УДК 004.056
DOI: http://dx.doi.org/10.21686/1818-4243-2020-2-73-79

В.А. Сизов[1], Д.М. Малиничев[2], В.В. Мочалов[3]

[1] Российский экономический университет им. Г.В. Плеханова, Москва, Россия
[2] Российский государственный социальный университет, Москва, Россия
[3] Национальный исследовательский ядерный университет «МИФИ», Москва, Россия

Совершенствование нормативно-правовой базы информационной безопасности для устройств терминального доступа государственной информационной системы

Целью исследования *является повышение эффективности управления информационной безопасностью для государственных информационных систем (ГИС) с устройствами терминального доступа за счет совершенствования нормативно-правовых актов, которые должны быть логически увязаны между собой и не противоречить друг другу, а также использовать единый профессиональный тезаурус, позволяющий понимать и описывать процессы в области информационной безопасности.*

В настоящее время государственные информационные системы с устройствами терминального доступа используются для обеспечения реализации законных интересов граждан при информационном взаимодействии с органами государственной власти [1].

Одним из типов таких систем являются системы общего пользования [2]. Они предназначены для оказания электронных услуг гражданам, таких как оплата налогов, получение справок, подача заявлений и иных сведений.

Обрабатываемые персональные данные могут относиться к специальным, биометрическим, общедоступным и иным категориям [3]. Различные категории персональных данных, сосредоточенные в большом объёме о большом числе граждан, могут привести к значительному ущербу в результате их утечки, а значит, это создаёт информационные риски.

Существуют несколько основных типов архитектур государственных информационных систем: системы на основе «тонкого клиента»; системы на основе одноранговой сети; файл -серверные системы; центры обработки данных; системы с удаленным доступом пользователей; использование разных типов операционных систем (гетерогенность среды); использование прикладных программ, независимых от операционных систем; использование выделенных каналов связи [4]. Такое разнообразие и неоднородность государственных информационных систем с одной стороны, и необходимость качественного государственного регулирования в области информационной безопасности в этих системах, с другой стороны, требуют изучения и развития нормативно-правовых актов, учитывающих в первую очередь особенности систем, имеющих типовую современную архитектуру «тонкого клиента».

Материалы и методы исследования. *Защита государственной информационной системы регламентируется большим числом нормативно-правовых актов, которые постоянно совершенствуются с изменением и дополнением контента. На содержательном уровне она включает в себя множество этапов, таких как формирование требований к ГИС, разработка системы защиты, её внедрение, аттестация. Защищаемая информация обрабатывается в целях исполнения законодательства и обеспечения функционирования органов власти. Необходимость защиты конфиденциальной информации определяется законодательством Российской Федерации [5,6]. Поэтому для оценки качества нормативно-правовой базы информационной безопасности для устройств терминального доступа государственной информационной системы в работе проводится анализ основных нормативно-правовых актов и на его основе методом аналогии разрабатываются предложения по совершенствованию имеющихся регулирующих документов в области информационной безопасности.*

Результаты. *В работе разработаны предложения по совершенствованию нормативно-правовой базы информационной безопасности для устройств терминального доступа государственной информационной системы*

– для единообразия и унификации обоснованы термины с соответствующими определениями для их установления в документы ФСТЭК или Росстандарта;

– правила формирования требований к терминалам, которые должны быть аналогом требований к средствам вычислительной техники в «Концепции защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации».

Выводы. *Предложены общие рекомендации по защите информации в государственных информационных системах, использующих архитектуру «тонкого клиента», а также обоснованы специфичные угрозы, отсутствующие в банке угроз ФСТЭК и определены направления дальнейшего обеспечения информационной безопасности для рассматриваемого класса государственных информационных систем. В связи с большим числом заинтересованных субъектов, участвующих в согласовании и выработки единых решений, более конкретное рассмотрение поднятых проблем и вопросов возможно только с привлечением к обсуждению представителей уполномоченных федеральных органов исполнительной власти и представителей бизнеса.*

Ключевые слова: *защищенные информационные системы, информационная безопасность, государственная информационная система, тонкий клиент, центр обработки данных.*

Valeriy A. Sizov[1], Dmitry M. Malinichev[2], Vadim V. Mochalov[3]

[1] Plekhanov Russian University of Economic, Moscow, Russia
[2] Russian State Social University, Moscow, Russia
[3] National Research Nuclear University, Moscow, Russia

Improvement of the Regulatory Framework of Information Security for Terminal Access Devices of the State Information System

The aim of the study *is to increase the effectiveness of information security management for state information systems (SIS) with terminal access devices by improving regulatory legal acts that should be logically interconnected and not contradict each other, as well as use a single professional thesaurus that allows understanding and describe information security processes.*

Currently, state information systems with terminal access devices are used to ensure the realization of the legitimate interests of citizens in information interaction with public authorities [1].

One of the types of such systems are public systems [2]. They are designed to provide electronic services to citizens, such as paying taxes, obtaining certificates, filing of applications and other information.

The processed personal data may belong to special, biometric, publicly available and other categories [3]. Various categories of personal data, concentrated in a large volume about a large number of citizens, can lead to significant damage as a result of their leakage, which means that this creates information risks.

There are several basic types of architectures of state information systems: systems based on the "thin client"; peer-to-peer network systems; file server systems; data processing centers; systems with remote user access; the use of different types of operating systems (heterogeneity of the environment); use of applications independent of operating systems; use of dedicated communication channels [4]. Such diversity and heterogeneity of state information systems, on the one hand, and the need for high-quality state regulation in the field of information security in these systems, on the other hand, require the study and development of legal acts that take into account primarily the features of systems that have a typical modern architecture of "thin customer".

Materials and research methods. *The protection of the state information system is regulated by a large number of legal acts that are constantly being improved with changes and additions to the content. At the substantive level, it includes many stages, such as the formation of SIS requirements, the development of a security system, its implementation, and certification. The protected information is processed in order to enforce the law and ensure the functioning of the authorities. The need to protect confidential information is determined by the legislation of the Russian Federation [5, 6]. Therefore, to assess the quality of the regulatory framework of information security for terminal access devices of the state information system, the analysis of the main regulatory legal acts is carried out and on the basis of it, proposals are developed by analogy to improve existing regulatory documents in the field of information security.*

Results. *The paper has developed proposals for improving the regulatory framework of information security for terminal access devices of the state information system*

– for uniformity and unification, the terms with corresponding definitions are justified for their establishment in the documents of the Federal Service for Technical and Export Control (FSTEC) or Rosstandart;

– rules for the formation of requirements for terminals, which should be equivalent requirements for computer equipment in the "Concept for the protection of computer equipment and automated systems from unauthorized access to information".

Conclusion. *General recommendations on information protection in state information systems using the "thin client" architecture are proposed, specific threats that are absent in the FSTEC threat bank are justified, and directions for further information security for the class of state information systems under consideration are identified. Due to the large number of stakeholders involved in the coordination and development of unified solutions, a more specific consideration of the problems and issues raised is possible only with the participation of representatives of authorized federal executive bodies and business representatives for discussion.*

Keywords: *secure information systems, information security, state information system, thin client, data processing center.*

Введение

Цифровизация различных сфер человеческой деятельности и использование различного рода государственных информационных систем позволяет добиться увеличения конкурентоспособности экономики и уровня развития общества, а также обеспечивает реализацию законных интересов граждан при информационном взаимодействии с органами государственной власти [1]. Одним из типов таких систем являются системы общего пользования [2]. Они предназначены для оказания электронных услуг гражданам, таких как оплата налогов, получение справок, подача заявлений и иных сведений. Такие системы тесно связаны с использованием больших объемов персональных данных граждан. Обрабатываемые персональные данные могут относиться к специальным, биометрическим, общедоступным и иным категориям [3]. Различные категории персональных данных, сосредоточенные в большом объеме о большом числе граждан, могут привести к значительному ущербу в результате их утечки, а значит, это создает информационные риски. Другим типом государственной информационной системы являются закрытые системы межведомственного взаимодействия и документооборота. В таких системах обрабатывается конфиденциальная и служебная тайна тех органов власти, которые используют эти системы. Объективно сказать, какой тип системы больше уязвим и нанесет больше ущерба нельзя ввиду многих особенностей и различий, делающих каждую государственную информационную систему уникальной. Одним из показателей, характеризующим проектную защищенность ГИС является ее архитектура. Выделяют следующие типы архитектур: системы на основе

«тонкого клиента»; системы на основе одноранговой сети; файл-серверные системы; центры обработки данных; системы с удаленным доступом пользователей; использование разных типов операционных систем (гетерогенность среды); использование прикладных программ, независимых от операционных систем; использование выделенных каналов связи [4]. Таким образом, несмотря на явную, описанную в Приказе ФСТЭК №17, и неявную классификацию, выполненную по различным другим признакам государственных информационных систем, меры по их защите применяются индивидуально посредством выбора этих мер: определения, дополнения, уточнения и адаптации базовых мер защиты информации.

Анализ существующей нормативно-правовой базы информационной безопасности для модели тонких клиентов государственной информационной системы

Защита государственной информационной системы – это сложный процесс, регламентируемый большим числом нормативно-правовых актов. Он включает в себя множество этапов, как формирование требований, разработка системы защиты, ее внедрение, аттестация.

Государственные информационные системы обрабатывают конфиденциальную информацию, необходимость защиты которой определяется законодательством Российской Федерации [5, 6]. Защищаемая информация обрабатывается в целях исполнения законодательства и обеспечения функционирования органов власти. Приказ ФСТЭК № 17 устанавливает три класса защищенности информационных систем, определяемых на основании трех уровней значимости, обрабатываемой в них информации и масштабе информационной системы. Уровень значимости информации имеет градацию от 1 до 3 и определяется возможность степенью ущерба от нарушения свойств информации (конфиденциальность, целостность и доступность), а также от масштаба государственной информационной системы (федеральная, региональная, муниципальная). В зависимости от категории информации определяется ее уровень значимости: УЗ 1, УЗ 2, УЗ 3. Уровень значимости зависит от степени ущерба, в результате нарушения конфиденциальности, целостности или доступности информации. Самый высокий уровень значимости УЗ 1, самый низкий УЗ 3.

Требования для каждого класса ГИС определяются согласно Приказу ФСТЭК № 17. Они накладывают требования к антивирусным средствам защиты, средствам обнаружения вторжений, межсетевым экранам и так далее. СТР-К определяет требования для защиты информации от утечек по техническим каналам. По требованию заказчика может применяться РД АС.

Требуемый класс ГИС определяется исходя из категории информации, которая в ней обрабатывается и масштаба ГИС согласно Приложению № 1 к Приказу ФСТЭК № 17. Для их определения производится изучение документов и опрос заказчика. После определения требуемого класса ГИС определяется базовый перечень методов защиты информации согласно Приложению № 2 к Приказу ФСТЭК № 17. Всего предусмотрено 113 мер, из них 48 необходимы для всех классов государственных информационных систем и 30, необязательные ни для одного из классов ГИС, но возможные для реализации в качестве мер усиления или компенсации. Использование устройств терминального доступа предусмотрено мерой защиты информации ЗИС.14 «Использование устройств терминального доступа для обработки информации». Эта мера является необязательной для всех классов государственных информационных систем. Такие терминальные устройства должны быть ограничены в своих возможностях по обработке и хранению информации. Эти функции и меры защиты информации должны быть перенесены на сервер обработки информации.

Для детализации внедряемых мер необходимо руководствоваться Методическим документом «Меры защиты информации в ГИС», который определяет свойства и усиления мер. После выбора базового перечня мер из них исключаются меры, направленные на технологии, не используемые в данной информационной системе. Каждой из внедряемых мер защиты информации прилагается перечень необходимых и рекомендуемых усилений к реализации меры. В случае невозможности реализации одной из предусмотренных мер применяются компенсирующие меры, направленные на исключение угрозы. После могут применяться дополнительные меры, предусмотренные другими нормативно-правовыми документами.

В связи с тем, что государственные информационные системы зачастую предназначены для обработки персональных данных, то документы, предъявляющие требования к защите и аттестации государственных информационных систем, как правило, включают в себя и требования к защите и обработке персональных данных [3, 7]. Хотя состав и содержание мер для этих систем тождественны, однако актуальные угрозы для них могут быть различны. В этой связи минимальный состав и содержание

мер определяется по нижней границе требований к обеим системам. Различные уровни защищенности, установленные для государственных информационных систем и информационных систем персональных данных, накладывают дополнительные сложности и вносят неразбериху, фактор неизвестности и неопределенности, что влечет за собой информационные риски.

Использование устройств терминального доступа регламентируется пунктом 20.11 Приказа ФСТЭК № 17 [8], пунктом 8.11 Приказа ФСТЭК №21 [7], разделом ЗИС.14 Методического документа ФСТЭК «Меры защиты информации в государственных информационных системах» [9].

Обоснование мер по защите информации в государственных информационных системах для модели тонких клиентов

Меры по защите информации в государственных информационных системах для модели тонких клиентов должны включать в себя программно-технические, организационно-правовые, инженерно-технические. Программно-технические меры защиты информации заключаются в обеспечении защищенного подключения терминала к терминальному серверу государственной информационной системы с использованием криптографических протоколов и алгоритмов. Для этого должны использоваться криптографические шлюзы, обеспечивающие необходимый уровень защиты, подтвержденный сертификатами соответствия. Программно-аппаратные меры, направленные на обеспечение управление доступом, регистрацию и учет, целостность информации и информационной системы выполняются на терминальном сервере. Необходимо запретить возможность подключения к терминальному серверу с терминала-клиента с использованием учетных записей системного администратора и администратора информационной безопасности.

Терминальные устройства рекомендуется выделить в отдельную подсеть и отделить от основной сети организации сертифицированным межсетевым экраном. Межсетевой экран должен быть настроен таким образом, чтобы обеспечить сетевую безопасность терминальных устройств и исключить возможность установления подключений с другими хостами, кроме терминального сервера. Это особенно важно для создания замкнутой программной среды и минимизации соответствующих рисков [10]. Терминалы должны иметь возможность шифрования аутентификационной информации пользователя и проводить взаимную аутентификацию с терминальным сервером. Для этих целей должны использоваться сертифицированные криптопровайдеры и криптопротоколы. Рекомендуется использовать двухфакторную аутентификацию, подразумевающую использование пары логин-пароль и аппаратного аутентификатора. Возможно размещение совместно с межсетевым экраном и криптографического шлюза, работающего в режиме туннелирования (в частности, такое позволяет протокол IPsec).

Для исключения внедрения вредоносного кода в образ терминальной операционной системы при ее загрузке в память рабочей станции должна быть обеспечена доверенная сетевая загрузка. Она может быть достигнута за счет проведения контроля временных интервалов процесса штатной загрузки [11].

Терминалы необходимо располагать таким образом, чтобы затруднить потенциальному злоумышленнику визуальный съем информации с экранов. В зависимости от необходимости вывода и/или ввода акустической информации необходимо обеспечить защиту акустической информации с применением средств акустической и виброакустической защиты. При необходимости вывода информации на принтер для печати необходимо обеспечить сетевую безопасность такого подключения, а также отсутствие закладных устройств в принтере.

Разработка предложений по совершенствованию нормативно-правовой базы информационной безопасности для модели тонких клиентов государственной информационной системы

Нормативно-правовые акты должны быть логически увязаны между собой, дополнять друг друга и не противоречить. Необходим единый глоссарий, позволяющий понимать и описывать процессы. Сложилась такая ситуация, что термины и определения зачастую имеют различное толкование в разных документах. В частности, в государственных стандартах и документах Гостехкомиссии применяется термин «автоматизированная система», а в федеральных законах и документах ФСТЭК «информационная система». Различные документы дают разные определения и для других понятий. Отсутствует четкое определение, утвержденное регуляторами в области информационной безопасности, что подразумевается под понятиями «тонкий клиент», «терминал», «терминальный сервер» и так далее. Отсутствует документация и требования для сертификации терминалов и терминальных серверов, а имеющаяся документация только вносит путаницу и создает коллизии. Так, Приказ ФСТЭК №17 устанавливает необходимость наличия

сертификата у средств вычислительной техники, используемых в государственных информационных системах, не менее пятого класса. Требования руководящего документа СВТ сложно или невозможно выполнить для тонких клиентов, так как они ограничены в объеме памяти и вычислительных возможностях. Регистрация и учет, средства разграничения доступом и иные средства защиты информации располагаются на терминальном сервере. Но в данном случае нарушается концепция защиты от НСД, подразумевающая, что СВТ изначально поставляется на рынок как готовые элементы [12,13]. Таким образом, ни в Приказе ФСТЭК №17, ни в РД СВТ нет четких требований к тонким клиентам, а профили защиты операционных систем не предназначены для оценки программно-аппаратных средств. Методический документ «Меры защиты информации в государственных информационных системах» так же не вносит ясности, так как предлагает только пример тонкого клиента без четкого его описания и определения, а также накладывает некоторые нечеткие требования. Возникает необходимость в отдельных документах, определяющих требования к тонким клиентам и их взаимодействию с терминальным сервером и государственной информационной системой.

Для единообразия и унификации необходимо установить в документах ФСТЭК или Росстандарта следующие термины с соответствующими определениями, применяемые при проведении работ по стандартизации в области защиты информации: терминал, тонкий клиент, терминальный сервер. ГОСТ 25868-91 устанавливает определение терминала, как «устройство ввода-вывода, обеспечивающее взаимодействие пользователей в локальной вычислительной сети или с удаленной ЭВМ через средства телеобработки данных». Как видно из этого определения, оно не оговаривает ограничения, свойства и параметры, которым должны удовлетворять терминалы.

Требования для терминалов должны устанавливаться для отдельных структурных элементов (терминалов) и являться аналогом требований для СВТ [13] в Концепции защиты информации от НСД [12]. Должны включать в себя:

- доступный объем долговременной памяти;
- доступный объем временной памяти;
- механизмы очистки временной и долговременной памяти;
- поддержка протоколов сетевого взаимодействия;
- поддержка криптографических протоколов.

Требования по использованию терминальных устройств в государственных информационных системах должны являться дополнением к Приказу ФСТЭК №17 и одновременно являться аналогом требований к АС в Концепции защиты информации от НСД [12,14]. Должны включать в себя:

- порядок сетевого взаимодействия терминального сервера и терминала-клиента;
- протоколы шифрования и аутентификации терминального сервера и терминалов-клиентов;
- модель управления доступом;
- модель нарушителей;
- полномочия пользователей;
- технологию обработки информации.

Заключение

Были исследованы нормативно-правовые акты, предъявляющие требования по защите информации, и научные источники, описывающие процесс защиты государственных информационных систем, использующих архитектуру «тонкого клиента». Для создания надежной системы защиты информации необходимо иметь в ее основе интеграционный процесс в виде документации, требований и рекомендаций, описание наилучших практик и решений. Настоящее состояние нормативно-правовой базы свидетельствует о недостаточной проработке в глоссарии, описании процессов и требований, касающихся защиты государственных информационных систем, использующих архитектуру «тонкого клиента». Отсутствие точных определений, количественных характеристик, специфичных требований, рекомендаций и угроз не позволяет говорить о возможности достижения синергетического эффекта зрелой системы защиты информации. Необходимость дальнейшего совершенствования нормативно-правовой базы и дальнейшие шаги, предложенные в данной исследовательской работе, позволяют определить основные направления этого процесса.

Предложены общие рекомендации по защите информации в государственных информационных системах, использующих архитектуру «тонкого клиента», предложены специфичные угрозы, отсутствующие в банке угроз ФСТЭК и заданы направления дальнейшего развития. В связи с большим числом заинтересованных сторон, необходимостью согласования и выработки единых решений, более конкретное рассмотрение поднятых проблем и вопросов возможно только с привлечением к обсуждению представителей уполномоченных федеральных органов исполнительной власти и представителей бизнеса.

Литература

1. Болгарский А.И. Защита информации в государственных информационных системах // Вестник УрФО. Безопасность в информационной сфере. 2011. № 2. С. 48–50.

2. Сабанов А.Г., Мельниченко П.А. Предоставление защищенного доступа к информационным системам массового использования при оказании государственных услуг в электронном виде // Вестник Российской таможенной академии. 2011. № 3. С. 73–78.

3. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: утв. постановлением Правительства Рос. Федерации от 1 ноября 2012 г. № 1119 // Российская газета, № 256, 07.11.2012.

4. Проект методического документа. Методика определения угроз безопасности информации в информационных системах [Электрон. ресурс] // Федеральная служба по техническому и экспортному контролю России. Режим доступа: https://fstec.ru/component/attachments/download/812

5. Об информации, информационных технологиях и о защите информации (с изменениями на 23 апреля 2018 года): федеральный закон Российской Федерации от 27 июля 2006 г. №149–ФЗ. // Российская газета, № 165, 29.07.2006.

6. О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации (с изменениями на 11 мая 2017 года): утвержден постановлением Правительства Российской Федерации от 6 июля 2015 г. № 676 // Собрание законодательства Российской Федерации, № 28, 13.07.2015, ст.4241.

7. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (с изменениями на 23 марта 2017 года) : утверждем приказом ФСТЭК от 18 февраля 2013 г. № 21 // Российская газета, № 107, 22.05.2013.

8. Об утверждении Требований по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (с изменениями на 15 февраля 2017 года): утвержден приказом ФСТЭК от 11 февраля 2013 г. № 17 // Российская газета, № 136, 26.06.2013.

9. Меры защиты информации в государственных информационных системах. Методический документ ФСТЭК России от 11 февраля 2014 г.

10. Лемке Е.А., Лубкин И.А. Создание защищенной терминальной системы // Решетневские чтения. 2013. Т. 2. № 17. С. 306–308.

11. Тищенко Е.Н., Буцик К.А., Деревяшко В.В. Модель доверенной сетевой загрузки «тонкого клиента» с нейтрализацией «внутреннего нарушителя» // Известия ЮФУ. Технические науки. 2015. № 5 (166). С. 37–47.

12. Руководящий документ Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации Утверждена решением Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электрон. ресурс]. Режим доступа: https://fstec.ru/component/attachments/download/299.

13. Гатчин Ю.А., Теплоухова О.А. Алгоритм аутентификации участников информационного взаимодействия при удаленной загрузке операционной системы на тонкий клиент // Научно–технический вестник информационных технологий, механики и оптики. 2016. Т. 16. № 3. С. 497–505.

14. Малиничев Д.М., Ермашов А.В. Обеспечение защиты информации в компании от несанкционированного доступа с помощью отечественных продуктов средств защиты информации // Colloquium–journal. 2019. № 11–1 (35). С. 101–103.

References

1. Bolgarskiy A.I. Information protection in state information systems. Vestnik UrFO. Bezopasnost' v informatsionnoy sfere = Bulletin of the Urals Federal District. Security in the information field. 2011; 2: 48-50. (In Russ.)

2. Sabanov A.G., Mel'nichenko P.A. Providing secure access to mass use information systems in the provision of public services in electronic form. Vestnik Rossiyskoy tamozhennoy akademii= Bulletin of the Russian Customs Academy. 2011; 3: 73-78. (In Russ.)

3. On approval of requirements for the protection of personal data during their processing in personal data information systems: approved. Government Decree Ros. Federation of November 1, 2012 No. 1119. Rossiyskaya gazeta = Russian newspaper; N 256, 07.11.2012. (In Russ.)

4. Draft guidance document. Methodology for identifying threats to information security in information systems [Internet]. Federal'naya sluzhba po tekhnicheskomu i eksportnomu kontrolyu Rossii = Federal Service for Technical and Export Control of Russia. Available from: https://fstec.ru/component/attachments/download/812. (In Russ.)

5. On information, information technology and information protection (as amended on April 23, 2018): Federal Law of the Russian Federation of

July 27, 2006 No. 149-F3. Rossiyskaya gazeta = Russian newspaper; N 165, 29.07.2006. (In Russ.)

6. On requirements for the procedure for the creation, development, commissioning, operation and decommissioning of state information systems and the further storage of information contained in their databases (as amended on May 11, 2017): approved by the Government of the Russian Federation on July 6, 2015 g. No. 676. Sobraniye zakonodatel'stva Rossiyskoy Federatsii, N 28, 13.07.2015, st.4241 = Meeting of the legislation of the Russian Federation, N 28, 07/13/2015, Art. 421. (In Russ.)

7. 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 (as amended on March 23, 2017): we approve by order of the FSTEC of February 18, 2013 No. 21. Rossiyskaya gazeta = Russian newspaper; N 107, 22.05.2013. (In Russ.)

8. On approval of the requirements for the protection of information not constituting state secrets contained in state information systems (as amended on February 15, 2017): approved by order of the FSTEC of February 11, 2013 No. 17. Rossiyskaya gazeta = Russian newspaper; N 136, 26.06.2013. (In Russ.)

9. Mery zashchity informatsii v gosudarstvennykh informatsionnykh sistemakh. Metodicheskiy dokument FSTEK Rossii ot 11 fevralya 2014 g = Information security measures in state information systems. Methodological document of the FSTEC of Russia dated February 11, 2014. (In Russ.)

10. Lemke Ye.A., Lubkin I.A. Creating a secure terminal system. Reshetnevskiye chteniya = Reshetnev readings. 2013; 2; 17: 306-308. (In Russ.)

11. Tishchenko Ye.N., Butsik K.A., Derevyashko V.V. The model of trusted network load of the «thin client» with the neutralization of the «internal intruder». Izvestiya YUFU. Tekhnicheskiye nauki = News of SFU. Technical science. 2015; 5 (166): 37-47. (In Russ.)

12. Rukovodyashchiy dokument Kontseptsiya zashchity sredstv vychislitel'noy tekhniki i avtomatizirovannykh sistem ot nesanktsionirovannogo dostupa k informatsii Utverzhdena resheniyem Gosudarstvennoy tekhnicheskoy komissii pri Prezidente Rossiyskoy Federatsii ot 30 marta 1992 g = Guiding document The concept of protecting computer equipment and automated systems from unauthorized access to information Approved by the decision of the State Technical Commission under the President of the Russian Federation of March 30, 1992. [Internet]. Available from: https://fstec.ru/component/attachments/download/299. (In Russ.)

13. Gatchin YU.A., Teploukhova O.A. Authentication algorithm for information interaction participants when remotely loading the operating system on a thin client. Nauchno-tekhnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki = Scientific and Technical Bulletin of Information Technologies, Mechanics and Optics. 2016; 16; 3: 497-505. (In Russ.)

14. Malinichev D.M., Yermashov A.V. Ensuring the protection of information in the company from unauthorized access using domestic products of information protection. Colloquium-journal = Colloquium-journal. 2019; 11-1 (35): 101-103. (In Russ.)

Сведения об авторах

Валерий Александрович Сизов
Д.т.н., профессор, профессор кафедры прикладной информатики и информационной безопасности
Российский экономический университет им. Г.В.Плеханова,
Москва, Россия
Эл. почта: sizovva@gmail.com

Дмитрий Михайлович Малиничев
К.т.н., доцент, доцент кафедры информационной безопасности
Российского государственного социального университета, Москва, Россия
Эл. почта: mmm_63@list.ru

Вадим Вячеславович Мочалов
Инженер
Национальный исследовательский ядерный университет «МИФИ», Москва, Россия
Эл. почта: vadimmoch@yandex.ru

Information about the authors

Valery A. Sizov
Dr. Sci. (Engineering), Professor, Professor of the Department of Applied Informatics and Information Security
Plekhanov Russian University of Economic,
Moscow, Russia
E-mail: sizovva@gmail.com

Dmitry M. Malinichev
Cand. Sci. (Engineering), Associate Professor, Associate Professor of the Department of Information Security
Russian State Social University, Moscow, Russia
E-mail: mmm_63@list.ru

Vadim V. Mochalov
Engineer
National Research Nuclear University,
Moscow, Russia
E-mail: vadimmoch@yandex.ru