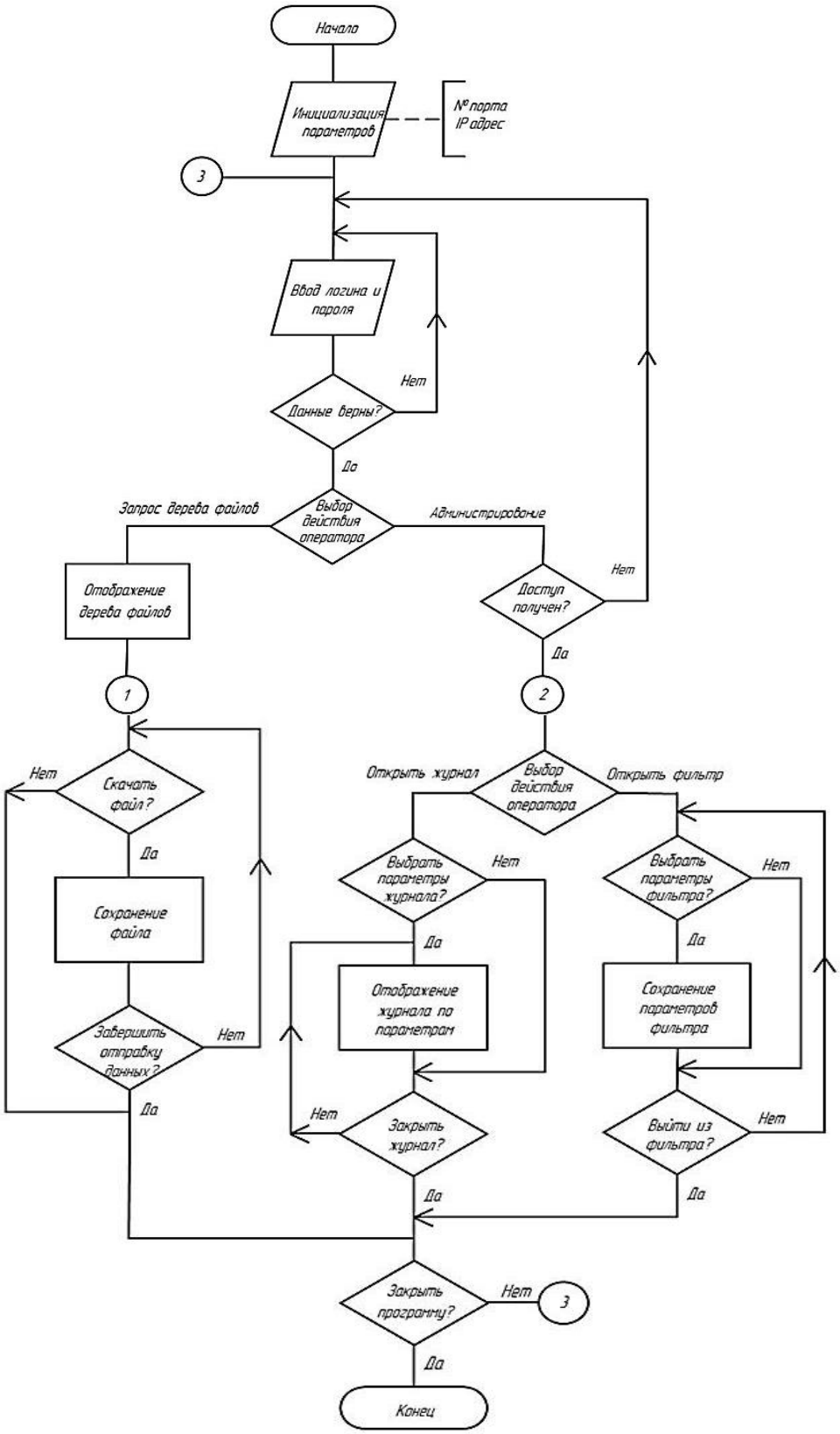

Рис. 5. Часть алгоритма работы серверного ПО

Fig. 5. Part of the server software algorithm

Серверная часть является совокупностью следующих модулей:

– модуль передачи файла предназначен для передачи обрабатываемой информации между сервером и клиентом;

– модуль работы с файлами на носителях предназначен для работы с содержимым съемного носителя. Данный модуль отвечает за считывание данных и дерева файлов, запрашиваемых со стороны клиента;

– модуль выполнения функций администратора предназначен для проверки правильности введенного пароля пользователем, смены пароля по требованию;

– модуль обмена сообщениями «Клиент – Сервер» предназначен для обработки запросов, принятых от клиента, и формирования ответов на соответствующие запросы;

– модуль фильтрации и аудита является подсистемой разграничения доступа к передаваемым файлам. Данный модуль при запросе файла обращается к параметрам фильтра. Если файл подходит под критерии параметров фильтра, файл передается на клиентскую часть. Каждый факт передачи файлов фиксируется в журнале логов.

Разработанные структурная и функциональные схемы позволяют определить полный список зависимостей между модулями системы, а также определить условия их взаимодействия. Составленные алгоритмы работы клиентской и серверной частей ПО описывают логику работы программно-аппаратного шлюза управления потоками данных при работе с внешними носителями.

Заключение

Предложена структура и функциональные особенности работы программно-аппаратного комплекса обеспечения защиты управления потоками данных при работе с внешними носителями на основе технологии однонаправленного шлюза данных. С учетом сформированных требований к функционалу программно-аппаратного комплекса был разработан алгоритм функционирования серверной и клиентской части программного средства, осуществлен и обоснован выбор аппаратной платформы для реализации серверной части, разработаны соответствующие рекомендации для реализации программно-аппаратного комплекса на любой платформе.

Список источников

1. Денисенко В. В., Арзамасов Е. В. Безопасность однонаправленной передачи данных // Науч.-практ. электрон. журн. «Аллея Науки». 2018. № 6 (22). URL: https://www.alley-science.ru/domains_data/files/64June20185/BEZOPASNOST%20ODNONAPRAVLENNOY%20PEREDAChI%20DANNYH.pdf (дата обращения: 16.06.2025).

2. Степанов Е. О. Разработка программно-аппаратного комплекса по защите информации систем терминального доступа на основе применения технологии однонаправленной передачи данных // Кибербезопасность: технические и правовые аспекты защиты информации: материалы Межвуз. студенч. науч.-практ. конф. (Москва, 27 апреля 2022 г.). Волгоград: Изд-во ИП Черняева Юлия Игоревна (Изд. дом «Сириус»), 2022. URL: https://elibrary.ru/download/elibrary_49250020_18404214.pdf (дата обращения: 16.06.2025).

3. Ахметбеков А. Д., Доля А. В. Методика организации передачи информации между открытым и закрытым сегментом информационных систем Центра информационно-аналитического обеспечения и мониторинга // Евразийское научное объединение. 2020. № 10-2 (68). С. 81–84.

4. Гончаров С. Н., Соколов С. Ю., Фомченко В. Н. Разработка безопасной автоматизированной системы управления информационными потоками // Информационная безопасность и защита информации: сб. ст. в 2 т. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2017. Т. 2. С. 7–16.

5. Архангельская А. В., Архангельский В. Г., Калмыков В. В. О тестировании макета однонаправленного шлюза // Безопасность информационных технологий. 2014. Т. 21. № 3. С. 44–54.

6. Воронцов А. Г., Петунин С. А. Организация однонаправленных сетей передачи информации в условиях защищенной среды // Вопр. кибербезопасности. 2017. № 2 (20). С. 21–29. URL: https://elibrary.ru/download/elibrary_29925546_12485330.pdf (дата обращения: 16.06.2025).

7. Колосов М. И. Разработка системы комплексного противодействия угрозам информационной безопасности при использовании внешних накопителей данных в автоматизированной информационной системе // Актуальные проблемы науки и техники: сб. науч. ст. по материалам VII Междунар. науч.-практ. конф. (Уфа, 14 января 2022 г.). Уфа: ООО «Научно-издательский центр "Вестник науки"», 2022. С. 68–74.

8. Питкевич П. И. Методы резервирования данных для критически важных ИТ-систем предприятия // Universum: технические науки. 2021. № 10-1 (91). С. 25–28.

9. Калуцкий И. В., Шумайлова В. А., Никулин Д. А. Создание системы защиты от утечки конфиденциальных данных // Инфокоммуникации и информационная безопасность: состояние, проблемы и пути решения: сб. науч. ст. по материалам III Всерос. науч.-практ. конф. (Курск, 11–13 мая 2016 г.): в 2 ч. Курск: Изд-во Юго-Запад. гос. ун-та, 2016. С. 156–160. URL: https://swsu.ru/structura/up/fivt/k_tele/IRBIS_11_GENR_elib_textbooks_bn1598.pdf#page=156 (дата обращения: 16.06.2025).

References

1. Denisenko V. V., Arzamasov E. V. Bezopasnost' odnonapravlennoi peredachi dannykh [Security of unidirectional data transmission]. *Nauchno-prakticheskii elektronnyi zhurnal «Alleia Nauki»*, 2018, no. 6 (22). Available at: https://www.alley-science.ru/domains_data/files/64June20185/BEZOPASNOST%20ODNONAPRAVLENNOY%20PEREDAChI%20DANNYH.pdf (accessed: 16.06.2025).

2. Stepanov E. O. Razrabotka programmno-apparatnogo kompleksa po zashchite informatsii sistem terminal'nogo dostupa na osnove primeneniia tekhnologii odnonapravlen-

noi peredachi dannykh [Development of a hardware and software package for information protection of terminal access systems based on the application of unidirectional data transmission technology]. *Kiberbezopasnost': tekhnicheskie i pravovye aspekty zashchity informatsii: materialy Mezhvuzovskoi studencheskoi nauchno-prakticheskoi konferentsii (Moskva, 27 aprelia 2022 g.).* Volgograd, Izd-vo IP Cherniaeva Iuliia Igorevna (Izd. dom «Sirius»), 2022. Available at: https://elibrary.ru/download/elibrary_49250020_18404214.pdf (accessed: 16.06.2025).

3. Akhmetbekov A. D., Dolia A. V. Metodika organizatsii peredachi informatsii mezhdu otkrytym i zakrytym segmentom informatsionnykh sistem Tsentra informatsionno-analiticheskogo obespecheniia i monitoringa [The methodology of organizing information transfer between the open and closed segment of information systems of the Center for Information and Analytical Support and Monitoring]. *Evraziiskoe nauchnoe ob"edinenie*, 2020, no. 10-2 (68), pp. 81-84.

4. Goncharov S. N., Sokolov S. Iu., Fomchenko V. N. Razrabotka bezopasnoi avtomatizirovannoi sistemy upravleniia informatsionnymi potokami [Development of a secure automated information flow management system]. *Informatsionnaia bezopasnost' i zashchita informatsii: sbornik statei v 2 t.* Sarov, FGUP «RFIaTs-VNIIEF», 2017. Vol. 2. P. 7-16.

5. Arkhangel'skaia A. V., Arkhangel'skii V. G., Kalmykov V. V. O testirovanii maketa odnonapravlennogo shliuza [About testing the unidirectional gateway layout]. *Bezopasnost' informatsionnykh tekhnologii*, 2014, vol. 21, no. 3, pp. 44-54.

6. Vorontsov A. G., Petunin S. A. Organizatsiia odnonapravlennykh setei peredachi informatsii v usloviiakh zashchishchennoi sredy [Organization of unidirectional information transmission networks in a secure environment]. *Voprosy kiberbezopasnosti*, 2017, no. 2 (20), pp. 21-29. Available at: https://elibrary.ru/download/elibrary_29925546_12485330.pdf (accessed: 16.06.2025).

7. Kolosov M. I. Razrabotka sistemy kompleksnogo protivodeistviia ugrozam informatsionnoi bezopasnosti pri ispol'zovanii vneshnikh nakopitelei dannykh v avtomatizirovannoi informatsionnoi sisteme [Development of a comprehensive system for countering threats to information security when using external data storage devices in an automated information system]. *Aktual'nye problemy nauki i tekhniki: sbornik nauchnykh statei po materialam VII Mezhdunarodnoi nauchno-prakticheskoi konferentsii (Ufa, 14 ianvaria 2022 g.).* Ufa, OOO «Nauchno-izdatel'skii tsentr "Vestnik nauki"», 2022. Pp. 68-74.

8. Pitkevich P. I. Metody rezervirovaniia dannykh dlia kriticheski vazhnykh IT-sistem predpriiatiia [Data backup methods for mission-critical enterprise IT systems]. *Universum: tekhnicheskie nauki*, 2021, no. 10-1 (91), pp. 25-28.

9. Kalutskii I. V., Shumailova V. A., Nikulin D. A. Sozdanie sistemy zashchity ot utechki konfidentsial'nykh dannykh [Creation of a protection system against confidential data leakage]. *Infokommunikatsii i informatsionnaia bezopasnost': sostoianie, problemy i puti resheniia: sbornik nauchnykh statei po materialam III Vserossiiskoi nauchno-prakticheskoi konferentsii (Kursk, 11–13 maia 2016 g.): v 2 ch.* Kursk, Izd-vo Iugo-Zapad. gos. un-ta, 2016. Pp. 156-160. Available at: https://swsu.ru/structura/up/fivt/k_tele/IRBIS_11_GENR_elib_textbooks_bn1598.pdf#page=156 (accessed: 16.06.2025).

Статья поступила в редакцию 14.07.2025; одобрена после рецензирования 12.08.2025; принята к публикации 17.10.2025
The article was submitted 14.07.2025; approved after reviewing 12.08.2025; accepted for publication 17.10.2025

Информация об авторах / Information about the authors

Валентина Юрьевна Кузнецова – кандидат технических наук, доцент; доцент кафедры высшей и прикладной математики; Астраханский государственный технический университет; arhelia@bk.ru

Ирина Юрьевна Квятковская – доктор технических наук, профессор; заведующий кафедрой высшей и прикладной математики; Астраханский государственный технический университет; i.kvyatkovskaya@astu.org

Елена Прокофьевна Карлина – доктор экономических наук, профессор; профессор кафедры производственного менеджмента; Астраханский государственный технический университет; e_karlina@list.ru

Даниил Александрович Сапельников – студент, направление обучения «Информационные системы и технологии»; Астраханский государственный университет имени В. Н. Татищева; daniil.s.a@mail.ru

Valentina Yu. Kuznetsova – Candidate of Technical Sciences, Assistant Professor; Assistant Professor of the Department of Higher and Applied Mathematics; Astrakhan State Technical University; arhelia@bk.ru

Irina Yu. Kvyatkovskaya – Doctor of Technical Sciences, Professor; Head of the Department of Higher and Applied Mathematics; Astrakhan State Technical University; i.kvyatkovskaya@astu.org

Elena P. Karlina – Doctor of Economic Sciences, Professor; Professor of the Department of Production Management; Astrakhan State Technical University; e_karlina@list.ru

Daniil A. Sapelnikov – Student, training area “Information Systems and Technology”; Astrakhan Tatishchev State University; daniil.s.a@mail.ru