



**СЕРТИФИКАЦИЯ АППАРАТНЫХ, АППАРАТНО-ПРОГРАММНЫХ
И ПРОГРАММНЫХ СРЕДСТВ, ПРИМЕНЯЕМЫХ ДЛЯ ОБЕСПЕЧЕНИЯ
КИБЕРБЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ И РЕСУРСОВ
ГОСУДАРСТВЕННЫХ ОРГАНОВ И ОРГАНИЗАЦИЙ, А ТАКЖЕ ОБЪЕКТОВ
КРИТИЧЕСКИ ВАЖНОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ**
(порядок и требования при сертификации)

ПРАВОВЫЕ ОСНОВЫ

Приказ председателя Службы государственной безопасности от 15 ноября 2024 г. №114
«Об утверждении Положения о порядке сертификации аппаратных, аппаратно-программных и программных средств, применяемых для обеспечения кибербезопасности информационных систем и ресурсов»

Постановление Президента Республики Узбекистан от 19 февраля 2024 года № ПП-75
"О дополнительных мерах по дальнейшему повышению роли законов в регулировании общественных отношений и качества нормотворческого процесса"

Закон Республики Узбекистан от 15 апреля 2022 года № ЗРУ-764
«О Кибербезопасности»

Закон Республики Узбекистан от 27 февраля 2023 года № ЗРУ–819
«О техническом регулировании»



ПРОЦЕССЫ СЕРТИФИКАЦИИ ПО ТРЕБОВАНИЯМ КИБЕРБЕЗОПАСНОСТИ



ДОКУМЕНТЫ, КОТОРЫЕ ДОЛЖНЫ БЫТЬ ПРИЛОЖЕНЫ К ЗАЯВКЕ

Руководство пользователя и администратора по установке, настройке средств обеспечения кибербезопасности, а также установочные файлы программы, информация о функциональных возможностях программного обеспечения средств обеспечения кибербезопасности

С

Образец маркировки аппаратных и аппаратно-программных средств, обеспечивающих кибербезопасность, сведения о сертификате соответствия, полученном от другого органа по сертификации в соответствии с требованиями информационной безопасности

Н

Товарно-сопроводительные документы и импортируемых аппаратно-программных программных средств кибербезопасности

А

Копия охранного документа (свидетельства, патента или приложения к ним) о регистрации соответствующего объекта, подтверждающего права на объекты интеллектуальной собственности, или копия лицензионного договора на его использование

Н

Информация о процессе производства средств обеспечения кибербезопасности при подаче заявки на сертификацию серийного производства

Г

Компилируемый исходный код программного обеспечения средств кибербезопасности, участвующих в обработке конфиденциальной информации, описание программного обеспечения и конструкторская документация для аппаратных и аппаратно-программных средств

Е



Порядок сертификации	1-схема	2-схема	3- схема	4- схема
Подача заявки на сертификацию	√	√	√	√
Принятие решения по заявке	√	√	√	√
Выбор образцов средств обеспечения кибербезопасности	√	√	√	√
Идентификация образцов средств обеспечения кибербезопасности	√	√	√	√
Разработка и утверждение программы испытания	√	√	√	√
Проведение испытания средств обеспечения кибербезопасности	√	√	√	√
Оценка производственных условий производителя средств кибербезопасности	-	-	√	-
Анализ пакета документов (документов представленных заявителем, документов собранных в процессе сертификации и нормативных документов)	√	√	√	√
Оформление сертификата соответствия	√	√	√	√
Проведение периодической оценки	-	-	√	-

- 1-схема – сертификация средств обеспечения кибербезопасности с четко указанной версией и контрольной суммой;
2-схема – сертификация партии средств обеспечения кибербезопасности;
3-схема – сертификация серийно выпускаемых средств обеспечения кибербезопасности;
4-схема – применяется для сертификации средств обеспечения кибербезопасности в конкретной версии, специально разработанной для каждого объекта.



ОТБОР И ИДЕНТИФИКАЦИЯ ОБРАЗЦОВ

Осуществляется
в течение двух рабочих дней
со дня принятия решения



Тип (модель), номер, дата
изготовления, дата создания файлов в
исходном коде программных продуктов,
наименование производителя, страна
нахождения производителя и
информация, содержащаяся в
требованиях нормативных документов,
идентификационные знаки



При несоответствии образцов
средств обеспечения
кибербезопасности нормативным
требованиям или документам,
прилагаемым к заявке, отбор
образцов органом по сертификации
не производится и отказывается в
проведении работ
по сертификации



Заявитель может повторно подать заявку
в орган по сертификации, устранив
недостатки, выявленные в процессе
идентификации



ПРОВЕДЕНИЕ РАБОТ ПО ИСПЫТАНИЯМ



Продолжительность испытательных работ устанавливается в соответствии с методами испытаний



Если выявленные несоответствия не будут устранены в установленные сроки или если несоответствия будут обнаружены повторно в выдаче сертификата соответствия будет отказано



Отобранные образцы вместе с программой испытаний будут представлены в испытательную лабораторию в течение трех дней

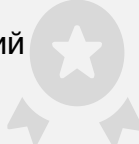


Испытательная лаборатория оформляет протоколы испытаний по результатам испытаний



Заявитель устраняет все несоответствия в установленные сроки и предоставляет органу по сертификации программное обеспечение для продолжения испытаний

Утвержденные протоколы испытаний представляются в орган по сертификации



В протоколах испытаний указывается заключение о соответствии или несоответствии средств обеспечения кибербезопасности требованиям нормативных документов.



В случае выявления несоответствий в процессе тестирования заявитель уведомляется о необходимости устранения выявленных несоответствий в срок не более одного месяца



Протоколы испытаний подписываются ответственными специалистами, проводившими испытания, и утверждаются руководителем испытательной лаборатории



Программа испытания разрабатывается и согласовывается с заявителем



Испытательные работы могут проводиться в испытательной лаборатории, на объектах производителя и на месте эксплуатации



СЕРТИФИКАЦИЯ СЕРИЙНОГО ПРОИЗВОДСТВА



Сертификат соответствия

Допускается модификация программного обеспечения в пределах одной версии



Неограниченное количество

Сертификат действителен для любого **(неограниченного)** количества программного обеспечения



Обновление

Обновление программного обеспечения не требует повторной сертификации

Общие затраты на сертификацию могут быть распределены на стоимость всех реализуемых экземпляров программного обеспечения

Среднее время смены версий программного обеспечения составляет 3 года

Оформленный сертификат соответствия действителен в течение этого периода!

ДРУГИЕ СХЕМЫ СЕРТИФИКАЦИИ

Сертификат соответствия действителен **только для 1 экземпляра или партии** программного обеспечения

При сертификации следующего комплекта программного обеспечения затраты, выделяемые на сертификацию, **не уменьшаются**

Сертификат соответствия действителен для ограниченного количества программного обеспечения **(только для 1 комплекта или партии)**

После каждого обновления программное обеспечение должно быть **повторно сертифицировано**



ОЦЕНКА УСЛОВИЙ ПРОИЗВОДСТВА СРЕДСТВ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Подготовка



При отрицательных результатах испытаний оценка производственных условий не проводится. Для оценки условий производства орган по сертификации создает комиссию из соответствующих специалистов

Анализ



Перед оценкой условий производства предоставленная информация анализируется и разрабатывается программа оценки условий производства

Срок



Срок оценки условий производства не должен превышать десяти рабочих дней. Оценка условий производства проводится в присутствии созданной комиссии и заявителя или его представителя

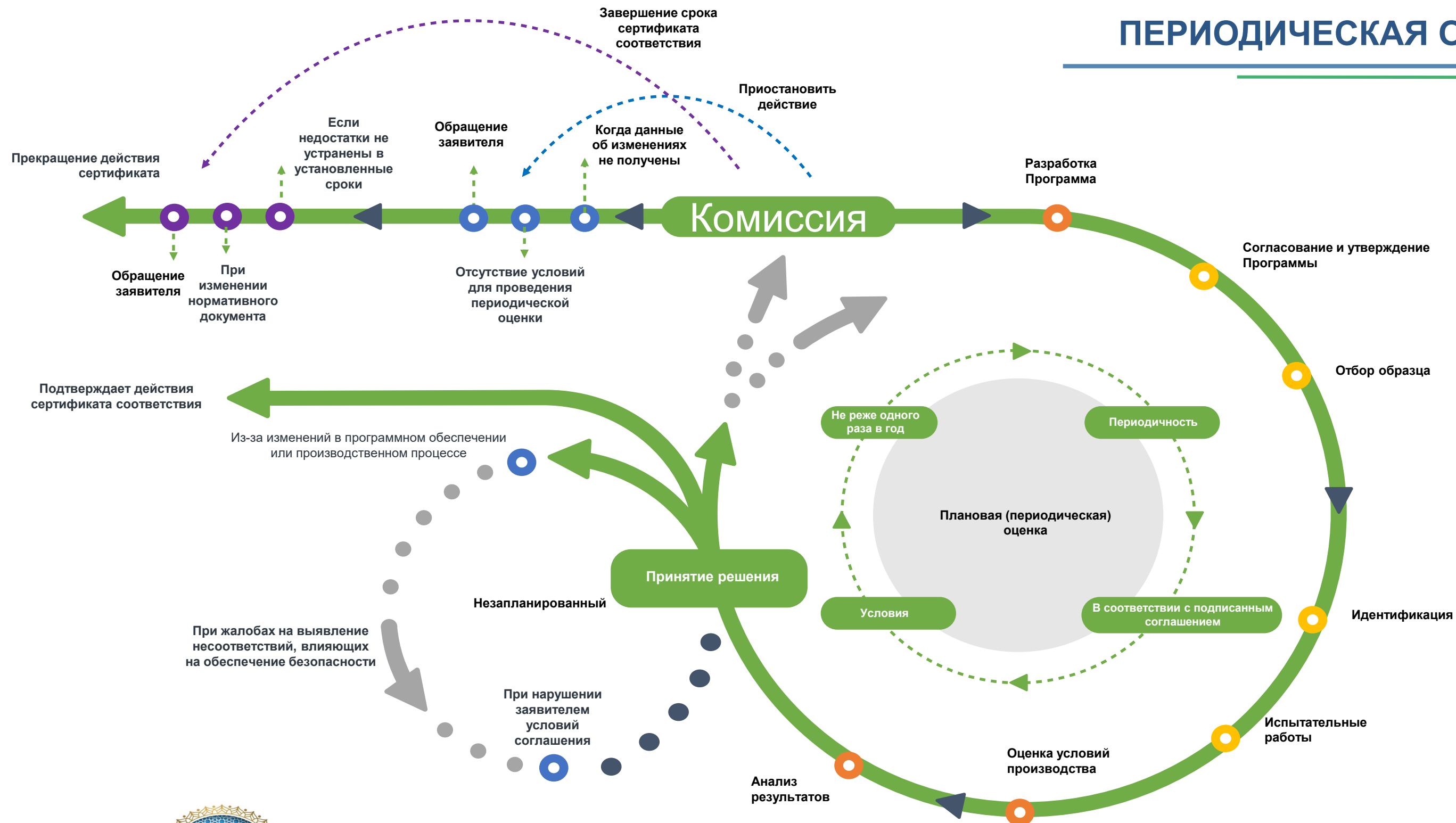
Результат



По результатам оценки составляется акт в двух экземплярах и подписывается членами комиссии и заявителем или его представителем. Один экземпляр акта передается заявителю, а второй экземпляр в орган по сертификации



ПЕРИОДИЧЕСКАЯ ОЦЕНКА



ОФОРМЛЕНИЕ, ОТКАЗ ИЛИ ПЕРЕОФОРМЛЕНИЕ СЕРТИФИКАТА СООТВЕТСТВИЯ

Сертификат соответствия выдается в течение трех рабочих дней с момента получения положительных результатов всех процессов сертификации (протокол испытаний и акт оценки производственных условий)

- Без указания даты истечения срока действия средств кибербезопасности с указанием точной версии и контрольной суммы;
- Выдается сроком на три года для серийно выпускаемых средств кибербезопасности

В случае внесения изменений в исходный код серийно выпускаемого программного обеспечения средств кибербезопасности, что приведет к изменению контрольной суммы исходного кода, заявитель должен внести изменения в версию этого программного обеспечения, а также предоставить информацию, описывающую эти внесенные изменения, в орган по сертификации в течение 3 рабочих дней

Орган по сертификации анализирует предоставленную заявителем информацию в течение 10 рабочих дней.

По результатам анализа орган по сертификации в письменной форме уведомляет заявителя о необходимости проведения ресертификации или подтверждает действительность ранее оформленного сертификата соответствия средству обеспечения кибербезопасности

В случае возможности выявления изменений, внесенных в исходный код сертифицированных средств кибербезопасности, повторная сертификация проводится в отношении измененной части программного обеспечения



СПАСИБО ЗА ВНИМАНИЕ!



Республика Узбекистан, г. Ташкент,
ул. Тараса Шевченко, 20



Телефон: (99871) 203 00 28



E-mail: itsoft@csec.uz
Veb-sayt: www.csec.uz

