УДК 004.415.535
DOI: 10.33764/2618-981X-2019-9-30-34

ПРОВЕДЕНИЕ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Владимир Алексеевич Кривенцев
Управление Федеральной службы по техническому и экспортному контролю по Сибирскому федеральному округу, 630091, Россия, г. Новосибирск, Красный пр., 41, старший государственный инспектор, e-mail: kriventsev@list.ru

Валентин Валерьевич Селифанов
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, Плахотного, 10, доцент кафедры информационной безопасности, тел. (383)343-91-11, e-mail: sfo1@mail.ru

Полина Александровна Звягинцева
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, старший преподаватель кафедры информационной безопасности, тел. (383)343-91-11, e-mail: p.a.zvjaginceva@sgugit.ru

Дается краткое описание состояния рынка отечественных операционных систем, которые могут проходить аттестацию в составе автоматизированной системы. Приводится описание того, что включают в себя аттестационные испытания объекта информатизации, программа аттестационных испытаний, методики аттестационных испытаний и протокол аттестационных испытаний.

Ключевые слова: аттестационные испытания, автоматизированная система.

BENCHMARK TESTING OF A SECURE EXECUTION AUTOMATED SYSTEM

Vladimir A. Kriventsev
Department of the Federal Service for Technical and Export Control of the Siberian Federal District, 41, Krasny Prospect St., Novosibirsk, 630091, Russia, Senior State Inspector, e-mail: kriventsev@list.ru

Valentin V. Selifanov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Associate Professor, Department of Information Security, phone: (383)343-91-11, e-mail: sfo1@mail.ru

Polina A. Zviagintcheva
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Senior Lecturer, Department of Information Security, phone: (383)343-91-11, e-mail: p.a.zvjaginceva@sgugit.ru

A brief description of the state of the market of domestic OS, which can be certified as part of the AU are given. In addition, the description of what includes certification tests of the object of Informatization, the program of certification tests, methods of certification tests and the Protocol of certification tests is made.

Key words: attestation tests, automated system.

На данный период времени в России осуществляется постепенный переход систем на продукцию отечественного производителя, в том числе в сфере информационной безопасности. Как правило, для таких систем характерно использование внутренних механизмов защиты и, соответственно, осуществляется переход на сертификацию ОС, как вида СЗИ [1].

В качестве объекта исследования берется система защиты автоматизированной системы, а как предмет исследования рассматривается система защиты автоматизированной системы от несанкционированного доступа.

В таком случае, единственным документом доступным для построения систем высокого уровня (средства защиты информации третьего класса и выше) является профиль защиты [2].

ИТ.САВЗ.Г2.ПЗ и ИТ.ОС.А2.ПЗ – документы, в которых изложены требования к безопасности конкретных средств и информационных систем.

ГОСТ РО 0043-003-2012 – «Аттестация объектов информатизации. Общие положения» [3].

ГОСТ РО 0043-004-2013 – «Аттестация объектов информатизации. Программа и методики аттестационных испытаний» [4].

Существующие средства защиты информации, а именно DallasLock, SecretNet, Страж и подобные им, сертифицированы и могут проходить в дальнейшем сертификацию по документу «Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации», аттестационные испытания проводятся по документу «Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации». Данные документы между собой коррелируются [5, 6].

Для прохождения аттестации средства защиты информации должны быть сертифицированы. Таким образом, получается, что средства защиты информации имеют сертификацию по классу защищенности, а не по классу защиты, как это требуют приказы ФСТЭК. В соответствии с этим существуют только профили защиты, которые удовлетворяют данным требованиям.

Одна из проблем заключается в том, что необходимо подобрать такую операционную систему, которая удовлетворяла бы всем требованиям, выдвигаемым к системам такого класса [7].

В ходе исследования данной темы был произведен сравнительный анализ операционных систем российской разработки, а именно:

- «Astra Linux Special Edition»;
- РОСА DX «КОБАЛЬТ» 1.0;
- МСВСфера 6.3 АРМ;
- «Циркон 36К»;
- Альт Линукс СПТ 6.0.

Стоит отметить, что все представленные операционные системы способны осуществлять управление доступом к различным изделиям, входящим в состав современных автоматизированных систем.

Сравнительный анализотечественных операционных систем приведен в таблице.

	AstraLinux Special Edition	РОСА DX «КОБАЛЬТ» 1.0	МСВ Сфера 6.3 АРМ	Циркон 36К	Альт Линукс СПТ 6.0
Ядро ОС	Linux 4.2.0	Linux 3.0.69	CentOS 6.7	CentOS GNU/Linux 6.5	Linux 2.6.32
Базовый дистрибутив	Debian	Mandriva Linux (Red Hat Linux)	Red Hat Linux	Red Hat Enterprise Linux	Red Hat Linux
РД СВТ	2 класс тип А	5 класс	-	5 класс	4 класс
РД НДВ	2 уровень	4 уровень	4 уровень	4 уровень	3 уровень
РД АС	1Б	1Г	1Г	1Г	1В

«AstraLinux SpecialEdition» сертифицирована в системах сертификации средств защиты информации Минобороны, ФСТЭК и ФСБ России, а также включена в единый реестр российских программ Минкомсвязи России.

В настоящее время при аттестации автоматизированной системы [3] на соответствие требованиям по безопасности информации, функции, которые реализует операционная система, как средство защиты от несанкционированного доступа, должны соответствовать требованиям класса защищенности 1Б [6].

Аттестационные испытания объекта информатизации включают:

а) анализ

- структуры объекта информатизации;
- комплекса технических средств;
- программного обеспечения;
- системы защиты информации.

б) проверку наличия сертификатов соответствия на продукцию, используемую в целях защиты информации;

в) аттестационные испытания системы защиты информации объекта информатизации в реальных условиях эксплуатации;

г) оформление протоколов аттестационных испытаний. Протоколы подписывают специалисты, проводившие испытания, и утверждает орган по аттестации. Протоколы должны содержать описание проведенных измерений, испытаний, расчетов, а также их результаты и выводы о соответствии этих результатов требованиям безопасности информации;

д) оформление заключения по результатам аттестационных испытаний. Заключение подписывается членами аттестационной комиссии, утверждается органом по аттестации и доводится до заявителя.

Программа аттестационных испытаний АС содержит перечень конкретных работ, которые требуется провести для оценки и подтверждения выполнения предъявляемых требований безопасности информации.

Программа аттестационных испытаний АС включает:

- проверку структуры, состава и условий эксплуатации АС;
- проверку достаточности представленных документов и соответствия их содержания установленным требованиям;
- аттестационные испытания системы защиты информации объекта информатизации в реальных условиях эксплуатации;

− проведение испытаний АС на соответствие требованиям по защите информации от несанкционированного доступа;

− подготовку отчетной документации и оценку результатов испытаний аттестуемой АС;

− оформление материалов аттестационных испытаний.

Методики аттестационных испытаний должны содержать подробное описание и порядок выполнения практических действий, осуществляемых при оценке системы защиты информации, перечень требований, подлежащих проверке и условий, в которых проводится проверка.

Методики аттестационных испытаний АС должны включать:

− описание и порядок выполнения практических действий;

− перечень требований, подлежащих проверке и условий, в которых проводится проверка;

− критерии, по которым делаются выводы о соответствии аттестуемого объекта информатизации требованиям безопасности информации на каждом этапе проводимых работ.

Протокол аттестационных испытаний должен включать:

− вид испытаний;

− объект испытаний;

− дату и время проведения испытаний;

− место проведения испытаний;

− перечень использованной в ходе испытаний аппаратуры (наименование, тип, заводской номер, номер свидетельства о поверке и срок его действия);

− перечень нормативно-методических документов, в соответствии с которыми проводились испытания;

− результаты измерений.

Протоколы испытаний подписываются экспертами – членами аттестационной комиссии, проводившими испытания, с указанием должности, фамилии и инициалов [9].

Таким образом можно сказать, что выбор операционных систем для аттестации АС по требованиям класса 1Б очень мал и на данный момент среди операционных систем отечественной разработки существует лишь одна, которая удовлетворяет этому требованию, а именно AstraLinux Special Edition 1.5. Помимо этого, у данной системы есть ряд преимуществ, а именно она сертифицирована в системах сертификации средств защиты информации Минобороны, ФСТЭК и ФСБ России и включена в единый реестр российских программ Минкомсвязи России. Система уже введена в действие и на ней построена информационная система Национального центра управления обороной РФ [10,11].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Приказ Минкомсвязи России «Об утверждении плана импортозамещения программного обеспечения» от 1 апреля 2015 № 96.

2. ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

3. ГОСТ РО 0043-003-2012. Аттестация объектов информатизации. Общие положения.

4. ГОСТ РО 0043-004-2013. Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний.

5. Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» утвержденный решением председателя Гостехкомиссии России от 1992 г.

6. Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утвержденный решением председателя Гостехкомиссии России от 30.05.1992 г.

7. Приказ ФСТЭК России № 55 от 3 апреля 2018 г. «Положение о системе сертификации средств защиты информации».

8. Информационное Сообщение ФСТЭК России об утверждении Требований безопасности информации к операционным системам от 18 октября 2016 г. № 240/24/4893.

9. Положение по аттестации объектов информатизации по требованиям безопасности информации, утверждено председателем Гостехкомиссии России 25.11.1994 – М.: Гостехкомиссия РФ, 1994.

10. Селифанов В. В. Оценка эффективности системы защиты информации государственных информационных систем от несанкционированного доступа // Интеграция науки, общества, производства и промышленности сборник статей Международной научно-практической конференции. 2016. – С. 109-113.

11. Оценка эффективности системы защиты информации ИСПДН с учетом профиля защиты / В. В. Селифанов, П. А. Звягинцева, А. С. Голдобина, Ю. А. Исаева // Вестник СГУГиТ. – 2017. – Т. 22, № 4. – С. 220–225.