УДК 004.9+004.05
DOI: 10.53403/9785951505460_469

СЕРТИФИКАЦИЯ КАК ОСНОВНОЙ СПОСОБ ПОДТВЕРЖДЕНИЯ БЕЗОПАСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Камышева Наталья Сергеевна (NSKamysheva @vniief.ru), Шагаева София Владимировна

ФГУП «РФЯЦ-ВНИИЭФ», г. Саров Нижегородской обл.

В докладе рассмотрены основные аспекты процессов сертификации изделий информационных технологий, проведен сравнительный анализ двух обязательных систем сертификации средств защиты информации – ФСТЭК России и Минобороны России, и альтернативных способов подтверждения безопасности программного обеспечения.

Ключевые слова: информация, информационная безопасность, сертификация, информационные технологии, защита информации, программное обеспечение.

CERTIFICATION AS THE KEY METHOD OF CONFIRMING THE SOFTWARE SECURITY

Kamysheva Natalia Sergeevna (NSKamysheva@vniief.ru), Shagaeva Sofia Vladimirovna

FSUE «RFNC-VNIIEF», Sarov Nizhny Novgorod region

The report considers the main aspects of the processes of certification of information technology products, a comparative analysis of two mandatory systems for certification of information security tools – the FSTEC of Russia and the Ministry of Defense of Russia, and alternative ways to confirm the safety of software are performed.

Keywords: information, information security, certification, information technology, information security, software.

Введение

В настоящее время огромную важность приобретают вопросы подтверждения безопасности программного обеспечения, поскольку в первую очередь сертификация предусмотрена для обеспечения защиты конфиденциальной информации заданного уровня. Данный процесс является одним из важнейших методов повышения степени защищенности информационной инфраструктуры, а также частью государственной политики в рамках реализации Доктрины информационной безопасности Российской Федерации.

Пристальное внимание отечественных разработчиков в последние годы привлекает вопрос повышения рейтинга на внутреннем потребительском рынке и закрепления позиций на нем за счет своевременного устранения недостатков и уязвимостей, направленного на сохранение качества программной продукции на конкурентоспособном уровне.

К числу основных задач сертификации относится оказание значительного содействия государственным регуляторам в формировании рынка защищенных информационных технологий и средств их обеспечения, а также оказание содействия потребителю, получающему возможность делать выбор в пользу безопасных и качественных программных решений.

Аспекты процессов сертификации изделий информационных технологий

Сертификация – это процесс, который связан с проведением оценки соответствия (подтверждением соответствия) изделий информационных технологий (изделий-ИТ) предъявляемым требованиям безопасности, которые зафиксированы в определенной документации. Сертификация бывает обязательной и добровольной, в зависимости от сферы применения изделия и порядка ее регулирования подведомственными государственными и негосударственными структурами.

К изделиям-ИТ, подлежащим обязательной сертификации в России, относятся [1]:

– средства противодействия иностранным техническим разведкам, а также средства контроля эффективности противодействия иностранным техническим разведкам;

– средства технической защиты информации, включая средства, в которых они реализованы, а также средства контроля эффективности технической защиты информации;

– средства обеспечения безопасности информационных технологий, включая защищенные средства обработки информации.

В области сертификации в России имеется три основных регулятора – Федеральная служба безопасности Российской Федерации (ФСБ России), Федеральная

служба по техническому и экспортному контролю Российской Федерации (ФСТЭК России) и Министерство обороны Российской Федерации (Минобороны России).

Поскольку ФСБ России регулирует процессы, связанные с подтверждением безопасности криптографических средств, – далее речь пойдет про изделия-ИТ, не содержащие встроенные криптографические функции, и сертифицируемые в системе ФСТЭК России, и Минобороны России.

Для повышения уровня беспристрастности при оценке безопасности процесс сертификации разделен на несколько уровней независимых проверок. Главными участниками процесса являются заявитель на сертификацию, испытательная лаборатория, орган по сертификации, и федеральный орган, который своим решением назначает одну, из ряда аккредитованных организаций, испытательную лабораторию и орган по сертификации, которые проводят независимую оценку изделия предъявляемым требованиям безопасности [1–2].

На каждом этапе сертификации не исключено множество вопросов и замечаний, которые заявителю потребуется устранять в процессе. Если замечания не устранены в регламентированный срок и в полном объеме испытательная лаборатория и орган оставляет за собой право выдать заявителю отрицательное заключение. В случае успешного прохождения сертификационных испытаний заявитель получает сертификат соответствия требованиям безопасности информации.

Сертификационные испытания занимают в среднем от 9 месяцев [1–2], состоят из множества сложных для заявителя этапов, при этом сертификат соответствия выдается не каждому заявителю. Кроме этого, для организаций, производящих независимую оценку на предмет соответствия требованиям изделий-ИТ, обрабатываемых защищаемую информацию, процедура осложнится тем, что в ближайшем будущем регулятором будет установлена персональная ответственность для экспертов аккредитованных испытательных лабораторий за выпускаемые протоколы испытаний и технические заключения.

Проверить прошел ли тот или иной продукт сертификацию можно на сайте ФСТЭК России в соответствующем систематически обновляемом реестре. Там публикуются требования по безопасности, которым соответствует прошедшее сертификацию изделие, сведения о схеме сертификации и участниках процесса. В свою очередь реестр продукции сертифицированной в системе Минобороны России является закрытым, и, содержащиеся в нем сведения не подлежат публикации в открытых источниках.

Для обеспечения дополнительного контроля качества при проведении аккредитованными организациями сертификации изделий-ИТ раз в несколько лет регулятор осуществляет плановый инспекционный контроль испытательных лабораторий и органов. Проверка проводится в соответствии с множественными критериями аккредитации, а результаты экспертизы фиксируются в акте.

В случае выявления регулятором несоответствий, предъявляемым к лаборатории и органу требованиям, действие разрешительного на осуществление деятельности аттестата аккредитации приостанавливается до момента устранения зафиксированных актом замечаний. В случае не устранения замечаний в установленный регулятором срок, организация полностью лишается права осуществления деятельности, и все действующие проекты по сертификации передаются в другую аккредитованную организацию для их завершения.

Рассмотрим основные этапы сертификации. К основным этапам сертификационных испытаний относится [1–2]:

– подача заявки и получение решения на сертификацию;

– контрактация с назначенными решением испытательной лабораторией и органом;

– отбор испытательного образца(ов);

– разработка методик испытаний, и согласование их в назначенном органе;

– проведение сертификационных испытаний согласно утвержденным методикам;

– прохождение экспертизы отчетных материалов испытаний в органе;

– прохождение экспертизы отчетных материалов испытаний в ФСТЭК России или в Минобороны России.

Остановимся на основах нормативно-методической базы, которой руководствуются участники процесса сертификации линии ФСТЭК России и Минобороны России.

ФСТЭК России и Минобороны России непрерывно совершенствует меры, направленные на повышение эффективности и достоверности результатов оценки соответствия изделий предъявляемым требованиям безопасности информации, разрабатывает дополнительные нормативно-методические документы, стандарты и регламенты.

Так с 2018 года выпущено новое Положение о системе сертификации средств защиты информации, утвержденное приказом ФСТЭК России от 03.04.2018 г. № 55 [1]. С момента вступления в силу положения, изготовители изделий-ИТ, заявляющиеся на сертификацию по схеме серийного производства должны иметь в наличии соответствующие лицензии ФСТЭК России, документированные и внедренные процедуры безопасной разработки программного обеспечения, а также обеспечить должную техническую поддержку изделий в процессе эксплуатации пользователями.

В свою очередь в 2020 году Минобороны России выпущено новое открытое Положение о системе сертификации средств защиты информации, предназначенных для применения в Вооруженных Силах Российской Федерации, утвержденное приказом Министра обороны РФ 29.09.2020 г. № 488 [2]. Обновленное положение выпущено с целью совершенствования системы сертификации и обеспечения изделиями, прошедшими сертификацию, защиты сведений, составляющих государственную тайну и информацию ограниченного доступа.

Существуют различные типы заявляемых на сертификацию изделий. Для типовых средств защиты информации, таких как средства антивирусной защиты, доверенной загрузки, межсетевые экраны, системы обнаружения вторжения, средства съема машинных носителей информации, операционные системы, ФСТЭК России выпущен набор специальных методических документов, называемых профилями защиты и содержащими набор требований безопасности к определенному классу объекта оценки.

Средства защиты информации, не относящиеся к типовым, проходят сертификацию на соответствие техническим условиям или задания по безопасности, описывающим требования к конкретному объекту

оценки [1]. В дынном случае набор функций безопасности объекта определяется и документируется самим разработчиком, со ссылками на профили защиты или иные нормативно-методические документы, в том числе отраслевые.

Обращаю внимание на обязательность сертификации, заявляющихся изделий, на предмет соответствия приказу ФСТЭК России № 76, устанавливающего требования к разработке, проведению испытаний, и поддержке безопасности средства, соответствующего определенному уровню доверия [3]. В дополнение к приказу ФСТЭК России совместно с ведущими специалистами Института системного программирования разработана и введена в действие методика выявления уязвимостей и не декларированных возможностей в программном обеспечении [4].

Методика предназначена для организаций, осуществляющих работы по созданию программных, программно-технических средств технической защиты информации, средств обеспечения безопасности информационных технологий, включая защищённые средства обработки информации, заявителей на сертификации, а также для испытательных лабораторий и органов по сертификации, выполняющих работы по сертификации средств на соответствие обязательным требованиям по безопасности информации [4].

Также нормативно-методической помощью российским разработчика служит национальный стандарт ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» [5]. Данный стандарт устанавливает общие требования к содержанию и порядку выполнения работ, связанных с созданием безопасного программного обеспечения и формированием среды обеспечения оперативного устранения выявленных пользователями ошибок программного обеспечения и уязвимостей программы.

Кроме этого, в ближайшее время государственными регуляторами планируются к выпуску новые национальные стандарты и нормативные документы, которые значительно повысят качество и глубину исследований программного обеспечения на предмет его безопасности, в частности:

– ГОСТ Р 70262.1-2022 «Защита информации. Идентификация и аутентификация. Уровни доверия идентификации»;

– пересмотренный ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования»;

– ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Руководство по оценке безопасности разработки программного обеспечения»;

– ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Руководство по проведению динамического анализа программного обеспечения»;

– ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Руководство по проведению статического анализа. Общие требования»;

– ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Управление безопасностью программного обеспечения при использовании заимствованных и привлекаемых компонентов»;

– ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Доверенный компилятор языков Си/Си++. Общие требования»;

– ГОСТ Р «Защита информации от несанкционированного доступа. Термины и определения»;

– обновленные профили защиты и т. д.

Широкий спектр нормативно-методической базы и сложность ее восприятия разработчиками программного обеспечения, являются предпосылками к привлечению компетентных специалистов, специализирующихся в этой области. Учитывая непрерывное ужесточение требований безопасности информации, привлечение компетентных специалистов разработчиками зачастую осуществляется на этапе разработки продукта и его подготовки к прохождению сертификационных испытаний.

Сравнительный анализ двух обязательных систем сертификации средств защиты информации – ФСТЭК России и Минобороны России

Доказательство безопасности изделий-ИТ, предназначенных для применения в Вооруженных Силах Российской Федерации, будет иметь соответствующую специфику, так и система сертификации ФСТЭК России имеет характерные черты. В настоящем разделе более глубоко рассмотрен каждый этап сертификации и проведен сравнительный анализ отличительных особенностей прохождения данных этапов по линии ФСТЭК России и Минобороны России.

1) Подача заявки и получение решения на сертификацию.

Первым шагом заявителя является подача заявки на сертификацию и сопутствующей документации в соответствующее управление ФСТЭК России или Минобороны России. Заявка оформляется по установленным типовым формам регулятора. При намерении пройти сертификацию заявитель должен подготовить конструкторскую, программную и эксплуатационную документацию на свое изделие.

К заявке, направляемой в ФСТЭК России [1], прилагаются базовые документы, такие как:

– технические условия;

– техническое задание (в случае, если планируется проведение сертификации на соответствие требованиям по безопасности информации, изложенным в техническом задании);

– задание по безопасности (в случае необходимости его разработки в соответствии с требованиями по безопасности информации);

– формуляр;

– договор с лицом, обладающим исключительными правами на средство, о предоставлении заявителю права на сертификацию, эксплуатацию или производство средства, а также на техническую поддержку средства (прилагается в случае, если заявитель не обладает исключительными правами).

При формировании заявки на сертификацию, направляемой в Минобороны России [2], заявителю требуется представить регулятору помимо базовых документов, как и в системе ФСТЭК России, дополнительные документы, такие как:

– информационная справка;

– тактико-техническое (техническое) задание на создание (модернизацию) средства защиты информации (при наличии);

– схема деления средства защиты информации на составные части (при наличии).

В информационной справке помимо основной информации, такой как сведения, о заявителе, разработчике, указываются:

– сведения о военном представительстве Министерства обороны на предприятии заявителя (при наличии):

– сведения об органе военного управления, осуществляющем функции государственного заказчика средства защиты информации (при наличии):

– сведения о довольствующем органе Министерства обороны (при наличии):

– сведения об опытно-конструкторской работе, в рамках которой разработано (модернизировано) средство защиты информации (при наличии);

– сведения о присвоении конструкторской и (или) программной документации литеры «О1», когда и кем присвоена;

– наличие предписаний на эксплуатацию и документов, подтверждающих отсутствие специальных электронных устройств перехвата информации, на средство защиты информации и его составные части;

– перечень составных частей средства защиты информации, на которые требуется оформление отдельных сертификатов соответствия.

Заявка, направляемая в Минобороны России, базово отражает аналогичные сведения, как и заявка ФСТЭК России, но при этом не предусматривает указание испытательной лаборатории.

Если регулятор сочтет предоставляемые на рассмотрение сведения неполными, неоднозначными или не советующими требованиям по безопасности информации, заявителю потребуется выдать необходимые разъяснения или дополнить направляемый вместе с заявкой комплект документов.

ФСТЭК России и Минобороны России рассматривает заявку на сертификацию и прилагаемые к ней документы в течение месяца со дня получения заявки и сопутствующей документации. После рассмотрения федеральным органом заявки, выпускается решение на сертификацию, на основании которого заявитель контрактуется с назначенной решением испытательной лабораторией и органом [1–2].

2) Контрактация с назначенными решением испытательной лабораторией и органом.

Процесс контрактации заявителя с лабораторией и органом является стандартным и в случае с системой сертификации ФСТЭК России производится на условиях, которые, как правило, обговариваются при обращении заявителя в ту или иную испытательную лабораторию. Список аккредитованных лабораторий и органов опубликован в открытых источниках. Заявитель отражает в направляемой регулятору заявке лабораторию, с которой условия сотрудничества для него наиболее приемлемы.

Система Минобороны России работает немного иначе. Реестр аккредитованных испытательных лабораторий и органов по линии Минобороны России является закрытым и при первом обращении заявителя на сертификацию регулятор оставляет за собой право определить наиболее подходящую с его точки зрения испытательную лабораторию, исходя из оцениваемого опыта работы закрытого списка аккредитованных организаций именно с тем типом изделия, которое заявляется на сертификацию.

Орган по сертификации в обоих случаях определяется по тем же признакам, а также с учетом географического расположения по отношению к другим участниками сертификации. В некоторых случаях функции органа по сертификации могут быть возложены на федеральный орган, то есть на соответствующего регулятора.

3) Отбор испытательного образца(ов).

Как только заявитель готов к началу работ, испытательная лаборатория производит отбор образца испытаний. Сертификация проводится только на образцах, конструкция, состав и технология, которых должна быть полностью идентична образцам, поставляемым потребителю [1]. Исходя из выбранной схемы сертификации, отбору образцов может быть подвергнута вся партия изделий. Количество образцов серийно производимых изделий, подлежащих отбору, определяется заявителем и испытательной лабораторией исходя из условий статистической достоверности и с учетом затрат заявителя в случае, если при проведении испытаний предусматривается разрушение (нарушение функционирования) образца(ов) средства.

Для подтверждения идентичности образцов, поставляемых потребителю, эксперты, производящие отбор, фиксируют в акте контрольные суммы изделия посредством специального программного инструментария. В случае необходимости дополнительного отбора недостающих исходных данных, проводится повторная процедура.

В случае с системой Минобороны России отбор осуществляется в присутствии уполномоченных представителей заявителя, военного представительства Министерства обороны на предприятии заявителя (при наличии) в сроки, установленные договором, заключенным заявителем с испытательной лабораторией [2].

4) Разработка методик испытаний, и согласование их в назначенном органе.

Как только объект оценки, включая необходимую для прохождения сертификации документацию, попадает в испытательную лабораторию, эксперты создают испытательный стенд и преступают к исследованию изделия, документации, предварительному тестированию изделия, необходимому для разработки методик испытаний. В методиках описывается состав и порядок испытаний заявляемого на сертификацию изделия, методы испытаний и применяемые средства [1–2].

Нельзя не отметить наличие типовых методик, которые на своем практическом опыте разрабатывают лаборатории. Но учитывая разнообразие заявляемых на сертификацию изделий и различный уровень предъявляемых к ним требований, типовые методики зачастую существенно уточняются.

По завершению описания методик материалы направляются испытательной лабораторией в орган по сертификации на экспертизу. В течение 10 рабочих дней согласно положению ФСТЭК России, орган по сертификации рассматривает методики и при отсутствии недостатков утверждает их [1–2]. Согласно положению Минобороны России, методики испытаний рассматриваются органом по сертификации в течение 30 рабочих дней [2]. В случае выявления недостатков орган по сертификации возвращает методики на доработку и в обоих случаях в течение десяти календарных дней испытательная лаборатория обязана устранить недостатки методик испытаний.

5) Проведение сертификационных испытаний согласно утвержденным методикам.

После утверждения органом методик начинаются сертификационные испытания, которые являются наиболее сложным и трудоемким этапом, поскольку анализ исходных кодов изделия на предмет отсутствия уязвимостей и недостатков это не единственная составляющая сертификационных испытаний. Базово он включает в себя проверку документации на изделие, проведение самих испытаний и проверку производства в случае сертификации по схеме серийного производства [1–2].

При этом отдельное внимание стоит уделить процессу документальной проверки, проводимой испытательной лабораторией и подходам к проведению испытаний. Также ФСТЭК России делается большой упор на проверку самих процессов разработки, производства и технической поддержки продукта, включая процессы исправления уязвимостей и недостатков, а также доставки исправлений (обновлений) пользователю [1].

В обеих системах сертификации документальная проверка проводится испытательной лабораторией в соответствии с объемом предъявляемых к объекту оценки требований. Заявитель предоставляет в испытательную лабораторию комплект документации, которая требуется для прохождения сертификационных испытаний в его частном случае. Документальная проверка считается успешно пройденной после устранения выявленных в процессе экспертизы замечаний в случае их наличия.

При проведении испытаний под контролем ФСТЭК России проводится ряд таких исследований, как функциональное тестирование, статический анализ, динамический анализ, анализ скрытых каналов, проверка организации процессов безопасной разработки, производства и технической поддержки, в зависимости от объема установленных требований безопасности [1].

В системе Минобороны России проводятся испытания соответствия реальных и декларируемых в документации функциональных возможностей изделия, испытания на соответствие требованиям защищенности от несанкционированного доступа к информации, контроль отсутствия недекларированных возможностей программного обеспечения [2].

Испытания средств защиты информации в системе Минобороны России для серийного производства осуществляются только после присвоения заказчиком конструкторской и (или) программной документации на средства защиты информации литеры не ниже «О1». В процессе испытаний испытательной лабораторией производится предварительная проверка производства, и делаются выводы о его соответствии или несоответствии [2].

Все результаты испытаний и проверок документируются в протоколах испытаний, содержащих подробные сведения в зависимости от объема испытаний [1–2].

Протоколы испытаний подписывают специалисты испытательной лаборатории, проводившие сертификационные испытания.

По завершении испытаний и проверок, предусмотренных методикой испытаний, оформляется техническое заключение о соответствии (несоответствии) средства требованиям по безопасности информации. Техническое заключение утверждает руководитель испытательной лаборатории [1–2].

Испытания изделий проводятся в сроки, установленные договором, заключенным заявителем с испытательной лабораторией. В случае несоответствия объекта оценки требованиям по безопасности информации соответствующее техническое заключение направляется заявителю [1–2].

Заявитель по линии ФСТЭК России должен устранить выявленные несоответствия и проинформировать об этом испытательную лабораторию в соответствии с договором на проведение сертификационных испытаний [1]. Заявитель по линии Минобороны России должен устранить выявленные несоответствия и проинформировать испытательную лабораторию в соответствии с регламентированным положением сроком, составляющим 60 рабочих дней с момента получения уведомления [2].

Повторные сертификационные испытания проводятся в соответствии с договором на проведение сертификационных испытаний в объеме, необходимом для проверки устранения выявленных при проведении сертификационных испытаний несоответствий. По результатам повторных сертификационных испытаний оформляются протоколы повторных испытаний и техническое заключение [1–2].

6) Прохождение экспертизы отчетных материалов испытаний в органе.

Материалы сертификационных испытаний представляются испытательной лабораторией в орган по сертификации для прохождения экспертизы. Орган по сертификации проводит оценку поступивших материалов на соответствие требованиям положений по сертификации и установленным решением требованиям по безопасности информации. В том числе проверяется отсутствие в средстве уязвимостей или недекларированных возможностей, соответствие средства требованиям по безопасности информации, отсутствие информации об угрозах безопасности, связанных с его применением [4].

Срок проведения оценки материалов сертификационных испытаний в системе ФСТЭК России устанавливается договором между заявителем и органом по сертификации, но не должен превышать 45 календарных дней с момента поступления в орган по сертификации всех документов [1]. Минобороны России проводит оценку материалов испытаний в течение 25 рабочих дней с даты их поступления в орган по сертификации [2].

По результатам оценки материалов сертификационных испытаний орган по сертификации оформляет экспертное заключение о возможности (невозможности) выдачи сертификата соответствия. Экспертное заключение утверждает руководитель органа по сертификации [1–2].

В случае если органом по сертификации сделаны выводы об отсутствии полноты проведенных испытаний в соответствии с программой и методиками испытаний, орган по сертификации подготавливает заключение органа по сертификации о недостатках и направляет материалы испытаний в испытательную лабораторию для их устранения. Испытательная лаборатория устраняет недостатки, в том числе требующие проведения повторных испытаний, в течение 20 рабочих дней со дня поступления в испытательную лабораторию заключения о недостатках согласно положению Минобороны России и направляет в орган по сертификации доработанные материалы [2]. Согласно требованиям ФСТЭК России, сроки устранения замечаний регламентированы договором [1].

7) Прохождение экспертизы отчетных материалов испытаний в ФСТЭК России или в Минобороны России.

При положительном экспертном заключении от органа по сертификации, ФСТЭК России до 45 календарных дней рассматривает результаты сертификационных испытаний и экспертное заключение [1]. При отсутствии недостатков регулятор принимает решение о выдаче сертификата соответствия. При выявлении в материалах испытаний недостатков регулятор возвращает материалы в орган по сертификации на доработку с приложением описания выявленных недостатков.

Орган по сертификации, испытательная лаборатория и заявитель в срок, установленный ФСТЭК России, составляющий не более 90 календарных дней со дня подписания уведомления, обязаны устранить выявленные недостатки, при необходимости повторно пройти сертификационные испытания средства и представить регулятору доработанные материалы испытаний. При принятии решения о выдаче сертификата соответствия, сертификат соответствия подписывает руководитель со стороны ФСТЭК России, а сведения о выданном сертификате соответствия вносятся в открытый государственный реестр.

В случае с системой сертификации Минобороны России помимо положительного заключения орган по сертификации готовит проект сертификата соответствия, который подписывается руководителем Минобороны России в течение 5 рабочих дней со дня поступления положительного заключения и проекта сертификата соответствия [2].

Таким образом, были рассмотрены особенности прохождения этапов сертификации под контролем ФСТЭК России и Минобороны России.

Способы подтверждения безопасности программного обеспечения

В качестве альтернативного способа подтверждения безопасности изделий-ИТ помимо прохождения сертификации изготовителями производится независимый аудит безопасности с привлечением компетентных организаций имеющих право на осуществление данной деятельности, в том числе испытательных лабораторий. Основное отличие аудита от сертификации состоит в том, что аудит не имеет цели подтвердить соответствие требованиям безопасности в виде документа государственного образца – сертификата соответствия.

Различают аудиты безопасности организаций, информационных систем, программного кода, систем менеджмента. Аудит безопасности может быть внутренним или внешним, проводиться на соответствие любым требованиям, состав работ может носить как технический, так и организационно-нормативный характер. В некоторых случаях аудит направлен на проведение различных форм статического и динамического тестирования подсистем и сегментов, анализ документации, а также на интервьюирование для оценки уровня осведомленности специалистов в вопросах обеспечения информационной безопасности. В других случаях в рамках аудита безопасности может проводиться комплексный анализ защищенности, анализ уязвимостей, тестирование на проникновение.

Ключевым результатом проведения аудита безопасности является получение заказчиком полного описания состояния защищенности обрабатываемой информации, а также рекомендаций по устранению существующих изъянов, выявленных в процессах защиты информации. Решение российских разработчиков о проведении независимого аудита безопасности изделий-ИТ принимается как минимум с целью оценки реального уровня защиты, выявления слабых мест в процессах защиты информации и получения рекомендации, направленных на повышение уровня информационной безопасности.

Аудит безопасности является актуальным направлением повышения уровня защищенности изделий-ИТ, направленным на исключение угроз безопасности. Стоит отметить, что аудит безопасности является неотъемлемой частью современных и подтвердивших свою эффективность систем менеджмента качества, систем управления информационной безопасностью, а также аттестованных средств, обеспечивающих защиту обрабатываемой информации.

Заключение

Стоит отметить, что несертифицированные средства защиты информации в российских государственных информационных системах, информационных системах персональных данных, а также на объектах критической информационной инфраструктуры использовать или запрещено, или не рекомендуется. Аттестаты соответствия на государственные информационные системы выдаются органом по сертификации, только если требования безопасности реализуются за счет сертифицированных средств защиты. Что касается информационных систем персональных данных, к ним требования по аттестации предъявляются не в каждом случае, но требования по безопасности информации в сравнении с защитой государственных информационных систем, практически идентичны. Похожая ситуация наблюдается с объектами критической информационной инфраструктуры, включая автоматизированные системы управления технологическим процессом. На данных объекта должны использоваться только отечественные продукты и сертифицированные средства защиты информации.

В текущих реалиях нестабильной геополитической ситуации государством задан курс на уход от «бумажной» безопасности в сторону реальной. При прохождении сертификации заявителями обеспечивается соответствие изделий-ИТ требованиям безопасности информации, а также устранение уязвимостей, и недостатков программного обеспечения, что гарантированно подтверждает его безопасность.

Список литературы

1. Положение о сертификации средств защиты информации, утвержденное приказом ФСТЭК России от 03.04.2018 г. №55.

2. Положение о системе сертификации средств защиты информации, утвержденное приказом Министра обороны Российской Федерации от 29.09.2020 г. №488.

3. Приказ ФСТЭК России от 2 июня 2020 г. N 76 «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий».

4. Методики выявления уязвимостей и не декларированных возможностей в программном обеспечении, утвержденная ФСТЭК России 25.12.2020 г.