ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056

DOI: 10.21822/2073-6185-2026-53-2-142-152 Оригинальная статья/ Original article

Метод протоколирования аттестационных испытаний автоматизированной системы в защищенном исполнении

А.Д. Трофимович
Российский государственный университет нефти и газа (НИУ) имени И.М. Губкина,
119991, Москва, Ленинский пр-т., д.65, Россия

Резюме. Цель. Целью исследования является разработка метода протоколирования результатов аттестационных испытаний автоматизированной системы в защищенном исполнении, отражающего необходимые и достаточные мероприятия для проверки требований по защите информации в зависимости от установленного уровня защищённости системы. **Метод.** В качестве методов научного познания используются: описание, анализ, систематизация, оценка рисков информационной безопасности, теория защиты информации. **Результат.** На примере системы, использующей программно-технические средства под управлением операционной системы Linux, обоснованы методы проведения аттестационных испытаний и описываются необходимые результаты, подтверждающие соответствие автоматизированной системы требованиям по информационной безопасности. Приводится обоснование необходимого перечня программных средств контроля, использование которых позволит в полной мере оценить безопасность тестируемой системы. В материале отражены необходимые, в соответствии с требованиями по аттестации, проверки антивирусных программ и защиты от несанкционированного доступа,а также требования к сертификационным испытаниям системы защиты виртуализации и проверки телекоммуникационного оборудования. **Вывод.** Научная новизна результатов состоит в том, что в работе впервые, на основе анализа научных работ и актуальных нормативно-правовых актов РФ сформулирован и применен на практике общий методологический подход и создана методика протоколирования аттестационных испытаний автоматизированных систем в защищенном исполнении. Метод, представленный в работе, может использоваться при проведении аттестационных испытаний различных автоматизированных систем и позволяет максимально наглядно продемонстрировать соответствие системы актуальным требованиям по защите информации и значительно сократит сроки разработки аттестационных документов, тем самым, уменьшая стоимость работ по аттестации.

Ключевые слова: информационная безопасность, требования, руководящие документы, аттестационные испытания, протоколирование, автоматизированная система.

Для цитирования: А.Д. Трофимович. Метод протоколирования аттестационных испытаний автоматизированной системы в защищенном исполнении. Вестник Дагестанского государственного технического университета. Технические науки. 2026;53(2):142-152. DOI:10.21822/2073-6185-2026-53-2-142-152

Method for recording Certification Tests of an Automated System in a Secure Design

A.D. Trofimovich
I.M. Gubkin Russian State University of Oil and Gas (NRU),
65 Leninsky Ave., Moscow 119991, Russia

Abstract. Objective. The purpose of the study is to develop a method for logging the results of certification tests of an automated system in a secure design, reflecting the necessary and sufficient measures to verify information security requirements depending on the established security level of the system. The scientific novelty of the article lies in the fact that for the first time, based on the analysis of scientific papers and current regulatory legal acts of the Russian

Federation, a general methodological approach has been formulated and put into practice, and a methodology for logging certification tests of automated systems in secure execution has been created. **Method.** The following methods of scientific knowledge are used: description, analysis, systematization, assessment of information security risks, theory of information protection. **Result.** Using the Linux system as an example, this article substantiates the methods for conducting certification tests and describes the results confirming the automated system's compliance with information security requirements. It also provides a rationale for the list of software controls used to assess the security of the system under test. The material covers the necessary checks for antivirus software and protection against unauthorized access, as well as requirements for certification testing of virtualization protection systems and testing of telecommunications equipment. **Conclusion.** The method presented in this paper can be used in conducting certification tests of various automated systems. It will make it possible to demonstrate the system's compliance with current information security requirements as clearly as possible and significantly reduce the time required for the development of certification documents, thereby reducing the cost of certification work.

Keywords: information security, requirements, guidance documents, certification, logging, automated system.

For citation: A.D. Trofimovich. Method for recording Certification Tests of an Automated System in a Secure Design**.** Herald of Daghestan State Technical University. Technical Sciences. 2026;53(2):142-152. (In Russ) DOI:10.21822/2073-6185-2026-53-2-142-152

Введение. Методология и процесс проведения испытаний демонстрируется на примере автоматизированной системы в защищенном исполнении (далее – АСЗИ), имеющей 3-ий уровень защищенности персональных данных [1], класс защищенности К3 [2] и 3-ю категорию значимости объекта критической информационной инфраструктуры (далее – ОКИИ) [3], программно-технические средства (далее – ПТС) которой используют операционные системы Linux.

Аттестационная комиссия осуществляет оценку соответствия реализованных на объекте информатизации (далее – ОИ) технических решений по защите информации, а также оценивает их достаточность для защиты от актуальных угроз, связанных с данным ОИ. Перед проведением аттестации АСЗИ ОКИИ необходимо провести всестороннюю оценку системы на способность противодействовать различным угрозам информационной безопасности: оценку текущего состояния защиты информации и соответствие её нормированному значению [4]; оценку степени защищённости от компьютерных атак [5]; оценку актуальных для АСЗИ ОКИИ угроз безопасности информации [6].

Аттестация АСЗИ ОКИИ завершается проведением испытаний на соответствии системы требованиям Федеральной службы по техническому и экспортному контролю (далее – ФСТЭК) России по защите информации [7]. По итогам испытаний составляется Протокол аттестационных испытаний АСЗИ. В Протоколе должны указываться название проверки, дата утверждения программы и методики испытаний ОИ, запланированные сроки и место проведения, а также стандарты выполнения требований по информационной безопасности. В Протоколе излагаются критерии и исходная информация, необходимые для проведения испытаний, инструменты, используемые для оценки эффективности мер защиты от несанкционированного проникновения, а также объяснение того, как будет проводиться процедура тестирования. Результаты оценки АСЗИ на соответствие требованиям по защите информации должны быть отражены не только в Протоколе, но и в Заключении по результатам аттестационных испытаний. В Заключении указываются назначение АСЗИ, его цели и перечень используемых программных средств; устанавливается уровень безопасности системы. Заключение содержит подробную информацию о специалистах, ответственных за проведение процесса сертификации, и конкретную дату утверждения методик тестирования АСЗИ ОКИИ; указывается продолжительность времени тестирования, приводятся ссылки на соответствующие руководящие документы ФСТЭК России,

регулирующие меры по обеспечению безопасности значимых объектов критической информационной инфраструктуры, государственных информационных систем и персональных данных, обрабатываемых в АСЗИ, являющихся информационными системами персональных данных [8].

Множество трудов отечественных и зарубежных исследователей посвящено требованиям к порядку и организации оценки соответствия АСЗИ требованиям по информационной безопасности, а также проведению работ по аттестации АСЗИ. Среди них известны работы А.Е. Вантеевой [9], И.Р. Зулькарнеева [10], В.А. Кривенцева [11], Д.В. Гавриленко [12], С.А. Макеева [13], А.П. Голушко [14], Н.В. Медведева [15], Е.В. Бурьковой [16], А.В. Барабанова [17,18], С.И. Алешникова [19], А.С. Голдобиной [20], А.А. Стариковой [21], В.В. Селифанова [22].

Постановка задачи. По достоинству оценивая высокую значимость трудов перечисленных авторов и отмечая наличие разработанных подходов, определяющих требования к порядку и организации оценки соответствия системы требованиям по защите информации и проведению работ по аттестации АСЗИ, следует отметить, что до настоящего времени отсутствуют системные методологические исследования, посвященные методам проведения аттестационных испытаний АСЗИ и формированию Протокола, отражающего их результаты. Целью аттестационных испытаний является подтверждение соответствия системы требованиям нормативных документов по защите информации. В связи с этим, основной задачей является применение программно-аппаратных средств, которые позволяют получить достоверные данные о возможности системы противостоять попыткам несанкционированного доступа.

Методы исследования. Для оценки соответствия принятых на объекте информатизации технических мер по защите информации от несанкционированного доступа (воздействия на информацию) требованиям по защите информации и их достаточности для защиты от актуальных для объекта информатизации угроз безопасности информации, необходимо использовать следующие критерии: успешно – все необходимые условия соблюдены и все предъявляемые требования выполняются; не успешно – хотя бы одно из необходимых условий не соблюдено или хотя бы одно из предъявляемых требований не выполняется.

При оценке ОИ необходимо провести следующие испытания: испытания системы защиты информации путем осуществления тестирования ее функций безопасности (функциональное тестирование); анализ уязвимостей с использованием средств контроля эффективности защиты информации от несанкционированного доступа; испытания системы защиты информации путем осуществления попыток несанкционированного доступа (воздействия) в обход системы защиты информации с использованием средств тестирования. На момент проведения испытаний должны быть предоставлены и соблюдаться условия и исходные данные: ОИ должен функционировать в штатном режиме; аттестационной комиссии должна быть представлена документация на ОИ; аттестационной комиссии должен быть предоставлен доступ к программно-техническим средствам ОИ и доступ к консолям управления средств защиты информации (далее – СрЗИ) ОИ. Состав программных, программно-технических средств и СрЗИ ОИ должен соответствовать указанному в документе «Технический паспорт ОИ». В процессе аттестационных испытаний используются следующие программные средства контроля, сертифицированные ФСТЭК России [23], указанные в табл. 1.

При проведении испытаний дополнительно применяются утилиты gostsum из состава сертифицированной операционной системы специального назначения Astra Linux Special Edition и integrity_checker из состава сертифицированного программного изделия Kaspersky Endpoint Security. В процессе сертификационных испытаний и протоколирования результатов аттестационных испытаний АСЗИ проверяется выполнение требований по информационной безопасности.

Таблица 1. Перечень возможных программных средств контроля, используемых в процессе аттестационных испытаний
Table 1. List of possible software controls used in the certification testing process

№	Наименование Name	Заводской номер Factory Number	Сведения о сертификате соответствия ФСТЭК России, сроке технической поддержки, специальный защитный знак (идентификатор) Information about the FSTEC of Russia certificate of conformity, technical support period, special security mark (identifier)
1.	Программный комплекс «Средство анализа защищенности «Сканер - ВС»	———	Для каждого программного средства контроля указывается номер сертификата соответствия ФСТЭК России, срок его действия, срок действия технической поддержки производителя и специальный защитный знак (идентификатор)
2.	Программа поиска и гарантированного уничтожения информации на дисках TERRIER версии 3.0	———	
3.	Программа фиксации и контроля целостности информации ФИКС-UNIX 1.0	———	
4.	Средство анализа защищенности «RedCheck Professional»	———	

Любое отклонение от этих требований влечет за собой выдачу отрицательных Протокола и Заключения по результатам проведения аттестационных испытаний АСЗИ, так как проведение аттестационных испытаний не подразумевает количественного или частичного их выполнения (испытания можно либо пройти, когда выполнены все требования, либо нет). В таком случае необходимо инициировать повторное прохождение аттестационных испытаний, после устранения выявленных на объекте информатизации недостатков. Перечень работ по аттестации АСЗИ включает:

1. Проведение оценки соответствия: технического паспорта объекта информатизации; акта классификации информационной (автоматизированной) системы; акта категорирования значимых объектов критической информационной инфраструктуры Российской Федерации; состава и содержания эксплуатационной документации на систему защиты информации объекта информатизации и документов по защите информации владельца объекта информатизации требованиям по защите информации и Порядку организации и проведения работ по аттестации объектов информатизации.
2. Проверка выполнения требований нормативно-правовых актов Правительства Российской Федерации, ФСТЭК России по категорированию объектов критической информационной инфраструктуры.
3. Проведение обследования объекта информатизации на предмет оценки соответствия объекта информатизации и условий его эксплуатации требованиям по защите информации, а также документам, представленным заказчиком.
4. Проверка наличия документов, содержащих результаты анализа уязвимостей, проведенного на этапах предварительных или приемочных испытаний системы защиты информации объекта информатизации.
5. Проверка наличия сведений о средствах защиты информации, установленных на объекте информатизации, в реестре сертифицированных средств защиты информации, ведение которого осуществляет ФСТЭК России в соответствии с Положением о системе сертификации средств защиты информации, утвержденным приказом ФСТЭК России от 3 апреля 2018 г. № 55 (в случае наличия требования об обязательном применении сертифицированных средств защиты информации), или документов, подтверждающих проведение оценки соответствия средств защиты информации требованиям по безопасности информации в формах, отличных от сертификации.
6. Проверка наличия у владельца объекта информатизации работников, ответственных за обеспечение защиты информации в ходе эксплуатации объекта информатизации,

в том числе за проведение оценки угроз безопасности информации, управление (администрирование) системой защиты информации (администраторов безопасности), управление конфигурацией объекта информатизации, реагирование на инциденты, информирование и обучение персонала, контроль за обеспечением уровня защиты информации, а также проверку достаточности установленных для них обязанностей в соответствии с требованиями по защите информации.

7. Проведение оценки уровня знаний и умений работников владельца объекта информатизации, ответственных за обеспечение защиты информации, в соответствии с установленными для них обязанностями в эксплуатационной документации и документах по защите информации владельца объекта информатизации.
8. Проведение оценки соответствия принятых на объекте информатизации организационных мер требованиям по защите информации и их достаточности для защиты от актуальных для объекта информатизации угроз безопасности информации.
9. Оформление протокола аттестационных испытаний АСЗИ.
10. Оформление заключение по результатам аттестационных испытаний АСЗИ.

Методы и результаты проведения аттестационных испытаний на автоматизированных рабочих местах (АРМ) и серверах АСЗИ представлены в табл. 2.

Таблица 2. Методы и результаты проведения аттестационных испытаний на АРМ и серверах АСЗИ

Table 2. Methods and results of certification tests on automated workstations and servers of an automated system in a secure design

№	Метод испытания Test method	Результат испытаний Test result
Наименование испытания: оценка соответствия принятых на объекте информатизации технических мер по защите информации от несанкционированного доступа (воздействия на информацию) требованиям по защите информации и их достаточности для защиты от актуальных для объекта информатизации угроз безопасности информации		
1.	В ходе испытания выборочно на ПТС АСЗИ осуществить попытку доступа к защищаемому информационному ресурсу под учетной записью тестового пользователя, не имеющего прав доступа к ресурсу. Проверить наличие записи в журналах СрЗИ от НСД о попытке доступа к информационному ресурсу.	Попытка доступа к защищаемому информационному ресурсу (папка другого пользователя) под учетной записью тестового пользователя должна быть неудачна и зарегистрирована в СрЗИ от НСД. Результат: *не успешно/успешно*
2.	В ходе испытания выборочно на ПТС АСЗИ осуществить вход в ОС под учетной записью тестового пользователя. Проверить наличие записи в журналах СрЗИ от НСД информации о дате и времени события, результате попытки, логине и хеше пароля.	При входе под учетной записью тестового пользователя на выбранных ПТС АСЗИ в СрЗИ от НСД должна осуществляться регистрация даты и времени события, результат попытки, логин и хеш пароля. Результат: *не успешно/успешно*
3.	В ходе испытания выборочно на ПТС АСЗИ под тестовой учетной записью осуществить запуск и завершение программ, предназначенных для обработки защищаемых файлов. Проверить наличие записи в журналах СрЗИ от НСД о дате и времени запуска, имени (идентификаторе) программы, идентификаторе субъекта доступа, запросившего программу, результате запуска.	При запуске (завершении) на выбранных ПТС АСЗИ программ под тестовой учетной записью, предназначенных для обработки защищаемых файлов, в СрЗИ от НСД должна проводиться регистрация запуска (завершения). Регистрационные записи должны содержать следующие параметры: дату и время запуска; имя (идентификатор) программы (процесса, задания; идентификатор субъекта доступа, запросившего программу (процесс, задание); результат запуска (успешный, неуспешный). Результат: *не успешно/успешно*
4.	В ходе испытания выборочно на ПТС АСЗИ проверить соответствие контрольных сумм файлов СрЗИ значениям, приведенным в формулярах. При проведении испытаний применяются ФИКС-UNIX 1.0, утилиты gostsum в составе операционной системы Astra Linux SE и integrity_checker из состава Kaspersky Endpoint Security.	Контрольные суммы СрЗИ на выбранных ПТС АСЗИ должны соответствовать указанным в формуляре (результаты снятия контрольных сумм ПТС АСЗИ под управлением операционной системы Linux должны указываться в Приложении к Протоколу). Результат: *не успешно/успешно*
5.	В ходе испытания выборочно на ПТС АСЗИ проверить количество неуспешных попыток входа и время блокировки на установленный промежуток времени.	На ПТС АСЗИ после 5 неуспешных попыток ввода заведомо неправильного пароля учётная запись пользователя должна блокироваться. Блокировка должна сохраняться не менее 30 минут, по истечению которых должно становиться доступно окно входа в операционную систему. Результат: *не успешно/успешно*
6.	В ходе испытания выборочно на ПТС АСЗИ проверить настройки характеристик пароля от учетной записи. На ОИ должны обеспечиваться следующие характеристики пароля: наличие строчных и прописных букв, цифр или спецсимволов; длина пароля не менее n-числа символов для пользователей и не менее n-числа символов для привилегированных учетных записей; в пароле присутствует не менее n символов, отличного от общего регистра символов пароля; максимальное время действия	На выбранных ПТС АСЗИ должна быть произведена попытка смены пароля тестового пользователя на пароль, не удовлетворяющий указанным требованиям. В ходе проверке должно быть установлено, что на выбранных ПТС АСЗИ: нельзя установить пароль, который не содержит строчные или прописные буквы, цифры или спецсимволы; нельзя установить пароль, который содержит менее n-числа символов для пользователей и не менее n-числа символов

№	Метод испытания Test method	Результат испытаний Test result
	пароля; минимальное время действия пароля; запрещено использование n-числа последних использованных паролей при создании новых паролей. Характеристики 1-2 проверить путем попыток изменения пароля на выбранных ПТС на несоответствующий указанным требованиям. Характеристики 3-6 проверить в консоли управления СрЗИ от НСД или сертифицированной ОС.	для привилегированных учетных записей; в СрЗИ от НСД для всех ПТС установлено максимальное время действия пароля, минимальное время действия пароля, запрещено использование n-числа последних использованных паролей при создании новых паролей. Результат: *не успешно/успешно*
7.	В ходе испытания выборочно на ПТС АСЗИ проверить контроль физических портов, путем подключения к выбранным ПТС АСЗИ по USB различных устройств, неучтенных на ОИ (Флеш накопитель, USB-модем). При подключении к физическим портам в СрЗИ от НСД должны регистрироваться: дата и время, логическое имя (номер), идентификатор субъекта доступа.	При подключении к выбранным ПТС АСЗИ по USB неучтенных устройств (Флеш накопитель, USB-модем) должна происходить их блокировка, при этом в СрЗИ от НСД должны быть зарегистрированы события, содержащие следующие параметры: дата и время подключения; логическое имя (номер); идентификатор субъекта доступа. Результат: *не успешно/успешно*
8.	В ходе испытания выборочно на ПТС АСЗИ проверить наличие антивируса и актуальность баз. Для ПТС на базе Kaspersky Endpoint Security для Linux: под учетной записью администратора в консоли ввести команду «kesl-control --app-info», после выполнения команды в консоль выводится информация об антивирусе Kaspersky Endpoint Security для Linux (Название, версия, политика, информация о лицензии, дата последнего выпуска баз приложения, запущенные задачи); ввести команду «systemctl status kesl», убедиться, что антивирус запущен.	На ПТС на базе Kaspersky Endpoint Security для Linux: должна быть выведена информация о наличии антивирусного ПО Kaspersky Endpoint Security для Linux, базы должны быть актуальны; должна быть выведена информация, подтверждающая, что антивирус запущен. Результат: *не успешно/успешно*
9.	На ПТС ОИ пользователю должна быть доступна функция «Гарантированного удаления» файлов. Под учетной записью администратора проверить включение вкладки «Затирание данных», количество циклов затирания не менее трех. Качество затирания файлов проверяется с использованием программы поиска и гарантированного уничтожения информации на дисках TERRIER версии 3.0.	На ПТС ОИ вкладка «Затирание данных» должна быть включена, должно быть установлено 3 цикла затирания. Результат: *не успешно/успешно*
10.	В ходе испытания выборочно на ПТС АСЗИ осуществить попытку внедрения тестовой вредоносной программы с помощью USB Флеш-накопителя (на время проведения испытания функция блокировки интерфейсов ввода (вывода) на АРМ в СрЗИ от НСД должна быть отключена). Для испытания на USB Флеш-накопитель необходимо заранее записать специальный тестовый командный файл, который не содержит фрагментов вирусного кода. После чего USB Флеш-накопитель должен быть подключен к выбранным ПТС АСЗИ.	После подключения USB Флеш-накопителя, содержащего тестовый командный файл, к выбранным ПТС АСЗИ, программа должна быть обнаружена и заблокирована антивирусной программой. Результат: *не успешно/успешно*
11.	В ходе испытания на ОИ провести выявление и анализ уязвимостей с помощью сертифицированного средства анализа защищенности «RedCheck».	В АСЗИ должен быть организован процесс анализа и устранения уязвимостей. По результатам сканирования должны быть предоставлены отчеты об уязвимостях (должны указываться в Приложении к Протоколу). Для уязвимостей, которые невозможно устранить и/или использовать в АСЗИ актуальными нарушителями ввиду применения компенсирующих мер, Заказчиком должны быть оформлены Протоколы «О невозможности эксплуатации уязвимостей». Результат: *не успешно/успешно*
12.	В ходе проведения проверки выборочно на ПТС АСЗИ создать тестовый пользователь «Test», создать папку для резервного копирования и начать тестирование. При тестировании проверить соответствие реальных прав доступа тестового пользователя «Test», с правами, указанными в матрице доступа (ролевой модели правил разграничения доступа) АСЗИ «Технического паспорта.».	В ходе проверки попытки доступа к ПО, чтения, записи, копирования, удаления файлов, не соответствующих правам тестового пользователя, должны сопровождаться отказом в выполнении. Тестирование должно подтвердить соответствие прав доступа тестового пользователя, указанным в матрице доступа (ролевой модели правил разграничения доступа) АСЗИ «Технического паспорта …». Результат: *не успешно/успешно*
13.	Выборочно на ПТС АСЗИ проверить, что ПО, в том числе СрЗИ, установленное на ПТС ОИ, соответствует указанному в «Техническом паспорте». В ходе испытания на ПТС АСЗИ проверить наличие СрЗИ от НСД. Под учетной записью авторизованного пользователя в консоли ввести команду-запрос статуса СрЗИ от НСД, после выполнения команды в консоль вывести информацию о СрЗИ от НСД.	На ПТС АСЗИ должно отсутствовать ПО, в том числе СрЗИ, которое не должно быть указано в «Техническом паспорте». Должна быть выведена информация о наличии СрЗИ от НСД. Результат: *не успешно/успешно*

Обсуждение результатов. В табл. 2 показаны проверки АРМ и серверов, которые комплексно охватывают ключевые аспекты безопасности: контроль доступа к ресурсам (проверка прав, неудачные попытки входа с блокировкой учётной записи), регистрацию событий в СрЗИ от НСД, проверку сложности паролей и политики их смены, контроль целостности ПО через сверку контрольных сумм, блокировку и аудит подключения внешних USB-устройств, наличие и актуальность антивирусных баз, функцию гарантированного удаления файлов, тестирование антивирусной защиты от внедрения вредоносного ПО, анализ уязвимостей с использованием сертифицированного средства анализа

защищенности, а также проверку соответствия установленного ПО (включая СрЗИ) технической документации. Их содержание является достаточным и универсальным для оценки защищённости конечных узлов системы, так как позволяет проверить выполнение требований по идентификации и аутентификации, аудиту, контролю целостности, антивирусной защите, управлению съёмными носителями и реагированию на инциденты. Методы и результаты проведения аттестационных испытаний для систем защиты виртуализации Linux представлены в табл. 3.

Таблица 3. Методы и результаты проведения аттестационных испытаний для систем защиты виртуализации Linux

Table 3. Methods and results of certification tests for Linux virtualization protection systems

№	Метод испытания Test method	Результат испытаний Test result
Наименование испытания: оценка соответствия принятых на объекте информатизации технических мер по защите информации от несанкционированного доступа (воздействия на информацию) требованиям по защите информации и их достаточности для защиты от актуальных для объекта информатизации угроз безопасности информации		
1.	*Проверки для виртуальной инфраструктуры, реализованной на основе сертифицированной ФСТЭК России операционной системы специального назначения «Astra Linux Special Edition»*	
1.1.	В ходе проверки под учетной записью пользователя виртуальной машины (далее – ВМ) предпринять попытку подключения по протоколу SSH/RDP к виртуальной машине, к которой для данного пользователя доступ разрешен, с верным логином и паролем.	В результате проверки пользователем ВМ должен быть получен доступ к виртуальной машине, при этом консоль управления виртуальными машинами пользователю ВМ должна быть недоступна – нет прав на изменение настроек, удаление, перемещение, останова и запуска виртуальной машины. Результат: *не успешно/успешно*
1.2.	В ходе проверки под учетной записью пользователя ВМ предпринять попытку подключения по протоколу SSH/RDP к виртуальной машине, к которой для данного пользователя доступ разрешен, с неверным логином и паролем.	В результате проверки пользователю ВМ должно быть отказано в доступе к виртуальной машине. Результат: *не успешно/успешно*
1.3.	В ходе проверки под учетной записью пользователя ВМ осуществить доступ по протоколу SSH/RDP к виртуальной машине, к которой для данного пользователя доступ запрещен.	В результате проверки пользователю ВМ должно быть отказано в доступе к виртуальной машине. Результат: *не успешно/успешно*
1.4.	В ходе проверки под учетной записью АВИ предпринять попытку подключения к консоли управления виртуальными машинами с верным логином и паролем.	В результате проверки администратором ВИ должен быть получен доступ к консоли управления виртуальными машинами. Результат: *не успешно/успешно*
1.5.	В ходе проверки под учетной записью АВИ предпринять попытку подключения к консоли управления виртуальными машинами с неверным логином и паролем.	В результате проверки администратору ВИ должно быть отказано в доступе к консоли управления виртуальными машинами. Результат: *не успешно/успешно*
1.6.	В ходе проверки под учетной записью АВИ предпринять попытку запуска виртуальной машины, к которой для данного администратора ВИ доступ разрешен, с верным логином и паролем.	В результате проверки администратор ВИ должен получить доступ к данной виртуальной машине. Результат: *не успешно/успешно*
1.7.	В ходе проверки под учетной записью АВИ предпринять попытку запуска виртуальной машины, к которой для данного администратора ВИ доступ разрешен, с неверным логином и паролем.	В результате проверки администратору ВИ должно быть отказано в доступе к данной виртуальной машине. Результат: *не успешно/успешно*
1.8.	В ходе проверки под учетной записью АВИ предпринять попытку запуска виртуальной машины, к которой для данного администратора ВИ доступ запрещен.	В результате проверки администратору ВИ должно быть отказано в доступе к данной виртуальной машине. Результат: *не успешно/успешно*
2.	*Проверки для виртуальной инфраструктуры, реализованной на основе сертифицированного ФСТЭК России программного комплекса «Средства виртуализации «Брест» (далее – ПК СВ «Брест»)*	
2.1.	В ходе проверки под учетной записью АВИ предпринять попытку подключения к произвольному виртуальному серверу в обход консоли управления ПК СВ «Брест»	Не должно получиться подключиться к виртуальному серверу. Результат: *не успешно/успешно*
2.2.	В ходе проверки под учетной записью АВИ при включенной консоли управления ПК СВ «Брест» предпринять попытку подключения к произвольному виртуальному серверу с неверным логином или паролем	Не должно получиться подключиться к виртуальному серверу. Результат: *не успешно/успешно*
2.3.	В ходе проверки под учетной записью АВИ при включенной консоли управления ПК СВ «Брест» предпринять попытку подключения к произвольному виртуальному серверу с верным логином и паролем	Подключение к виртуальному серверу должно произойти успешно. Результат: *не успешно/успешно*
2.4.	В ходе проверки под учетной записью АВИ предпринять попытку подключения к произвольному виртуальному серверу в обход консоли управления ПК СВ «Брест» через веб-интерфейс	Не должно получиться подключиться к виртуальному серверу. Результат: *не успешно/успешно*
2.5.	В ходе проверки под учетной записью АВИ при включенной консоли управления ПК СВ «Брест» предпринять попытку подключения к произвольному виртуальному серверу через веб-интерфейс с неверным логином или паролем	Не должно получиться подключиться к виртуальному серверу. Результат: *не успешно/успешно*
2.6.	В ходе проверки под учетной записью АВИ при включенной консоли управления ПК СВ «Брест» предпринять попытку подключения к произвольному виртуальному серверу через веб-интерфейс с верным логином или паролем	Подключение к виртуальному серверу должно произойти успешно. Результат: *не успешно/успешно*

В табл. 3 продемонстрированы практические проверки систем защиты виртуализации, которые фокусируются на проверке функций идентификации, аутентификации

и разграничения доступа: инфраструктура на Astra Linux тестируется на возможность подключения пользователей виртуальных машин (ВМ) и администраторов виртуальной инфраструктуры (АВИ) к ВМ и консоли управления с верными/неверными учётными данными, а также запрет доступа к неразрешённым ресурсам; для ПК СВ «Брест» испытания направлены на выявление возможности обхода консоли управления (в том числе через веб-интерфейс) и проверку аутентификации при подключении к виртуальным серверам. Успешное прохождение проверок свидетельствует о корректной настройке прав доступа к виртуальной инфраструктуре. Методы и результаты проверки используемого в АСЗИ телекоммуникационного оборудования представлены в табл. 4.

Таблица 4. Методы и результаты проверки используемого в АСЗИ телекоммуникационного оборудования

Table 4. Methods and results of verification of telecommunication equipment used in the automated system in a secure design

№	Метод испытания Test method	Результат испытаний Test result
Наименование испытания: оценка соответствия принятых на объекте информатизации технических мер по защите информации от несанкционированного доступа (воздействия на информацию) требованиям по защите информации и их достаточности для защиты от актуальных для объекта информатизации угроз безопасности информации		
1.	В ходе испытания выборочно предпринять попытку подключения к сетевому оборудованию и межсетевому экрану с неверным логином или паролем.	В результате проверки пользователю должно быть отказано в доступе к консолям управления. В журналах логов должна появиться запись о попытке доступа к устройству. Результат: *не успешно/успешно*
2.	В ходе испытания выборочно предпринять попытку подключения к сетевому оборудованию и межсетевому экрану с верным логином и паролем.	В результате проверки пользователю должен быть разрешен доступ к консолям управления. В журналах логов должна появиться запись о успешной попытке доступа к устройству. Результат: *не успешно/успешно*
3.	В ходе испытания проверить корректность присвоения учетных записей администраторам, которые имеют доступ к консолям сетевого оборудования и межсетевого экрана	Каждый администратор должен иметь свою уникальную учетную запись, логин и пароль. Результат: *не успешно/успешно*
4.	В ходе испытания проверить настройки характеристик пароля от учетной записи администратора. На ОИ должны обеспечиваться следующие характеристики пароля: наличие строчных и прописных букв, цифр или спецсимволов; длина пароля не менее n-числа символов для пользователей и не менее n-числа символов для привилегированных учетных записей; в пароле присутствует не менее n символов, отличного от общего регистра символов пароля; максимальное время действия пароля; минимальное время действия пароля; запрещено использование n-числа последних использованных паролей при создании новых паролей.	Администраторы должны подтвердить соответствие паролей от своих учетных записей актуальным требованиям по защите информации. Результат: *не успешно/успешно*
5.	В ходе испытания выборочно под учетной записью администратора осуществить запуск консолей сетевого оборудования и межсетевого экрана. Проверить наличие записи в журналах логов о дате и времени запуска, идентификаторе субъекта доступа, запустившего консоль, результате запуска.	При запуске консолей сетевого оборудования и межсетевого экрана под учетной записью администратора, в журналах логов должна проводиться регистрация запусков. Регистрационные записи должны содержать следующие параметры: дату и время запуска; идентификатор субъекта доступа, запустившего консоль; результат запуска (успешный, неуспешный). Результат: *не успешно/успешно.*

Для используемого телекоммуникационного оборудования в табл. 4 подробно описаны: проверка попыток входа с неверными и верными учётными данными, корректность присвоения уникальных учётных записей администраторам, соответствие характеристик паролей установленным требованиям безопасности, а также регистрация событий доступа в журналах. Для каждого метода указан ожидаемый результат (успешная/неуспешная проверка и наличие соответствующих записей в логах). Всё это позволяет сделать вывод о соответствии или несоответствии оборудования требованиям информационной безопасности, в контексте выполнения мер защиты информации от несанкционированного доступа.

Вывод. Таким образом, проведение аттестационных испытаний, подтвержденное положительными Протоколом испытаний АСЗИ и Заключением по результатам аттестационных испытаний, созданным на основе Протокола, по представленному в работе методу протоколирования аттестационных испытаний АСЗИ на соответствие требования по безопасности информации, свидетельствует о том, что автоматизированная система устойчива к внешним воздействиям на информацию, циркулирующую в ней, и соответствует требованиям по защите информации, установленным нормативными документами ФСТЭК

России. Протокол и Заключение заверяются специалистами аттестационного органа, которые осуществляли аттестационные испытания данной системы, и утверждаются руководителем этого органа. После этого, Органом по аттестации, который проводил работы по сертификации системы, принимается решение о выдаче Аттестата соответствия на данный ОИ. В дальнейшем, Владельцу ОИ следует помнить о том, что, в соответствии с требованиями приказа ФСТЭК России от 29.04.2021 № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну», ему необходимо инициировать проведение ежегодного контроля уровня защиты информации в АСЗИ (при этом не реже одного раза в 2 года с привлечением Лицензиата ФСТЭК России) с оформлением протоколов и отражением в «Техническом паспорте…» на АСЗИ. Протоколы контроля защиты информации АСЗИ не реже одного раза в 2 года представляются Владельцем ОИ в ФСТЭК России (территориальный орган ФСТЭК России). Научная новизна результатов заключается в том, что в работе впервые разработана и применена на практике методика протоколирования аттестационных испытаний АСЗИ. Предлагаемый метод, изложенный в исследовании, значительно упрощает аттестацию АСЗИ, показывая реальный уровень информационной безопасности рассматриваемого объекта информатизации, сильно сокращая время разработки документации и снижая затраты на проведение процедуры аттестации.

Библиографический список:

1. Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных". URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102160483&ysclid=mhnu9xiea0530228819
2. Приказ ФСТЭК России от 11.02.2013 № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17?ysclid=mhnu4wo9w1625032675
3. Приказ ФСТЭК России от 25.12.2017 № 239 "Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры". URL: http://publication.pravo.gov.ru/document/0001201803270041
4. Методический документ ФСТЭК России от 02.05.2024 "Методика оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации". URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-2-maya-2024-g?ysclid=mhnu6o2ogd555215018;
5. Методический документ Национального координационного центра по компьютерным инцидентам "Методические рекомендации по проведению мероприятий по оценке степени защищенности от компьютерных атак"// Официальный сайт Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. <https://gossopka.ru/upload/iblock/a63/hwj5wwz7is5zm42pyzl587s52jubuer7/Metodicheskie-rekomendatsii-po-otsenke-stepeni-zashchishchennosti.pdf
6. Методический документ ФСТЭК России от 05.02.2021 "Методика оценки угроз безопасности информации" Официальный сайт Федеральной службы по техническому и экспортному контролю. URL:https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g?ysclid=mhnu5weg1u594814950
7. Приказ ФСТЭК России от 29.04.2021 № 77 "Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну". Официальный интернет-портал правовой информации. URL: <http://publication.pravo.gov.ru/document/0001202108100027
8. Приказ ФСТЭК России от 18.02.2013 № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных". Официальный сайт Федеральной службы по техническому и экспортному контролю. URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21?ysclid=mhnu4gjs7g182687367
9. Вантеева А.Е., Омельченко Т.А., Никишова А.В. Исследование возможности повышения эффективности процесса аттестации объекта информатизации // НБИ технологии. - 2022. - Т.16.

- № 1. - С. 5-9. - DOI: 10.15688/NBIT.jvolsu.2022.1.1;
10. Зулькарнеев И.Р., Козлов А.Е., Семакин А.Е. Автоматизация процесса аттестации по требованиям безопасности информации // Безопасность информационного пространства. - 2018. - № 43-1(172). - С. 171-174.;
11. Кривенцев В.А., Селифанов В.В., Звягинцева П.А. Проведение аттестационных испытаний автоматизированной системы в защищенном исполнении // Интерэкспо Гео-Сибирь. - 2019.;
12. Гавриленко Д.В. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации / Д. В. Гавриленко. — Текст : непосредственный // Молодой ученый. - 2013. - № 5 (52). - С. 143-148.;
13. Макеев С.А. Содержание программы и методик проведения аттестационных испытаний информационных систем на соответствие требованиям безопасности информации // Правовая информатика. - 2015. - № 3.;
14. Голушко А.П. Отсутствие форм организационно-распорядительных документов как проблема аттестации объектов информатизации на соответствие требованиям безопасности информации // Актуальные проблемы авиации и космонавтики. - 2017. - № 13.;
15. Медведев Н.В., Квасов П.М., Цирлов В.Л. Стандарты и политика информационной безопасности автоматизированных систем // Вестник МГТУ им. Н.Э. Баумана. Серия «Приборостроение». - 2010. - № 1. - С. 103-111;
16. Бурькова Е.В. Задача оценки защищенности информационных систем персональных данных // Вестник ЧГУ. - 2016. - № 1. - С. 112-118;
17. Барабанов А.В., Марков А.С., Цирлов В.Л. Методический аппарат оценки соответствия автоматизированных систем требованиям безопасности информации // Спецтехника и связь. - 2011. - № 3. - С. 48-52;
18. Барабанов А.В. Методика оценки соответствия автоматизированных систем требованиям по защите информации от несанкционированного доступа с применением выборочного контроля // Вестник МГТУ им. Н.Э. Баумана. Серия «Приборостроение». - 2011. - № SPEC. - С. 104-115;
19. Алешников С.И., Дёмин С.А., Фёдоров С.Б., Фёдоров А.С. Проблемы информационной безопасности организации (предприятия) и пути их решения // Вестник Балтийского федерального университета им. И. Канта. Серия: Физико-математические и технические науки. - 2013. - № 10. - С. 147-154;
20. Голдобина А.С., Селифанов В.В. Оценка эффективности средств защиты государственных информационных систем // Интерэкспо Гео-Сибирь. - 2019. - Т.6. - № 1. - С. 115-121;
21. Старикова А.А., Макарова Д.Г. Оценка эффективности управления системой защиты информации в государственных информационных системах // Интерэкспо Гео-Сибирь. - 2017.;
22. Селифанов В.В., Гордеев А.С., Карманов И.Н. Требования по защите информации при межсетевом взаимодействии государственных информационных систем с иными информационными системами // Интерэкспо Гео-Сибирь. - 2018. - № 7. - С. 277-282;
23. Приказ ФСТЭК России от 03.04.2018 № 55 «Об утверждении Положения о системе сертификации средств защиты информации». Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/document/0001201805140022.

References:

1. Decree of the Government of the Russian Federation dated November 01, 2012 No. 1119 "On Approval systems" http://pravo.gov.ru/proxy/ips/?docbody=&nd=102160483&ysclid=mhnu9xiea0530228819 (In Russ)
2. Order of the FSTEC of Russia dated February 11, 2013 No. 17 "On Approval of Requirements for the Protection of Information not constituting a State Secret contained in State Information systems": https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17?ysclid=mhnu4wo9w1625032675 (In Russ)
3. Order of the FSTEC of Russia dated December 25, 2017 No. 239 "On approval of requirements for ensuring the security of significant objects of critical information infrastructure". http://publication.pravo.gov.ru/document/0001201803270041 (In Russ)
4. Methodological document of the FSTEC of Russia dated May 02, 2024 "Methodology for assessing the indicator of the state of technical information protection and ensuring the security of significant objects of the critical information infrastructure of the Russian Federation". https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-2-maya-2024-g?ysclid=mhnu6o2ogd555215018 (In Russ)
5. Methodological document of the National Coordination Center for Computer Incidents "Methodological recommendations for measures to assess the degree of protection against computer attacks" https://gossopka.ru/upload/iblock/a63/hwj5wwz7is5zm42pyzl587s52jubuer7/Metodicheskie-rekomendatsii-po-otsenke-stepeni-zashchishchennosti.pdf (In Russ)
6. Methodological document of the FSTEC of Russia dated February 05, 2021 "Methodology for assessing

information security threats". https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g?ysclid=mhnu5weg1u594814950 (In Russ)
7. Order of the FSTEC of Russia dated April 29, 2021 No. 77 "On Approval of the Procedure for Organizing and Conducting Work on Certification of Informatization Facilities for Compliance with the Requirements for the Protection of Restricted Access Information that is not a State Secret". http://publication.pravo.gov.ru/document/0001202108100027 (In Russ)
8. Order of the FSTEC of Russia dated February 18, 2013 No.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". https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21?ysclid=mhnu4gjs7g182687367 (In Russ)
9. Vanteeva A. E., Omelchenko T. A., Nikishova A.V. Investigation of the possibility of increasing the effectiveness of the certification process of an object of informatization. *NBI tehnologii.* 2022;16(1):5-9. DOI: 10.15688/NBIT.jvolsu.2022.1.1 (In Russ)
10. Zulkarneev I. R., Kozlov A. E., Semakin A. E. Automation of the certification process for information security requirements. *Bezopasnost informacionnogo prostranstva*. 2018;43-1(172):171-174. (In Russ)
11. Kriventsev V.A., Selifanov V.V., Zvyagintseva P.A. Conducting certification tests of an automated system in a secure design. *Interekspo Geo_Sibir*. - 2019. DOI: 10.33764/2618-981X-2019-9-30-34 (In Russ)
12. Gavrilenko D.V. Organizational structure of the system of certification of informatization facilities according to information security requirements. Text:direct. *Molodoi uchenii*. 2013;5(52):143-148 (In Russ)
13. Makeev S.A. The content of the program and methods of certification testing of information systems for compliance with information security requirements. *Pravovaya informatika*. 2015;3:19-23. (In Russ)
14. Golushko A.P. The lack of forms of organizational and administrative documents as a problem of certification of informatization facilities for compliance with information security requirements. *Aktualnie problemi aviacii i kosmonavtiki*. 2017; 2(13):200-202. (In Russ)
15. Medvedev N.V., Kvasov P.M., Cirlov V.L. Standards and information security policy of automated systems. *Vestnik MGTU im. N.E. Baumana. Seriya «Priborostroenie»*. 2010;1:103-111. (In Russ)
16. Burkova E.V. The task of assessing the security of personal data information systems. Vestnik ChGU. – 2016;1:112-118. (In Russ)
17. Barabanov A.V., Markov A.S., Cirlov V.L. Methodological apparatus for assessing the compliance of automated systems with information security requirements. *Spetstekhnika i svyaz*. 2011;3:48-52. (In Russ)
18. Barabanov A.V. Methodology for assessing the compliance of automated systems with the requirements for protecting information from unauthorized access using selective control. *Vestnik MGTU im. N.E. Baumana. Seriya «Priborostroenie»*. 2011; no. SPEC:104-115. (In Russ)
19. Aleshnikov S.I., Demin S.A., Fedorov S.B., Fedorov A.S. Problems of information security of an organization (enterprise) and ways to solve them. *Vestnik Baltiiskogo federalnogo universiteta im. I. Kanta. Seriya: Fiziko-matematicheskie i tekhnicheskie nauki*. 2013;10:147-154. (In Russ)
20. Goldobina A.S., Selifanov V.V. Evaluation of the effectiveness of protection tools for state information systems. *Interekspo Geo_Sibir*. 2019; 6(1):115-121. (In Russ)
21. Starikova A.A., Makarova D.G. Evaluation of the effectiveness of information security system management in state information systems. *Interekspo Geo_Sibir*. 2017. (In Russ)
22. Selifanov V.V., Gordeev A.S., Karmanov I.N. Information security requirements for inter-network interaction of state information systems with other information systems. *Interekspo Geo_Sibir*. 2018;7: 277-282. (In Russ)
23. Order of the FSTEC of Russia dated April 03, 2018 No. 55 "On approval of the Regulations on the Certification system of information security tools".Oficialnii internet_portal pravovoi informacii, available at: http://publication.pravo.gov.ru/document/0001201805140022 (In Russ)

Сведения об авторе:

Трофимович Александр Дмитриевич, аспирант, кафедра комплексной безопасности критически важных объектов, swdi95@yandex.ru

Information about the author:

Alexander D. Trofimovich, Postgraduate Student**,** Department of Integrated Security of Critical Facilities, swdi95@yandex.ru

Конфликт интересов/Conflict of interest.

Автор заявляет об отсутствии конфликта интересов/The author declare no conflict of interest.

Поступила в редакцию/Received 07.02.2026**.**

Одобрена после рецензирования/Reviced 29.03.2026.

Принята в печать/Accepted for publication 20.05.2026.