Особенности построения информационных систем в случае неоднородной конфигурации комплекса технических средств

Г. П. Акимова, А. Ю. Даниленко

Федеральный исследовательский центр "Информатика и управление" РАН, Москва, Россия

Аннотация. В статье рассмотрен подход к организации работы предприятия, имеющего в составе вычислительной техники как автономные рабочие места, так и рабочие места, соединенные локальной сетью при наличии серверных компьютеров. Предложен способ конфигурирования программного обеспечения, позволяющий существенно упростить совместную работу сотрудников, а также унифицировать меры по обеспечению информационной безопасности.

Ключевые слова: операционная система; архитектура программного обеспечения; автоматизированные информационные системы; экспорт и импорт данных.

DOI 10.14357/20718632240305 **EDN** NZZGDK

Введение

Широкое внедрение информационных технологий во все сферы жизни общества, именуемое в последнее время цифровизацией, требует создания все большего числа автоматизированных информационных систем (АИС) различного назначения [1]. Эти системы, предназначенные для автоматизации деловых процессов организаций всех форм собственности, существенно ускоряют работу и предоставляют возможность гибкого управления.

Как правило, для АИС коллективного пользования рассматривается клиент-серверная архитектура, предполагающая наличие центрального сервера и нескольких автоматизированных рабочих мест (АРМ), подключаемых к серверу с помощью каналов связи, объединенных в локальную вычислительную сеть (ЛВС). При этом на сервере располагается база данных с информационными объектами, с которыми работают пользователи АИС, имеется база данных пользователей и реализованы алгоритмы предоставления доступа пользователей к объектам. В [2] рассмотрены варианты взаимодействия организаций, в которых внедрены системы электронного документооборота (СЭД), путем обмена данными между серверами.

Однако существует большое число организаций, не имеющих ЛВС вовсе, либо не все компьютеры сотрудников подключены к ЛВС, т.е. конфигурация технических средств неоднородна, и, как следствие, сотрудники организации работают на автономных АРМ, а передача данных между ними осуществляется на внешних носителях информации (машинные носители информации, МНИ). Понятно, что при такой организации работы каждый сотрудник выполняет свою работу независимо от остальных, данные передаются в случае необходимости, совместная работа затруднена. Кроме того, сотрудники имеют возможность использовать

в работе программные средства, которые часто плохо совместимы друг с другом, в результате страдают деловые процессы всего коллектива.

Для решения задачи организации совместной работы сотрудников, оптимизации деловой логики организации и архитектуры всего комплекса технических средств предлагается установить АИС на серверы и на все АРМ, включая автономные. С целью обеспечения корректного обмена данными целесообразно установить на всех рабочих местах одинаковое вспомогательное программное обеспечение (ПО).

1. Конфигурация рабочего места пользователя

Для решения задачи оптимизации совместной работы сотрудников организации при любой конфигурации АРМ предлагается использовать АИС, построенные по технологии тонкого клиента, где в качестве клиентского рабочего места используется один из стандартных web-браузеров, входящих в состав операционной системы (ОС), а не специально написанное приложение. При наличии соединения АРМ с сервером АИС через ЛВС специальных действий по конфигурированию рабочего места не требуется, однако требуется занести данные сотрудника в БД пользователей АИС, расположенной на сервере, т.е. создать учетную запись, ввести свойства пользователя, которые требуются для работы данной АИС. Заметим, что в последнее время появилось требование использовать при разработке АИС отечественные ОС и прикладное ПО [3].

На автономных АРМ, не соединенных с ЛВС, необходимо установить серверное ПО из состава АИС, включая систему управления базами данных (СУБД). В этом случае на АРМ располагается и база данных с теми информационными объектами, с которыми работает данный пользователь. Такая конфигурация возможна, поскольку современные компьютеры обладают достаточными ресурсами для установки на них указанного ПО. В начале сеанса работы с АИС требуется убедиться, что сервер АИС на автономном компьютере запущен (если данное ПО запускается автоматически при загрузке АРМ), либо запустить его вручную. В ходе запуска клиентского приложения, т.е. web-браузера, следует ввести адрес локального компьютера, обратив внимание на корректное указание как самого адреса, так и номера порта. Эти данные задаются при установке серверных компонент АИС на АРМ. В случае автономного АРМ не требуется создание отдельной БД пользователей, безопасность информации обеспечивается организационными мерами, антивирусными средствами и общеобъектовыми средствами защиты, в том числе средствами противодействия утечкам информации по техническим каналам (п. 2.3).

2. Архитектура в пределах подразделения

2.1. Ситуация исключительно автономных АРМ

Схема обмена данными в случае использования в подразделении исключительно автономных АРМ представлена на Рис. 1. Данный вариант архитектуры предназначен для использования в подразделениях при отсутствии возможности использования вычислительной сети.

В этом случае обмен информацией между АРМ сотрудников подразделения происходит на внешних носителях информации. Обмен данными может быть реализован в двух вариантах: полная синхронизация данных на всех АРМ и обмен только теми информационными объектами, которые требуются для выполнения служебных задач конкретного сотрудника. При использовании второго варианта уменьшается объем передаваемых данных, не требуются специальные действия по обеспечению синхронности информации, а также передаются только те данные, которые реально нужны сотруднику.

Технически обмен информацией реализуется с помощью процедур экспорта и импорта, при этом требуется реализация алгоритма идентификации информационных объектов внутри подразделения, позволяющая обрабатывать один и тот же объект несколькими пользователями на разных АРМ.

В АИС для обеспечения возможности обмена информацией, в том числе синхронизации данных, должны быть реализованы:

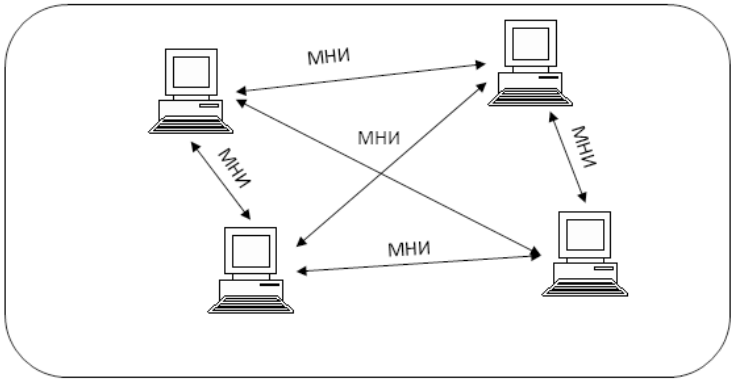

Рис. 1. Вариант автономных АРМ

– отбор для экспорта информационных объектов, измененных или созданных за указанный период времени;

– экспорт отобранных объектов с формированием файлов согласованного формата;

– запись сформированных файлов на внешний носитель или передачу по каналам связи;

– импорт информационных объектов из полученных по каналам связи или на внешнем носителе файлов;

– корректная обработка конфликтов при вводе данных.

Обработка конфликтов, возникающих при вводе данных информационного объекта, уже существующего в БД, представляет собой отдельную задачу. В частности, можно постановить, что вводимая информация всегда является единственно правильной (или актуальной), в этом случае уже имеющийся в БД объект заменяется целиком. Возможен вариант, когда для разрешения конфликта требуется решение оператора. Наиболее сложный в реализации вариант логики работы может предусматривать априорное задание для каждого атрибута источника правильных значений, например, для системы электронного документооборота, значение реквизита «Краткое содержание» всегда приходит от Пользователя 1, срок завершения работы от Пользователя 2, а стоимость работы определяется исключительно Пользователем 3.

Задача совместной работы для успешного решения требует также разработки и реализации методики идентификации информационных объектов в разных БД. Это может быть реализовано путем использования в качестве идентификаторов GUID – Global unique identifier – при том, что организационными мерами обеспечивается возможность ввода нового информационного объекта исключительно с одного рабочего места с дальнейшей его передачей в другие БД.

2.2. Автономные АРМ при наличии каналов связи и сервера

На Рис. 2. представлен вариант смешанной схемы взаимодействия: организация совместной работы при наличии автономных АРМ и АРМ, работающих в клиент-серверном режиме

В этом случае часть АРМ подключаются к серверу и работают с информацией (БД и файловые ресурсы), размещенной на сервере, но при этом в подразделении используются и автономные АРМ. Соответственно, обмен данными между пользователями происходит как с помощью МНИ, так и с использованием ЛВС и общего сервера. При этом возможно информационное взаимодействие между автономными АРМ и АРМ, подключенными к ЛВС.

При такой организации работы на серверном компьютере хранятся и обрабатываются данные всех пользователей АИС в подразделении, работающих через ЛВС, поэтому требуется принять меры для разграничения доступа. Во многих случаях наиболее предпочтительной является политика управления доступом, предполагающая равные права на действия с информационными объектами всех пользователей. Для учета особенностей деловой логики подразделения в АИС может быть реализована возможность администрирования доступа к информационным объектам и действиям с ними на программном уровне, не являющаяся средством защиты информации.

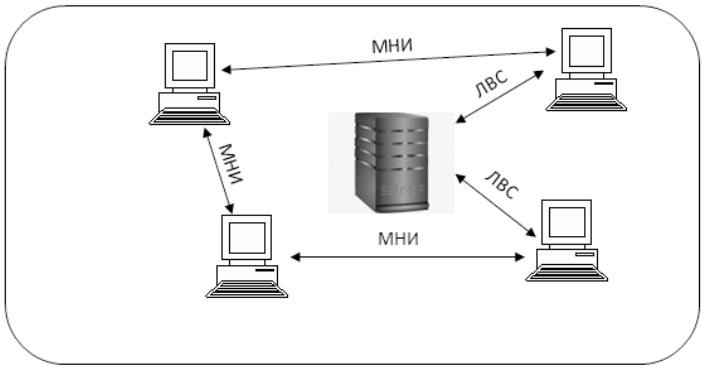

Рис. 2. Клиент-серверный вариант и автономные АРМ

На автономных АРМ пользователи работают со своими информационными объектами, для корректного обмена данными, в том числе в ходе их синхронизации, могут быть применены все возможности, перечисленные в п. 2.1. В случае получения пользователем, работающим в клиент-серверном режиме, данных с автономного АРМ на внешнем носителе он может занести их на сервер АИС. Допустима и обратная ситуация, когда информационный объект передается с сервера на автономный АРМ через один из АРМ в ЛВС. Безопасность данных при этом обеспечивается организационными мерами.

2.3. Обеспечение информационной безопасности

Во всех рассмотренных случаях безопасность информации обеспечивается общеобъектовыми средствами защиты, организационными мерами и средствами защиты информации (СЗИ), размещаемыми на сервере АИС, а также на локальном АРМ. СЗИ включают антивирусные средства, СЗИ в составе ОС и СУБД как на сервере, так и на клиентском АРМ. В случае, если предполагается разграничение доступа пользователей к информационным объектам, размещаемым на сервере, может потребоваться реализация алгоритмов управления доступом по дискреционной модели в составе отдельного модуля, диспетчера доступа. Требования в части обеспечения безопасности определены действующей нормативной базой, в частности [4-6].

Общеобъектовые СЗИ могут включать в себя средства защиты информации от утечки по техническим каналам, что исключает утечку данных по каналам электропитания и заземления, например, [7, 8]. Организационные меры обеспечивают соблюдение требований регламентов и инструкций по соблюдению режима работы, а также подготовку пользователей к работе с АИС. В ряде случаев могут потребоваться решения, направленные на ограничение физического доступа к техническим средствам АИС такие, как аппаратно-программные модули доверенной загрузки и ограничение доступа посторонних лиц в помещения.

Конфигурация и состав применяемых СЗИ определяется моделью угроз и нарушителя безопасности информации [9].

3. Взаимодействие подразделений

3.1. Обмен данными на внешних носителях

Рассмотрим конфигурацию, при которой в каждом подразделении функционирует полноценно сконфигурированная АИС, но каналы связи между подразделениями отсутствуют (Рис. 3).

В этом случае обмен данными между подразделениями осуществляется только с помощью внешних носителей информации. При этом в каждом подразделении следует выделить один АРМ (на рисунке обозначен как «Точка входа») для обмена данными с внешними подразделениями, т.е. для записи информации на внешние носители и для чтения полученных данных с последующим их вводом в БД АИС. Внутри подразделения обмен информацией может быть реализован любым из описанных ранее способов.

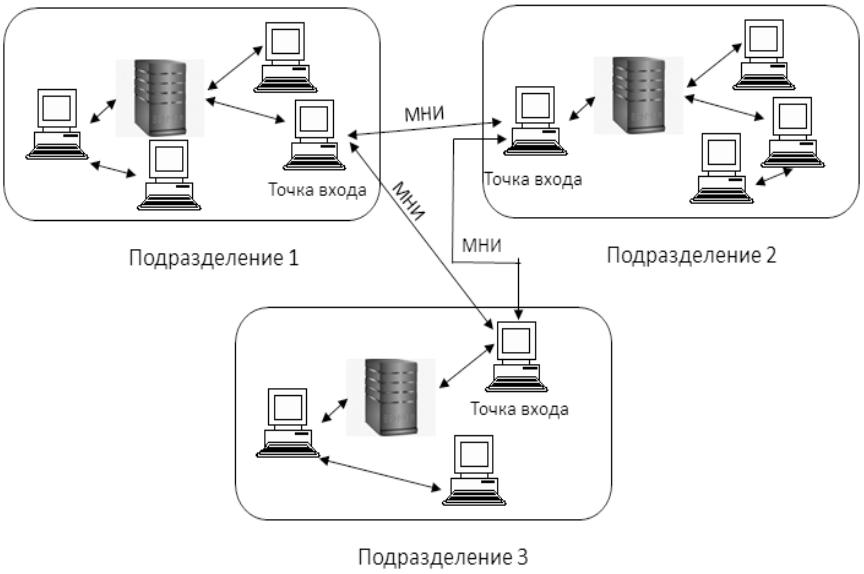

Рис. 3. Обмен данными между подразделениями на МНИ

Конфиденциальность данных в этом случае обеспечивается организационными мерами, основной частью которых должны быть процедуры предоставления доступа сотрудникам к полученным извне информационным объектам, а также контроль записи информации на МНИ для отправки во внешние подразделения. Указанные действия должны выполнять специально выделенные сотрудники, полномочия которых определяются отдельным приказом, а действия регламентируются соответствующими инструкциями.

3.2. Обмен данными с использованием каналов связи

Данный вариант предполагает обмен данными между серверами подразделений, причем каждый сервер технически может взаимодействовать с любым другим, но могут быть наложены ограничения, обусловленные деловой логикой организации (Рис. 4).

Основным отличием от рассмотренного ранее варианта с применением внешних носителей

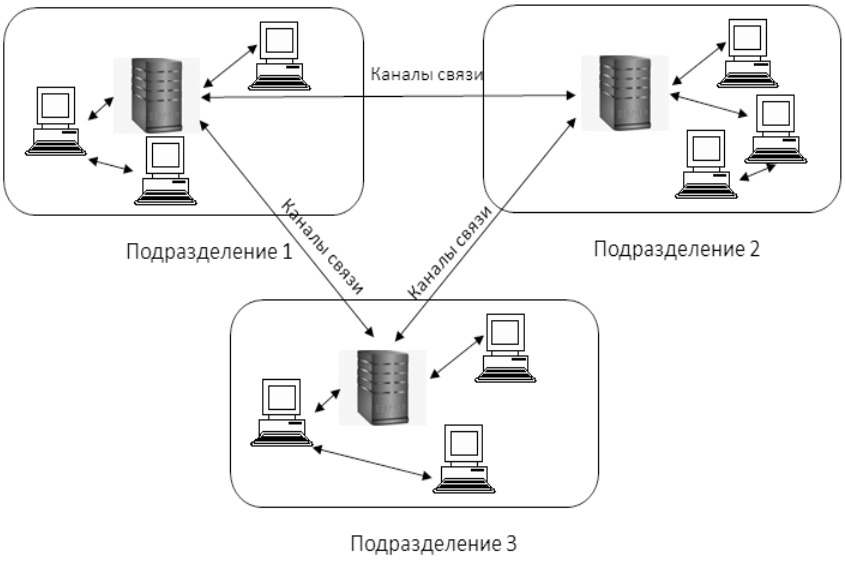

Рис. 4. Обмен данными между подразделениями по каналам связи

является использование защищенных каналов связи между подразделениями и отсутствие точки входа отдельного АРМ для обмена данными с внешними подразделениями. Для обеспечения конфиденциальности в данном случае требуется реализация полноценных СЗИ, обеспечивающих разграничение доступа по дискреционной и, при необходимости, по мандатной модели. Предоставление доступа к полученной информации выполняется либо административным персоналом, либо по запрограммированным алгоритмам, предусматривающим предоставление полученного материала конкретным сотрудникам в зависимости от тематики.

Аналогично право отправки документов во внешние подразделения должно быть разграничено как организационными мерами, так и программными средствами.

Заключение

Предложенный в статье подход к автоматизации деятельности организаций, имеющих неоднородную конфигурацию технических средств, не требует серьезных финансовых затрат для его реализации, однако его использование может существенно облегчить работу сотрудников и, как следствие, активизировать деловые процессы. Установка на автономных АРМ полного комплекта ПО из состава АИС позволяет организовать работу всех сотрудников по единому алгоритму, стандартизовав состав и формы обрабатываемых документов, а также порядок работы с ними. Таким образом, становится возможным реализовать на всех рабочих местах одинаковые методы обеспечения информационной безопасности, не допуская применения различных СЗИ и антивирусных средств. Кроме того, внедрение одной и той же АИС во всей организации позволит провести обучение персонала быстро и качественно.

Обмен информацией с использованием внешних носителей не представляет большой сложности в случае использования на всех компьютерах организации одинаковых методов экспорта и импорта и стандартных форматов передаваемых пакетов данных. Предлагаемый подход позволяет оптимально решить задачу совместной работы автономных АРМ и АРМ, работающих в клиент-серверном режиме.

Литература

1. Программа "Цифровая экономика Российской Федерации" http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf
2. Г. П. Акимова, А. Ю. Даниленко, Е. В. Пашкина, М. А. Пашкин, А. А. Подрабинович, И. В. Туманова. Возможности развития современных систем электронного документооборота. // Труды ИСА РАН. 2022. Т. 72. Выпуск 3. С. 97–104. DOI: 10.14357/20790279220310.
3. Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд. Постановление Правительства России от 16 ноября 2015 г. № 1236.
4. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. / Приказ ФСТЭК России от 11 февраля 2013 г. № 17.
5. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. / Приказ ФСТЭК России от 18 февраля 2013 г. № 21.
6. Государственный реестр сертифицированных средств защиты информации. URL https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153- sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00.
7. Способы и средства защиты информации от утечки по техническим каналам. Компания «СёрчИнформ». https://searchinform.ru/analitika-v-oblasti-ib/utechki-informatsii/sluchai-utechki-informatsii/tekhnicheskie-kanaly-utechki-informatsii/sposoby-i-sredstva-zaschity-informatsii-ot-utechki-po-tekhnicheskim-kanalam.
8. Н. Б. Пышкин, В. И. Василец. Защита информации от несанкционированной утечки и негласного съема (перехвата) по техническим каналам. // Мир и Безопасность. 2010. №6. https://www.vrsystems.ru/stati/zashita_informacii_ot_nesankcionirovannoi_utechki_i_neglasnogo_sema_(perexvata)_po_texnicheskim_kanalam.htm.
9. ГОСТ Р 51583 – 2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении.

Акимова Галина Павловна. Федеральный исследовательский центр «Информатика и управление» РАН, Москва, Россия. Ведущий научный сотрудник, кандидат технических наук. Область научных интересов: системное программирование, системный анализ, информационные технологии, влияние человеческого фактора, информационно-аналитические системы, электронный документооборот, электронный архив. E-mail: akimova@isa.ru

Даниленко Андрей Юрьевич. Федеральный исследовательский центр «Информатика и управление» РАН, Москва, Россия. Старший научный сотрудник, кандидат физико-математических наук. Область научных интересов: системное программирование, системный анализ, информационные технологии, электронный документооборот, информационная безопасность, защита данных. E-mail: danilenko@isa.ru

Features of Building Information Systems in the Case of a Heterogeneous Configuration of Complex of Technical Means

G. P. Akimova, A. Yu. Danilenko

Federal Research Center “Computer Science and Control” of Russian Academy of Sciences, Moscow, Russia

Abstract. The article discusses an approach to organizing the work of an enterprise that has computer equipment that includes both autonomous workstations and workstations connected by a local network with server computers. A method for configuring software has been proposed to significantly simplify the collaboration of employees, as well as unify measures to ensure information security.
Keywords: operating system; software architecture; automated information systems; data export and import.

DOI 10.14357/20718632240305 **EDN** NZZGDK

References

1. Programma "Tsifrovaya ekonomika Rossiyskoy Federatsii" [Program "Digital Economy of the Russian Federation"]. http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf.
2. G. P. Akimova, A. YU. Danilenko, Ye. V. Pashkina, M. A. Pashkin, A. A. Podrabinovich, I. V. Tumanova. Vozmozhnosti razvitiya sovremennykh sistem elektronnogo dokumentooborota. // Trudy ISA RAN. 2022. T. 72. Vypusk 3. S. 97–104. DOI: 10.14357/20790279220310. [G.P. Akimova, A.Yu. Danilenko, E.V. Pashkina, M.A. Pashkin, A.A. Podrabinovich, I.V. Tumanova. Opportunities for the development of modern electronic document management systems. // Proceedings of ISA RAS. 2022. T. 72. Issue 3. pp. 97–104. DOI: 10.14357/20790279220310].
3. Ob ustanovlenii zapreta na dopusk programm¬nogo obespecheniya, proiskhodyashchego iz inostran¬nykh gosudarstv, dlya tseley osushchestvleniya zakupok dlya obespecheniya gosudarstvennykh i munitsipal'nykh nuzhd. Postanovleniye Pravi¬tel'stva Rossii ot 16 noyabrya 2015 g. № 1236. [On establishing a ban on the admission of software originating from foreign countries for the purposes of procurement to meet state and municipal needs. Decree of the Russian Government of November 16, 2015 No. 1236.].
4. Ob utverzhdenii trebovaniy o zashchite informa¬tsii, ne sostavlyayushchey gosudarstvennuyu taynu, soderzhashcheysya v gosudarstvennykh informatsi¬onnykh sistemakh. / Prikaz FSTEK Rossii ot 11 fevralya 2013 g. № 17. [On approval of requirements for the protection of information that does not constitute a state secret, contained in state information systems. / Order of the FSTEC of Russia dated February 11, 2013 No. 17].
5. Ob utverzhdenii sostava i soderzhaniya organi¬zatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh perso¬nal'nykh dannykh. / Prikaz FSTEK Rossii ot 18 fevralya 2013 g. № 21. [On approval of the composition and content of organizational and technical measures to ensure the security of personal data during their processing in personal data information systems. / Order of the FSTEC of Russia dated February 18, 2013 No. 21].
6. Gosudarstvennyy reyestr sertifitsirovan¬nykh sredstv zashchity informatsii. URL https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00. [State register of certified information security means. URL https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00].
7. Sposoby i sredstva zashchity informatsii ot utechki po tekhnicheskim kanalam. Kompaniya «SorchInform». https://searchinform.ru/analitika-v-oblasti-ib/utechki-informatsii/sluchai-utechki-informatsii/tekhnicheskie-kanaly-utechki-informatsii/sposoby-i-sredstva-zaschity-informatsii-ot-utechki-po-tekhnicheskim-kanalam. [Methods

and means of protecting information from leakage through technical channels. «SearchInform» company. https://searchinform.ru/analitika-v-oblasti-ib/utechki-informatsii/sluchai-utechki-informatsii/tekhnicheskie-kanaly-utechki-informatsii/sposoby-i-sredstva-zaschity-informatsii-ot-utechki-po- tekhnicheskim-kanalam].

8. N. B. Pyshkin, V. I. Vasilets. Zashchita informatsii ot nesanktsionirovannoy utechki i neglasnogo s"yema (perekhvata) po tekhnicheskim kanalam. // Mir i Bezopasnost'. 2010. №6. https://www.vrsystems.ru/stati/zashita_informacii_ot_nesankcionirovannoi_utechki_i_neglasnogo_sema_(perexvata)_po_texnicheskim_kanalam.htm. [N. B. Pyshkin, V. I. Vasilets. Protection of information from unauthorized leaks and secret removal (interception) through technical channels. // Peace and Security. 2010. No. 6. https://www.vrsystems.ru/stati/zashita_informacii_ot_nesankcionirovannoi_utechki_i_neglasnogo_sema_(perexvata)_po_texnicheskim_kanalam.htm].
9. GOST R 51583 – 2014. Zashchita informatsii. Poryadok sozdaniya avtomatizirovannykh sistem v zashchishchennom ispolnenii. [GOST R 51583 – 2014. Information protection. The procedure for creating automated systems in a secure design].

Akimova Galina P. Ph.D.(Eng.), Leading Research Scientist, Federal Research Center “Computer Science and Control” of Russian Academy of Sciences, 44/2 Vavilova str., Moscow, 119333, Russia, research interests: system programming, system analysis, information technology, the influence of the human factor, information and analytical systems, electronic document management, electronic archive. E-mail: akimova@isa.ru

Danilenko Andrey Yu. Ph.D. (Phys.-Math.), Senior Research Scientist, Federal Research Center “Computer Science and Control” of Russian Academy of Sciences, 44/2 Vavilova str., Moscow, 119333, Russia, research interests: system programming, system analysis, information technology, electronic document management, information security, data protection. E-mail: danilenko@isa.ru