

ИНСТРУКЦИЯ

для Заявителя на сертификацию программного обеспечения по требованиям информационной безопасности

I. ЭТАП ПОДГОТОВКИ ЗАЯВКИ НА СЕРТИФИКАЦИЮ

Действия заявителя на сертификацию:

1. Заполнить проект заявки на сертификацию ПО согласно образцу (*Приложение 1*) в соответствии с «**Инструкцией по заполнению заявки на сертификацию**» (*Приложение 2*) и оформить сопроводительное письмо согласно образцу (*Приложение 3*) в формате .doc или .pdf.

2. Подготовить комплект документов, которые должны быть приложены к заявке на сертификацию ПО (в формате .doc или .pdf).

Перечень документов, которые должны быть приложены к заявке на сертификацию ПО:

- 1) **Описание программы** (пояснения в разделе IV, шаблон в Приложении 4);
- 2) **Руководство пользователя** (инструкция по эксплуатации) и **Руководство администратора** (инструкция по установке, настройке и управлению);
(допускается объединение в одном документе);
- 3) **Техническое задание** на создание ПО;
(только для ПО, разрабатываемого по заказу конкретного государственного органа в соответствии со стандартом O'z DSt 1987:2018)
- 4) **Товарно-сопроводительная документация** на сертифицируемую партию ПО;
(только при сертификации по схеме № 2, см. «Инструкцию по заполнению заявки», шаг 10)
- 5) **Нормативные документы на продукцию;**
(только при сертификации по схеме № 3, см. «Инструкцию по заполнению заявки», шаг 10)
- 6) **Действующий сертификат соответствия на применяемое средство криптографической защиты информации (СКЗИ),** выданный уполномоченным Органом по сертификации СКЗИ во исполнение Постановления Президента Республики Узбекистан № ПП-614 от 03.04.2007г.
(только для ПО, предназначенного для передачи конфиденциальной информации, см. п.5.3).

Требования к содержанию документов, которые должны быть приложены к заявке на сертификацию ПО, приведены в разделе IV настоящей Инструкции.

3. Направить подготовленный проект Заявки и сопроводительного письма в формате Word **вместе с комплектом документов** в Орган по сертификации ИКТ на электронную почту itsoft@csec.uz.

Специалисты Органа по сертификации ИКТ проверят корректность оформления Заявки и при необходимости укажут на недостатки в оформлении, которые надо исправить.

ВНИМАНИЕ:

Предоставляемый комплект документов необходим для определения требований, на соответствие которым будет проведена сертификация, а также для расчета стоимости работ по сертификации.
При отсутствии у заявителя возможности предоставить полный комплект документов заявка на сертификацию будет отклонена!

4. Распечатать полученные от Органа по сертификации ИКТ скорректированные Заявку и сопроводительное письмо, подписать их, зарегистрировать письмо, отсканировать их и направить в Орган по сертификации ИКТ на электронную почту itsoft@csec.uz.

Специалисты Органа по сертификации ИКТ проведут в установленном порядке рассмотрение представленной официальной Заявки, выполнят расчет стоимости работ по сертификации и предоставят проект договора на выполнение работ по сертификации.

II. ЭТАП ЗАКЛЮЧЕНИЯ ДОГОВОРА НА СЕРТИФИКАЦИЮ

Действия заявителя на сертификацию:

5. Распечатать полученный от Органа по сертификации ИКТ договор на сертификацию в 2 экземплярах, подписать их, поставить печать и передать оба экземпляра в Орган по сертификации ИКТ.

Специалисты Органа по сертификации ИКТ обеспечат подписание и регистрацию договора, после чего можно будет получить один экземпляр договора и провести оплату по нему.

6. После получения от Органа по сертификации ИКТ подписанного и зарегистрированного экземпляра договора произвести в установленные сроки оплату согласно условиям договора.

ВНИМАНИЕ:

Невыполнение в установленные сроки условий договора на сертификацию в части выполнения соответствующей оплаты является основанием для расторжения договора!

III. ЭТАП ПРОВЕДЕНИЯ СЕРТИФИКАЦИОННЫХ ИСПЫТАНИЙ

Действия заявителя на сертификацию:

7. Не позднее установленных в договоре сроков предоставить в ГУП «Центр кибербезопасности»:
- установочные файлы ПО;
 - полный не компилированный исходный код ПО;
 - информацию, перечисленную в разделе IV настоящей Инструкции;
 - необходимые вспомогательные средства, указанные в договоре.

Требования к ПО, а также к аппаратному обеспечению и информации, которые должны быть представлены в испытательную лабораторию, **приведены в разделе V** настоящей Инструкции.

8. Согласовать с испытательной лабораторией все условия, необходимые для проведения испытаний конкретного представленного на сертификацию ПО (например - предоставление тестового доступа к веб-приложениям, содействие в инсталляции ПО, организация коммуникаций с разработчиками ПО и т.п.) и выполнить данные условия.

ВНИМАНИЕ:

Невыполнение в установленные сроки условий договора на сертификацию в части предоставления сертифицируемого ПО (включая его исходный код) в испытательную лабораторию ГУП «Центр кибербезопасности» является основанием для расторжения договора!

Специалисты заявителя на сертификацию могут по согласованию присутствовать при проведении сертификационных испытаний исходного кода ПО для получения уверенности в обеспечении конфиденциальности их интеллектуальной собственности.

9. При получении от испытательной лаборатории информации о необходимых коррективах в ПО или в технической документации - своевременно выполнить их и предоставить в испытательную лабораторию.

ВНИМАНИЕ:

Невыполнение требуемых коррективов в ПО является основанием для отказа в выдаче сертификата соответствия!

IV.

Требования к содержанию документов, которые должны быть приложены к заявке на сертификацию ПО

Требования к Описанию программы

4.1 Сведения о ПО

4.1.1 Наименование ПО: Необходимо указать наименование ПО (включая его версию и релиз), **полностью соответствующее** указанному в заявке на сертификацию согласно “Инструкции по оформлению заявки”.

ВНИМАНИЕ:

**Расхождения в наименовании ПО
в предоставляемых документах или в самом ПО
является основанием для отказа в сертификации!**

4.1.2 Назначение ПО: Необходимо указать область применения ПО (например – “Программный продукт предназначен для обеспечения передачи сгенерированных фискальных документов в режиме реального времени оператору фискальных данных с функцией печати чеков”).

4.1.3 Передача конфиденциальных данных: В случае, если ПО предназначено для передачи какого-либо из видов конфиденциальной информации (указанных в Постановлении Президента Республики Узбекистан № ПП-614 от 03.04.2007г.) необходимо указать конкретный вид конфиденциальной информации и способы её защиты – имеется ли в ПО собственный криптографический модуль или применяются внешнее ПО или устройство, применяемые API, СКЗИ и протоколы, формат файлов, используемые веб-адреса, получатели и источники данных.

4.1.4 Язык программирования: Необходимо указать применявшиеся при разработке ПО язык программирования и среду разработки (фреймворк). Если применялось несколько языков программирования, необходимо перечислить все языки и фреймворки, с указанием компонентов ПО, которые были написаны на каждом из применявшихся языков программирования.

4.1.5 Среда разработки: Необходимо указать применявшуюся при разработке ПО среду разработки (например – “Microsoft Visual Studio Enterprise 2022”).

4.1.6 СУБД: В случае, если в состав ПО входит база данных, необходимо указать применяемую СУБД (например – “MySQL v.8.0.32”). Если в данном ПО не требуется база данных, необходимо указать - «Не применяется».

4.1.7 ОС и требования к программной среде и аппаратному обеспечению: Необходимо указать операционные системы, с которыми совместимо ПО, (а также другие программы, которые должны быть установлены для корректной

инсталляции и функционирования ПО) и требования к аппаратному обеспечению, необходимые для функционирования ПО (например – “*Microsoft Windows 10, 11; процессор не хуже типа 16 CPUs x Intel(R) Xeon(R) CPU E5-2690 0 @ 2.90GHz; ОЗУ типа DDR3 емкостью не менее 4 GB; ПЗУ емкостью не менее 16 GB; видеокарта типа 3D Memory не менее 256 MB*”).

4.1.8 Сведения об архитектуре ПО:

Необходимо привести:

- 1) Графическую блок-схему клиент-серверной информационной системы (должна содержать названия основных частей системы (например модули «Сервер, Клиент, БД») и реализуемые связи с другими информационными системами (с указанием названия других систем).
- 2) Описания каждой из основных частей (модулей) клиент-серверной информационной системы (наименование, предназначение, с какими модулями и как взаимодействует).
- 3) Описания взаимосвязей клиент-серверной информационной системы с другими информационными системами (как реализована взаимосвязь с другими информационными системами, обмен какими данными проводится при взаимодействии систем).

4.1.9 Перечень внешних серверов, с которыми осуществляется связь при инсталляции и функционировании ПО:

В случае, если инсталляция или функционирование ПО не могут осуществляться без связи с внешними серверами, необходимо указать точный адрес сервера в сети Интернет и причину, по которой необходима данная связь (например – “*при инсталляции ПО ОС Windows осуществляет проверку подлинности сертификата ПО, направляя по протоколу HTTPS запрос в удостоверяющий Центр по адресу 192.168.123.132*”).

Если существует возможность избежать установления связи с внешними серверами, необходимо указать о такой возможности и сообщить об ограничениях, возникающих при инсталляции или функционировании ПО без внешних связей.

Если в данном ПО не предусмотрена связь с внешними серверами, необходимо указать - «Связь с внешними серверами не осуществляется».

4.1.10 Виды информации, передаваемой и принимаемой с внешних серверов:

В случае, если инсталляция или функционирование ПО не могут осуществляться без связи с внешними серверами, необходимо указать соответствующий протокол и формат передачи информации (например – “*Идентификационные данные с клиентского приложения передаются в определяемый провайдером персональных данных ЦОД по протоколу TLS 3.0 в формате, соответствующем O’z DSt 3349:2018*»).

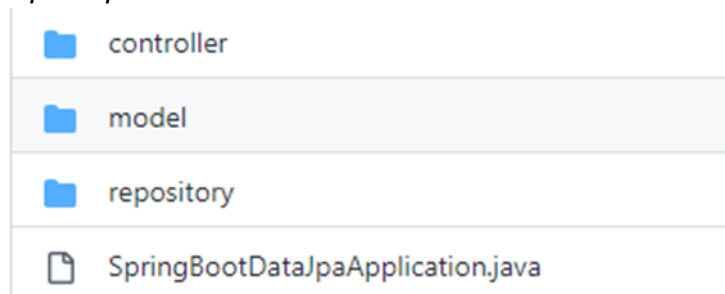
4.1.11 Хэш-значение (контрольная сумма) архивного файла (в формате zip) с не скомпилированным исходным кодом ПО или хэш-значения (контрольные суммы) каждого скомпилированного исполняемого файла ПО:

Контрольные суммы должны вычисляться по O’z DSt 1106:2009 (2-алгоритм).

4.2 Описание исходного кода

4.2.1 Структура исходного кода: Необходимо перечислить все компоненты ПО (можно в виде скриншотов директории с папками и файлами компонентов).

Пример:



4.2.2 Описание компонентов: Необходимо описать предназначение и функции каждого из указанных в п. 4.2.1 компонентов.

Пример:

Компонент "Controller" обеспечивает «связь» между пользователем и системой с использованием REST API.

Контролирует и направляет обмен данными между пользователем и системой.

Данный компонент состоит из 1 файла:



4.2.3 Описание файлов по каждому компоненту: Необходимо привести описание каждого из указанных в п. 4.2.2 файлов по следующему шаблону.

Название компонента	согласно п.4.2.1	
Название файла	Количество строк кода	Описание
согласно п.4.2.2	точное значение в цифрах	Пример - Состоит из функции работы с CRUD операции (чтение, запись, обновление, удаление) в таблицу БД Tutorials

4.2.4 Описание функций сетевого взаимодействия: Необходимо привести описание каждой функции, обеспечивающей выполнение указанных при выполнении п. 4.1.9-4.1.10 внешних связей, по следующему шаблону.

Название функции	Путь	Протокол	Структура принимаемых данных	Структура передаваемых данных	Описание
public Sender()	/src/sender/sender.java 23 -32 строка	HTTP	Address: String, Message: string	Message: string, File: Binary	Предназначена для отправки сообщения и файлов по почте SMTP

ВНИМАНИЕ:

Не указанные в Описании программы функции сетевого взаимодействия классифицируются как недокументированные возможности ПО, что является основанием для отказа в сертификации!

V.

ТРЕБОВАНИЯ К ПО, АППАРАТНОМУ ОБЕСПЕЧЕНИЮ И ИНФОРМАЦИИ, КОТОРЫЕ ДОЛЖНЫ БЫТЬ ПРЕДСТАВЛЕНЫ В ИСПЫТАТЕЛЬНУЮ ЛАБОРАТОРИЮ



1.1. Требования к предоставляемому на сертификационные испытания ПО

В испытательную лабораторию должны быть предоставлены:

- 1) - Некомпилированный полный исходный код всего ПО,
включая все его системы (подсистемы, отдельные части, компоненты, модули)
- для ПО, разработанного на интерпретируемых языках программирования;

Совместно с исходным кодом должны быть предоставлены хэш-значение архивного файла (контрольная сумма) с некомпилированным исходным кодом, вычисленная по O'z DSt 1106:2009 (2-алгоритм).

- 2) - Компилированный полный исходный код ПО (инсталлятор)
- для ПО, разработанного на компилируемых языках программирования;

Совместно с исполняемыми файлами должны быть предоставлены их хэш-значения (контрольные суммы), вычисленные по O'z DSt 1106:2009 (2-алгоритм).

- 3) - В случае, если в состав сертифицируемого ПО входит база данных, она также должна быть предъявлена в испытательную лабораторию.



1.2. Требования к аппаратному средству.

Действия заявителя на сертификацию:

Для проведения функционального тестирования в испытательную лабораторию необходимо на период испытаний предоставить (в установленные в договоре на сертификацию сроки) аппаратное средство, для функционирования на котором предназначено сертифицируемое ПО.

Информация для сведения:

- 1) *Примеры предоставляемого для испытаний аппаратного средства - персональный компьютер, планшет, ноутбук, контрольно-кассовая машина, мобильный телефон, ключ E-Kalit, фискальный модуль, принтер для чеков, сканер чеков, сим-карта и т.п.*
- 2) *Прием аппаратного средства в испытательную лабораторию и его возврат заявителю после проведения сертификационных испытаний документально регистрируются.*

В случае, если аппаратное средство является стационарным (например - сервер) и находится в эксплуатации, заявитель может официально обратиться в испытательную лабораторию с просьбой о проведении части сертификационных испытаний (функционального тестирования) размещенного на нём ПО путем дистанционного доступа.

ВНИМАНИЕ:

В таких случаях испытательная лаборатория не несет ответственности за возможность возникновения в период сертификационных испытаний каких-либо сбоев в функционировании предоставленного для испытаний стационарного аппаратного средства или любого размещенного на нём ПО.



5.3 Требования к криптографической защите

Информация для сведения:

- 1) В случае, если при функционировании сертифицируемого ПО осуществляется **передача конфиденциальной информации**, эта информация должна быть защищена программным или аппаратно-программным средством криптографической защиты информации (СКЗИ).
- 2) Перечень сведений, отнесенных к конфиденциальной информации, утвержден Постановлением Кабинета Министров от 7 ноября 2011 года № 296.
- 3) До подачи заявки на сертификацию ПО, применяемое при его функционировании **СКЗИ должно быть сертифицировано** согласно Постановлению Президента Республики Узбекистан № ПП-614 «О мерах по организации криптографической защиты информации в Республике Узбекистан» уполномоченным органом по сертификации.

Действия заявителя на сертификацию:

К заявке на сертификацию ПО необходимо приложить копию сертификата на СКЗИ.

ВНИМАНИЕ:

Отсутствие сертифицированного СКЗИ в ПО, предназначенном для передачи конфиденциальной информации, является основанием для отказа в сертификации!

При необходимости дополнительные пояснения
по выполнению настоящей Инструкции можно получить
в Органе по сертификации ИКТ ГУП «Центр кибербезопасности»:
г.Ташкент, Мирзо-Улугбекский район, ул. Т.Шевченко, 20
тел.: (998-71) 203-00-28 **e-mail: itsoft@csec.uz**

