

О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449

Во исполнение пункта 4 Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449 «О совершенствовании государственного регулирования в области защиты информации» Совет Министров Республики Беларусь ПОСТАНОВЛЯЕТ:

1. Внести изменения в следующие постановления Совета Министров Республики Беларусь:

1.1. в постановлении Совета Министров Республики Беларусь от 15 мая 2013 г. № 375 «Об утверждении технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/ВУ)»:

преамбулу изложить в следующей редакции:

«На основании подпункта 1.6 пункта 1 статьи 8 Закона Республики Беларусь от 5 января 2004 г. № 262-З «О техническом нормировании и стандартизации» Совет Министров Республики Беларусь ПОСТАНОВЛЯЕТ:»;

слово «прилагаемый» исключить;

после слов «с 1 января 2014 г.» дополнить постановление словом «(прилагается)»;

дополнить постановление частями следующего содержания:

«Установить, что документы об оценке соответствия средств защиты информации, выданные (принятые) в Национальной системе подтверждения соответствия Республики Беларусь до 14 марта 2020 г., действительны до окончания срока их действия.

Предоставить право Оперативно-аналитическому центру при Президенте Республики Беларусь разъяснять вопросы применения технического регламента ТР 2013/027/ВУ.»;

технический регламент Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/ВУ), утвержденный этим постановлением, изложить в новой редакции (прилагается);

1.2. в постановлении Совета Министров Республики Беларусь от 12 августа 2014 г. № 783 «О служебной информации ограниченного распространения и информации, составляющей коммерческую тайну»:

преамбулу изложить в следующей редакции:

«Во исполнение абзаца четвертого статьи 23 Закона Республики Беларусь от 5 января 2013 г. № 16-З «О коммерческой тайне» и абзаца второй части первой статьи 2 Закона Республики Беларусь от 4 января 2014 г. № 102-З «О внесении изменений и дополнений в Закон Республики Беларусь «Об информации, информатизации и защите информации» Совет Министров Республики Беларусь ПОСТАНОВЛЯЕТ:»;

в пункте 1:

слово «прилагаемое» исключить;

дополнить пункт словом «(прилагается)»;

в Положении о порядке проставления ограничительного грифа «Для служебного пользования», грифа «Коммерческая тайна» и ведения делопроизводства по документам, содержащим служебную информацию ограниченного распространения и информацию, составляющую коммерческую тайну, утвержденном этим постановлением:

абзац первый пункта 1 изложить в следующей редакции:

«1. В настоящем Положении в соответствии с частями второй и четвертой статьи 18¹ Закона Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» и абзацем четвертым статьи 23 Закона Республики Беларусь «О коммерческой тайне» определяются:»;

из части первой пункта 6, части седьмой пункта 7 и пункта 15 слово «нормативными» исключить;

в приложении к этому постановлению:

из абзаца пятого пункта 9 слова «, к действующим паролям, закрытым ключам электронно-цифровой подписи» исключить;

пункты 13–15 изложить в следующей редакции:

«13. Совокупность сведений об объекте информатизации, включенном в Государственный реестр критически важных объектов информатизации.

14. Сведения о системе информационной безопасности критически важного объекта информатизации.

15. Сведения, полученные в результате проведения аудита системы информационной безопасности критически важного объекта информатизации и контроля за технической и криптографической защитой информации на критически важном объекте информатизации.».

2. Признать утратившим силу постановление Совета Министров Республики Беларусь от 30 марта 2012 г. № 293 «О некоторых вопросах безопасной эксплуатации и надежного функционирования критически важных объектов информатизации».

3. Настоящее постановление вступает в силу с 14 марта 2020 г.

Премьер-министр Республики Беларусь

С.Румас

УТВЕРЖДЕНО

Постановление
Совета Министров
Республики Беларусь
15.05.2013 № 375
(в редакции постановления
Совета Министров
Республики Беларусь
12.03.2020 № 145)

ТЕХНИЧЕСКИЙ РЕГЛАМЕНТ

Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/ВУ)

Статья 1. Область применения

1. Технический регламент Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/ВУ) распространяется на выпускаемые в обращение на территории Республики Беларусь средства защиты информации независимо от страны происхождения, за исключением средств шифрованной, других видов специальной связи и криптографических средств защиты государственных секретов.

2. Настоящим техническим регламентом устанавливаются требования к средствам защиты информации в целях обеспечения национальной безопасности, а также предупреждения действий, вводящих в заблуждение потребителей относительно назначения и качества средств защиты информации.

Статья 2. Термины и их определения

В настоящем техническом регламенте используются термины, значения которых определены в Законе Республики Беларусь от 24 октября 2016 г. № 437-З «Об оценке соответствия техническим требованиям и аккредитации органов по оценке соответствия»,

Указе Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации», а также следующие термины и их определения:

аккредитованная испытательная лаборатория (центр) – юридическое лицо Республики Беларусь, аккредитованное для проведения испытаний в определенной области аккредитации;

выпуск средств защиты информации в обращение – поставка (предоставление права использования) или ввоз средств защиты информации (в том числе отправка со склада изготовителя или отгрузка без складирования) в целях их распространения (реализации) на территории Республики Беларусь в ходе коммерческой деятельности на безвозмездной или возмездной основе;

заявитель на проведение сертификации средства защиты информации (далее – заявитель) – юридическое лицо либо индивидуальный предприниматель, обратившиеся с заявкой на сертификацию средства защиты информации;

изготовитель – юридическое лицо либо индивидуальный предприниматель, осуществляющие от своего имени производство (разработку) или производство (разработку) и реализацию (предоставление права использования) средств защиты информации и ответственные за их соответствие обязательным для соблюдения техническим требованиям;

критические параметры – параметры, связанные с обеспечением безопасности, несанкционированное раскрытие или модификация которых снижает безопасность средства защиты информации или защищаемой им информации;

лицо, принимающее декларацию о соответствии, – изготовитель или уполномоченное изготовителем лицо либо продавец (поставщик), принимающие (принявшие) декларацию о соответствии. При этом лицом, принимающим декларацию о соответствии, может быть только юридическое лицо Республики Беларусь либо индивидуальный предприниматель, зарегистрированный в Республике Беларусь;

носитель информации – материальный объект, в котором информация находит свое отображение и (или) хранится;

орган по сертификации – юридическое лицо Республики Беларусь, аккредитованное для выполнения работ по сертификации и регистрации деклараций о соответствии в определенной области аккредитации;

применение по назначению – использование средств защиты информации в соответствии с назначением, указанным в эксплуатационных документах;

продавец (поставщик) – юридическое лицо или индивидуальный предприниматель, зарегистрированные в Республике Беларусь или ином государстве – члене Евразийского экономического союза, которые осуществляют реализацию средств защиты информации (в том числе ввозимых (ввезенных) на территорию Республики Беларусь или иного государства – члена Евразийского экономического союза из третьей стороны) и несут ответственность за несоответствие средств защиты информации требованиям настоящего технического регламента;

средства защиты государственных секретов – технические, программные, криптографические и другие средства, используемые для защиты государственных секретов, а также средства контроля эффективности защиты государственных секретов;

средства защиты информации – средства защиты государственных секретов, средства криптографической защиты информации, средства технической защиты информации;

уполномоченное изготовителем лицо – юридическое лицо или индивидуальный предприниматель, зарегистрированные в Республике Беларусь, которые на основании гражданско-правового договора с изготовителем осуществляют действия от имени этого изготовителя при оценке соответствия и выпуске средств защиты информации (в том числе ввозимых (ввезенных) на территорию Республики Беларусь) в обращение, а также несут

ответственность за несоответствие средств защиты информации требованиям настоящего технического регламента.

Статья 3. Правила выпуска в обращение средств защиты информации

Средства защиты информации выпускаются в обращение в установленном порядке при их соответствии настоящему техническому регламенту, а также другим техническим регламентам, действие которых распространяется на эти средства защиты.

Средства защиты информации, соответствие которых требованиям настоящего технического регламента не подтверждено, не должны быть маркированы знаком соответствия техническому регламенту Республики Беларусь и не допускаются к выпуску в обращение.

Статья 4. Требования информационной безопасности

1. Средства защиты информации должны быть разработаны и изготовлены таким образом, чтобы, применяя их по назначению и выполняя требования к их эксплуатации и техническому обслуживанию, они обеспечивали:

- выполнение функций в соответствии с эксплуатационными документами;
- защиту от несанкционированного раскрытия и (или) модификации критических параметров;
- контроль целостности конфигурации;
- самотестирование;
- контроль доступа к функциям управления и настройкам;
- сохранение работоспособности при обработке некорректных данных.

2. Наименование и (или) обозначение средств защиты информации (тип, марка, модель), их параметры и характеристики, наименование и (или) товарный знак изготовителя, наименование страны-изготовителя должны быть нанесены непосредственно на средства защиты информации либо их носители, а также они должны быть указаны в прилагаемых к ним эксплуатационных документах.

3. Если сведения, приведенные в пункте 2 настоящей статьи, невозможно нанести непосредственно на средства защиты информации или их носители, то они могут указываться только в эксплуатационных документах, прилагаемых к средствам защиты информации. При этом наименование изготовителя и (или) его товарный знак, наименование и обозначение средств защиты информации (тип, марка, модель) должны быть нанесены на упаковку.

4. Маркировка средств защиты информации должна быть разборчивой и нанесена на доступную для осмотра поверхность средств защиты информации или их носители.

5. Эксплуатационные документы средств защиты информации должны включать:

- информацию, перечисленную в пункте 2 настоящей статьи;
- информацию о назначении средств защиты информации;
- основные потребительские свойства или характеристики;
- правила и условия безопасной эксплуатации (использования);
- правила и условия хранения, перевозки, реализации, монтажа и утилизации (при необходимости установления требований к ним);
- информацию о мерах, которые следует предпринять при обнаружении неисправности;
- местонахождение изготовителя, информацию для связи с ним;
- наименование и местонахождение уполномоченного изготовителем лица, импортера, информацию для связи с ним;
- дату изготовления средств защиты информации;
- обязательства изготовителя (уполномоченного изготовителем лица) по установке, сопровождению и поддержке средств защиты информации.

6. Маркировка и эксплуатационные документы выполняются на государственных языках Республики Беларусь – белорусском и (или) русском.

Статья 5. Обеспечение соответствия требованиям информационной безопасности

Соответствие средств защиты информации настоящему техническому регламенту обеспечивается выполнением его технических требований непосредственно либо выполнением требований государственных стандартов, взаимосвязанных с настоящим техническим регламентом, в результате применения которых на добровольной основе обеспечивается соблюдение требований настоящего технического регламента, перечень которых утверждается Оперативно-аналитическим центром при Президенте Республики Беларусь.

Методы исследований (испытаний) средств защиты информации устанавливаются во взаимосвязанных с настоящим техническим регламентом государственных стандартах, а в случае, если такие методы исследований (испытаний) в этих государственных стандартах не установлены, – в методиках испытаний, согласованных с органом по сертификации.

Статья 6. Подтверждение соответствия требованиям информационной безопасности

1. Процедуры подтверждения соответствия средств защиты информации требованиям информационной безопасности выполняются согласно Правилам подтверждения соответствия Национальной системы подтверждения соответствия Республики Беларусь. Особенности подтверждения соответствия средств защиты информации требованиям информационной безопасности могут устанавливаться Оперативно-аналитическим центром при Президенте Республики Беларусь.

2. Перед выпуском в обращение средства защиты информации должны быть подвергнуты процедуре подтверждения соответствия требованиям информационной безопасности настоящего технического регламента в форме сертификации или декларирования соответствия.

3. Подтверждению соответствия требованиям информационной безопасности настоящего технического регламента путем сертификации подлежат средства защиты информации, которые будут использоваться для:

- технической защиты государственных секретов;
- создания систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено;
- создания систем информационной безопасности критически важных объектов информатизации;
- обеспечения целостности и подлинности электронных документов.

Требования информационной безопасности, на соответствие которым осуществляется сертификация, определяются Оперативно-аналитическим центром при Президенте Республики Беларусь в зависимости от специфики средств защиты информации.

4. Подтверждение соответствия требованиям информационной безопасности настоящего технического регламента средств защиты информации, не предназначенных для использования в целях, указанных в пункте 3 настоящей статьи:

- осуществляется путем декларирования соответствия;
- может быть проведено в форме обязательной сертификации.

5. Орган по сертификации проводит сертификацию средств защиты информации согласно схемам:

- схема 1с – для серийно выпускаемых средств защиты информации;
- схема 3с – для партии средств защиты информации;

схема 4с – для единичного изделия.

6. Заявитель представляет средства защиты информации для подтверждения соответствия.

7. При проведении работ по сертификации средств защиты информации:

7.1. орган по сертификации:

проводит анализ документов, представленных заявителем, в течение не более 20 рабочих дней со дня подачи заявки;

заключает договор на проведение работ по сертификации средств защиты информации;

проводит идентификацию средств защиты информации и отбор образцов для испытаний (для средств криптографической защиты информации проводит контрольную компиляцию (трансляцию) исходных модулей с включением их в акт отбора образцов);

организует проведение испытаний образца (образцов) средств защиты информации в аккредитованной испытательной лаборатории (центре) на соответствие требованиям настоящего технического регламента и взаимосвязанных с настоящим техническим регламентом государственных стандартов;

проводит анализ состояния производства (схема 1с);

выдает сертификат соответствия настоящему техническому регламенту в рамках Национальной системы подтверждения соответствия Республики Беларусь;

заключает с заявителем соглашение по сертификации (схема 1с);

осуществляет периодическую оценку сертифицированных средств защиты информации посредством испытаний образцов этих средств и (или) анализа состояния производства (схема 1с);

7.2. заявитель:

подает заявку на проведение работ по сертификации средств защиты информации с комплектом документов, который включает:

технические условия (при наличии);

задание по безопасности и протокол его оценки в аккредитованной испытательной лаборатории (центре);

эксплуатационные документы;

тексты программ, описания применения, функциональную спецификацию безопасности (для средств криптографической защиты информации);

документы, регламентирующие порядок выпуска обновлений программных, программно-аппаратных средств технической защиты информации (схема 1с);

протокол (протоколы) испытаний, проведенных в аккредитованных испытательных лабораториях (центрах) (при наличии);

товаросопроводительные документы (схемы 3с, 4с);

заключает договор на проведение работ по сертификации средств защиты информации;

предоставляет средства защиты информации для проведения идентификации и отбора образцов для испытаний;

обеспечивает аккредитованную испытательную лабораторию (центр) необходимыми документами и информацией;

создает условия для проведения анализа состояния производства (схема 1с);

заключает с органом по сертификации соглашение по сертификации (схема 1с);

создает условия для проведения периодической оценки сертифицированных средств защиты информации (схема 1с);

7.3. аккредитованная испытательная лаборатория (центр):

заключает договор на проведение испытаний;

проводит испытания средств защиты информации.

Орган по сертификации имеет право запросить дополнительную техническую (конструкторскую) документацию (тексты и описания программных средств, методики и программы испытаний, спецификации, сборочные чертежи, чертежи сборочных единиц и деталей, электрические схемы, иные документы и материалы, согласно которым изготавливается средство защиты информации), необходимую для подтверждения соответствия средства защиты информации требованиям информационной безопасности настоящего технического регламента.

Протоколы сертификационных испытаний программных средств криптографической защиты информации, проведенных в аккредитованных испытательных лабораториях (центрах), могут применяться в течение пяти лет.

8. Подтверждение соответствия средств защиты информации путем декларирования соответствия проводится:

8.1. при принятии заявителем декларации о соответствии на основании собственных доказательств по схеме:

1д – для серийно выпускаемых средств защиты информации;

2д – для партии средств защиты информации (для единичного изделия);

8.2. при принятии заявителем декларации о соответствии на основании собственных доказательств и доказательств, полученных с участием органа по сертификации и (или) аккредитованной испытательной лаборатории (центра), по схеме:

3д – для серийно выпускаемых средств защиты информации;

4д – для партии средств защиты информации (для единичного изделия).

9. Применяя схемы декларирования, указанные в пункте 8 настоящей статьи:

9.1. орган по сертификации:

устанавливает наличие всех документов, необходимых для регистрации декларации о соответствии, предусмотренных законодательством об административных процедурах; выясняет полномочия лица, принимающего декларацию о соответствии, на принятие такой декларации;

анализирует правильность и полноту оформления декларации о соответствии;

регистрирует декларацию о соответствии;

9.2. лицо, принимающее декларацию о соответствии:

формирует документы, подтверждающие соответствие средств защиты информации установленным требованиям и правомочность принятия декларации о соответствии;

осуществляет контроль в процессе производства средств защиты информации (схемы 1д, 3д);

проводит испытания средств защиты информации (схемы 1д, 2д);

принимает декларацию о соответствии;

предоставляет средства защиты информации для испытаний (схемы 3д, 4д);

подает заявление на регистрацию декларации о соответствии с документами, предусмотренными законодательством об административных процедурах;

заключает договор на проведение испытаний (схемы 3д, 4д);

9.3. аккредитованная испытательная лаборатория (центр):

заключает договор на проведение испытаний (схемы 3д, 4д);

проводит испытания средств защиты информации (схемы 3д, 4д).

10. Изготовитель осуществляет производственный контроль и принимает все необходимые меры, для того чтобы процесс производства обеспечивал соответствие средств защиты информации требованиям настоящего технического регламента.

Требования к процессам производства и контроля, а также результаты их контроля должны быть оформлены документально.

11. Заявитель (лицо, принявшее декларацию о соответствии) обеспечивает хранение комплекта документов на средства защиты информации для:

серийно выпускаемых средств защиты информации – в течение не менее 10 лет со дня снятия с производства (прекращения производства) средств защиты информации;

партии средств защиты информации – в течение не менее 10 лет со дня реализации последнего изделия из партии.

Комплект документов должен предоставляться органам государственного контроля (надзора) по их требованию в соответствии с законодательством.

Статья 7. Маркировка знаком соответствия

1. Средства защиты информации, соответствующие требованиям информационной безопасности и прошедшие процедуру подтверждения соответствия, должны маркироваться знаком соответствия техническому регламенту Республики Беларусь.

2. Маркировка средств защиты информации знаком соответствия техническому регламенту Республики Беларусь осуществляется перед их выпуском в обращение.

3. Знак соответствия техническому регламенту Республики Беларусь наносится любым способом, обеспечивающим четкое и ясное изображение в течение всего срока службы средств защиты информации, на:

каждую единицу технических и программно-аппаратных средств защиты информации;

каждый носитель информации программных средств защиты информации;

упаковку.

При невозможности нанесения знака соответствия техническому регламенту Республики Беларусь непосредственно на средство защиты информации (если размер средства защиты информации или его тип не позволяют нанести знак соответствия) допускается нанесение его на наименьшей потребительской упаковке (таре) и указание его в прилагаемых к средству защиты информации эксплуатационных документах. В случае отсутствия упаковки на такие средства защиты информации знак соответствия приводится в прилагаемых к ним эксплуатационных документах.