**Технологии промышленной разработки**

**программного обеспечения.**

**Сертификация**

**(ТПР ПО)**

Лекция №1

**I. Тема** **Сертификация программного обеспечения**

1.1 Юридические и понятийные основы

Основным законодательным актом, устанавливающим понятия и процедуры сертификации, права и обязанности сторон, задействованных в сертификации и т.д., является Федеральный Закон «О техническом регулировании» от 27.12.2002 N 184 [1].

*Настоящий Федеральный закон регулирует отношения, возникающие при:*

*разработке, принятии, применении и исполнении обязательных требований к продукции, в том числе зданиям и сооружениям (далее - продукция), или к продукции и связанным с требованиями к продукции процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации; (в ред. Федеральных законов от 01.05.2007 N 65-ФЗ, от 21.07.2011 N 255-ФЗ)*

*применении и исполнении на добровольной основе требований к продукции, процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, а также к выполнению работ или оказанию услуг в целях добровольного подтверждения соответствия; (в ред. Федерального закона от 05.04.2016 N 104-ФЗ)*

*оценке соответствия.*

…

***безопасность продукции и связанных с ней процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации*** *(далее - безопасность) - состояние, при котором отсутствует недопустимый риск, связанный с причинением вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений;*

…

***декларирование соответствия*** *- форма подтверждения соответствия продукции требованиям технических регламентов;*

***декларация о соответствии*** *- документ, удостоверяющий соответствие выпускаемой в обращение продукции требованиям технических регламентов;*

***заявитель*** *- физическое или юридическое лицо, которое для подтверждения соответствия принимает декларацию о соответствии или обращается за получением сертификата соответствия, получает сертификат соответствия; (в ред. Федерального закона от 01.05.2007 N 65-ФЗ)*

***знак обращения на рынке*** *- обозначение, служащее для информирования приобретателей, в том числе потребителей, о соответствии выпускаемой в обращение продукции требованиям технических регламентов; (в ред. Федерального закона от 21.07.2011 N 255-ФЗ)*

***знак соответствия*** *- обозначение, служащее для информирования приобретателей, в том числе потребителей, о соответствии объекта сертификации требованиям системы добровольной сертификации; (в ред. Федеральных законов от 21.07.2011 N 255-ФЗ, от 05.04.2016 N 104-ФЗ)*

***идентификация продукции*** *- установление тождественности характеристик продукции ее существенным признакам;*

…

***орган по сертификации*** *- юридическое лицо или индивидуальный предприниматель, аккредитованные в соответствии с законодательством Российской Федерации об аккредитации в национальной системе аккредитации для выполнения работ по сертификации; (в ред. Федерального закона от 23.06.2014 N 160-ФЗ)*

***оценка соответствия*** *- прямое или косвенное определение соблюдения требований, предъявляемых к объекту;*

***подтверждение соответствия*** *- документальное удостоверение соответствия продукции или иных объектов, процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг требованиям технических регламентов, документам по стандартизации или условиям договоров; (в ред. Федеральных законов от 01.05.2007 N 65-ФЗ, от 05.04.2016 N 104-ФЗ)*

***продукция*** *- результат деятельности, представленный в материально-вещественной форме и предназначенный для дальнейшего использования в хозяйственных и иных целях;*

…

***сертификация*** *- форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, документам по стандартизации или условиям договоров; (в ред. Федеральных законов от 01.05.2007 N 65-ФЗ, от 05.04.2016 N 104-ФЗ)*

***сертификат соответствия*** *- документ, удостоверяющий соответствие объекта требованиям технических регламентов, документам по стандартизации или условиям договоров; (в ред. Федеральных законов от 01.05.2007 N 65-ФЗ, от 05.04.2016 N 104-ФЗ)*

***система сертификации*** *- совокупность правил выполнения работ по сертификации, ее участников и правил функционирования системы сертификации в целом;*

*…*

***техническое регулирование*** *- правовое регулирование отношений в области установления, применения и исполнения обязательных требований к продукции или к продукции и связанным с требованиями к продукции процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, а также в области применения на добровольной основе требований к продукции, процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг и правовое регулирование отношений в области оценки соответствия; (в ред. Федеральных законов от 01.05.2007 N 65-ФЗ, от 21.07.2011 N 255-ФЗ, от 05.04.2016 N 104-ФЗ)*

***технический регламент*** *- документ, который принят международным договором Российской Федерации, подлежащим ратификации в порядке, установленном законодательством Российской Федерации, или в соответствии с международным договором Российской Федерации, ратифицированным в порядке, установленном законодательством Российской Федерации, или указом Президента Российской Федерации, или постановлением Правительства Российской Федерации, или нормативным правовым актом федерального органа исполнительной власти по техническому регулированию и устанавливает обязательные для применения и исполнения требования к объектам технического регулирования (продукции или к продукции и связанным с требованиями к продукции процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации); (в ред. Федеральных законов от 21.07.2011 N 255-ФЗ, от 05.04.2016 N 104-ФЗ)*

Пример в приказе МЧС РФ от 08.07.2002 г. №320 «Технический регламент о требованиях пожарной безопасности».

Центральным органом по сертификации в России является Росстандарт (Федеральное **агентство** по техническому регулированию и метрологии). Портал о сертификации РОССТАНДАРТ.ИНФО <https://rosstandart.info/>

<https://rosstandart.info/certificates.html>

1.2 Виды сертификации:

Документ Технические Условий

Гигиеническая сертификация

Cвидетельство о безопасности конструкции транспортного средства

Свидетельство о государственной регистрации

Сертификация ГОСТ

обязательная

добровольная

Сертификат пожарной безопасности

Сертификат происхождения

Сертификация систем менеджмента качества (Сертификат ISO) **НА СООТВЕТСТВИЕ**[**ГОСТ Р ИСО 9001-2001**](https://docs.cntd.ru/document/1200015262)**(ИСО 9001:2000)** [2]

Отказное письмо

Протокол испытаний

Разрешение Ростехнадзора

Экологический сертификат соответствия

Экспертное заключение

1.3 Обязательная сертификация по ГОСТ Р

Типы сертификационных документов:

* Сертификат, оформляемый по нормам Технических Регламентов Таможенного Союза, каждый из которых регламентирует нормы производства, поставки, оценки качества конкретной группы изделий.
* Сертификат, который оформляется в системе ГОСТ Р. Это национальный российский разрешительный документ, получение которого происходит, если на товар еще не выпущен соответствующий Техрегламент, и если продукт попал в перечни ПП РФ№982 от 1.12.09 (регламентирует списки товаров для обязательной сертификации).
* Сертификаты, получаемые в отдельных системах оценки качества – пожарный, экологический, гигиенический и так далее.

Стадии проведения:

* Составление официального заявления на проведение обязательной сертификации продукции.
* Направление заявки в аттестованный орган параллельно с документационным комплектом (в комплект документации должны быть включены все основные данные о товаре, включая техдокументацию, а также информация о компании-заявителе, поставщиках и других участниках жизненного цикла продукта).
* Отбор по специальному алгоритму образцов изделия/вещества.
* Проведение экспертизы в лаборатории, где образцы проверяются согласно утвержденным нормами обязательной сертификации требованиям, протоколирование процесса.
* Если предусмотрено схемой оценки качества – экспертиза безопасности производства.
* Принятие сотрудниками органа решения касательно выдачи обязательного сертификата соответствия.
* Составление, регистрация и, далее, получение документа.
* Маркировка подконтрольных изделий.

1.4 Сертификация ПО [2]

Сертификация программного обеспечения – это процедура, направленная на подтверждение соответствия данного компонента нормам и стандартам, действующим на территории России, выполняемая Госстандартом по заявке заинтересованного лица и завершаемая получением сертификационного документа [2] <https://rosstandart.info/sertifikaty/programm.html>.

Программное обеспечение сертифицируется как техническое изделие, от качества которого зависит успешное функционирование компьютера. Сертификация ПО не обязательна, поскольку оно не входит в единый перечень продукции, подлежащей обязательной сертификации (Постановление Правительства РФ от 1 декабря 2009 г. N 982 "Об утверждении единого перечня продукции, подлежащей обязательной сертификации, и единого перечня продукции, подтверждение соответствия которой осуществляется в форме принятия декларации о соответствии"). Если оформление разрешительного документа по линии сертификации не входит в планы производителя либо продавца, можно получить отказное письмо. Отказное письмо необходимо для проведения таможенного контроля либо для заключения делового соглашения.

Но Сертификации подлежит программное обеспечение, используемое в: измерительных и информационных системах; контроллерах и вычислительных блоках; различных средствах измерения (как встроенных, так и автономных).

В состав документации, направляемой вместе с заявкой на сертификацию, могут, например, входить документы по ГОСТ ЕСПД 19.201-78 (Спецификация, ТЗ, Руководство пользователя, протоколы квалификационного тестирования и др.)

1.5 Государственная регистрация программ

ПРИКАЗ МИНИСТЕРСТВА ЭКОНОМИЧЕСКОГО РАЗВИТИЯ РФ ОТ 5 АПРЕЛЯ 2016 Г. № 211

ОБ УТВЕРЖДЕНИИ ПРАВИЛ ОФОРМЛЕНИЯ ЗАЯВКИ НА ГОСУДАРСТВЕННУЮ РЕГИСТРАЦИЮ ПРОГРАММЫ ДЛЯ ЭЛЕКТРОННЫХ ВЫЧИСЛИТЕЛЬНЫХ МАШИН ИЛИ БАЗЫ ДАННЫХ, ПРАВИЛ СОСТАВЛЕНИЯ ДОКУМЕНТОВ, ЯВЛЯЮЩИХСЯ ОСНОВАНИЕМ ДЛЯ ОСУЩЕСТВЛЕНИЯ ЮРИДИЧЕСКИ ЗНАЧИМЫХ ДЕЙСТВИЙ ПО ГОСУДАРСТВЕННОЙ РЕГИСТРАЦИИ ПРОГРАММЫ ДЛЯ ЭЛЕКТРОННЫХ ВЫЧИСЛИТЕЛЬНЫХ МАШИН ИЛИ БАЗЫ ДАННЫХ, И ИХ ФОРМ, ПОРЯДКА ГОСУДАРСТВЕННОЙ РЕГИСТРАЦИИ ПРОГРАММЫ ДЛЯ ЭЛЕКТРОННЫХ ВЫЧИСЛИТЕЛЬНЫХ МАШИН И БАЗЫ ДАННЫХ, ПЕРЕЧНЯ СВЕДЕНИЙ О ЗАРЕГИСТРИРОВАННОЙ ПРОГРАММЕ ДЛЯ ЭЛЕКТРОННЫХ ВЫЧИСЛИТЕЛЬНЫХ МАШИН ИЛИ БАЗЕ ДАННЫХ, ПУБЛИКУЕМЫХ В ОФИЦИАЛЬНОМ БЮЛЛЕТЕНЕ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ, ПЕРЕЧНЯ СВЕДЕНИЙ, УКАЗЫВАЕМЫХ В СВИДЕТЕЛЬСТВЕ О ГОСУДАРСТВЕННОЙ РЕГИСТРАЦИИ ПРОГРАММЫ ДЛЯ ЭЛЕКТРОННЫХ ВЫЧИСЛИТЕЛЬНЫХ МАШИН ИЛИ БАЗЫ ДАННЫХ, ФОРМЫ СВИДЕТЕЛЬСТВА О ГОСУДАРСТВЕННОЙ РЕГИСТРАЦИИ ПРОГРАММЫ ДЛЯ ЭЛЕКТРОННЫХ ВЫЧИСЛИТЕЛЬНЫХ МАШИН, ФОРМЫ СВИДЕТЕЛЬСТВА О ГОСУДАРСТВЕННОЙ РЕГИСТРАЦИИ БАЗЫ ДАННЫХ"(с изменениями на 21 декабря 2023 года)

Государственная услуга:

Государственная регистрация программы для электронных вычислительных машин или базы данных и выдача свидетельств о государственной регистрации программы для электронных вычислительных машин или базы данных, их дубликатов

Документы:

Заявление о государственной регистрации программы для ЭВМ или базы данных

Дополнение к заявлению на государственную регистрацию программы для ЭВМ или базы данных

Согласие на обработку персональных данных

Согласие на указание сведений об авторе

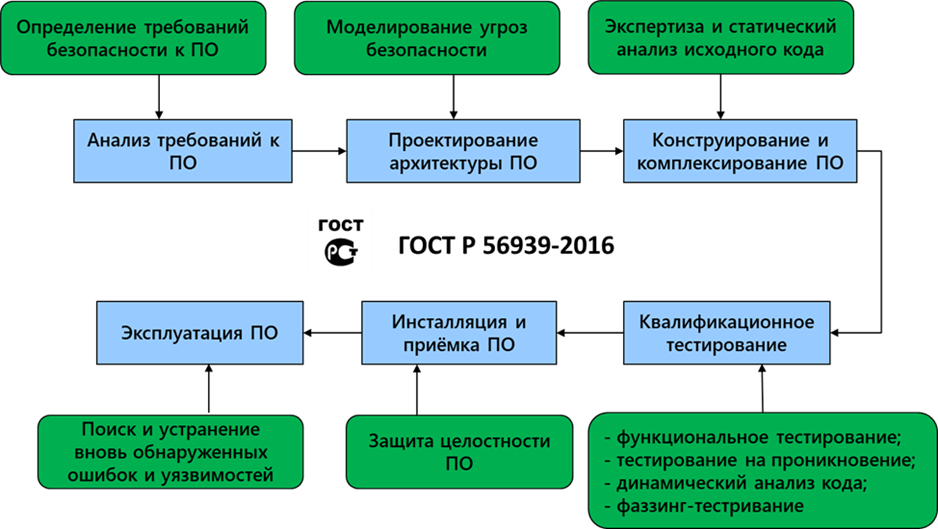
Ходатайство об исправлении очевидных и технических ошибок в заявке

Прочие

1.4 Сертификация при разработке безопасного ПО

Актуальным стандартом, описывающим требования и комплекс мер, реализуемых в процессе разработки БПО, является ГОСТ Р 56939-2016 [3], который предъявляет требования к комплексу мер по разработке безопасного ПО (БПО) и к перечню документации, которая должна быть создана перед началом, в процессе разработки и на этапе эксплуатации этого ПО. Предполагается, что появление и устранение уязвимостей программы может быть предотвращено, а устранение – достигнуто путём реализации разработчиком программного обеспечения соответствующих мер на всём протяжении процессов жизненного цикла ПО.

Меры по разработке БПО, представленные в ГОСТ Р 56939-2016, выражены в форме требования, рекомендации или допустимого действия, предназначенных для поддержки достижения результатов реализации мер. На основе этого стандарта можно сформировать эталонный жизненный цикл БПО , показанный нп рисунке, взятом из магистерской диссертации Романова В.В. (МАИниу, 2024 г.).



На этапе «Анализ требований к ПО» разработчик ПО должен определить требования по безопасности к разрабатываемому ПО.

На этапе «Проектирование архитектуры ПО» разработчик должен выполнить моделирование угроз безопасности информации. После этого необходимо провести уточнение архитектуры программы с учётом результатов моделирования угроз безопасности.

На этапе «Проектирование архитектуры ПО» разработчик должен выполнить моделирование угроз безопасности информации. После этого необходимо провести уточнение архитектуры программы с учётом результатов моделирования угроз безопасности.

На этапе «Анализ требований к ПО» разработчик ПО должен определить требования по безопасности к разрабатываемому ПО.

На этапе «Проектирование архитектуры ПО» разработчик должен выполнить моделирование угроз безопасности информации. После этого необходимо провести уточнение архитектуры программы с учётом результатов моделирования угроз безопасности.

На этапе «Конструирование и комплексирование ПО» при разработке ПО разработчик должен использовать только идентифицированные инструментальные средства. ПО реализуется на основе уточнённого проекта архитектуры ПО. В процессе разработке необходимо проводить экспертизу исходного кода, а также его статический анализ.

На этапе «Квалификационное тестирование ПО» проводятся функциональное и фаззинг тестирование, тестирование на проникновение, а также динамический анализ кода программы.

На этапе «Инсталляция и приемка ПО» необходимо обеспечить защиту ПО от угроз безопасности информации, связанных с нарушением целостности, в процессе его передачи пользователю.

На этапе эксплуатации ПО необходимо реализовать и использовать процедуры отслеживания и исправления обнаруженных ошибок и уязвимостей ПО. Помимо этого, необходимо систематически вести поиск уязвимостей разработанного ПО.

Контексты *сертификации*:

ГОСТ 28195—89 Оценка качества программных средств. Общие положения

ГОСТ 28806—90 Качество программных средств. Термины и определения

ГОСТР 50922-96 ЗАЩИТА ИНФОРМАЦИИ. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

ИСО/МЭК 15292:2001 Информационная технология. Методы и средства обеспечения безопасности. Процедуры регистрации профилей защиты

ГОСТ Р ИСО/МЭК 15408-1—2008 Информационная технология. Методы

и средства обеспечения безопасности. Критерии оценки безопасности

информационных технологий. Часть 1. Введение и общая модель

ГОСТ Р ИСО/МЭК 15408-2—2008 Информационная технология. Методы

и средства обеспечения безопасности. Критерии оценки безопасности

информационных технологий. Часть 2. Функциональные требования безопасности

ГОСТ Р ИСО/МЭК 15408-3—2008 Информационная технология. Методы

и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

ГОСТ Р 51275-2006 Защита информации. ОБЪЕКТ ИНФОРМАТИЗАЦЦ. ФАКТОРЫ, ВОЗДЕЙСТВУЮЩИЕ НА ИНФОРМАЦИЮ

**«О техническом регулировании» (от 27.12.2002 N 184, 01.05.2007 N 65-ФЗ, от 21.07.2011 N 255-ФЗ, 23.06.2014 N 160-ФЗ, от 05.04.2016 N 104-ФЗ)**

ГОСТР 56939-2016 Защита информации РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ Общие требования

ГОСТ Р 71207-2024 РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. Статический анализ программного обеспечения. Общие требования

ЛИТЕРАТУРА

1. ФЗ РФ «О техническом регулировании» 27 декабря 2002 г. N 184-ФЗ
2. Сертификация программного обеспечения | Росстандарт (rosstandart.info) <https://rosstandart.info/sertifikaty/programm.html>
3. ГОСТ Р ИСО 9001-2001 Системы менеджмента качества ТРЕБОВАНИЯ Quality management systems. Requirements
4. ГОСТ Р 56939-2016 Защита информации РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ Общие требования