УДК: 004.62:004.94+004.8

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ И ПРОЦЕССОВ РАЗРАБОТКИ И ВНЕДРЕНИЯ НАУКОЕМКОЙ ТЕХНИКИ МЕЖОТРАСЛЕВЫМИ КОМПЛЕКСАМИ СТАНДАРТОВ.

Часть 2. Система «Информационные технологии»

Будкин Ю.В., д-р техн. наук, профессор, ФГБУ «Институт стандартизации»

В статье представлены результаты исследований межотраслевых систем и комплексов стандартов с целью их актуализации и использования для обеспечения информационных систем и процессов разработки и внедрения наукоемкой техники. Вторая часть направлена на исследование системы ГОСТ Р 34.XXX «Информационные технологии», состоящей из четырех невзаимосвязанных комплексов стандартов. Установлено, что для предприятий промышленного комплекса востребованы комплексы стандартов на «Автоматизированные системы» и «Криптографическую защиту информации». Комплекс стандартов на «Автоматизированные системы» актуализирован в области применения документации системы в различных видах деятельности (управление, исследования, проектирование и т.п.), включая их сочетания, и устанавливает требования к видам, наименованию, комплектности и обозначению документов, разрабатываемых на стадиях создания АС.

Отмечена разработка стандартов, не входящих в комплекс «Автоматизированные системы», но устанавливающих требования к испытаниям АС. Целесообразно актуализировать комплекс стандартов на «Автоматизированные системы» совместно с актуализацией комплексов стандартов: ГОСТ 24.XXX (ЕСС АСУ) и ГОСТ 19.XXX (ЕСПД), а также стандартами ГОСТ 25.XXX (САПР). Это позволит решить задачу согласования нормативно-технической документации для создания и применения автоматизированных систем в промышленных предприятиях. Комплекс стандартов на «Криптографическую защиту информации» является базовыми для обеспечения надежной аутентификации сторон информационного обмена и защиты данных в процессе информационного обмена. Предложено гармонизировать комплекс стандартов с ГОСТ 25.XXX (САПР). Это позволит обеспечить достоверность и целостность информации (в том числе с использованием алгоритмов цифровой подписи) при ее обработке, хранении и передаче.

Ключевые слова: информационные системы и процессы, машиностроение, стандарт, автоматизированная система управления, система автоматизированного проектирования

ВВЕДЕНИЕ

В настоящее время система 34 состоит из 28 разнородных стандартов, определяющих различные объекты и аспекты стандартизации. Перечень рассмотренных стандартов, входящих в систему ГОСТ 34.XXX.

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АСУ – автоматизированная система управления
ДЭ – документ электронный
ЕСКД – Единая система конструкторской документации
ЕСТД – Единая система технологической документации
ЕСПД – Единая система программной документации
ЕСС АСУ – Единая система стандартов автоматизированных систем управления
ЖЦИ– жизненный цикл изделия
CALS (ИПИ)– информационная поддержка жизненного цикла изделий
ИТ – информационная технология
КД – конструкторская документация
НД – нормативный документ (нормативная документация)

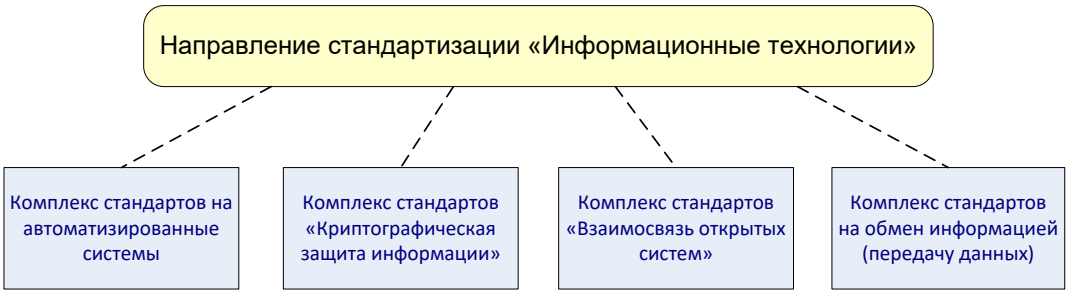

Рис. 1. Структура стандартов системы 34 «Информационные технологии»

и национальных стандартов машиностроения и приборостроения
САПР – Система автоматизированного проектирования
СРПП – Система разработки и постановки продукции на производство
ЭВМ-электронно-вычислительная машина
ЭД– эксплуатационный документ (эксплуатационная документация)

МЕЖОТРАСЛЕВОЙ КОМПЛЕКС «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ»

В состав стандартов системы 34 входят следующие невзаимосвязанные комплексы стандартов (см. рис. 1):

1. Комплекс стандартов на автоматизированные системы (КС АС).
2. Комплекс стандартов «Криптографическая защита информации» (КС КЗИ).
3. Комплекс стандартов на обмен информацией (передачу данных).
4. Комплекс стандартов «Взаимосвязь открытых систем» (КС ВОС).

Из этих 4-х комплексов интерес с точки зрения применимости предприятиями и организациями ОПК реально представляют комплекс стандартов на автоматизированные системы и комплекс стандартов «Криптографическая защита информации».

Комплексы стандартов на обмен информацией (передачу данных) и «Взаимосвязь открытых систем» (КС ВОС) являются достаточно низкоуровневыми документами, устанавливающими требования к технической реализации отдельных аспектов стандартизации [1–4]. Реально ссылки на эти стандарты в технических заданиях на разработку продукции ОПК вероятнее всего устанавливаться не будут, т.к. это во-первых, слишком технические указания, во-вторых, они напрямую не входят в ДСОП.

КОМПЛЕКС СТАНДАРТОВ НА АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ (КС АС)

КС АС задумывался в конце 80-х годов как всеобъемлющий комплекс взаимоувязанных межотраслевых документов. Объектами стандартизации являются АС различных (причем любых!) видов и все виды их компонентов, а не только ПО и БД.

КС АС рассчитан на взаимодействие заказчика и разработчика. Аналогично SO /IEC /IEEE 12207:2017 «Системы и разработка программного обеспечения — процессы жизненного цикла программного обеспечения» предусмотрено, что заказчик может разрабатывать АС для себя сам (если создаст для этого специализированное подразделение). Однако формулировки КС АС не ориентированы на столь явное и, в известном смысле, симметричное отражение действий обеих сторон, как ISO12207. Поскольку КС АС в основном уделяет внимание содержанию проектных документов, распределение действий между сторонами обычно делается отталкиваясь от этого содержания.

Все стандарты КС АС межгосударственные. Степень обязательности определяется указанием на их применение. Стандарты КС АС по сути стали методической поддержкой, причем чаще для заказчиков, имеющих в стандарте набор требований к содержанию ТЗ и проведению испытаний АС.

КС АС включает 2 блока (системы) стандартов – систему стандартов на базы данных (БД) и непосредственно стандарты на АС (см. рис. 2).

В 80-х годах сложилось положение, при котором в различных отраслях и областях деятельности использовалась плохо согласованная или несогласованная нормативно-техническая документация на различные АС. Это затрудняло интеграцию систем, обеспечение их эффективного совместного функционирования. Действовали различные комплексы и системы стандартов, устанавливающие требования к различным видам АС.

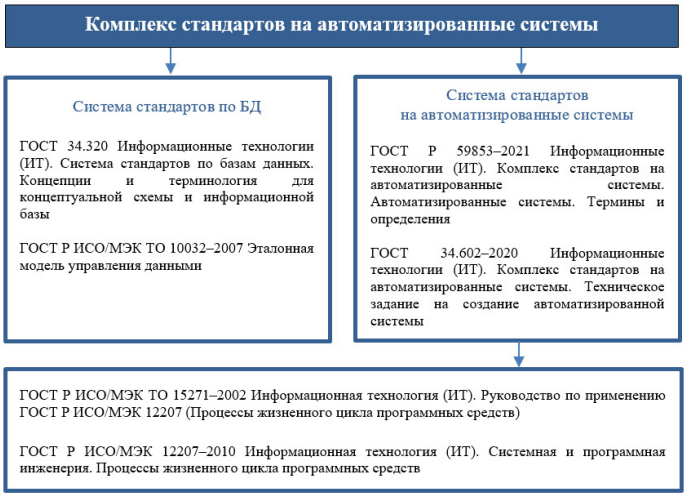

Рис. 2. Структура комплекса стандартов на автоматизированные системы

Практика применения стандартов показала, что в них применяется по существу (но не по строгим определениям) единая система понятий, есть много общих объектов стандартизации, однако требования стандартов не согласованы между собой, имеются различия по составу и содержанию работ, различия по обозначению, составу, содержанию и оформлению документов и пр.

Конечно, эта ситуация отчасти отражала и естественное многообразие условий разработки АС, целей разработчиков, применяемых подходов и методик.

В этих условиях можно было провести анализ такого многообразия и далее поступить, например, одним из двух во многом противоположных способов:

1. Выработать одну обобщенную понятийную и терминологическую систему, общую схему разработки, общий набор документов с их содержанием и определить их как обязательные для всех АС.
2. Определить также одну общую понятийную и терминологическую систему, обобщенный комплекс системных требований, набор критериев качества, но предоставить максимальную свободу в выборе схемы разработки, состава документов и других аспектов, наложив только минимум обязательных требований, которые позволяли бы:

– определять уровень качества результата;
– выбирать те конкретные методики (с их моделями ЖЦ, набором документов и др.), которые наиболее подходят к условиям разработки и соответствуют используемым информационным технологиям;
– работать, таким образом, с минимальными ограничениями эффективных действий проектировщика АС.

Разработчики комплекса стандартов 34 выбрали способ, близкий к первому из указанных выше, то есть пошли по пути, более близкому к схемам конкретных методик, чем к стандартам типа ISO 12207. Тем не менее, благодаря общности понятийной базы стандарты остаются применимыми в весьма широком диапазоне случаев.

Степень адаптивности формально определяется возможностями:

– опускать стадию эскизного проектирования и объединять стадии «Технический проект» и «Рабочая документация»;
– опускать этапы, объединять и опускать большинство документов и их разделов;
– вводить дополнительные документы, разделы документов и работы;
– динамически создавая т. н. частные технические задания, позволяя достаточно гибко формировать ЖЦ АС (как правило, этот прием используют на уровне крупных единиц (подсистем, комплексов), ради которых считается оправданным создавать ЧТЗ, однако нет никаких существенных оснований сильно ограничивать этот способ управления ЖЦ).

Стадии и этапы, выполняемые организациями — участниками работ по созданию АС, устанавливаются в договорах и техническом задании, что близко к подходу ИСО.

Введение единой, достаточно качественно определенной терминологии, наличие достаточно разумной классификации работ, документов, видов обеспечения и др. безусловно полезно. КС АС способствует более полной и качественной стыковке действительно разных систем, что особенно важно в условиях, когда разрабатывается все больше сложных комплексных АС, например, типа CAD/CAM/CAE/MRP, которые включают в свой состав в российской терминологии АСУТП, АСУП, САПР-конструктора, САПР-технолога, АСНИ и др. системы.

ГОСТ Р 59853-2021 «Информационные технологии (ИТ). Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» устанавливает основные термины и определения в области создания АС. Определено несколько важных положений, отражающих особенности АС как объекта стандартизации, например: «в общем случае АС состоит из программно-технических (ПТК), программно-методических (ПМК) комплексов и отдельных компонентов организационного, технического, программного и информационного обеспечения».

Разделение понятий ПТК и АС закрепляло принцип, по которому АС есть не «ИС с БД», но:

– ***автоматизированная система;*** система, состоящая из комплекса средств автоматизации, реализующего информаци-

онную технологию выполнения установленных функций, и персонала, обеспечивающего его функционирование;

1. В зависимости от вида деятельности выделяют, например, следующие виды АС: автоматизированные системы управления (АСУ), системы автоматизированного проектирования (САПР), автоматизированные системы научных исследований (АСНИ) и др.
2. В зависимости от вида управляемого объекта (процесса) АСУ подразделяют, например, на АСУ технологическими процессами (АСУТП), АСУ предприятиями (АСУП) и т.д.

– программно-технический комплекс автоматизированной системы; программно-технический комплекс АС; ПТК АС: Совокупность совместно функционирующих технических, программных и информационных средств, предназначенных для выполнения определенного набора функций АС.

Эти определения указывают на то, что АС — это, в первую очередь, персонал, принимающий решения и выполняющий другие управляющие действия, поддержанный организационно-техническими средствами.

Еще одним важным положением является понятие «Типовое проектное решение», определяемое в стандарте как «проектное решение, предназначенное для повторного использования». Сама же типизация представляет собой совокупность действий (комплекс мероприятий), направленных на повторное использование проектного решения или средства.

Направлениями унификации и типизации являются:

– использование ограниченного числа типов, моделей и версий;
– определение унифицированных типовых решений (использование заранее определенных рядов моделей, конфигураций, состава и комплектации);
– применение типовых способов использования;
– выбор основных фирм-производителей и фирм-поставщиков из заранее определенного списка.

Вообще в проектах систем можно выделить следующие объекты стандартизации, унификации и типизации:

– функциональные задачи;
– методики и алгоритмы;
– технологии обработки данных;
– информационные технологии;
– архитектурные решения;
– информационное обеспечение;
– интерфейсы пользователей;
– прикладное программное обеспечение;
– системно-технические решения;
– информационная безопасность;
– инструментальные средства разработки приложений;
– средства управления и администрирования;
– методы и средства сопровождения системы.

При создании ИАС взамен организационно-функциональной ориентации системы предлагается функционально-технологическая ориентация. При этом классификация задач по технологиям обработки данных позволяет выделить технологические блоки, являющиеся общими и типовыми для нескольких или всех функциональных задач. Функционирование ИАС в целом происходит на основе унифицированной технологической цепочки, состоящей из типовых технологических блоков.

Технологические блоки составляют ядро системы, обеспечивают автоматизацию основных операций по подготовке, сбору, обработке данных и предоставлению результатов. Для реализации этих блоков желательно применять готовые фирменные продукты.

Функциональные задачи «встраиваются» в технологические блоки в виде наполнения, описаний (метаданных), процедур и объектов. Для методической и алгоритмической совместимости приложений должна быть организована их централизованная разработка и сопровождение.

ГОСТ 34.602–2020 «Информационные технологии (ИТ). Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы» устанавливает требования к содержанию и структуре технического задания (ТЗ) на создание автоматизированной системы. ТЗ является ключевым документом взаимодействия сторон и основным исходным документом для создания АС и его приемки. ТЗ определяет важнейшие точки взаимодействия заказчика и разработчика. Указано, что ТЗ разрабатывает организация-разработчик, но формально выдает ТЗ разработчику заказчик.

ГОСТ 34.601–90 «Информационная технология (ИТ). Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания» устанавливает стадии и этапы выполнения работ по созданию АС, но не предусматривает сквозных процессов в явном виде. Имеют отношение к документированию из них три:

1. Эскизный проект (ЭП).
2. Технический проект (ТП).
3. Разработка рабочей документации (РД).

Эскизный проект следует после стадии Техническое задание и служит для разработки предварительных проектных решений.

Технический проект описывает будущую систему со всех ракурсов. Документы стадии ТП должны после прочтения

оставлять после себя полную ясность в предлагаемых подходах, методах, архитектурных и технических решениях. На следующей фазе уже поздно будет описывать подходы и обосновывать технические решения, так что фаза П является ключом к успешной сдаче работ, так как все многообразие требований ТЗ должно находить отражение в документах фазы П. На этапе П система может вообще не существовать.

Рабочая документация предназначена для успешного развертывания, ввода в действие и дальнейшей эксплуатации новой системы. Это документы, содержащие совершенно конкретные сведения, описывающие физически существующие сущности, в отличие от фазы П.

ГОСТ 34.201-2020 «Информационные технологии (ИТ). Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем» устанавливает виды, комплектность и правила обозначения документов при создании АС. Это базовый документ, в котором приводится полный перечень документации КС АС, рекомендации по кодированию документов, определено к каким стадиям проекта относятся документы, а также как их можно объединять между собой.

Стандарт делит все документы по двум осям — время и предметная область. Если посмотреть табл. 2 стандарта, то это деление хорошо видно (колонки «Стадия создания» и «Часть проекта»).

Предметная область разделена на «виды обеспечения». Автоматизированная система в представлении разработчиков ГОСТ представляет собой совокупность железа, программ и каналов связи, которая обрабатывает приходящую из разных источников информацию в соответствии с некими алгоритмами и выдает результаты обработки в виде документов, структур данных или управляющих воздействий (по сути – модель простейшего «автомата» из теории автоматического регулирования). Для того, чтобы полностью описать этот «автомат», сделаны следующие срезы системы (разделы документации, аналогично понятию как точки зрения в черчении в CAD):

Математическое обеспечение (МО), отвечающее на вопросы: какая логика зашита внутри «черного ящика», почему выбраны именно эти алгоритмы, именно такие формулы и именно такие коэффициенты.

МО никак не касается программной реализации, но МО бывает очень плотно связано с предметной областью (например, при разработке автоматизированных систем дорожного движения (ГОСТ 34.401 «Информационная технология. Комплекс стандартов на автоматизированные системы. Средства технические периферийные автоматизированных систем дорожного движения. Типы и технические требования».) управляющие алгоритмы для систем управления дорожным движением требуется согласовать в ГИБДД перед тем, как их будет согласовывать заказчик [5]. Именно для подобных случаев их выделяют в отдельный документ – в ГИБДД никому не интересно, на какой ОС будет работать сервер приложения, а вот какой знак и ограничение скорости выскочит на табло в дождь или в снег очень даже интересно. Они отвечают за свою часть, и ничего другого подписывать не собираются. С другой стороны, когда они подписали, не будет вопросов к технической стороне вопроса — почему выбрали те, а не другие табло или светофоры).

Информационное обеспечение (ИО). Второй срез системы, определяющий циркулирующую в АС информацию. В информационном обеспечении описываются состав и маршруты прохождения информации внутри и снаружи системы, логическая организация информации в системе, описание справочников и систем кодирования.

Примечание: основная описательная часть приходится на этап ТП, но на этапе РД возникают некоторые «рудименты», унаследованные от эпохи больших ЭВМ, такие как «Каталог баз данных» (понятно, что раньше он содержал именно то, что написано в названии), или «Ведомость машинных носителей информации» (понятно, что раньше в нем были номера магнитных барабанов или бобин с пленкой). Отсюда вытекает, что на фазе РД номенклатура документов раздела «Информационное обеспечение» требует пересмотра.

Программное обеспечение (ПО). Срез, определяющий при помощи каких программных средств выполняются алгоритмы, описанные в МО, обрабатывающие информацию, описанную в ИО. Тут дается архитектура системы, обоснование выбранных программных технологий, их описание (всякие системные вещи: языки программирования, операционные системы и т.п.). Также здесь описывают как организованы средства обработки информации (очереди сообщений, хранилища, средства резервного копирования, решения по доступности, всякие пулы приложений и т.п.).

Техническое обеспечение (ТО). Определяет документирование технических средств, используемых при создании АС или ее частей (т.е. документации, обеспечивающей разработку, изготовление, приемку и монтаж технических средств). Всего по стандарту требуется разработать 22 документа, из них 9 на стадии ТП.

Стандарт предусматривает описание всего технического обеспечения, включая компьютеры (само «железо») и сети, инженерные системы и даже строительную часть (если потребуется). Все это по жизни регламентируется большим количеством специализированных в этих областях стандартов и нормативных актов, согласуется в разных организациях и поэтому стандарт предусматривает, что удобнее

все дробить на части и согласовывать (править) по частям. В то же время стандарт позволяет объединять некоторые документы друг с другом (что имеет смысл делать, если всю документы согласует один человек)

Примечание: кроме того, имея в виду требования к учету и хранению технических документов, конкретные документы у заказчика могут разойтись по разным архивам, в зависимости от предмета описания, что является еще одним аргументом в пользу дробления документации.

Организационное обеспечение (ОО). На стадии ТП раздел содержит всего один документ «Описание организационной структуры», в котором требуется рассказать заказчику, к чему он должен готовиться в плане изменения штатной оргструктуры (возможно потребуется организовать новый отдел для эксплуатации системы, ввести новые должности и т.п.). Однако на стадии РД появляется документ, который хотелось бы рассмотреть отдельно, т.к. он явно требуют исключения из номенклатуры документов. Это «Описание технологического процесса обработки данных (включая телеобработку)», который представляет собой явный «рудимент» эпохи перфокарт.

Общесистемные решения (ОР). Стандартом предусмотрено 17 документов раздела ОР. Особенностью является то, что практически все они содержат информацию не для эксплуатантов АС (ИТ-специалистов на производстве), а для менеджеров, экономистов и т.п. (это всевозможные сметы, расчеты и краткие описание автоматизируемых функций). Кроме того, в состав ОР входит мега-документ под названием «Пояснительная записка к техническому проекту», в который по факту записывают вообще все полезное содержание стадии ТП. (подобный радикальный подход бывает в определенных случаях оправдан и даже взаимно выгоден и заказчику и исполнителю работ).

Кроме того, определены виды и комплектность документов на программные средства и виды и комплектность документов на технические средства, используемые при создании АС или ее частей.

Виды и комплектность документов на программные средства, используемые при создании АС (ее частей), — по ГОСТ 19.101 «Единая система программной документации. Виды программ и программных документов».

Виды и комплектность документов на технические средства, используемые при создании АС или ее частей (т.е. документации, обеспечивающей разработку, изготовление, приемку и монтаж технических средств), по ГОСТ 2.102–2013 «Единая система конструкторской документации. Виды и комплектность конструкторских документов» и по ГОСТ Р 2.601–2019 «Единая система конструкторской документации (ЕСКД). Эксплуатационные документы» в части эксплуатационных документов.

ГОСТ Р 59792–2021 Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды испытаний автоматизированных систем распространяется на автоматизированные системы (АС), используемые в различных видах деятельности (исследование, проектирование, управление и т. п.), включая их сочетания, создаваемые в организациях, объединениях и на предприятиях (далее – организациях).

Стандарт определяет, что устанавливает испытания АС представляют собой процесс проверки выполнения заданных функций системы, определения и проверки соответствия требованиям ТЗ количественных и (или) качественных характеристик системы, выявления и устранения недостатков в действиях системы, в разработанной документации. Для АС устанавливают три основные виды испытаний: предварительные; опытная эксплуатация и приемочные, при этом допускается:

1. Дополнительно проведение других видов испытаний АС их частей.
2. Классификация приемочных испытаний в зависимости от статуса приемочной комиссии (состав членов комиссии и уровень его утверждения).
3. Устанавливать виды испытаний и статус приемочной комиссии в договоре и (или) ТЗ.

КОМПЛЕКС СТАНДАРТОВ НА КРИПТОГРАФИЧЕСКУЮ ЗАЩИТУ ИНФОРМАЦИИ

В КСКЗИ входят 4 стандарта, определяющих различные аспекты применения криптографической защиты информации:

1. ГОСТ Р 34.10–2012 «Информационная технология (ИТ). Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»
2. ГОСТ 34.11–2018 «Информационная технология (ИТ). Криптографическая защита информации. Функция хэширования»
3. ГОСТ 34.12–2018 «Информационная технология (ИТ). Криптографическая защита информации. Блочные шифры»
4. ГОСТ Р 34.13–2015 «Информационная технология (ИТ). Криптографическая защита информации. Режимы работы блочных шифров»

Стандарты вводят определение криптографической защиты информации как защиты информации с помощью ее криптографического преобразования. В настоящее время криптографические методы являются базовыми для обеспечения надежной аутентификации сторон информационного обмена и защиты данных в процессе информационного обмена.

К средствам криптографической защиты информации (СКЗИ) относятся аппаратные, программно-аппаратные и программные средства, реализующие криптографические алгоритмы преобразования информации с целью:

- защиты информации при ее обработке, хранении и передаче;
- обеспечения достоверности и целостности информации (в том числе с использованием алгоритмов цифровой подписи) при ее обработке, хранении и передаче;
- выработки информации, используемой для идентификации и аутентификации субъектов, пользователей и устройств;
- выработки информации, используемой для защиты аутентифицирующих элементов защищенной АС при их выработке, хранении, обработке и передаче.

Базовыми структурами современной криптографии являются: блочный шифр, криптографическая хэш-функция (функция хэширования) и электронная подпись (Надо сказать, что ГОСТ оперирует термином ЭЦП, а федеральный закон «Об электронной подписи» – ЭП).

Криптографические методы предусматривают шифрование и кодирование информации. Различают два основных метода шифрования: симметричный и асимметричный. В первом из них один и тот же ключ (хранящийся в секрете) используется и для зашифрования, и для расшифрования данных.

ГОСТ Р 34.12 и ГОСТ Р 34.13 устанавливают основные требования к выполнению СКЗИ с помощью ассиметричных шифров.

В асимметричных методах используются два ключа. Один из них, несекретный (он может публиковаться вместе с другими открытыми сведениями о пользователе), применяется для шифрования, другой (секретный, известный только получателю) – для расшифрования. Самым популярным из асимметричных является метод RSA, основанный на операциях с большими (100-значными) простыми числами и их произведениями.

Криптографические методы позволяют надежно контролировать целостность как отдельных порций данных, так и их наборов (таких как поток сообщений); определять подлинность источника данных; гарантировать невозможность отказаться от совершенных действий.

В основе криптографического контроля целостности лежат два понятия: хэш-функция и электронная подпись (ЭП).

ГОСТ Р 34.11 содержит описание алгоритма и процедуры вычисления хэш-функции для любой последовательности двоичных символов, которые применяются в криптографических методах защиты информации, в том числе в процессах формирования и проверки электронной цифровой подписи.

Стандарт разработан взамен ГОСТ Р 34.11. Необходимость разработки нового стандарта вызвана потребностью в создании хэш-функции. соответствующей современным требованиям к криптографической стойкости и требованиям стандарта ГОСТ Р 34.10 к электронной цифровой подписи.

Стандарт терминологически и концептуально увязан с международными стандартами ИСО 2382–2, ИСО/МЭК 9796. серии ИСО/МЭК 14888 и серии ИСО/МЭК 10118.

Хэш-функция – это труднообратимое преобразование данных (односторонняя функция), реализуемое, как правило, средствами симметричного шифрования со связыванием блоков. Результат шифрования последнего блока (зависящий от всех предыдущих) и служит результатом хэш-функции.

Поскольку подписываемые документы — переменного (и как правило достаточно большого) объёма, в схемах ЭП зачастую подпись ставится не на сам документ, а на его хэш. Для вычисления хэша используются криптографические хэш-функции, что гарантирует выявление изменений документа при проверке подписи. Хэш-функции не являются частью алгоритма ЭП, поэтому в схеме может быть использована любая надёжная хэш-функция.

Использование хэш-функций дает следующие преимущества:

- вычислительная сложность. Обычно хэш цифрового документа делается во много раз меньшего объёма, чем объём исходного документа, и алгоритмы вычисления хэша являются более быстрыми, чем алгоритмы ЭП. Поэтому формировать хэш документа и подписывать его получается намного быстрее, чем подписывать сам документ.

- совместимость. Большинство алгоритмов оперирует со строками бит данных, но некоторые используют другие представления. Хэш-функцию можно использовать для преобразования произвольного входного текста в подходящий формат.

- целостность. Без использования хэш-функции большой электронный документ в некоторых схемах нужно разделять на достаточно малые блоки для применения ЭП. При верификации невозможно определить, все ли блоки получены и в правильном ли они порядке.

Использование хэш-функции не обязательно при электронной подписи, а сама функция не является частью алгоритма ЭП, поэтому хэш-функция может использоваться любая или не использоваться вообще.

Примечание: в большинстве ранних систем ЭП использовались функции с секретом, которые по своему назначению близки к односторонним функциям. Такие системы уязвимы к атакам с использованием открытого ключа, так как, выбрав произвольную цифровую подпись и применив к ней алгоритм верификации, можно получить исходный текст. Чтобы избежать этого, вместе с цифровой подписью используется хэш-функция, то есть, вычисление подписи осуществляется не относительно самого документа, а относительно его хэша. В этом случае в результате верификации можно получить только хэш исходного текста, следовательно, если используемая хэш-функция криптографически стойкая, то получить исходный текст будет вычислительно сложно, а значит атака такого типа становится невозможной.

ГОСТ Р 34.10 содержит описание процессов формирования и проверки электронной подписи, реализуемой с использованием операций в группе точек эллиптической кривой, определенной над конечным простым полем.

Необходимость разработки стандарта вызвана потребностью в реализации электронной подписи разной степени стойкости в связи с повышением уровня развития вычислительной техники. Стойкость электронной подписи основывается на сложности вычисления дискретного логарифма в группе точек эллиптической кривой, а также на стойкости используемой хэш-функции по ГОСТ Р 34.11.

Электронная подпись – это специфический электронный реквизит, подтверждающий целостность и неизменность визируемых данных (в т.ч. документации). Она выступает средством контроля подлинности электронных данных и подтверждения ее авторства.

Законодательством установлены 2 типа электронного визирования: простая и усиленная (неквалифицированная или квалифицированная) подписи.

Простой электронной подписью (ПЭП) называют визирование в электронном формате, подтверждающее факт создания данной визы конкретным лицом с помощью различных способов идентификации (паролей, кодов).

Особенностью ПЭП служит то обстоятельство, что такая идентификация лишь определяет лицо, подписавшее документ, и не предоставляет возможности установления неизменности визы и подтвержденных ею сведений после заверения.

Следует также отметить некоторые нестыковки, например на сайте Росстандарта указано, что ГОСТ 34.311 имеет одинаковую силу с ГОСТ Р 34.11 «в связи с идентичностью».

Комплекс стандартов на обмен информацией (КС ОИ) изначально определяет низкоуровневые технические и технологические вопросы интерфейсного характера и формализации в области передачи данных.

Комплекс стандартов взаимосвязь открытых систем (КС ВОС) определяет технические и технологические вопросы взаимодействия информационных систем. Практически весь комплекс стандартов создан методом прямого применения стандартов ИСО и МЭК, что обеспечивает его гармонизацию с международными стандартами в области терминологии и концепций.

ВЫВОДЫ

Стандарты серии ГОСТ Р ИСО 15536, регламентирующие требования к компьютерному моделированию выполнения эргономических требований с помощью компьютерных манекенов и моделей тела, а также правила верификации функций и валидации размеров компьютерного манекена для систем моделирования. Эта серия стандартов представляется очень востребованной для использования в САПР, поэтому считаем целесообразным провести пересмотр стандартов этой серии с учетом требований, предъявляемых к включению нормативных документов в состав документов по стандартизации оборонной продукции. Это позволит легитимно осуществлять проверку эргономических требований непосредственно в системах проектирования и в некоторых случаях действительно отказаться от изготовления физических (материальных) макетов.

Направление стандартизации «Информационная технология» (или «Информационные технологии» как указаны в некоторых стандартах), если считать за направление область стандартизации, указываемую после номера стандарта), представляет собой несистематизированную совокупность межгосударственных стандартов (ГОСТ), национальных стандартов (ГОСТ Р) и национальных стандартов, созданных методом прямого применения стандартов ИСО и МЭК (ГОСТ Р ИСО/МЭК).

КС АС требует вывода из системы 34 и требует переосмысления совместно системой стандартов ЕСС АСУ и ЕСПД, а также стандартами САПР.

Список использованных источников и литературы

1. Баранов Д.А., Будкин Ю.В., Миронов А.Н., Ниязова Ю.М Совершенствование процесса создания наукоемких изделий ракетно-космического машиностроения на основе перехода к платформенному рискориентированному проектированию с учетом неполной информации о временных, финансовых и санкционно-технических ограничениях // Технология машиностроения. 2021. № 3. С. 54–62.
2. Анисимов Н.Р., Фролов В.А., Будкин Ю.В., Князев А.В. Новые подходы к обеспечению безопасности роботов в промышленной среде // Информационно-экономические аспекты стандартизации и технического регулирования. 2022. № 1 (65). С. 12–17.
3. Будкин Ю.В., Соколов Ю.А., Фролов В.А. Алгоритмы искусственного интеллекта в естественных и искусственных источниках излучения. Часть 2. Излучение высококонцентрированными источниками нагрева // Информационно-экономические аспекты стандартизации и технического регулирования. 2022. № 5 (69). С. 27–34.
4. Бурый А.С. Цифровые двойники как основа парадигмы развития прикладных информационных систем // Информационно-экономические аспекты стандартизации и технического регулирования, 2022. № 6 (70). С. 24-30.
5. Постановление Правительства Москвы от 31 октября 2006 г. № 860-ПП «О внедрении современных технологий автоматизированного управления дорожным движением в городе Москве».

PROVISION OF INFORMATION SYSTEMS AND PROCESSES FOR THE DEVELOPMENT AND IMPLEMENTATION OF SCIENCE-INTENSIVE TECHNOLOGY WITH INTERSECTORAL COMPLEXES OF STANDARDS.

Part 2. System "Information Technology"

Budkin Yu.V., Doctor of Engineering Sciences, FSBI "RSI"

The article presents the results of research on interbranch systems and sets of standards in order to update and use them to provide information systems and processes for the development and implementation of high technology. The second part is aimed at researching the GOST R 34.XXX "Information Technology" system, which consists of four unrelated sets of standards. It has been established that for enterprises of the industrial complex, sets of standards for "Automated systems" and "Cryptographic information protection" are in demand.

The set of standards for "Automated Systems" has been updated in the field of application of system documentation in various types of activities (management, research, design, etc.), including their combinations, and establishes requirements for the types, name, completeness and designation of documents developed at the stages creating AS. The development of standards that are not included in the "Automated Systems" complex, but which establish requirements for NPP testing, is noted. It is advisable to update the set of standards for "Automated Systems" together with the update of the sets of standards: GOST 24.XXX (ESS ACS) and GOST 19.XXX (ESPD), as well as GOST 25.XXX (CAD) standards. This will solve the problem of harmonization of regulatory and technical documentation for the creation and use of automated systems in industrial enterprises. The complex of standards for "Cryptographic information protection" is the basic one for ensuring reliable authentication of the parties to the information exchange and data protection in the process of information exchange. It is proposed to harmonize the set of standards with GOST 25.XXX (CAD). This will ensure the reliability and integrity of information (including the use of digital signature algorithms) during its processing, storage and transmission.

Keywords: information systems and processes, mechanical engineering, standard, automated control system, computer-aided design system

References

1. Baranov D.A., Budkin Yu.V., Mironov A.N., Niyazova Yu.M. Improvement of the process of creation of science-intensive products of rocket and space engineering on the basis of transition to platform risk-oriented design taking into account incomplete information about time and financial action and technical limitations // Engineering Technology, 2021, no. 3, pp. 54–62.
2. Anisimov N.R., Frolov V.A., Budkin Yu.V., Knyazev A.V. New approaches to ensuring the safety of robots in the industrial environment // Information and economic aspects of standardization and technical regulation, 2022, no. 1 (65), pp. 12–17.
3. Budkin Yu.V., Sokolov Yu.A., Frolov V.A. Artificial intelligence algorithms in natural and artificial radiation sources. Part 2. Radiation from highly concentrated heating sources // Information and economic aspects of standardization and technical regulation, 2022, no. 5 (69), pp. 27–34.
4. Bury A.S. Digital twins as the basis of the paradigm of the development of applied information systems // Information and economic aspects of standardization and technical regulation, 2022, no. 6 (70), pp. 24–30.
5. Decree of October 31, 2006 no. 860-PP "On the introduction of modern technologies for automated traffic control in the city of Moscow".