

---

*П. И. Братухин, В. П. Шахин*

## ОБЕСПЕЧЕНИЕ КАЧЕСТВА ПРОДУКЦИИ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Уровень качества продукции устанавливается в нормативных документах — стандартах (требования, добровольные к соблюдению) и технических регламентах (требования, обязательные к соблюдению). Контроль соблюдения этих требований обеспечивается сертификацией соответственно как добровольной, так и обязательной.

В соответствии с Федеральным законом «О техническом регулировании» нормативными документами, на соответствие которым может проводиться добровольная сертификация, являются требования добровольных систем сертификации.

К обязательным требованиям в соответствии с названным законодательным актом относятся требования, соблюдение которых обеспечивает безопасность для жизни и здоровья людей, имущества и окружающей среды.

Все остальные требования к продукции и процессам ее производства являются добровольными для соблюдения.

В то же время покупатель (заказчик) продукции вправе установить свои условия (требования), при выполнении которых он приобретет конкретную продукцию. Именно на эти случаи рассчитаны добровольные системы сертификации. При этом добровольность понимается как желание изготовителя подтвердить выполнение установленных требований покупателя.

Содержание собственно процесса сертификации, включая сертификационные испытания, не зависит от ее обязательности или добровольности. Для изготовителя продукции ее сертификация всегда является обязательной процедурой. Разница состоит лишь в том, на каком уровне устанавливается обязательность сертификации: на уровне государства (федеральным законом или указом Президента РФ), на уровне субъекта Федерации (законом субъекта Федерации или постановлением правительства), на уровне министерства или ведомства (приказом, условиями конкурса).

Технический прогресс в области информационных технологий привел к тому, что без компьютеризации невозможен прогресс человечества в целом. Однако интенсивное развитие информационных технологий представляет собой в то же время источник угроз жизни и здоровью людей, окружающей среде, материальным и духовным ценностям общества. Особенно наглядно это проявляется в техносфере, где наиболее широко применяются современные средства информатизации (информационно-вычислительные или компьютерные системы).

Определенный уровень безопасности техносферы обеспечивается созданием и поддержанием в первую очередь стабильности и устойчивости функционирования входящих в нее вычислительных и программных средств и зависит от степени выполнения разработчиками (поставщиками) этих средств требований, установленных в нормативных документах: в технических регламентах, в стандартах, в требованиях систем добровольной сертификации.



К сожалению, на современном этапе в состав обязательных требований не включены требования по обеспечению информационной безопасности сложных систем и объектов, таких как транспортные системы, электростанции, производственные комплексы, системы управления органов государственной власти и т. п., которые определяют конечный результат функционирования названных систем, т. е. их безопасность для жизни и здоровья людей, имущества и окружающей среды.

Технология в общем смысле — совокупность методов обработки, изготовления, изменения состояния, свойств, формы сырья, материала или полуфабриката в процессе производства или наука о способах воздействия на сырье, материалы или полуфабрикаты соответствующими орудиями производства.

Информационная технология — система взаимосвязанных методов и способов сбора, накопления, хранения, поиска, обработки и выдачи информации потребителю.

Компьютерная технология — система взаимосвязанных методов и способов сбора, накопления, хранения, поиска, обработки и выдачи информации потребителю с применением вычислительных и программных средств, т. е. информационная технология, где орудиями производства служат вычислительные и программные средства.

Основным понятием в области информационных технологий является информация, представляющая собой сведения о лицах, предметах, событиях, явлениях и процессах, представленные в форме, обеспечивающей возможность их хранения и передачи.

С появлением электронных вычислительных машин появился термин «данные», под которым стали понимать информацию, представленную в цифровой форме, пригодной для обработки средствами вычислительной техники, т. е. на электронном носителе.

Данные недоступны пользователю без программ, выполняемых на вычислительных средствах. Т. е. три составляющие компьютерной (информационно-вычислительной) системы — **данные, программы и вычислительные средства** — неразделимы при рассмотрении и использовании и представляют собой **информационно-вычислительную систему**.

При этом потребность в сертификации средств информатизации (вычислительных и программных средств информационно-вычислительных систем) обусловлена такими целями, как:

- обеспечение высокого уровня качества всех компонентов ИВС;
- обеспечение безопасности функционирования ИВС;
- проведение единой технической политики при создании и использовании этих средств.

Информационная безопасность ИВС представляется интегральной характеристикой ее качества.

Следует назвать две основные группы характеристик информационной безопасности, связанной с программно-информационными продуктами:

- функциональная полнота и корректное выполнение заданных функций назначения;
- отсутствие недекларированных функций в программных и вычислительных средствах (средствах информатизации).

Если две названные группы характеристик соответствуют установленным требованиям, то возникает проблема обеспечения целостности и сохранности программно-информационных продуктов, т. е. проблема их защиты от несанкционированного доступа (НСД).

Стержневой характеристикой качества является функциональная полнота и корректное выполнение заданных функций ИВС, ибо если ИВС не решает в заданном объеме задач, то нет необходимости ее защищать от несанкционированного доступа и вообще применять по назначению.

Корректное выполнение заданных функций назначения означает:

- точное, однозначное и полное выполнение всех заданных функций;
- выполнение всех заданных видов операций с данными;
- простой и удобный интерфейс для пользователя;
- возможность обеспечения детализации прав доступа;



- взаимодействие с внешними информационными системами;
- масштабируемость;
- возможность расширения функций и взаимодействия с внешними системами.

Одновременное выполнение перечисленных требований характеризует высокий уровень качества ИВС как программно-информационного продукта.

Документы, применяемые для сертификации средств компонентов ИВС, должны содержать конкретные и однозначные характеристики, а также способы измерения характеристик, обеспечивающие идентификацию этих компонентов и возможность полно и достоверно подтвердить соответствие объекта сертификации установленным требованиям.

Состав общих требований к характеристикам ИВС и ее компонентам:

- полнота состава характеристик, обеспечивающих положительное решение задач с использованием данного средства информатизации;
- однозначное значение каждой характеристики, не допускающее ее различное толкование;
- возможность повторения результата оценки (измерения);
- документальное подтверждение требуемого значения;
- однозначная связь с содержанием эксплуатационных документов;
- конкретность способов оценки значения характеристик.

Особенность программных средств заключается в том, что они, с одной стороны, представляют собой технологию обработки данных и, с другой стороны, сами являются изделием производственно-технического назначения и, следовательно, имеют свои характеристики качества в составе функционирующей информационно-вычислительной системы.

**Состав требований к характеристикам программных средств, выполнение которых определяет безопасность применения ИВС:**

1) Требования к составу программных средств.

Программные средства (далее — ПС) должны обеспечивать решение задач в соответствии с функциональным назначением, требованиями нормативных правовых документов и требованиями системы сертификации.

2) Требования к характеристикам идентификации.

Характеристиками идентификации являются:

- состав программ и эксплуатационных документов;
- реквизиты организации-разработчика;
- сведения о версии;
- сведения о регистрации;
- описание контрольных вариантов для демонстрации корректности функционирования;
- состав нормативных правовых актов и выписки из них, относящиеся к ПС.

3) Требования к обработке данных.

Обработка данных включает:

- манипулирование данными;
- обработку текста;
- обработку календарной даты;
- импорт/экспорт данных;
- графику (при необходимости);
- мультимедиа;
- статистику.

4) Требования к информационной совместимости.

Взаимодействие компонентов ПС, используемых в одной организации, должно быть организовано либо через единую базу данных, либо через файлы обмена данными установленного состава и структуры.



При вводе данных в единую базу данных должны быть использованы единые словари и классификаторы, состав и содержание которых должны быть приведены в эксплуатационных документах.

Формы входных и выходных документов и состав данных, размещаемых в них, должны соответствовать требованиям нормативных правовых документов.

Состав и форматы данных для организации обмена информацией с внешними организациями должны соответствовать:

- требованиям нормативных правовых документов;
- протоколам обмена, согласованным взаимодействующими организациями.

5) Требования к целостности и сохранности программ и данных.

Обеспечение целостности и сохранности программ и данных (с учетом возможностей системных программных средств) включает:

- разграничение доступа пользователей к программам и данным;
- обеспечение целостности программ и данных;
- копирование и восстановление программ и данных.

6) Требования к интерфейсу пользователя.

Характеристиками интерфейса пользователя являются:

- язык взаимодействия пользователя с ПС;
- экранные окна;
- оперативная помощь пользователю;
- средства управления выводом;
- унификация элементов интерфейса пользователя.

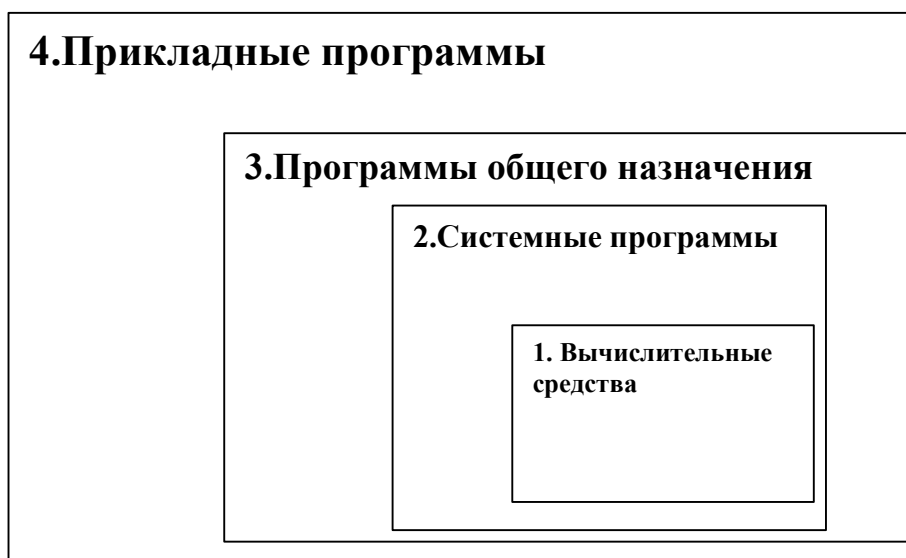
Безопасность информационно-вычислительных систем можно оценить с помощью трех основных групп показателей.

**Первая группа** — показатели, связанные с электробезопасностью, санитарно-гигиенической безопасностью, электромагнитной совместимостью, пожаробезопасностью и т. д. вычислительных средств.

**Вторая группа** — показатели соответствия средств информатизации заданным требованиям в части функциональной полноты, корректности выполнения функциональных задач и устойчивости функционирования.

**Третья группа** — показатели отсутствия аппаратных и программно-информационных дефектов (в том числе недеklarированных функций).

Таким образом, структура и последовательность характеристик безопасности представляется в следующем виде (рис. 1):



Этапы проверки конфигураций ИВС	Техническая безопасность	Функциональная полнота и устойчивость функционирования	Отсутствие «закладок»
1. ПЭВМ	1.1	1.2	1.3
2. ПЭВМ + Системные ПС (ОС)	-	2.2	2.3
3. ПЭВМ + ПС общего назначения (ОС + СУБД)	-	3.2	3.3
4. ПЭВМ + ОС + СУБД + Прикл. ПС	-	4.2	4.3

Последовательность проверок: слева – направо сверху – вниз.

Проверка текущей позиции в таблице проводится, если проверены все позиции выше и левее.

