Учебное пособие

ПИТЕР

Юрий Андреевич Родичев

Информационная безопасность

Национальные стандарты Российской Федерации

2-е издание

РЕКОМЕНДОВАНО ДЛЯ СТУДЕНТОВ, ОБУЧАЮЩИХСЯ ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ 10.00.00 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Юрий Андреевич Родичев

Информационная безопасность. Национальные стандарты Российской Федерации

Серия «Учебник для вузов (Питер)»

Текст предоставлен правообладателем
http://www.litres.ru/pages/biblio_book/?art=41130803
Информационная безопасность. Национальные стандарты Российской Федерации / Родичев Юрий: Питер; Санкт-Петербург; 2019
ISBN 978-5-4461-1275-3

Аннотация

В учебном пособии рассмотрено более 230 действующих открытых документов национальной системы стандартизации Российской Федерации, включая международные и межгосударственные стандарты в области информационной безопасности.

Учебное пособие предназначено для студентов высших учебных заведений, обучающихся по специальностям в области информационной безопасности, слушателей курсов повышения квалификации по проблемам защиты информации, а также

специалистов и руководителей в области разработки и эксплуатации информационно-телекоммуникационных систем и обеспечения информационной безопасности.

Рекомендовано к изданию редакционно-издательским советом федерального государственного автономного образовательного учреждения высшего образования «Самарский национальный исследовательский университет имени академика С. П. Королева» в качестве учебного пособия для студентов, обучающихся по программам высшего образования укрупненной группы специальностей и направлений подготовки 10.00.00 «Информационная безопасность».

Содержание

Юрий Родичев
Информационная безопасность. Национальные стандарты Российской Федерации

Моей любимой внучке Алисе посвящаю.

Не грусти. Рано или поздно все станет понятно, все станет на свои места и выстроится в единую красивую схему, как кружева. Станет понятно, зачем все было нужно, потому что все будет правильно.
Льюис Кэрролл. Алиса в Стране чудес

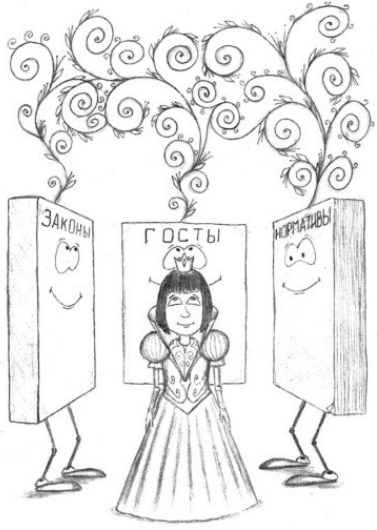
Рецензенты:

доктор педагогических наук, профессор кафедры корпоративных информационных систем, электронных сервисов и интеллектуальных информационных технологий Самарского государственного экономического университета

А. Г. Абросимов;

доктор технических наук, профессор Самарского национального исследовательского университета имени академика С. П. Королева

В. С. Кузьмичев.



Перечень сокращений

АС – автоматизированная система

АСЗИ – АС в защищенном исполнении

АСУ ТП – автоматизированная система управления производственными и технологическими процессами

ГИС – государственная информационная система

ЗБ – задание по безопасности

ИБ – информационная безопасность

ИС ОП – информационная система общего пользования

ИСПДн – информационная система персональных данных

ИТ – информационная технология

ИКТ – информационно-коммуникационные технологии

ИИСМиОБП – интегрированная интеллектуальная система мониторинга и обеспечения безопасности предприятия

ИСБ – интегрированные системы безопасности

КСБ – комплексные системы безопасности

КСЗ – комплекс средств защиты

МЭ – межсетевой экран

НДВ – недекларированная возможность

НСД – несанкционированный доступ

ОУД – оценочный уровень доверия

ОО – объект оценки

ПЗ – профиль защиты

ПО – программное обеспечение

ПС – программное средство

РД – руководящий документ

РИД – результат интеллектуальной деятельности

САВЗ – средство антивирусной защиты

СВТ – средство вычислительной техники

СЗИ – средство защиты информации

СКН – средства контроля съемных машинных носителей информации

СОВ – система обнаружения вторжений

СДЗ – средства доверенной загрузки

СМИБ – система менеджмента ИБ

СВТ – средство вычислительной техники

СоПД – составной пакет доверия

СКУД – система контроля и управления доступом

СОС – система охранной сигнализации

СОТ – система охранная телевизионная

СТС – система тревожной сигнализации

СКЗИ – средство криптографической защиты информации

СРД – система разграничения доступа

СЦН – система централизованного наблюдения

ФТБ – функциональные требования безопасности

Введение

В современном обществе информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности человека. Их эффективное применение является фактором ускорения экономического развития государства и формирования информационного общества.

Учитывая масштабы проникновения информационных технологий в повседневную жизнь граждан, организаций и органов власти всех уровней, а также высокий уровень зависимости создаваемых в стране информационных систем от импортных аппаратно-программных средств, особенно актуальным становится вопрос обеспечения необходимого уровня информационной безопасности страны в современном глобальном информационном мире.

Расширение областей применения информационных технологий порождает новые информационные угрозы. Возрастают масштабы компьютерной преступности, увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека, в том числе при обработке персональных данных с использованием информационных технологий.

В «Стратегии национальной безопасности Российской Федерации», утвержденной Указом Президента Российской

Федерации от 31.12.2015 г. № 683, отмечается появление новых форм противоправной деятельности с использованием информационно-коммуникационных технологий и уделяется особое внимание обеспечению информационной безопасности с учетом стратегических национальных приоритетов.

Важнейшим элементом комплексной системы защиты информации является нормативно-правовое обеспечение, заключающееся в разработке нормативных правовых актов, регламентирующих отношения в информационной сфере, а также нормативных методических документов по конкретным вопросам обеспечения информационной безопасности. Меры нормативно-правовой поддержки регулирования вопросов защиты информации в Российской Федерации определяются на основании:

- международных договоров и соглашений;
- законов Российской Федерации;
- указов и распоряжений Президента Российской Федерации;
- нормативных документов Правительства Российской Федерации;
- технических регламентов;
- национальных стандартов и стандартов организаций;
- нормативных правовых актов уполномоченных федеральных органов исполнительной власти.

Низшим звеном в иерархической системе документов яв-

ляются нормативные акты уровня учреждений, необходимость принятия которых отмечается в ряде нормативно-правовых документов федерального уровня.

Как отмечено в «Доктрине информационной безопасности Российской Федерации», утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646, отсутствие международных правовых норм, регулирующих межгосударственные отношения в информационном пространстве, а также механизмов и процедур их применения, учитывающих специфику информационных технологий, затрудняет формирование системы международной информационной безопасности, направленной на достижение стратегической стабильности и равноправного стратегического партнерства.

В последние годы в Российской Федерации существенно обновлена нормативно-правовая база в сфере информационных технологий и защиты информации. Значительные изменения произошли также и в национальной системе стандартизации и технического регулирования.

Все работы по стандартизации в России осуществляются на основе принятых Федеральных законов: «О техническом регулировании» от 27 декабря 2002 г. № 184-ФЗ и «О стандартизации в Российской Федерации» от 29 июня 2015 г. № 162-ФЗ, а также утвержденной распоряжением Правительства Российской Федерации от 24 сентября 2012 г. № 1762-р Концепцией развития национальной системы стан-

дартизации Российской Федерации на период до 2020 г.

После принятия закона 184-ФЗ от 27 декабря 2002 г. утратили силу два ранее принятых закона: «О сертификации продукции и услуг» от 10 июня 1993 г. № 5151-1 и «О стандартизации» от 10 июня 1993 г. № 5154-1. Все вопросы, связанные с функционированием национальной системы стандартизации, были перенесены в закон «О техническом регулировании». Однако в 2015 г. вновь был принят отдельный закон, регулирующий вопросы стандартизации в Российской Федерации (№ 162-ФЗ).

Основной причиной принятия нового закона «О стандартизации в Российской Федерации» явилась необходимость совершенствования государственного регулирования в сфере стандартизации, поскольку сложившаяся национальная система стандартизации в рамках закона о техническом регулировании не отвечала современным экономическим условиям. Национальное законодательство в сфере стандартизации нуждалось в коренной модернизации в соответствии с приоритетными направлениями развития стандартизации, закрепленными Концепцией развития национальной системы стандартизации в Российской Федерации от 24 сентября 2012 г.

В целях исключения дублирования областей применения Федерального закона «О техническом регулировании» и Федерального закона «О стандартизации в Российской Федерации» из сферы технического регулирования исключены во-

просы разработки и принятия стандартов национальной системы стандартизации. Однако вопросы применения на добровольной основе стандартов в целях обеспечения выполнения требований технических регламентов оставлены в предметной области закона «О техническом регулировании».

Закон «О техническом регулировании» регулирует отношения, возникающие при:

• разработке, принятии, применении и исполнении обязательных требований к продукции, в том числе зданиям и сооружениям, или к продукции и связанным с требованиями к продукции процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации;

• 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;

• оценке соответствия.

Одним из основных принципов стандартизации является добровольность применения документов по стандартизации.

В «Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы», утвержденной Указом Президента Российской Федерации от 9 мая 2017 г.

№ 203, подчеркивается необходимость осуществления интеграции российских стандартов в сфере информационных и коммуникационных технологий в соответствующие международные стандарты, а также обеспечения гармонизации межгосударственной и национальной систем стандартов в данной сфере. В настоящее время в России наряду с отечественной нормативной базой широко используются международные стандарты в области информационных технологий и защиты информации. Многие международные стандарты приняты и введены в действие в России в качестве национальных стандартов.

В соответствии с международными и национальными стандартами для обеспечения информационной безопасности компании необходимо:

1. Определить цели обеспечения информационной безопасности.

2. Создать эффективную систему управления информационной безопасностью.

3. Определить совокупность количественных и качественных показателей для оценки соответствия уровня информационной безопасности заявленным целям.

4. Использовать определенный инструментарий для реализации процесса обеспечения информационной безопасности и оценки уровня ее текущего состояния.

5. Применять эффективные методики анализа и управления рисками, позволяющие объективно оценить состояние

защищенности активов.

Все эти аспекты обеспечения информационной безопасности охватываются системой национальных стандартов Российской Федерации. Поэтому важнейшим условием повышения уровня информационной безопасности является подготовка высококвалифицированных специалистов в области защиты информации, обладающих необходимыми компетенциями и знаниями нормативных документов и национальных стандартов. В «Доктрине информационной безопасности Российской Федерации» 2016 г. в состав основных направлений обеспечения информационной безопасности России включено развитие кадрового потенциала в области обеспечения информационной безопасности и применения информационных технологий, а также обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности.

Целью данного учебного пособия является рассмотрение важнейших открытых действующих документов национальной системы стандартизации, включая международные и межгосударственные стандарты в области информационной безопасности по состоянию на начало 2019 г. С различной степенью подробности в пособии рассмотрено более 230 документов, действующих в Российской Федерации. Некоторые важнейшие стандарты описаны в пособии достаточно

подробно. Описания некоторых стандартов ограничиваются только целями их принятия, предметом регулирования и названиями разделов, что дает возможность получить представление о содержании стандарта в целом. Изучение данного учебного пособия дает возможность получить представление обо всей системе стандартов в области информационной безопасности. Это позволит оптимизировать поиск решения конкретных практических задач по защите информации. После нахождения возможного решения задачи необходимо будет обратиться к первоисточникам и изучить полный текст соответствующего стандарта или серии стандартов.

Все национальные стандарты, описанные в учебном пособии, сгруппированы по направлениям:

- основополагающие стандарты национальной системы стандартизации и стандартизации в области защиты информации;
- стандарты по менеджменту информационной безопасности;
- стандарты по безопасности информационно-телекоммуникационных систем;
- оценочные стандарты;
- стандарты по безопасности в финансовой сфере;
- стандарты по биометрии;
- стандарты по криптографии;
- стандарты по интегрированным системам безопасности.

В главе 1 рассматриваются национальные стандарты, устанавливающие основы национальной системы стандартизации Российской Федерации и основы стандартизации в сфере защиты информации.

Глава 2 посвящена комплексу стандартов по менеджменту информационной безопасности.

Глава 3 посвящена рассмотрению стандартов в области защиты информации в информационно-телекоммуникационных системах.

В главе 4 рассмотрены стандарты в области оценки соответствия требованиям безопасности.

В главе 5 описаны стандарты, регулирующие процессы защиты информации в финансовой сфере. Здесь также рассмотрены стандарты Банка России.

Глава 6 посвящена рассмотрению стандартов в области биометрии.

Глава 7 посвящена документам в области криптографической защиты информации.

Глава 8 посвящена стандартам по комплексным и интегрированным системам безопасности.

Отзывы, пожелания и замечания по данному учебному пособию можно направлять на кафедру безопасности информационных систем Самарского национального исследовательского университета имени академика С. П. Королева по адресу: 443086, г. Самара, Московское шоссе, 34, а также на электронную почту автора rodichev@ssau.ru.

Благодарности

Выражаю благодарность рецензентам учебного пособия Абросимову Александру Григорьевичу и Кузьмичеву Венедикту Степановичу за ценные советы по содержанию материалов.

Выражаю благодарность коллективу кафедры безопасности информационных систем Самарского университета имени академика С. П. Королева, в котором родилась идея подготовки такого учебного пособия, и лично заведующему кафедрой Осипову Михаилу Николаевичу за всестороннюю поддержку.

«Какой толк в книге, – подумала Алиса, – если в ней нет ни картинок, ни разговоров?» В связи с этим выражаю благодарность художнику Гридневу Андрею Сергеевичу за остроумные иллюстрации к главам пособия, которые повысили толк книги.

Большое спасибо руководителю проектной группы «Компьютерная и научно-популярная литература» Юлии Сергиенко за профессионализм и доброе отношение при подготовке к изданию книги.

Искреннее спасибо замечательному ведущему редактору редакции компьютерной и научно-популярной литературы Кристине Тульцевой за оперативность и профессионализм в доработке рукописи при подготовке к изданию.

Благодарю всех сотрудников издательского дома «Питер», принявших участие в редактировании рукописи и подготовке книги к изданию.

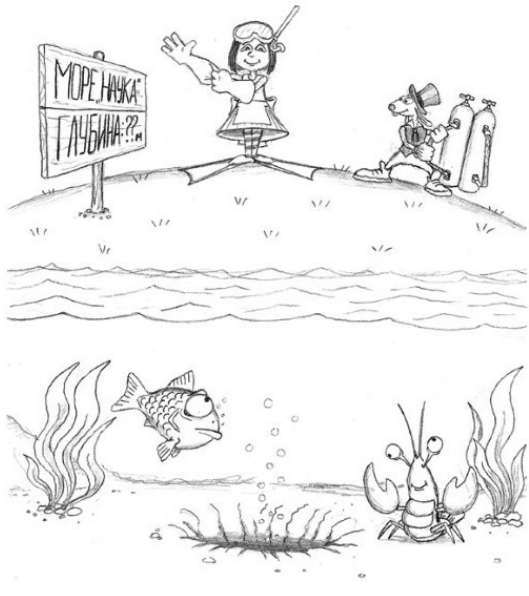
Глава 1
Основы технического регулирования и стандартизации в Российской Федерации

– Начните сначала, – серьезно сказал Король, – и читайте, пока не дойдете до конца; тогда остановитесь.

– …А уж кто хочет по-настоящему углубиться в науку, тот должен добраться до самого дна! Вот это и называется Законченное Низшее Образование! Но, конечно, это не каждому дано!..

– Мне вот так и не удалось по-настоящему углупиться! Не хватило меня на это. Так я и остался при высшем образовании…

Льюис Кэрролл. Алиса в Стране чудес



1.1. Общие замечания

Основным правовым документом в области технического регулирования и стандартизации до 2015 г. являлся Федеральный закон Российской Федерации «О техническом регулировании» № 184-ФЗ. Он был принят 27.12.2002 г. и вступил в силу с 1 июля 2003 г. В связи с его принятием утратил силу ряд ранее принятых законов и нормативных актов в области стандартизации и сертификации продукции и услуг. Среди таких документов, в частности, следует отме-

тить Федеральные законы Российской Федерации № 5151-1 от 10.06.1993 г. «О сертификации продукции и услуг» и № 5154-1 от 10.06.1993 г. «О стандартизации».

Одной из причин принятия закона явилась подготовка к вступлению Российской Федерации во Всемирную торговую организацию (ВТО), что, в свою очередь, потребовало реформирования существующей системы технического регулирования в соответствии с требованиями ВТО. В государствах – членах ВТО обязательные для применения требования к продукции устанавливаются в технических регламентах, утверждаемых органами власти, а национальные стандарты являются добровольными для применения. В России до принятия закона «О техническом регулировании» разделения требований на обязательные и применяемые на добровольной основе не существовало. Большинство требований носило обязательный характер и устанавливалось в государственных стандартах и нормативных документах федеральных органов исполнительной власти.

Федеральный закон «О техническом регулировании» № 184-ФЗ заложил основу принципиально новой системы сертификации и стандартизации в Российской Федерации. Фактически закон заложил основу для создания двухуровневой системы нормативных документов: технических регламентов, которые содержат обязательные требования безопасности, и добровольно применяемых стандартов. Иными словами, стандарты, даже государственные, перестали быть

обязательными для субъектов хозяйствующей деятельности. Сам термин «государственный стандарт» выведен из обращения. Вместо него введены новые понятия: «национальный стандарт», «международный стандарт», «региональный стандарт», «стандарт организации». Выведен из обращения также термин «отраслевой стандарт». Изменение правового статуса документов по стандартизации и самого понятия «стандартизация» обусловлено ориентацией российского законодателя на международную практику и сложившийся практический международный опыт в этой сфере деятельности.

Федеральным органом исполнительной власти Российской Федерации в области технического регулирования является Федеральное агентство по техническому регулированию и метрологии (Росстандарт, сайт агентства: www.gost.ru), созданное Указом Президента Российской Федерации от 20 мая 2004 г. № 649 «Вопросы структуры федеральных органов исполнительной власти». Агентство ведет свою деятельность в соответствии с Положением, утвержденным Постановлением Правительства Российской Федерации от 17 июня 2004 г. № 294.

Основными задачами агентства являются:

- реализация функций национального органа по стандартизации;
- обеспечение единства измерений;
- осуществление государственного контроля (надзора) за

соблюдением требований технических регламентов и обязательных требований стандартов;

• создание и ведение федерального информационного фонда технических регламентов и стандартов и единой информационной системы по техническому регулированию;

• оказание государственных услуг в сфере стандартизации, технического регулирования и метрологии.

В соответствии с Постановлением Госстандарта РФ от 30.01.2004 г. № 4 «О национальных стандартах Российской Федерации» со дня вступления в силу Федерального закона № 184-ФЗ «О техническом регулировании» национальными стандартами признаются государственные и межгосударственные стандарты, принятые Госстандартом России до 1 июля 2003 г. Впредь до вступления в силу соответствующих технических регламентов установленные ранее требования к продукции подлежат обязательному исполнению только в части, соответствующей целям:

• защиты жизни или здоровья граждан, имущества физических или юридических лиц, государственного или муниципального имущества;

• охраны окружающей среды, жизни или здоровья животных и растений;

• предупреждения действий, вводящих в заблуждение приобретателей.

Разработка документов национальной системы стандартизации ведется в рамках технических комитетов, создаваемых Росстандартом. В данном учебном пособии рассмотрены документы по стандартизации, разработанные следующими техническими комитетами:

- ТК 362 «Защита информации»;
- ТК 26 «Криптографическая защита информации»;
- ТК 22 «Информационные технологии»;
- ТК 355 «Технологии автоматической идентификации и сбора данных и биометрия»;
- ТК 098 «Биометрия и биомониторинг»;
- ТК 122 «Стандарты финансовых операций»;
- ТК 12 «Методология стандартизации»;
- ТК 536 «Методология межгосударственной стандартизации».

1.2. Федеральный закон Российской Федерации «О стандартизации в Российской Федерации»

Федеральный закон «О стандартизации в Российской Федерации» от 29 июня 2015 г. № 162-ФЗ устанавливает правовые основы стандартизации в Российской Федерации, в том числе функционирования национальной системы стандартизации, и направлен на обеспечение проведения единой государственной политики в сфере стандартизации. Он регулирует отношения в сфере стандартизации, включая отношения, возникающие при разработке, утверждении, изменении, отмене, опубликовании и применении документов по стандартизации. Закон полностью вступил в силу с 1 июля 2016 г., а отдельные его статьи введены в действие с 29 сентября 2015 г.

Закон вводит ряд понятий в предметной области.

Документ по стандартизации – документ, в котором для добровольного и многократного применения устанавливаются общие характеристики объекта стандартизации, а также правила и общие принципы в отношении объекта стандартизации, за исключением случаев, если обязательность применения документов по стандартизации устанавливается настоящим Федеральным законом.

Документы, разрабатываемые и применяемые в национальной системе стандартизации – национальный стандарт Российской Федерации, в том числе основополагающий национальный стандарт Российской Федерации, и предварительный национальный стандарт Российской Федерации, а также правила стандартизации, рекомендации по стандартизации, информационно-технические справочники.

Информационно-технический справочник – документ национальной системы стандартизации, утвержденный федеральным органом исполнительной власти в сфере стандартизации, содержащий систематизированные данные в определенной области и включающий в себя описание технологий, процессов, методов, способов, оборудования и иные данные.

Национальная система стандартизации – механизм обеспечения согласованного взаимодействия участников работ по стандартизации.

Национальный стандарт – документ по стандартизации, который разработан участником или участниками работ по стандартизации, по результатам экспертизы в техническом комитете по стандартизации или проектном техническом комитете по стандартизации утвержден федеральным органом исполнительной власти в сфере стандартизации и в котором для всеобщего применения устанавливаются общие характеристики объекта стандартизации, а также правила и

общие принципы в отношении объекта стандартизации.

Основополагающий национальный стандарт – национальный стандарт, разработанный и утвержденный федеральным органом исполнительной власти в сфере стандартизации, устанавливающий общие положения, касающиеся выполнения работ по стандартизации, а также виды национальных стандартов.

Предварительный национальный стандарт – документ по стандартизации, который разработан участником или участниками работ по стандартизации, по результатам экспертизы в техническом комитете по стандартизации или проектном техническом комитете по стандартизации утвержден федеральным органом исполнительной власти в сфере стандартизации и в котором для всеобщего применения устанавливаются общие характеристики объекта стандартизации, а также правила и общие принципы в отношении объекта стандартизации на ограниченный срок в целях накопления опыта в процессе применения предварительного национального стандарта для возможной последующей разработки на его основе национального стандарта.

Свод правил – документ по стандартизации, утвержденный федеральным органом исполнительной власти или Государственной корпорацией по атомной энергии «Росатом» и содержащий правила и общие принципы в отношении процессов в целях обеспечения соблюдения требований технических регламентов.

Стандарт организации – документ по стандартизации, утвержденный юридическим лицом, в том числе государственной корпорацией, саморегулируемой организацией, а также индивидуальным предпринимателем для совершенствования производства и обеспечения качества продукции, выполнения работ, оказания услуг.

Стандартизация – деятельность по разработке (ведению), утверждению, изменению (актуализации), отмене, опубликованию и применению документов по стандартизации и иная деятельность, направленная на достижение упорядоченности в отношении объектов стандартизации.

Технические условия – вид стандарта организации, утвержденный изготовителем продукции или исполнителем работы, услуги.

В соответствии со **статьей 6** закона порядок стандартизации в отношении оборонной продукции по государственному оборонному заказу, продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, продукции, сведения о которой составляют государственную тайну, а также процессов и иных объектов стандартизации, связанных с такой продукцией, устанавливается Правительством Российской Федерации.

Закон устанавливает следующие принципы стандартизации:

1) добровольность применения документов по стандартизации;

2) обязательность применения документов по стандартизации в отношении объектов стандартизации, предусмотренных статьей 6 закона, а также включенных в определенный Правительством Российской Федерации перечень документов по стандартизации, обязательное применение которых обеспечивает безопасность дорожного движения при его организации на территории Российской Федерации;

3) обеспечение комплексности и системности стандартизации, преемственности деятельности в сфере стандартизации;

4) обеспечение соответствия общих характеристик, правил и общих принципов, устанавливаемых в документах национальной системы стандартизации, современному уровню развития науки, техники и технологий, передовому отечественному и зарубежному опыту;

5) открытость разработки документов национальной системы стандартизации, обеспечение участия в разработке таких документов всех заинтересованных лиц, достижение консенсуса при разработке национальных стандартов;

6) установление в документах по стандартизации требований, обеспечивающих возможность контроля за их выполнением;

7) унификация разработки, утверждения, изменения, отмены, опубликования и применения документов по стандар-

тизации;

8) соответствие документов по стандартизации действующим на территории Российской Федерации техническим регламентам;

9) непротиворечивость национальных стандартов друг другу;

10) доступность информации о документах по стандартизации с учетом ограничений, установленных нормативными правовыми актами Российской Федерации в области защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа.

К документам в области стандартизации, используемым на территории Российской Федерации, относятся:

1) документы национальной системы стандартизации;

2) общероссийские классификаторы;

3) стандарты организаций, в том числе технические условия;

4) своды правил;

5) документы по стандартизации, которые устанавливают обязательные требования в отношении некоторых объектов стандартизации (оборонная продукция, продукция, используемая для защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с за-

конодательством Российской Федерации иной информации ограниченного доступа, продукции, сведения о которой составляют государственную тайну, и т. п.).

Документы национальной системы стандартизации не должны противоречить международным договорам Российской Федерации, федеральным законам, актам Президента Российской Федерации, актам Правительства Российской Федерации, нормативным правовым актам федеральных органов исполнительной власти и нормативным правовым актам Государственной корпорации по атомной энергии «Росатом», изданным в соответствии с установленными полномочиями. Разработчиками документов национальной системы стандартизации являются участники работ по стандартизации (в том числе физические лица).

При разработке национальных стандартов международные стандарты используются в качестве основы, за исключением случаев, если такое использование признано невозможным вследствие несоответствия требований международных стандартов климатическим и географическим особенностям Российской Федерации, техническим и/или технологическим особенностям или по иным основаниям либо Российская Федерация в соответствии с установленными процедурами выступала против утверждения международного стандарта или отдельного его положения.

Документы национальной системы стандартизации при-

меняются на добровольной основе одинаковым образом и в равной мере независимо от страны и/или места происхождения продукции (товаров, работ, услуг), если иное не установлено законодательством Российской Федерации.

Информационное обеспечение национальной системы стандартизации реализуется посредством ведения Федерального информационного фонда стандартов, создания и эксплуатации федеральных информационных систем, необходимых для его функционирования, официального опубликования, издания и распространения документов национальной системы стандартизации и общероссийских классификаторов. Федеральный информационный фонд стандартов является государственным информационным ресурсом.

1.3. Основы стандартизации в Российской Федерации

1.3.1. Основополагающие стандарты Российской Федерации

В соответствии с Федеральным законом «О стандартизации в Российской Федерации» в России действует Государственная система стандартизации. Законодательную и нормативную базу национальной системы стандартизации составляют:

- Федеральный закон «О стандартизации в Российской Федерации»;
- нормативно-правовые акты Правительства РФ по вопросам стандартизации;
- основополагающие стандарты Национальной системы стандартизации.

Основополагающие вопросы организации и практической деятельности в области стандартизации в Российской Федерации регламентированы в комплексе основополагающих национальных стандартов, правил и рекомендаций:

ГОСТ Р 1.0–2012 «Стандартизация в Российской Феде-

рации. Основные положения (с Изменением № 1)».

ГОСТ Р 1.1–2013 «Стандартизация в Российской Федерации. Технические комитеты по стандартизации. Правила создания и деятельности».

ГОСТ Р 1.2–2016 «Стандартизация в Российской Федерации. Стандарты национальные Российской Федерации. Правила разработки, утверждения, обновления, внесения поправок, приостановки действия и отмены».

ГОСТ Р 1.4–2004 «Стандартизация в Российской Федерации. Стандарты организаций. Общие положения».

ГОСТ Р 1.5–2012 «Стандартизация в Российской Федерации. Стандарты национальные. Правила построения, изложения, оформления и обозначения (с Поправкой, с Изменением № 1)».

ГОСТ Р 1.6–2013 «Стандартизация в Российской Федерации. Проекты стандартов. Правила организации и проведения экспертизы».

ГОСТ Р 1.7–2014 «Стандартизация в Российской Федерации. Стандарты национальные. Правила оформления и обозначения при разработке на основе применения международных стандартов (с Изменением № 1)».

ГОСТ Р 1.8–2011 «Стандартизация в Российской Федерации. Стандарты межгосударственные. Правила проведения в Российской Федерации работ по разработке, применению, обновлению и прекращению применения».

ГОСТ Р 1.9–2004 «Стандартизация в Российской Федера-

ции. Знак соответствия национальным стандартам Российской Федерации. Изображение. Порядок применения».

ГОСТ Р 1.10–2004 «Стандартизация в Российской Федерации. Правила стандартизации и рекомендации по стандартизации. Порядок разработки, утверждения, изменения, пересмотра и отмены».

ГОСТ Р 1.12–2004 «Стандартизация в Российской Федерации. Термины и определения».

ГОСТ Р 1.13-2004 «Стандартизация в Российской Федерации. Уведомления о проектах документов в области стандартизации. Общие требования (с Изменением № 1)».

ГОСТ Р 1.14–2017 «Стандартизация в Российской Федерации. Программа разработки национальных стандартов. Требования к структуре, правила формирования, утверждения и контроля за реализацией».

ГОСТ Р 1.15–2017 «Стандартизация в Российской Федерации. Службы стандартизации в организациях. Правила создания и функционирования».

ГОСТ Р 1.16–2011 «Стандартизация в Российской Федерации. Стандарты национальные предварительные. Правила разработки, утверждения, применения и отмены».

ГОСТ Р 1.17–2017 «Стандартизация в Российской Федерации. Эксперт по стандартизации. Общие требования».

ПР 50.1.008–2013 «Организация и проведение работ по международной стандартизации в Российской Федерации».

ПР 50.1.025–2007 «Методика формирования перечня на-

циональных стандартов и/или сводов правил, в результате применения которых на добровольной основе обеспечивается соблюдение требований технического регламента».

ПР 50.1.074–2004 «Подготовка проектов национальных стандартов Российской Федерации и проектов изменений к ним к утверждению, регистрации и опубликованию. Внесение поправок в стандарты и подготовка документов для их отмены».

Р 50.1.004–2011 «Подготовка межгосударственных стандартов для принятия и применения в Российской Федерации в качестве национальных стандартов».

Р 50.1.039–2002 «Разработка, обновление и отмена правил и рекомендаций по стандартизации, метрологии, сертификации, аккредитации и каталогизации».

Р 50.1.057–2006 «Комплектование, хранение, ведение и учет документов Федерального информационного фонда технических регламентов и стандартов и порядок предоставления пользователям информационной продукции и услуг. Основные положения».

Р 50.1.058–2011 «Методика оценки стоимости разработки и экспертизы национальных стандартов Российской Федерации».

Р 50.1.075–2011 «Разработка стандартов на термины и определения».

Представителями государств бывшего СССР 13 марта 1992 г. было подписано Соглашение о проведении согла-

сованной политики в области стандартизации. В нем заложены основы системы межгосударственной стандартизации. На межправительственном уровне был создан Межгосударственный совет по стандартизации, метрологии и сертификации (МГС). В области межгосударственной стандартизации действуют следующие основополагающие документы:

ГОСТ 1.0–2015 «Межгосударственная система стандартизации (МГСС). Основные положения».

ГОСТ 1.1–2002 «Межгосударственная система стандартизации. Термины и определения».

ГОСТ 1.2–2015 «Межгосударственная система стандартизации. Стандарты межгосударственные, правила и рекомендации по межгосударственной стандартизации. Правила разработки, принятия, обновления и отмены».

ГОСТ 1.3–2014 «Межгосударственная система стандартизации. Стандарты межгосударственные. Правила разработки на основе международных и региональных стандартов».

ГОСТ 1.4–2015 «Межгосударственная система стандартизации. Межгосударственные технические комитеты по стандартизации. Правила создания и деятельности».

ГОСТ 1.5–2001 «Межгосударственная система стандартизации. Стандарты межгосударственные, правила и рекомендации по межгосударственной стандартизации. Общие требования к построению, изложению, оформлению, содержанию и обозначению».

ПМГ 03–93 «Порядок регистрации и подготовки к изданию межгосударственных нормативных документов по стандартизации».

ПМГ 04–94 «Порядок распространения межгосударственных стандартов и нормативной документации Межгосударственного совета по стандартизации, метрологии и сертификации».

1.3.2. Основные положения системы стандартизации в Российской Федерации (ГОСТ Р 1.0–2012)

Национальный стандарт Российской Федерации ГОСТ Р 1.0–2012 «Стандартизация в Российской Федерации. Основные положения» введен в действие с 01.07.2013 г. взамен ранее принятого стандарта ГОСТ Р 1.0–2004.

Стандарт устанавливает основные положения по организации и проведению в Российской Федерации работ в области стандартизации, цели и принципы стандартизации, требования к документам в области стандартизации, правила их опубликования, распространения и применения, а также задачи международного сотрудничества в области стандартизации.

Стандарт устанавливает следующие принципы осуществления национальной стандартизации в Российской Федерации:

• добровольности применения заинтересованным лицом документов в области стандартизации и обязательности соблюдения указанным лицом требований, содержащихся в этих документах, в случае объявления об их использовании, а также в случае определения обязательности исполнения требований стандартов в рамках контрактных (договорных) обязательств;

• применения в установленном порядке на территории Российской Федерации международных и региональных стандартов, региональных сводов правил, стандартов иностранных государств и сводов правил иностранных государств;

• максимального учета мнения заинтересованных лиц при разработке документов в области стандартизации;

• обеспечения преемственности работ по стандартизации;

• обеспечения условий для единообразного применения документов в области стандартизации;

• открытости (прозрачности) процедур разработки документов в области стандартизации;

• обеспечения доступности документов в области стандартизации и информации о них для заинтересованных лиц;

• однозначности понимания требований, включаемых в документы в области стандартизации;

• соответствия документов в области стандартизации нормативным правовым актам Российской Федерации;

• прогрессивности и оптимальности требований докумен-

тов в области стандартизации;

• недопустимости разработки национальных стандартов Российской Федерации на объекты и аспекты стандартизации, стандартизованные на межгосударственном уровне;

• недопустимости разработки и применения национальных стандартов Российской Федерации, которые создают излишние препятствия международной торговле;

• унификации процессов разработки, хранения стандартов, а также процессов внесения в них изменений и обеспечения доступа к документам в области стандартизации;

• обеспечения системности и комплексности информационных ресурсов в области стандартизации с использованием информационных технологий;

15 обеспечения актуальности и достоверности информационных ресурсов в области стандартизации.

Раздел 5 стандарта посвящен организации работ по стандартизации и функциям национального органа по стандартизации (Федеральное агентство по техническому регулированию и метрологии – Росстандарт).

В разделах 6 и 7 описаны требования к документам в области стандартизации, порядок их опубликования и распространения.

Стандарт определяет также основные задачи международного сотрудничества в области стандартизации, а именно:

• гармонизация системы стандартизации в Российской

Федерации с международными, региональными, прогрессивными национальными системами стандартизации других стран;

• совершенствование фонда документов в области стандартизации, используемых в Российской Федерации;

• гармонизация национальных стандартов Российской Федерации с международными, региональными стандартами и национальными стандартами других стран;

• повышение качества отечественной продукции и ее конкурентоспособности на мировом рынке;

• содействие внедрению инноваций, проведению технологической модернизации и продвижению отечественной продукции на мировой рынок;

• активное привлечение представителей отечественной промышленности к разработке международных и региональных стандартов;

• разработка международных и межгосударственных стандартов на основе национальных стандартов Российской Федерации;

• улучшение нормативного обеспечения торгово-экономического и научно-технического сотрудничества Российской Федерации с другими странами и участие Российской Федерации в международном разделении труда;

• обеспечение защиты национальных интересов Российской Федерации при разработке международных и региональных стандартов;

• обеспечение единства измерений при взаимодействии с другими странами.

1.3.3. Правила разработки национальных стандартов (ГОСТ Р 1.2–2016)

Национальный стандарт Российской Федерации ГОСТ Р 1.2–2016 «Стандарты национальные Российской Федерации. Правила разработки, утверждения, обновления, внесения поправок, приостановки действия и отмены» введен в действие с 18.07.2016 г. взамен ГОСТ Р 1.2–2014. Стандарт устанавливает правила разработки и утверждения национальных стандартов Российской Федерации, проведения работ по их обновлению, внесению поправок, а также правила приостановки действия и отмены стандартов.

Разработку национальных стандартов осуществляют на основе программы разработки национальных стандартов в такой последовательности:

• организация разработки стандарта;

• разработка первой редакции проекта стандарта и ее публичное обсуждение;

• доработка проекта стандарта по результатам публичного обсуждения и его редактирование;

• подготовка окончательной редакции с учетом замечаний по результатам редактирования;

• проведение контроля проектов стандартов на соответ-

ствие правилам, установленным в ГОСТ Р 1.7 и/или ГОСТ Р 1.5, и требованиям к их оформлению (нормоконтроль);

• проведение экспертизы и подготовка мотивированного предложения об утверждении проекта стандарта в качестве национального стандарта, или об утверждении проекта национального стандарта в качестве предварительного национального стандарта, или об отклонении проекта национального стандарта;

• подготовка к утверждению, утверждение и регистрация стандарта.

В разделе 4 подробно описаны правила разработки и утверждения национальных стандартов в соответствии с указанной выше последовательностью.

Официальное опубликование утвержденного стандарта должно быть осуществлено незамедлительно, не позднее даты его введения в действие.

В разделе 5 описаны правила проведения работ по обновлению национальных стандартов, а в разделе 7 – правила осуществления отмены национальных стандартов.

1.3.4. Стандарты организаций (ГОСТ Р 1.4-2004)

Национальный стандарт Российской Федерации ГОСТ Р 1.4–2004 «Стандарты организаций. Общие положения» вве-

ден в действие с 01.07.2005 г. взамен ГОСТ Р 1.4–93. Он устанавливает объекты стандартизации и общие положения при разработке и применении стандартов организаций.

В соответствии с п. 4.1 данного стандарта стандарты организаций, в том числе коммерческих, общественных, научных организаций, саморегулируемых организаций, объединений юридических лиц, разрабатываются этими организациями в случаях и на условиях, указанных в статье 17 закона «О техническом регулировании».

ВНИМАНИЕ

Статья 17 утратила силу с 1 июля 2016 г. в связи с вступлением в силу соответствующих статей Федерального закона от 29.06.2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». В нем содержится статья 21 «Стандарты организаций и технические условия» в соответствии с которой:

1. Стандарты организаций разрабатываются организациями самостоятельно исходя из необходимости их применения для обеспечения целей, указанных в статье 3 настоящего Федерального закона.

2. Стандарты организаций и технические условия разрабатываются с учетом соответствующих документов национальной системы стандартизации.

3. Технические условия разрабатываются изготовителем и/или исполнителем и применяются в соответствии с условиями, установленными в договорах (контрактах).

4. Порядок разработки, утверждения, учета,

изменения, отмены и применения стандартов организаций и технических условий устанавливается организациями самостоятельно с учетом применимых принципов, предусмотренных статьей 4 настоящего Федерального закона.

5. Проект стандарта организации, а также проект технических условий перед их утверждением может представляться в соответствующий технический комитет по стандартизации или проектный технический комитет по стандартизации для проведения экспертизы, по результатам которой технический комитет по стандартизации или проектный технический комитет по стандартизации готовит соответствующее заключение.

Стандарты организации могут разрабатываться на применяемые в данной организации продукцию, процессы и оказываемые в ней услуги, а также на продукцию, создаваемую и поставляемую данной организацией на внутренний и внешний рынок, на работы, выполняемые данной организацией на стороне, и оказываемые ею на стороне услуги в соответствии с заключенными договорами.

Стандарты организации не должны противоречить требованиям технических регламентов, а также национальных стандартов. Порядок разработки, утверждения, учета, изменения и отмены стандартов организаций устанавливается организациями самостоятельно. Стандарты организации утверждает руководитель (заместитель руководителя) орга-

низации приказом и/или личной подписью на титульном листе стандарта в установленном в организации порядке. В случае утверждения стандарта организации приказом дату введения стандарта в действие устанавливают в приказе.

При необходимости проект стандарта может быть направлен организацией-разработчиком в специализированные организации для проведения экспертиз. Стандарт организации, разработанный и утвержденный одной организацией, может использоваться другой организацией в своих интересах только по договору с утвердившей его организацией.

Организация, разработавшая и утвердившая стандарт организации на продукцию, поставляемую на внутренний или внешний рынок, может при необходимости готовить предложения о разработке национального стандарта на основе этого стандарта.

1.3.5. Основные положения межгосударственной системы стандартизации (ГОСТ 1.0–2015)

Межгосударственный стандарт ГОСТ 1.0–2015 «Межгосударственная система стандартизации (МГСС). Основные положения» введен в действие 01.07.2016 г. взамен ГОСТ 1.0–92. Он устанавливает цели и принципы межгосударственной стандартизации, основные направления работ и объекты межгосударственной стандартизации, организаци-

онные основы межгосударственной системы стандартизации, категории документов по межгосударственной стандартизации и правила их применения.

Организацию работ по межгосударственной стандартизации осуществляет Межгосударственный совет по стандартизации, метрологии и сертификации.

Объектами межгосударственной стандартизации в соответствии со стандартом являются:

- общетехнические нормы и требования, в том числе единый технический язык, типоразмерные ряды и типовые конструкции изделий общемашиностроительного применения, совместимые программные и технические средства информационных технологий, справочные данные о свойствах материалов и веществ;
- объекты крупных промышленных и хозяйственных комплексов (транспорт, энергетика, связь и др.);
- объекты крупных межгосударственных социально-экономических и научно-технических программ;
- взаимопоставляемая продукция и услуги.

В зависимости от специфики объекта стандартизации и содержания устанавливаемых к нему требований применяют следующие основные виды межгосударственных стандартов:

- стандарты основополагающие;
- стандарты на продукцию;
- стандарты на услуги;

• стандарты на процессы;

• стандарты на методы контроля (испытаний, измерений, анализа);

• стандарты на термины и определения.

К документам по межгосударственной стандартизации относятся:

• межгосударственные стандарты;

• правила по межгосударственной стандартизации;

• рекомендации по межгосударственной стандартизации;

• межгосударственные классификаторы технико-экономической и социальной информации.

1.4. Основы стандартизации в области защиты информации

1.4.1. Основополагающие стандарты в сфере защиты информации

В системе стандартов в области защиты информации к основополагающим можно отнести следующие:

1. ГОСТ Р 50739–95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования».

2. ГОСТ Р 51188–98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство».

3. Р 50.1.053–2005 «Рекомендации по стандартизации. Информационные технологии. Основные термины и определения в области технической защиты информации».

4. Р 50.1.056–2005 «Рекомендации по стандартизации. Техническая защита информации. Основные термины и определения».

5. ГОСТ Р 50922–2006 «Защита информации. Основные термины и определения».

6. ГОСТ Р 53114–2008 «Защита информации. Обеспече-

ние информационной безопасности в организации. Основные термины и определения».

7. ГОСТ Р 51275–2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».

8. ГОСТ Р 52069.0–2013 «Защита информации. Система стандартов. Основные положения».

1.4.2. Основные термины в сфере защиты информации

Практически в каждом стандарте дается описание терминов в соответствующей предметной области. Описанию основных общих терминов в области защиты информации посвящен ряд специальных рекомендаций по стандартизации и национальных стандартов. Эти документы относятся к основополагающим в области защиты информации.

Р 50.1.053–2005 «Рекомендации по стандартизации. Информационные технологии. Основные термины и определения в области технической защиты информации».

Р 50.1.056–2005 «Рекомендации по стандартизации. Техническая защита информации. Основные термины и определения».

ГОСТ Р 50922–2006 «Защита информации. Основные термины и определения».

ГОСТ Р 53114–2008 «Защита информации. Обеспече-

ние информационной безопасности в организации. Основные термины и определения».

Указанные документы устанавливают основные термины и определения понятий в области защиты информации. Приведенные трактовки терминов рекомендуется использовать в правовой, нормативной, технической и организационно-распорядительной документации, научной, учебной и справочной литературе.

Следует отметить, что трактовка одних и тех же терминов в разных документах иногда различается. Более того, в нормативно-правовых документах последних лет, в том числе и в Федеральных законах, даются несколько другие трактовки терминов по сравнению с приведенными в ранее принятых стандартах. Кроме того, некоторые различия имеются и в определениях, приведенных в национальных и международных стандартах в области защиты информации. Как указано в ГОСТ Р 50922, приведенные в национальных документах термины можно при необходимости изменять, вводя в них производные признаки, раскрывая значения используемых в них терминов, указывая объекты, входящие в объем определяемого понятия. Изменения не должны нарушать объем и содержание понятий, определенных в стандартах.

Описание терминов, описывающих конкретные предметные области, даны в соответствующих разделах данного учебного пособия, где описаны конкретные стандарты. Ниже приведены основные термины с соответствующими опреде-

лениями, относящиеся к общим проблемам защиты информации.

Атака «отказ в обслуживании» – сетевая атака, приводящая к блокированию информационных процессов в автоматизированной системе.

Атака компьютерная – целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств.

Аутентификация (субъекта доступа) – действия по проверке подлинности субъекта доступа в автоматизированной информационной системе.

Аудит безопасности автоматизированной информационной системы – проверка реализованных в автоматизированной информационной системе процедур обеспечения безопасности с целью оценки их эффективности и корректности, а также разработки предложений по их совершенствованию.

Аудит информационной безопасности организации – систематический, независимый и документируемый процесс получения свидетельств деятельности организации по обеспечению ИБ и установлению степени выполнения в организации критериев ИБ.

Аттестация АС в защищенном исполнении – процесс комплексной проверки выполнения заданных функций АС

по обработке защищаемой информации на соответствие требованиям стандартов и/или нормативных документов в области защиты информации и оформления документов о ее соответствии выполнению функции по обработке защищаемой информации на конкретном объекте информатизации.

Аттестация объекта информатизации – деятельность по установлению соответствия комплекса организационно-технических мероприятий по защите объекта информатизации требованиям по безопасности информации.

Безопасность информации [данных] – состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность.

Безопасность информационной технологии – состояние защищенности информационной технологии, при котором обеспечиваются безопасность информации, для обработки которой она применяется, и информационная безопасность информационной системы, в которой она реализована.

Безопасность автоматизированной информационной системы – состояние защищенности автоматизированной информационной системы, при котором обеспечиваются конфиденциальность, доступность, целостность, подотчетность и подлинность ее ресурсов.

Блокирование доступа (к информации) – прекращение или затруднение доступа к информации лиц, имеющих на это право (законных пользователей).

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа к информации и/или воздействия на информацию или ресурсы ИС.

Вредоносная программа – программа, используемая для осуществления несанкционированного доступа к информации и/или воздействия на информацию или ресурсы автоматизированной информационной системы.

Доступность (информации [ресурсов автоматизированной информационной системы]) – состояние информации [ресурсов автоматизированной информационной системы], при котором субъекты, имеющие право доступа, могут реализовать их беспрепятственно.

Защита информации (ЗИ) – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Инцидент ИБ – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

В стандарте ГОСТ Р 53114 указаны следующие виды инцидентов:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по ИБ;

- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и технических средств;
- нарушение правил доступа.

Информационный процесс – процесс создания, сбора, обработки, накопления, хранения, поиска, распространения и использования информации.

Информационная технология – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационная сфера – совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.

Информационная безопасность организации – состояние защищенности интересов организации в условиях угроз в информационной сфере.

Идентификация – действия по присвоению субъектам и объектам доступа идентификаторов и/или по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Конфиденциальность (информации [ресурсов автоматизированной информационной системы]) – со-

стояние информации [ресурсов автоматизированной информационной системы], при котором доступ к ней [к ним] осуществляют только субъекты, имеющие на него право.

Криптографическая защита информации – защита информации с помощью ее криптографического преобразования.

Критически важная система информационной инфраструктуры (КСИИ) – информационно-управляющая или информационно-телекоммуникационная система, которая осуществляет управление или информационное обеспечение критическим объектом или процессом или используется для официального информирования общества и граждан, нарушение или прерывание функционирования которой может привести к чрезвычайной ситуации со значительными негативными последствиями.

Критический объект – объект или процесс, нарушение непрерывности функционирования которого может нанести значительный ущерб.

ПРИМЕЧАНИЕ

В Федеральном законе от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» даны следующие определения:

критическая информационная инфраструктура – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации

взаимодействия таких объектов;

объекты критической информационной инфраструктуры – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

Критерий обеспечения ИБ организации – показатель, на основании которого оценивается степень достижения цели (целей) ИБ организации.

Меры обеспечения информационной безопасности – совокупность действий, направленных на разработку и/или практическое применение способов и средств обеспечения ИБ.

Мониторинг безопасности информации (при применении информационных технологий) – процедуры регулярного наблюдения за процессом обеспечения безопасности информации при применении информационных технологий.

Недекларированные возможности – функциональные возможности средств вычислительной техники и программного обеспечения, не описанные или не соответствующие описанным в документации, которые могут привести к снижению или нарушению свойств безопасности информации.

Объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации,

используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

Объект защиты информации – информация или носитель информации или информационный процесс, который необходимо защищать в соответствии с целью ЗИ.

Оценка риска – выявление угроз безопасности информации, уязвимостей информационной системы, оценка вероятностей реализации угроз с использованием уязвимостей и оценка последствий реализации угроз для информации и информационной системы, используемой для обработки этой информации.

Оценка соответствия ИБ организации установленным требованиям – деятельность, связанная с прямым или косвенным определением выполнения или невыполнения в организации установленных требований ИБ.

Оценка соответствия требованиям по ЗИ – прямое или косвенное определение степени соблюдения требований по ЗИ, предъявляемых к объекту ЗИ.

Обеспечение информационной безопасности организации – деятельность, направленная на устранение (нейтрализацию, парирование) внутренних и внешних угроз информационной безопасности организации или на миними-

зацию ущерба от возможной реализации таких угроз.

Организационные меры обеспечения информационной безопасности – меры обеспечения ИБ, предусматривающие установление временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режимы работы объекта информатизации.

Политика информационной безопасности (организации) – формальное изложение правил поведения, процедур, практических приемов или руководящих принципов в области информационной безопасности, которыми руководствуется организация в своей деятельности.

Подотчетность (ресурсов автоматизированной информационной системы) – состояние ресурсов автоматизированной информационной системы, при котором обеспечиваются их идентификация и регистрация.

Подлинность (ресурсов автоматизированной информационной системы) – состояние ресурсов автоматизированной информационной системы, при котором обеспечивается реализация информационной технологии с использованием именно тех ресурсов, к которым субъект, имеющий на это право, обращается.

Правила разграничения доступа (в автоматизированной информационной системе) – правила, регламентирующие условия доступа субъектов доступа к объектам доступа в автоматизированной информационной системе.

Правовая защита информации – защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов, регулирующих отношения субъектов по защите информации, применение этих документов, а также надзор и контроль за их исполнением.

Программная закладка – преднамеренно внесенный в программное обеспечение функциональный объект, который при определенных условиях инициирует реализацию недекларированных возможностей программного обеспечения.

Программная закладка – скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие.

Система защиты информации – совокупность органов и/или исполнителей, используемой ими техники ЗИ, а также объектов ЗИ, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области ЗИ.

Сертификация на соответствие требованиям по безопасности информации – форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров.

Средство контроля эффективности ЗИ – средство ЗИ, предназначенное или используемое для контроля эффективности ЗИ.

Средство обнаружения вторжений – программное или программно-техническое средство, которое автоматизирует процесс контроля событий, протекающих в компьютерной системе или сети, а также самостоятельно анализирует эти события в поисках признаков инцидента информационной безопасности.

Средство защиты информации – техническое, программное, программно-техническое средство, вещество и/или материал, предназначенные или используемые для защиты информации.

Сертификация средств технической защиты информации – деятельность органа по сертификации по подтверждению соответствия средств технической защиты информации требованиям технических регламентов, положениям стандартов или условиям договоров.

Техническая защита информации – защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации, подлежащей защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

Техническая защита информации – деятельность, направленная на обеспечение некриптографическими метода-

ми безопасности информации (данных), подлежащей защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

Техническое средство обеспечения информационной безопасности – оборудование, используемое для обеспечения информационной безопасности организации некриптографическими методами.

Угроза — совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Угроза информационной безопасности организации – совокупность факторов и условий, создающих опасность нарушения информационной безопасности организации, вызывающую или способную вызвать негативные последствия (ущерб/вред) для организации.

Угроза (безопасности информации) – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения конфиденциальности, доступности и/или целостности информации.

Уязвимость (информационной системы) – свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации.

Уязвимость (информационной системы) – свойство информационной системы, предоставляющее возможность

реализации угроз безопасности обрабатываемой в ней информации.

Уязвимость (автоматизированной информационной системы) – недостаток или слабое место в автоматизированной информационной системе, которые могут быть условием реализации угрозы безопасности обрабатываемой в ней информации.

Физическая защита информации – защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

Целостность (информации [ресурсов автоматизированной информационной системы]) – состояние информации [ресурсов автоматизированной информационной системы], при котором ее [их] изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Эффективность защиты информации – степень соответствия результатов защиты информации цели защиты информации.

1.4.3. Система стандартов по защите информации (ГОСТ Р 52069.0–2013)

Национальный стандарт Российской Федерации ГОСТ Р

52069.0–2013 «Защита информации. Система стандартов. Основные положения» введен в действие с 01.09.2013 г. взамен ГОСТ Р 52069.0–2003. Он устанавливает цель, задачи и структуру системы стандартов по защите (некриптографическими методами) информации, объекты и аспекты стандартизации в данной области и является основополагающим национальным стандартом Российской Федерации в области защиты информации. Положения стандарта применяются при проведении работ по стандартизации в области противодействия техническим разведкам, технической защиты информации, обеспечения безопасности информации в ключевых системах информационной инфраструктуры.

Под **системой стандартов по защите информации** понимается совокупность взаимосвязанных стандартов, устанавливающих характеристики продукции, правила осуществления и характеристики процессов, выполнения работ или оказания услуг в области защиты информации.

Система стандартов по защите информации (ССЗИ) является составной частью национальной системы стандартизации Российской Федерации.

Основными задачами по формированию и развитию ССЗИ являются:

- установление основополагающих принципов построения, требований к составу и содержанию системы документов в области ЗИ;
- обеспечение единства терминологии в области ЗИ;

• упорядочение объектов и аспектов стандартизации в области ЗИ;

• обеспечение единства организационных и методических подходов к проведению работ по ЗИ;

• установление системы требований по ЗИ и методов контроля выполнения этих требований;

• установление общих технических требований к средствам ЗИ (СЗИ) и услугам по ЗИ;

• установление требований к методам и методикам испытаний и оценки качества СЗИ;

• установление требований к метрологическому, информационному и другим видам обеспечения ЗИ.

Основными объектами стандартизации ССЗИ являются:

1) ЗИ как область деятельности:

• противодействие техническим разведкам;

• техническая ЗИ;

• обеспечение безопасности информации в ключевых системах информационной инфраструктуры;

2) объекты ЗИ (промышленные объекты, объекты науки, энергетики, жизнеобеспечения, объекты органов управления, объекты информатизации, продукция);

3) угрозы безопасности информации и уязвимости объектов ЗИ;

4) организация и содержание работ по ЗИ;

5) методы (процессы, работы, технологии) ЗИ и методы контроля состояния ЗИ;

6) техника ЗИ (средства ЗИ, средства контроля эффективности ЗИ);

7) услуги по ЗИ.

Основными аспектами стандартизации в ССЗИ являются:

• термины и определения в области ЗИ;

• классификация в области ЗИ (угроз, уязвимостей, работ и услуг по ЗИ, техники ЗИ);

• требования к системе документов в области ЗИ;

• общие технические требования по ЗИ, предъявляемые к объектам;

• общие требования к организации и содержанию работ по ЗИ;

• общие технические требования к СЗИ и системе контроля эффективности ЗИ и методам их испытаний;

• методы контроля организации и эффективности ЗИ, методы измерений при проведении контроля;

• общие требования к организации, содержанию работ и результатам оказания услуг по ЗИ.

Система стандартов по защите информации включает следующие виды документов в области стандартизации по ЗИ:

• национальные стандарты Российской Федерации, в том числе ограниченного распространения, государственные во-

енные стандарты, национальные стандарты, оформленные на основе аутентичных переводов международных стандартов;

• межгосударственные стандарты;

• правила стандартизации, нормы и рекомендации в области стандартизации;

• общероссийские классификаторы технико-экономической и социальной информации;

• стандарты организаций;

• предварительные национальные стандарты;

• международные стандарты, региональные стандарты, региональные своды правил, стандарты иностранных государств и своды правил иностранных государств, принятые на учет национальным органом Российской Федерации по стандартизации, и их надлежащим образом заверенные переводы на русский язык.

В состав документов в области стандартизации по ЗИ могут входить:

• своды правил;

• нормативно-технические документы системы общих технических требований к видам вооружения и военной техники;

• международные стандарты, региональные стандарты, региональные своды правил, стандарты иностранных государств и своды правил иностранных государств, принятые на учет национальным органом Российской Федерации по стан-

дартизации, и их надлежащим образом заверенные переводы на русский язык.

Стандарты организаций по ЗИ разрабатываются организациями и утверждаются ими самостоятельно исходя из необходимости применения этих стандартов для целей стандартизации по ЗИ и не должны противоречить другим документам в области стандартизации по ЗИ, используемым на территории Российской Федерации.

Структура системы стандартов по ЗИ представлена на рис. 1.1.

Система стандартов по защите информации включает подсистемы стандартов в области:

- противодействия техническим разведкам;
- технической защиты информации;
- обеспечение безопасности информации в ключевых системах информационной инфраструктуры.

Рис. 1.1. Структура системы стандартов по ЗИ

В каждой области подсистемы стандартов ССЗИ включают следующие комплексы стандартов:

• комплекс общесистемных стандартов по ЗИ (общие требования по ЗИ в различных областях деятельности, терминология в области ЗИ);

• комплексы стандартов по ЗИ для различных классов объектов (общие требования к объекту защиты, классификация угроз и уязвимостей, требования к методам защиты и контроля эффективности защиты);

• комплексы стандартов по технике ЗИ (требования к системе защиты и контроля эффективности защиты);

• комплекс стандартов на услуги по ЗИ (требования по организации, содержанию работ, используемым методам оцен-

ки соответствия средств защиты и их эффективности, аттестации объектов информатизации по требованиям безопасности информации).

1.4.4. Факторы, воздействующие на информацию (ГОСТ Р 51275–2006)

Национальный стандарт Российской Федерации ГОСТ Р 51275–2006 «Защита информации. Объект информации. Факторы, воздействующие на информацию. Общие положения» введен в действие с 01.02.2008 г. взамен ранее принятого стандарта ГОСТ Р 51275–99.

Стандарт устанавливает классификацию и перечень факторов, воздействующих на безопасность защищаемой информации, в целях обоснования угроз безопасности информации и требований по защите информации на объекте информатизации.

Стандарт вводит ряд понятий, в частности:

Объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

Система обработки информации – совокупность технических средств и программного обеспечения, а также методов обработки информации и действий персонала, необходимых для выполнения автоматизированной обработки информации.

Закладочное средство – техническое средство [устройство] приема, передачи и обработки информации, преднамеренно устанавливаемое на объекте информатизации или в контролируемой зоне в целях перехвата информации или несанкционированного воздействия на информацию и/или ресурсы автоматизированной информационной системы.

Программная закладка – преднамеренно внесенный в программное обеспечение функциональный объект, который при определенных условиях инициирует реализацию недекларированных возможностей программного обеспечения.

Конец ознакомительного фрагмента.