УКАЗ ПРЕЗИДЕНТА РЕСПУБЛИКИ БЕЛАРУСЬ
16 апреля 2013 г. № 196

О некоторых мерах по совершенствованию защиты информации

Изменения и дополнения:

Указ Президента Республики Беларусь от 29 ноября 2013 г. № 529 (Национальный правовой Интернет-портал Республики Беларусь, 30.11.2013, 1/14649) <P31300529>;

Указ Президента Республики Беларусь от 1 апреля 2016 г. № 121 (Национальный правовой Интернет-портал Республики Беларусь, 06.04.2016, 1/16359) <P31600121>;

Указ Президента Республики Беларусь от 18 июня 2018 г. № 239 (Национальный правовой Интернет-портал Республики Беларусь, 21.06.2018, 1/17759) <P31800239>

(Извлечение)

В целях совершенствования технической и криптографической защиты информации п о с т а н о в л я ю:

1. Утвердить прилагаемое Положение о технической и криптографической защите информации в Республике Беларусь.

2. Внести изменения и дополнения в следующие указы Президента Республики Беларусь:

2.1. утратил силу;

2.2. в Указе Президента Республики Беларусь от 16 октября 2009 г. № 510 «О совершенствовании контрольной (надзорной) деятельности в Республике Беларусь» (Национальный реестр правовых актов Республики Беларусь, 2009 г., № 253, 1/11062; Национальный правовой Интернет-портал Республики Беларусь, 31.07.2012, 1/13654):

в пункте 21:

после абзаца третьего дополнить пункт абзацем следующего содержания:

«контроля за технической и криптографической защитой информации в государственных органах и иных организациях, являющихся собственниками (владельцами) объектов, на которых такая защита является обязательной в соответствии с законодательными актами, за исключением мероприятий по контролю за соблюдением законодательства о лицензировании, лицензионных требований и условий осуществления лицензируемого вида деятельности;»;

абзацы четвертый – двадцать восьмой считать соответственно абзацами пятым – двадцать девятым;

часть первую пункта 15 Положения о порядке организации и проведения проверок, утвержденного этим Указом, после слов «Оперативно-аналитическим центром» дополнить словами «при Президенте»;

2.3. в Положении о лицензировании отдельных видов деятельности, утвержденном Указом Президента Республики Беларусь от 1 сентября 2010 г. № 450 «О лицензировании отдельных видов деятельности» (Национальный реестр правовых актов Республики Беларусь, 2010 г., № 212, 1/11914; 2012 г., № 72, 1/13579):

название главы 21 изложить в следующей редакции:

«ГЛАВА 21
ДЕЯТЕЛЬНОСТЬ ПО ТЕХНИЧЕСКОЙ И (ИЛИ) КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ»;

пункт 201 изложить в следующей редакции:

«201. Лицензирование деятельности по технической и (или) криптографической защите информации (далее для целей настоящей главы – лицензируемая деятельность) осуществляется Оперативно-аналитическим центром при Президенте Республики Беларусь (далее – Оперативно-аналитический центр).»;

пункт 203 изложить в следующей редакции:

«203. Для целей настоящей главы и пункта 13 приложения 1 к настоящему Положению:

203.1. под информацией, для осуществления деятельности по технической защите которой требуется получение лицензии, понимается информация:

распространение и (или) предоставление которой ограничено;

обрабатываемая на критически важных объектах информатизации;

203.2. под информацией, для осуществления деятельности по криптографической защите которой требуется получение лицензии, понимается информация:

распространение и (или) предоставление которой ограничено, не содержащая сведений, отнесенных к государственным секретам;

обрабатываемая на критически важных объектах информатизации;

обрабатываемая в государственных информационных системах.»;

дополнить Положение пунктом 203^1 следующего содержания:

«203^1. Не требуется получения лицензии для выполнения работ по технической и (или) криптографической защите информации, если эти работы выполняются для собственных нужд обладателем информации, распространение и (или) предоставление которой ограничено, собственником (владельцем) критически важных объектов информатизации и государственных информационных систем.»;

в абзаце втором пункта 204 слова «содержит информацию, отнесенную к государственным секретам» заменить словами «предназначен для обработки информации, содержащей государственные секреты»;

абзац второй пункта 205 после слова «технической» дополнить словами «и (или) криптографической»;

в пункте 13 приложения 1 к этому Положению слова «защите информации, в том числе криптографическими методами, включая применение электронной цифровой подписи» заменить словами «и (или) криптографической защите информации»;

2.4. в Положении об отнесении объектов информатизации к критически важным и обеспечении безопасности критически важных объектов информатизации, утвержденном Указом Президента Республики Беларусь от 25 октября 2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации» (Национальный реестр правовых актов Республики Беларусь, 2011 г., № 121, 1/13026):

в части второй пункта 1 слово «содержащие» заменить словами «предназначенные для обработки информации, содержащей»;

в пункте 6:

в абзаце втором слова «обеспечению технической защиты» заменить словами «технической и криптографической защите»;

абзац шестой изложить в следующей редакции:

«осуществляет внешний контроль за обеспечением безопасности КВОИ в порядке, установленном ОАЦ;»;

часть первую пункта 16 дополнить абзацем шестым следующего содержания:

«наличия сведений, в том числе полученных от государственного органа, иной организации или физического лица, свидетельствующих о невыполнении владельцем КВОИ

требований, установленных эксплуатационной документацией на КВОИ и техническими нормативными правовыми актами.».

3. Установить, что юридические лица и индивидуальные предприниматели вправе осуществлять деятельность по технической и (или) криптографической защите информации на основании специальных разрешений (лицензий) на деятельность по технической защите информации, в том числе криптографическими методами, включая применение электронной цифровой подписи, выданных до вступления в силу настоящего Указа, до истечения срока их действия.

Внесение изменений и (или) дополнений в соответствии с настоящим Указом в специальные разрешения (лицензии), указанные в части первой настоящего пункта, производится при внесении в них иных изменений и (или) дополнений, продлении срока их действия, а также выдаче их дубликатов после вступления в силу настоящего Указа.

В случае, если при продлении срока действия либо выдаче дубликата специальных разрешений (лицензий), указанных в части первой настоящего пункта, одновременно осуществляется внесение в них изменений и (или) дополнений в соответствии с настоящим Указом, государственная пошлина за внесение таких изменений и (или) дополнений не взимается.

4. *Для служебного пользования.*

5. Совету Министров Республики Беларусь совместно с Оперативно-аналитическим центром при Президенте Республики Беларусь в шестимесячный срок обеспечить приведение актов законодательства в соответствие с настоящим Указом и принять иные меры по его реализации.

6. Настоящий Указ вступает в силу через шесть месяцев после его официального опубликования, за исключением подпункта 2.1 пункта 2, пунктов 4, 5 и данного пункта, которые вступают в силу со дня подписания настоящего Указа.

Президент Республики Беларусь **А.Лукашенко**

УТВЕРЖДЕНО

Указ Президента
Республики Беларусь
16.04.2013 № 196

ПОЛОЖЕНИЕ
о технической и криптографической защите информации в Республике Беларусь

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящее Положение определяет правовые и организационные основы технической и криптографической защиты информации в Республике Беларусь.

2. Требования настоящего Положения не распространяются на техническую защиту информации в системах шифрованной и других видов специальной связи, а также на криптографическую защиту информации, содержащей государственные секреты.

3. Для целей настоящего Положения применяются термины и их определения в значениях, определенных Законом Республики Беларусь от 10 ноября 2008 года «Об информации, информатизации и защите информации» (Национальный реестр правовых актов Республики Беларусь, 2008 г., № 279, 2/1552), Положением об отнесении объектов информатизации к критически важным и обеспечении безопасности критически важных объектов информатизации, утвержденным Указом Президента Республики Беларусь от 25 октября 2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации» (Национальный реестр правовых актов Республики

Беларусь, 2011 г., № 121, 1/13026), техническими нормативными правовыми актами, а также следующие термины и их определения:

криптографическая защита информации – деятельность, направленная на обеспечение конфиденциальности, контроля целостности и подлинности информации с использованием средств криптографической защиты информации;

несанкционированное воздействие на информацию – изменение или уничтожение информации, осуществляемое с нарушением установленных прав или правил;

несанкционированный доступ к информации – доступ к информации, осуществляемый с нарушением установленных прав или правил разграничения доступа;

перехват информации – неправомерное получение информации с использованием технических средств, осуществляющих обнаружение, прием и обработку информативных сигналов;

средства криптографической защиты информации – технические, программные, программно-аппаратные средства защиты информации, реализующие один или несколько криптографических алгоритмов (шифрование, выработка и проверка электронной цифровой подписи, хэширование, имитозащита) и криптографические протоколы, а также функции управления криптографическими ключами, механизмы идентификации и аутентификации;

средства технической защиты информации – технические, программные, программно-аппаратные средства защиты информации, предназначенные для защиты информации от ее утечки по техническим каналам, несанкционированного доступа, несанкционированных воздействий на информацию, блокирования правомерного доступа к ней, иных неправомерных воздействий на информацию, а также для контроля эффективности ее защищенности;

техническая защита информации – деятельность, направленная на обеспечение конфиденциальности, целостности, доступности и сохранности информации техническими мерами без применения средств криптографической защиты информации;

утечка информации по техническим каналам – неконтролируемое распространение информации от объекта информатизации через физическую среду до технического средства, осуществляющего перехват информации.

4. К объектам, на которых осуществляется техническая защита информации в соответствии с настоящим Положением, относятся:

объекты информатизации, предназначенные для обработки информации, содержащей государственные секреты;

информационные системы, предназначенные для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам;

критически важные объекты информатизации.

К объектам, на которых осуществляется криптографическая защита информации в соответствии с настоящим Положением, относятся:

государственные информационные системы в части обеспечения целостности и подлинности электронных документов;

информационные системы, предназначенные для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам;

критически важные объекты информатизации.

На объектах, указанных в абзацах третьем и четвертом части первой и третьем и четвертом части второй настоящего пункта, осуществляется техническая и криптографическая или только техническая защита информации в зависимости от возможного ущерба вследствие нарушения конфиденциальности, целостности, доступности, сохранности и подлинности защищаемой информации.

5. Требования настоящего Положения обязательны для применения:

собственниками (владельцами) критически важных объектов информатизации, объектов информатизации, предназначенных для обработки информации, содержащей государственные секреты, а также собственниками (владельцами) государственных информационных систем в части обеспечения целостности и подлинности электронных документов;

собственниками (владельцами) информационных систем, в которых обрабатывается служебная информация ограниченного распространения;

собственниками (владельцами) информационных систем, предназначенных для обработки информации о частной жизни физического лица и персональных данных, за исключением информационных систем, созданных с участием резидента Парка высоких технологий либо третьими лицами и используемых резидентом Парка высоких технологий при осуществлении деятельности в соответствии с пунктом 3 Положения о Парке высоких технологий, утвержденного Декретом Президента Республики Беларусь от 22 сентября 2005 г. № 12, которая связана с разработкой и (или) применением технологии реестра блоков транзакций (блокчейн);

государственными органами и иными государственными организациями, а также хозяйственными обществами, в отношении которых Республика Беларусь либо административно-территориальная единица, обладая акциями (долями в уставных фондах), может определять решения, принимаемые этими хозяйственными обществами, являющимися собственниками (владельцами) информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам.

Иные собственники (владельцы) объектов информатизации (в том числе информационных систем), за исключением указанных в части первой настоящего пункта, вправе руководствоваться требованиями настоящего Положения, если иное не предусмотрено законодательными актами.

6. Финансирование мероприятий по технической и криптографической защите информации осуществляется за счет и в пределах средств, предусмотренных в республиканском и местных бюджетах на содержание государственных органов и иных организаций (далее – организации), собственных средств организаций, а также иных источников, не запрещенных законодательством.

ГЛАВА 2
ОСНОВЫ ГОСУДАРСТВЕННОГО РЕГУЛИРОВАНИЯ И УПРАВЛЕНИЯ В СФЕРЕ ТЕХНИЧЕСКОЙ И КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

7. Государственное регулирование и управление в сфере технической и криптографической защиты информации осуществляются Президентом Республики Беларусь и Оперативно-аналитическим центром при Президенте Республики Беларусь (далее – ОАЦ).

8. Президент Республики Беларусь определяет единую государственную политику и осуществляет иное государственное регулирование в сфере технической и криптографической защиты информации.

9. ОАЦ:

9.1. определяет приоритетные направления технической и криптографической защиты информации;

9.2. координирует деятельность организаций по применению мер технической и криптографической защиты информации;

9.3. осуществляет контроль за технической и криптографической защитой информации в организациях;

9.4. определяет порядок:

технической защиты государственных секретов;

технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам;

аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам;

9.5. организует и осуществляет техническое нормирование и стандартизацию по вопросам технической и криптографической защиты информации;

9.6. осуществляет:

лицензирование деятельности по технической и (или) криптографической защите информации;

подтверждение соответствия и проведение государственной экспертизы средств технической и криптографической защиты информации, за исключением криптографических средств защиты государственных секретов, определяет порядок проведения такой экспертизы;

9.7. выступает заказчиком государственных научно-технических и иных программ и проектов, обеспечивает организацию и проведение научно-исследовательских, опытно-конструкторских и иных работ в сфере технической и криптографической защиты информации;

9.8. заключает в пределах своей компетенции международные договоры межведомственного характера;

9.9. разрабатывает проекты нормативных правовых актов, в том числе технических нормативных правовых актов, и принимает (издает) такие акты по вопросам технической и криптографической защиты информации;

9.10. осуществляет иные полномочия в сфере технической и криптографической защиты информации в соответствии с настоящим Положением и иными законодательными актами.

ГЛАВА 3
ПОРЯДОК ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

10. Организации – собственники (владельцы) объектов, на которых осуществляется техническая защита информации:

10.1. определяют перечни таких объектов;

10.2. обеспечивают проведение мероприятий по созданию систем защиты информации:

на объектах информатизации, предназначенных для обработки информации, содержащей государственные секреты, в порядке, предусмотренном законодательством о государственных секретах;

информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам;

10.3. организуют и проводят комплекс организационно-технических мероприятий, в результате которых документально подтверждается соответствие:

объектов информатизации, предназначенных для обработки информации, содержащей государственные секреты, требованиям законодательства о государственных секретах (далее – аттестация объектов информатизации);

систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, требованиям законодательства об информации, информатизации и защите информации (далее – аттестация систем защиты информации);

10.4. организуют и проводят комплекс мероприятий по технической защите информации, обрабатываемой на критически важных объектах информатизации, при создании систем безопасности этих объектов;

10.5. осуществляют методическое руководство деятельностью по применению мер технической защиты информации организациями, находящимися в их подчинении (входящими в состав), а также хозяйственными обществами, акции (доли в уставных фондах) которых принадлежат Республике Беларусь либо административно-территориальной единице и переданы в управление указанных организаций;

10.6. представляют в ОАЦ сведения о состоянии технической защиты информации в порядке, определяемом ОАЦ.

11. Мероприятия по технической защите информации, осуществляемые организациями, должны предусматривать:

на объектах информатизации, предназначенных для обработки информации, содержащей государственные секреты, – защиту информации от утечки по техническим каналам и несанкционированного доступа к ней в порядке, установленном законодательством о государственных секретах;

в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, и на критически важных объектах информатизации – защиту информации от несанкционированного доступа к ней и несанкционированного воздействия на нее в порядке, установленном законодательством об информации, информатизации и защите информации.

12. Работы по технической защите информации в организации проводятся подразделением технической защиты информации или иными подразделениями (должностными лицами), выполняющими функции по технической защите информации (далее – подразделение технической защиты информации).

13. Аттестация объектов информатизации и систем защиты информации проводится до ввода в эксплуатацию соответственно объектов информатизации, предназначенных для обработки информации, содержащей государственные секреты, и информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам.

14. В случае невозможности выполнения работ по технической защите информации силами подразделения технической защиты информации руководителем организации могут привлекаться организации, имеющие специальные разрешения (лицензии) на деятельность по технической и (или) криптографической защите информации в части соответствующих составляющих данный вид деятельности работ и услуг.

15. При осуществлении технической защиты информации используются средства технической защиты информации, имеющие сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь, или положительное экспертное заключение по результатам государственной экспертизы, проводимой ОАЦ.

16. Ответственность за организацию работ по технической защите информации возлагается на руководителя организации.

ГЛАВА 4
ПОРЯДОК КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

17. Решение об организации криптографической защиты информации принимается:

собственником (владельцем) информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, – при реализации комплекса мероприятий по созданию системы защиты информации;

собственником (владельцем) государственных информационных систем – при использовании в этих системах электронных документов;

владельцем критически важных объектов информатизации – при реализации комплекса мероприятий по созданию системы безопасности этих объектов.

18. Криптографическая защита информации осуществляется путем применения средств криптографической защиты информации, а также комплекса организационных мер.

19. Средства криптографической защиты информации, используемые в системах защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, и на критически важных объектах информатизации, подлежат сертификации в Национальной системе подтверждения соответствия Республики Беларусь на соответствие требованиям технических нормативных правовых актов или государственной экспертизе. Перечень технических нормативных правовых актов, а также требования к средствам криптографической защиты информации до введения в действие необходимых технических нормативных правовых актов определяются ОАЦ.

20. При осуществлении криптографической защиты служебной информации ограниченного распространения могут применяться только программно-аппаратные или технические средства криптографической защиты информации. Дополнительные организационные и технические меры по криптографической защите указанной информации определяются ОАЦ.

21. Работы по криптографической защите информации в организации проводятся подразделением технической защиты информации или иными подразделениями (должностными лицами), выполняющими функции по криптографической защите информации.

22. В случае невозможности выполнения работ по криптографической защите информации силами подразделения технической защиты информации или иными подразделениями (должностными лицами), выполняющими функции по криптографической защите информации, руководителем организации могут привлекаться организации, имеющие специальные разрешения (лицензии) на деятельность по технической и (или) криптографической защите информации в части соответствующих составляющих данный вид деятельности работ и услуг.

ГЛАВА 5
КОНТРОЛЬ ЗА ТЕХНИЧЕСКОЙ И КРИПТОГРАФИЧЕСКОЙ ЗАЩИТОЙ ИНФОРМАЦИИ

23. Контроль за технической и криптографической защитой информации (далее – контроль) проводится в целях проверки выполнения требований нормативных правовых актов в области технической и криптографической защиты информации организациями, указанными в части первой пункта 5 настоящего Положения.

24. Контроль осуществляется ОАЦ в форме проверок, проводимых в соответствии с планом проверок технической и криптографической защиты информации, размещаемым на официальном сайте ОАЦ в глобальной компьютерной сети Интернет не позднее 20 декабря года, предшествующего году проведения проверки.

Без включения в план, указанный в части первой настоящего пункта, проверки организаций могут назначаться начальником ОАЦ при наличии сведений, в том числе полученных от государственного органа, иной организации или физического лица, свидетельствующих о совершаемом (совершенном) нарушении требований нормативных правовых актов в области технической и криптографической защиты информации или о фактах возникновения предпосылок к несанкционированному распространению информации, распространение и (или) предоставление которой ограничено, или угроз безопасности критически важных объектов информатизации.

25. Проверки организаций, имеющих объекты информатизации, предназначенные для обработки информации, содержащей государственные секреты, проводятся в порядке, определенном настоящим Положением, с учетом требований законодательства о государственных секретах.

26. Для проведения проверки решением начальника ОАЦ назначается комиссия.

О назначении проверки организация письменно уведомляется не позднее 10 рабочих дней до начала ее проведения. Уведомление должно содержать сведения о дате начала проверки, сроках ее проведения, составе комиссии, а также о вопросах, подлежащих проверке.

27. Для проведения проверки на каждого члена комиссии оформляется предписание.

Предписание подписывается начальником ОАЦ или его уполномоченным заместителем и заверяется гербовой печатью ОАЦ.

28. Для проведения проверки разрабатывается план проверочных мероприятий, который утверждается начальником ОАЦ или его уполномоченным заместителем.

29. Проверка начинается с внесения предписания и представления комиссии руководителю организации или его уполномоченному заместителю.

При представлении комиссии руководителю организации или его уполномоченному заместителю доводится план проверочных мероприятий.

30. Проверочные мероприятия проводятся в присутствии определенных руководителем организации сотрудников подразделения технической защиты информации и (или) подразделения по защите государственных секретов.

31. В ходе проверки оцениваются:

31.1. наличие подразделения технической защиты информации, соответствие закрепленных за ним функций требованиям нормативных правовых актов в области технической и криптографической защиты информации;

31.2. наличие и содержание:

перечней объектов, на которых осуществляется техническая и криптографическая защита информации;

организационно-распорядительных документов, регламентирующих вопросы технической и криптографической защиты информации в организации;

документов, определяющих порядок и результаты проведения мероприятий по созданию систем защиты информации на объектах информатизации, предназначенных для обработки информации, содержащей государственные секреты, систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, аттестации объектов информатизации и систем защиты информации, вводу этих объектов и информационных систем в эксплуатацию;

31.3. эффективность и достаточность технических мер защиты информации на объектах, на которых осуществляется техническая защита информации, в реальных условиях эксплуатации;

31.4. порядок использования средств криптографической защиты информации;

31.5. эффективность и достаточность принятых мер по криптографической защите информации.

32. При проведении проверки председатель комиссии самостоятельно определяет методы и способы ее осуществления.

33. В случае обнаружения нарушений требований нормативных правовых актов в области технической и криптографической защиты информации, создающих угрозу национальной безопасности, начальник ОАЦ или его уполномоченный заместитель вправе вынести требование (предписание) о приостановлении обработки информации на объектах, на которых осуществляется техническая и криптографическая защита информации.

Требование (предписание), а также информация о выявленных нарушениях, повлекших его вынесение, непосредственно в ходе проверки доводятся до руководства организации, в которой выявлены нарушения. Руководство организации обязано принять меры по запрещению обработки информации на соответствующих объектах до устранения выявленных нарушений.

Об устранении нарушений организация в пределах срока, установленного в требовании (предписании), письменно сообщает в ОАЦ.

Начальник ОАЦ или его уполномоченный заместитель не позднее двух рабочих дней со дня получения уведомления принимает решение о возобновлении обработки информации на соответствующих объектах либо назначает проведение контрольной проверки устранения организацией выявленных нарушений, по итогам проведения которой не позднее двух рабочих дней со дня ее окончания выносит решение о возобновлении обработки информации.

При наличии объективных обстоятельств, не позволивших устранить нарушения, указанные в требовании (предписании), в установленные в нем сроки, по заявлению организации, поданному не позднее трех рабочих дней до дня истечения этих сроков с указанием соответствующих обстоятельств, начальником ОАЦ или его уполномоченным заместителем может быть принято решение о переносе сроков устранения нарушений. Решение о переносе сроков или об отказе в этом принимается не позднее двух рабочих дней со дня поступления заявления.

34. По результатам проверки комиссией составляется акт в количестве не менее двух экземпляров с отражением в нем экспертной оценки принятых мер по технической и криптографической защите информации в организации, выявленных нарушений и недостатков, предложений по их устранению.

В акте проверки устанавливается срок, в который организация обязана письменно информировать ОАЦ об устранении нарушений и недостатков, реализации предложений, содержащихся в акте проверки, который не может превышать шести месяцев.

Акт проверки составляется в течение пяти рабочих дней со дня окончания проверки и подписывается всеми членами комиссии.

Акт проверки в течение трех рабочих дней после его составления доводится председателем комиссии до руководителя организации или его уполномоченного заместителя, о чем делается соответствующая запись в акте, заверенная подписью этого руководителя (его заместителя).

Первый экземпляр акта в установленном порядке направляется в организацию, второй – остается в ОАЦ, а третий экземпляр акта направляется в вышестоящую по отношению к проверяемой организацию (при ее наличии).

35. При наличии возражений по акту проверки руководитель организации или его уполномоченный заместитель не позднее 15 рабочих дней со дня поступления акта в организацию представляет в ОАЦ в письменном виде возражения по его содержанию.

Обоснованность доводов, изложенных в возражениях, рассматривается ОАЦ не позднее 10 рабочих дней со дня их поступления. При необходимости по решению начальника ОАЦ для рассмотрения их обоснованности может быть назначена специальная комиссия. Результаты рассмотрения отражаются в письменном заключении, которое направляется в организацию. В целях дополнительного изучения обоснованности доводов, изложенных в возражениях, не позднее 10 рабочих дней со дня их поступления начальником ОАЦ может быть назначена дополнительная проверка организации.

36. Начальник ОАЦ или его уполномоченный заместитель по предложению председателя комиссии устанавливает порядок и сроки проведения мероприятий по контролю за устранением нарушений и недостатков, выявленных в ходе проверки.

37. Вынесенные по результатам проверки решение по акту проверки, требование (предписание) об устранении нарушений, а также действия (бездействие) членов комиссии могут быть обжалованы организацией в суд в порядке, установленном законодательными актами.

ГЛАВА 6
ПРОВЕДЕНИЕ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИХ И ОПЫТНО-КОНСТРУКТОРСКИХ РАБОТ В СФЕРЕ ТЕХНИЧЕСКОЙ И КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

38. Научно-исследовательские и опытно-конструкторские работы в сфере технической и криптографической защиты информации организуются и проводятся ОАЦ и иными организациями в целях:

изучения и анализа современных тенденций развития методов и средств технической и криптографической защиты информации;

создания нормативной правовой базы в сфере технической и криптографической защиты информации;

оценки вероятных и актуальных видов угроз защищаемой информации, а также определения оптимальных способов противодействия угрозам защищаемой информации;

обоснования необходимой степени защищенности объектов, на которых осуществляется техническая и криптографическая защита информации;

разработки предложений по формированию единой политики по технической и криптографической защите информации;

создания перспективных отечественных методов и средств защиты информации;

научно-методического обеспечения подтверждения соответствия средств защиты информации требованиям технических нормативных правовых актов.

39. Научно-исследовательские и опытно-конструкторские работы в сфере технической и криптографической защиты информации выполняются в порядке, установленном законодательством, в том числе техническими нормативными правовыми актами.