ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫЕ СИСТЕМЫ КАК ОБЪЕКТ ТЕХНИЧЕСКОГО РЕГУЛИРОВАНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ СИСТЕМ

В Федеральном законе «О техническом регулировании» отсутствует понятие «информационная безопасность», несмотря на то, что в иных нормативных документах (например, в Указе Президента РФ от 10 января 2000 года №24 «О Концепции национальной безопасности Российской Федерации», Федеральном законе от 20 февраля 1995 года №24-ФЗ «Об информации, информатизации и защите информации» и др.) оно достаточно широко используется. Однако статья 7 указанного закона предусматривает установление в технических регламентах минимально необходимых требований, обеспечивающих наряду с перечисленными в статье 7 закона другие виды безопасности.

Рассмотрим один из видов, а именно – компьютерную (информационную) безопасность. Это обусловлено тем, что широкая компьютеризация всех областей человеческой деятельности может нести в себе повышенную опасность, в том числе для жизни и здоровья людей, поскольку современная жизнь в большинстве ее аспектов оказалась зависимой от используемых средств вычислительной техники и практически весь окружающий нас мир управляется с их помощью. Особенно это касается таких систем, в которых компьютеры являются критически важными компонентами, коренным образом влияющими и на их состояние, и на функционирование, а также на другие виды безопасности. В качестве примеров можно привести ряд авиакатастроф, техногенных аварий, сбоев в банковских системах, причинами которых явились сбои и отказы средств вычислительной техники и ошибки в программном обеспечении.

Однако критически важный компонент любой системы составляют не только средства вычислительной техники, но и установленное на них программное обеспечение, и циркулирующие в них данные. Совокупность данных, программного обеспечения и средств вычислительной техники, объединенных в единый функциональный комплекс, представляет собой информационно-вычислительную (или компьютерную) систему (ИВС), предназначенную для сбора, хранения, обработки и выдачи информации потребителю (объекту управления).

Следовательно, в качестве объектов технического регулирования необходимо рассматривать и информационно-вычислительные системы как критически важные компоненты, обеспечивающие безопасность других систем. В этой связи необходимо сформулировать перечень минимально необходимых требований к ИВС, обеспечивающих безопасность их применения, а также предложить механизм оценки соблюдения этих требований.

БЕЗОПАСНОСТЬ ИВС

Вопросы качества управления сегодня занимают центральное место в общественно-хозяйственной жизни, и качество используемых при этом ИВС играет не последнюю роль. При современном уровне развития вычислительной техники времени для обработки на ЭВМ даже значительных объемов информации очень мало, поэтому зачастую вред, причиненный сбоями в работе ИВС, становится очевидным только после завершения ее работы. Вместе с тем заранее предугадать наступление негативных последствий сбоев крайне затруднительно, если вообще возможно.

Анализ российских законов, в частности Гражданского кодекса РФ, Закона РФ от 23 сентября 1992 года №3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных», Уголовного кодекса РФ и Закона РФ от 7 февраля 1992 года №2300-1 «О защите прав потребителей» (с последующими изменениями и дополнениями), показывает, что в действующем законодательстве не установлены специальные нормы гражданско-правовой ответственности перед пользователями ИВС за вред, причиняемый созданием и распространением программных средств. В то же время законами не предусмотрено и установление каких-либо гарантий поставщика на поставляемые программные средства, что дает возможность реализации на рынке программных продуктов на условиях as is (как есть, без

каких-либо гарантий). При этом эксплуатация программных средств осуществляется пользователем на свой страх и риск, а лицензионные соглашения касаются преимущественно прав поставщиков. Ответственность за вред, причиняемый созданием и распространением программ, регламентируется нормами ГК РФ, касающимися только ответственности за нарушение обязательств (ст. 393–406 ГК РФ), а этого явно не достаточно для обеспечения безопасности пользователей ИВС и компьютерных технологий в целом.

В то же время в США, государстве, являющемся родиной революции компьютерных технологий и связывающем свое будущее с лидерством именно в этой сфере, все чаще звучат призывы к обеспечению безопасности ИВС правовыми средствами.

Современные методы разработки программных средств, несмотря на бурное развитие инструментальных средств поддержки, все еще отстают от темпов повышения сложности реализуемых алгоритмов. Иными словами, современные способы создания программных средств принципиально не позволяют обеспечить абсолютно корректную работу программ, в связи с чем остается вероятность причинения пользователю вреда при использовании ИВС. Несмотря на то, что производители оборудования и разработчики программных средств непрерывно работают над повышением их надежности, полностью исключить любые сбои не представляется возможным.

Следовательно, необходимо совершенствование правовой базы использования ИВС, что может быть осуществлено в том числе через разработку и принятие соответствующего технического регламента.

Обеспечение безопасности ИВС следует рассматривать в двух аспектах. С одной стороны, необходимо обеспечить безопасность самой ИВС, а с другой стороны – обеспечить безопасность системы более высокого порядка при использовании ИВС. Очевидно, что наибольший вклад в решение этих задач может внести задание уровня качества используемых средств информатизации: чем выше качество компонентов ИВС, тем меньше риск нанесения вреда при их функционировании.

Исходя из вышесказанного можно сделать вывод о том, что ИВС как составная часть («мозговой центр») любой сложной системы управления является самостоятельным объектом производства и, следовательно, объектом технического регулирования. Отсюда следует необходимость установления обязательных требований к ИВС и их компонентам – требований, соблюдение которых должно исключать недопустимый риск, связанный с причинением вреда жизни или здоровью граждан, имуществу физических и юридических лиц, государственному и муниципальному имуществу, окружающей среде, а также с действиями, вводящими в заблуждение приобретателей.

Соблюдение обязательных требований должно обеспечивать достижение следующих целей:

– повышение уровня безопасности жизни или здоровья граждан, имущества физических и юридических лиц, государственного и муниципального имущества, экологической безопасности, безопасности жизни или здоровья животных и растений при применении информационных технологий и обеспечение соблюдения требований технических регламентов;
– обеспечение научно-технического прогресса;
– повышение конкурентоспособности продукции;
– обеспечение технической и информационной совместимости и взаимозаменяемости компонентов ИВС;
– обеспечение сопоставимости результатов исследований (испытаний) и измерений, технических и экономико-статистических данных.

СИСТЕМА ТЕХНИЧЕСКОГО РЕГУЛИРОВАНИЯ

Достижение поставленных целей может быть обеспечено Системой технического регулирования. Система технического регулирования в сфере информатизации – в общем случае это деятельность субъектов (юридических и физических лиц, органов власти и управления) по обеспечению выпуска средств информатизации и предоставлению услуг с их использованием, соответствующих установленным требованиям. Система представляет собой упорядоченную совокупность следующих элементов:

– нормативных правовых актов, устанавливающих обязательные требования к ИВС и их компонентам, включая требования к защите информации;
– национальных и международных стандартов, сводов правил, требований систем добровольной сертификации, устанавливающих требования к характеристикам качества ИВС и их компонент;
– методических документов по организации работ, связанных с сертификацией, в том числе с испытаниями;
– систем подтверждения соответствия (сертификации) установленным требованиям;
– органов контроля и надзора за соблюдением обязательных требований;
– органов управления, обеспечивающих функционирование Системы технического регулирования.

Важной функцией системы технического регулирования в сфере информатизации является обеспечение научно-методического и технологического единства регулирования отношений, связанных с применением средств информатизации в различных отраслевых системах технического регулирования по причине того, что ИВС представляют собой критически важный объект, создающий опасность причинения вреда в любой системе, где используется. При этом объектами технического регулирования могут являться:

– ИВС в целом;
– средства вычислительной техники в составе ИВС;
– программные средства информационно-вычислительных систем;
– программно-технические средства защиты информации;
– системы менеджмента качества средств вычислительной техники, программных средств, ин-

формационно-вычислительных систем и информационных услуг.

В соответствии с Законом «О техническом регулировании» субъектами технического регулирования в сфере информатизации являются органы государственной власти, органы местного самоуправления, организации и хозяйствующие субъекты, участвующие в отношениях, связанных с разработкой и контролем исполнения установленных законодательством Российской Федерации и другими нормативными документами (национальными стандартами, сводами правил и т.п.) требований к объектам технического регулирования.

В функции субъектов технического регулирования включены:

– нормативное правовое регулирование;
– нормативное техническое регулирование (стандартизация);
– оценка соответствия (сертификация);
– государственный контроль и надзор за соблюдением установленных обязательных требований;
– производство и использование средств вычислительной техники, программных средств и ИВС в целом.

Конкретные обязательные требования к безопасности ИВС должны быть включены в национальные стандарты, предназначенные в том числе для доказательства соблюдения требований технических регламентов. При этом безопасность ИВС определяется следующими группами факторов:

1. Уровнем качества функциональных характеристик средств информатизации и информационных ресурсов, в том числе:
– полнотой и корректностью данных;
– полнотой функций назначения;
– устойчивостью и корректностью выполнения заданных функций, в том числе при сбоях средств вычислительной техники, при наличии ошибок во входных данных и непреднамеренных действий персонала.
2. Отсутствием деструктивных элементов («закладок») в средствах вычислительной техники и в программных средствах.
3. Степенью защиты от несанкционированного доступа к ресурсам.

Безопасность АСУ обусловлена еще тремя группами факторов, а именно:

а) квалификацией персонала, использующего средства информатизации и информационные ресурсы;
б) уровнем охраны объекта информатизации, в том числе от стихийных природных явлений;
в) степенью защиты информационных ресурсов от различных видов технической разведки.

При этом безопасность информационно-вычислительной системы не должна снижать безопасность системы более высокого уровня, составной частью которой она является.

Таким образом, требования к ИВС также могут быть представлены в виде следующих групп:

– требования к техническим характеристикам информационно-вычислительных систем и их компонентов, соблюдение которых обеспечивает их корректное и устойчивое функционирование, технологическую совместимость, целостность и пр.;
– требования к качеству предоставления государственных информационных услуг;
– требования к защите информационных ресурсов.

При формировании требований целесообразно учитывать:

– экономическую обоснованность требований;
– соответствие требований уровню развития национальной экономики, уровню научно-технического развития сферы информационных технологий, а также характеристикам средств контроля и измерений характеристик объектов измерений;
– единство методических подходов при установлении требований в различных областях применения средств информатизации;
– гармонизацию с требованиями международных стандартов.

СЕРТИФИКАЦИЯ

Объективным инструментом, с помощью которого можно подтвердить установленный уровень качества продукции и услуг, а также выполнение установленных требований, в настоящее время является сертификация. Сертификация – процедура, посредством которой третья сторона письменно удостоверяет, что продукция и/или система менеджмента качества организации – производителя этой продукции соответствует установленным требованиям. При этом действия третьей стороны не должны зависеть ни от поставщика, ни от потребителя, в том числе при отсутствии аффелированности между участниками сертификации (органами по аккредитации, органами по сертификации) и заявителями. И в то же время недопустимо совмещение полномочий на аккредитацию и подтверждение соответствия. Органы по аккредитации (организации, создающие системы сертификации) должны быть независимы как от поставщиков (покупателей), так и от потребителей (заказчиков).

Сертификат соответствия – документ, выданный в соответствии с правилами системы сертификации и удостоверяющий, что продукция/система менеджмента качества соответствует требованиям конкретного нормативного документа.

Нормативные документы (стандарты), применяемые для сертификации, должны соответствовать требованиям Руководства ИСО/МЭК 7 «Требования к стандартам, применяемым при сертификации изделия», в подразделе 5.2 которого установлено, что «Требования должны быть четко оговорены вместе с необходимыми предельными значениями и допусками, а также методами испытаний для проверки заданных характеристик. Требования должны быть лишены субъективных элементов».

Поскольку системы сертификации могут создавать только организации (ведомства), независимые как от поставщика (покупателя), так и от потребителя (заказчика), то органы по сертификации в этих системах сертификации имеют такой же статус независимости, как и орган по аккредитации. Отсюда следует, что ведомства (агентства, службы, акционерные общества и пр.), создавшие собственные системы добровольной сертификации, не должны признавать сертификаты соответствия «своих» систем сертификации при проведении тендеров (аукционов) на закупки продукции для своих нужд или на продукцию, произведенную на подведомственных предприятиях.

Учредителями систем сертификации в соответствии с указанными положениями могут быть:

– федеральные службы надзора, не подчиненные министерствам;

– федеральные агентства, не имеющие в своем подчинении производственных предприятий;

– акционерные общества, научные и общественные организации, в учреждении которых не участвуют заказчики и поставщики сертифицируемой продукции.

Системы сертификации в общем случае нецелесообразно разделять на системы обязательной сертификации и системы добровольной сертификации, так как собственно процессы сертификации по своему содержанию в обоих случаях идентичны и представляют собой совокупность двух процессов:

а) измерение характеристик объекта сертификации, в том числе путем проведения испытаний (это функции испытательных центров и испытательных лабораторий);

б) проверка полноты проведенных испытаний, сравнение измеренных значений со значениями, которые установлены в нормативных документах (это функции органов по сертификации).

При этом обязательность сертификации для поставщиков и заказчиков устанавливается законодательно только по требованиям безопасности для конкретных видов продукции и конкретного состава характеристик этих видов продукции.

По другим видам продукции и требованиям к ней, которые не установлены законодательно, обязательность сертификации может быть установлена органами государственной власти (ведомствами), органами местного самоуправления при формировании условий проведения конкурсов при закупке продукции для собственных нужд. Проведение сертификации такой продукции (услуг) отнесено Законом «О техническом регулировании» к сфере добровольной сертификации. При этом устанавливать требования к продукции целесообразно поручать будущим заказчикам продукции.

В качестве примера можно привести Систему добровольной сертификации средств и систем в сфере информатизации «РОСИНФОСЕРТ» (регистрационный №РОСС RU.В244.04ИН01 от 29 июня 2005 года), которая является системой, независимой ни от заказчиков, ни от поставщиков средств информатизации.

Руководящий (аккредитующий) орган системы – Всероссийский НИИ проблем вычислительной техники и информатизации – не производит и не поставляет потребителям средства информатизации. Следовательно, независимыми являются как сам аккредитующий орган, так и аккредитованные им (признанные компетентными) в системе (подконтрольные ему) органы по сертификации. То есть Система сертификации «РОСИНФОСЕРТ» по критериям независимости при сертификации в полной мере соответствует требованиям Закона «О техническом регулировании».

Схема обеспечения качества информационно-вычислительных систем и обеспечение безопасности их использования представляется следующей:

1. Устанавливаются общие требования к информационно-вычислительным системам и информационным ресурсам критически важных систем (компонентов систем) в технических регламентах.
2. Требования, установленные в техническом регламенте, конкретизируются в национальных стандартах, в сводах правил, в требованиях систем добровольной сертификации с учетом особенностей продукции.
3. В правила проведения конкурсов (тендеров) включается обязательное условие выполнения требований, установленных в выше перечисленных правовых и нормативных документах.
4. Соответствие продукции (услуг) установленным требованиям подтверждается наличием сертификата соответствия.

В соответствии с этой схемой становится обязательной сертификация информационно-вычислительных систем, используемых в целях государственного и муниципального управления, а также для работы с информацией ограниченного доступа.

ВЫВОДЫ

1. Для обеспечения безопасности при использовании ИВС, как критически важных компонентов других технических систем, необходима разработка соответствующего технического регламента.
2. Для подтверждения соответствия требованиям технического регламента необходимо формирование комплекса национальных стандартов, сводов правил и требований систем добровольной сертификации.
3. Обязательные требования к безопасности ИВС должны являться составной частью общих требований к системе более высокого уровня, в состав которой входит ИВС.
4. Нормативные документы для сертификации информационно-вычислительных систем (их

компонент), систем менеджмента качества вычислительных и программных средств, государственных услуг в сфере информатизации должны по своему содержанию удовлетворять требованиям Руководства ИСО/МЭК 7.

ПОНЯТИЯ И ТЕРМИНЫ

Критическая система (критически важный компонент системы) – система (компонент системы), при нарушении работы или выходе из строя которой существует 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.

Технология – совокупность методов обработки, изготовления, изменения состояния, свойств, формы сырья, материала или полуфабриката в процессе производства. Конкретная технология в общем случае предполагает наличие трех определяющих составных элементов: материал, средства его обработки и методы обработки материала.

Информационная технология – организованная совокупность процессов, элементов, устройств и методов, используемых для обработки информации. Когда «сырьем для обработки» является информация в форме данных, а средством обработки являются средства вычислительной техники, то под информационной технологией понимается совокупность методов (способов) сбора, накопления, хранения, поиска, обработки и выдачи информации потребителю с использованием средств вычислительной техники. В такой интерпретации информационная технология – это компьютерная технология.

Далее рассматриваются только вопросы, относящиеся к компьютерным технологиям.

Программа – последовательность инструкций (кодов) для средства вычислительной техники, находящаяся в памяти этого средства.

Под *программными средствами* (ПС) понимается совокупность программ, связанных с ними данных и соответствующих им программных документов.

Цифровые информационные ресурсы (информационные ресурсы) – переведенная в цифровой код информация об окружающей действительности в форме данных, баз данных и программно-информационных продуктов, которая обрабатывается с использованием средств вычислительной техники.

Программы, если они не выполняются на вычислительных средствах, представляют собой цифровые информационные ресурсы, которые могут храниться, редактироваться, передаваться как обычные данные. При этом цифровые информационные ресурсы, как и программы, существуют только в *информационно-вычислительной системе* (ИВС).

Архитектура ИВС в общем виде может быть представлена структурой, включающей компоненты следующих уровней иерархии:

1. Основу ИВС составляют средства вычислительной техники (вычислительная техника – 40-й класс по Общероссийскому классификатору продукции). Средства вычислительной техники как самостоятельная продукция (вне информационно-вычислительной системы) относятся к классу машин и оборудования. Средства вычислительной техники вместе с системными ПС (операционными системами, средствами их расширения и др.) составляют аппаратно-программную платформу ИВС.
2. Следующий уровень составляют программные средства и информационные продукты вычислительной техники (50-й класс по Общероссийскому классификатору продукции). В их состав могут быть включены:
– программные средства общего назначения (системы управления базами данных, текстовые редакторы и пр.);
– прикладные ПС различного функционального назначения. Прикладные ПС, реализованные на аппаратно-программной платформе ИВС в совокупности с программными средствами общего назначения, обеспечивают решение функциональных задач ИВС;
– программно-информационные продукты (данные (базы данных), которые представляют собой входные, промежуточные и выходные результаты обработки информации).

Системы управления, критически важным компонентом которых являются информационно-вычислительные системы, в зависимости от степени участия персонала в принятии решения на основе результатов обработки информации могут быть разделены на три группы:

– первая группа – *автоматизированные информационно-справочные системы* (АИСС). АИСС – это совокупность информационно-вычислительной системы и персонала, который использует эту информационно-вычислительную систему для информационного обслуживания граждан и организаций;
– вторая группа – *автоматизированные информационные системы управления* (АСУ). АСУ – совокупность информационно-вычислительной системы и персонала, который использует эту информационно-вычислительную систему для принятия решений или решения прикладных задач в составе некоторой системы управления. К этому же классу следует отнести диспетчерские АСУ;
– третья группа – *автоматические информационные системы управления технологическими процессами* (АСУТП). АСУТП – это совокупность информационно-вычислительной системы и производственного объекта управления, на который результат обработки данных передается непосредственно, без вмешательства персонала.

Под *защитой информации* понимается совокупность правовых норм, организационных и технических средств, обеспечивающих:

– сохранность информации от случайного или неправомерного уничтожения, изменения, блокирования, копирования, передачи, распространения, а также от иных неправомерных действий;
– реализацию прав на доступ к информации;
– соблюдение конфиденциальности информации ограниченного доступа.

Кроме того, требуют однозначного толкования такие широко распространенные термины, как информатизация и средства информатизации.

Для целей настоящей статьи:

– *средства информатизации* – это средства вычислительной техники, программные средства, информационно-вычислительные системы;
– *информатизация* – процессы использования средств информатизации в деятельности организации.

НАУЧНЫЙ КОНСУЛЬТАНТ ВСЕРОССИЙСКОГО
НИИ ПРОБЛЕМ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ
И ИНФОРМАТИЗАЦИИ (ВНИИПВТИ)
П.И. Братухин,
ЗАВЕДУЮЩИЙ СЕКТОРОМ НАУЧНО-МЕТОДИЧЕСКОГО
ОБЕСПЕЧЕНИЯ СЕРТИФИКАЦИИ ПРОДУКЦИИ
И СИСТЕМ МЕНЕДЖМЕНТА КАЧЕСТВА СРЕДСТВ
ИНФОРМАТИЗАЦИИ ВНИИПВТИ
Ю.А. Панов,
ЗАВЕДУЮЩИЙ ОТДЕЛОМ НАУЧНО-МЕТОДИЧЕСКОГО
ОБЕСПЕЧЕНИЯ И АНАЛИЗА КАЧЕСТВА
ПРОДУКЦИИ ИНФОРМАТИЗАЦИИ ВНИИПВТИ
В.П. Шахин