ПРИКАЗ ОПЕРАТИВНО-АНАЛИТИЧЕСКОГО ЦЕНТРА ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ БЕЛАРУСЬ
16 января 2015 г. № 3

# О внесении дополнений и изменений в приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 30 августа 2013 г. № 62

В соответствии с подпунктом 9.4 пункта 9 Положения о технической и криптографической защите информации в Республике Беларусь, утвержденного Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации», и частью четвертой статьи 28 Закона Республики Беларусь от 10 ноября 2008 года «Об информации, информатизации и защите информации» ПРИКАЗЫВАЮ:

1. Внести в приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 30 августа 2013 г. № 62 «О некоторых вопросах технической и криптографической защиты информации» (Национальный правовой Интернет-портал Республики Беларусь, 10.09.2013, 7/2561) следующие дополнения и изменения:

1.1. преамбулу дополнить словами «и частью четвертой статьи 28 Закона Республики Беларусь от 10 ноября 2008 года «Об информации, информатизации и защите информации»;

1.2. Положение о порядке технической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, утвержденное этим приказом, изложить в новой редакции (прилагается);

1.3. в Положении о порядке криптографической защиты информации в государственных информационных системах, информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, и на критически важных объектах информатизации, утвержденном этим приказом:

1.3.1. в пункте 3:

абзац второй части первой изложить в следующей редакции:

«собственником (владельцем) информационной системы – на этапе проектирования системы защиты информации информационной системы;»;

часть вторую после слов «информационных систем» дополнить словами «, ГИС и владельцы КВОИ»;

1.3.2. в пункте 6:

первое предложение части первой после слов «информационной системы» дополнить словами «, ГИС и владельцем КВОИ»;

часть вторую после слов «информационную систему» дополнить словами «или в техническом задании на информационную систему»;

1.3.3. в пункте 9:

из части первой слова «на соответствие требованиям безопасности информации, содержащимся в документах согласно приложению» исключить;

часть вторую исключить;

части третью и четвертую считать соответственно частями второй и третьей;

1.3.4. абзац второй пункта 10 после слов «информационным сетям,» дополнить словами «сетям электросвязи общего пользования,»;

1.3.5. приложение к этому Положению изложить в новой редакции (прилагается);

1.4. Положение о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, утвержденное этим приказом, изложить в новой редакции (прилагается).

2. Настоящий приказ не распространяется на:

информационные системы, предназначенные для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам (далее – информационные системы), введенные в эксплуатацию до вступления его в силу, на срок действия аттестата соответствия системы защиты информации информационной системы требованиям по защите информации (далее – аттестат соответствия);

вновь создаваемые или модернизируемые информационные системы, на которые разрабатываются (корректируются) либо утверждены задания по безопасности. Аттестация систем защиты информации таких информационных систем и ввод их в эксплуатацию осуществляются в соответствии с законодательством, действовавшим до вступления в силу настоящего приказа.

По истечении срока действия аттестата соответствия собственники (владельцы) информационных систем, указанных в части первой настоящего пункта, проводят повторную аттестацию (обращаются за проведением повторной аттестации) систем защиты информации информационных систем в порядке, установленном приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 30 августа 2013 г. № 62 (с изменениями и дополнениями, внесенными в них настоящим приказом).

Собственники (владельцы) информационных систем, указанных в части первой настоящего пункта, вправе руководствоваться требованиями Положения о порядке технической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, и Положения о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, утвержденных приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 30 августа 2013 г. № 62 (с изменениями и дополнениями, внесенными в них настоящим приказом), без учета переходных положений, определенных частями первой и второй данного пункта.

3. Настоящий приказ вступает в силу после его официального опубликования.

**Начальник** **С.В.Шпегун**

УТВЕРЖДЕНО

Приказ
Оперативно-аналитического
центра при Президенте
Республики Беларусь
30.08.2013 № 62
(в редакции приказа
Оперативно-аналитического
центра при Президенте
Республики Беларусь
16.01.2015 № 3)

**ПОЛОЖЕНИЕ**
**о порядке технической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам**

## ГЛАВА 1
## ОБЩИЕ ПОЛОЖЕНИЯ

1. В настоящем Положении, разработанном в соответствии с подпунктом 9.4 пункта 9 Положения о технической и криптографической защите информации в Республике Беларусь, утвержденного Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации» (Национальный правовой Интернет-портал Республики Беларусь, 18.04.2013, 1/14225), устанавливается порядок технической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам (далее – информационные системы).

2. Для целей настоящего Положения термины и их определения используются в значениях, установленных 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 о технической и криптографической защите информации в Республике Беларусь, техническими нормативными правовыми актами, а также следующий термин и его определение:

политика информационной безопасности – совокупность документированных правил, процедур и требований в области защиты информации, действующих у собственника (владельца) информационной системы (далее, если не определено иное, – организация).

3. Для защиты информации в информационной системе создается система защиты информации, включающая комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации.

4. 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 Оперативно-аналитическим центром при Президенте Республики Беларусь (далее – ОАЦ).

5. Подключение информационных систем к сетям электросвязи общего пользования, в том числе к глобальной компьютерной сети Интернет, осуществляется при условии выполнения требований, предусмотренных в части первой пункта 10 настоящего Положения и в приложении к этому Положению.

6. 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).

7. В случае невозможности выполнения работ по технической защите информации силами подразделения технической защиты информации руководителем организации могут на договорной основе 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 (далее – специализированные организации).

8. Комплекс мероприятий по защите информации, подлежащей обработке в информационной системе, включает:

проектирование системы защиты информации;

создание системы защиты информации;

аттестацию системы защиты информации в соответствии с Положением о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, утвержденным приказом, утверждающим настоящее Положение;

обеспечение функционирования системы защиты информации в процессе эксплуатации информационной системы;

обеспечение защиты информации в случае прекращения эксплуатации информационной системы.

## ГЛАВА 2
## ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

9. На этапе проектирования системы защиты информации осуществляются:

классификация информации, хранящейся и обрабатываемой в информационной системе, в соответствии с законодательством об информации, информатизации и защите информации, в том числе техническими нормативными правовыми актами;

анализ организационной структуры информационной системы и информационных потоков в целях определения состава (количества) и мест размещения элементов системы (аппаратных и программных), ее физических и логических границ;

присвоение информационной системе класса типового объекта информатизации в порядке, установленном СТБ 34.101.30-2007 «Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация»;

определение требований к системе защиты информации в задании по безопасности на информационную систему (далее – задание по безопасности) или в техническом задании на информационную систему (далее – техническое задание).

10. Задание по безопасности разрабатывается в соответствии с техническими нормативными правовыми актами и с учетом требований согласно приложению к настоящему Положению в случае, если предполагается:

размещение составных частей (сегментов) информационной системы одновременно на территории двух и более областей Республики Беларусь либо одновременно на территории г. Минска и одной или нескольких областей Республики Беларусь;

подключение информационной системы к сетям электросвязи общего пользования, в том числе к глобальной компьютерной сети Интернет.

Требования к системам защиты информации иных информационных систем определяются в техническом задании, которое должно содержать:

цели создания системы защиты информации;

класс информационной системы;

сведения о взаимодействии с иными информационными системами (в случае предполагаемого взаимодействия);

перечень требований, определенных согласно приложению к настоящему Положению.

Задание по безопасности и техническое задание разрабатываются собственником (владельцем) информационной системы либо специализированной организацией и утверждаются собственником (владельцем) информационной системы.

Задание по безопасности подлежит оценке в аккредитованной испытательной лаборатории и после такой оценки направляется собственником (владельцем) информационной системы в ОАЦ для учета.

## ГЛАВА 3
## СОЗДАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

11. На этапе создания системы защиты информации осуществляются:

разработка политики информационной безопасности;

внедрение планируемых к использованию средств защиты информации, проверка их работоспособности и совместимости;

внедрение организационных мер по защите информации;

опытная эксплуатация системы защиты информации;

приемочные испытания системы защиты информации.

12. Политика информационной безопасности должна содержать:

цели создания системы защиты информации;

перечень субъектов и объектов информационной системы, сведения о месте их размещения и порядке информационного взаимодействия субъектов с объектами этой системы и объектов между собой;

способы разграничения доступа субъектов к объектам информационной системы;

права и обязанности субъектов информационной системы;

порядок взаимодействия с иными информационными системами (в случае предполагаемого взаимодействия);

перечень организационных мер, направленных на реализацию требований по созданию системы защиты информации;

порядок действий при возникновении угроз обеспечения конфиденциальности, целостности, доступности, подлинности и сохранности информации, в том числе чрезвычайных и непредотвратимых обстоятельств (непреодолимой силы), и при ликвидации их последствий.

13. В целях реализации политики информационной безопасности разрабатываются локальные нормативные правовые акты организации, регламентирующие порядок:

использования объектов информационной системы и их управления (администрирования);

резервирования и уничтожения информации;

защиты от вредоносного программного обеспечения;

выявления угроз, которые могут привести к сбоям, нарушению функционирования информационной системы;

реагирования на инциденты информационной безопасности;

контроля (мониторинга) за функционированием информационной системы.

14. В ходе внедрения средств защиты информации осуществляется их монтаж и наладка в соответствии с эксплуатационной документацией.

При проверке работоспособности и совместимости планируемых к использованию средств защиты информации осуществляется проверка корректности выполнения такими средствами требований безопасности в реальных условиях эксплуатации и во взаимодействии с элементами информационной системы.

15. Внедрение организационных мер защиты информации осуществляется в целях реализации требований, изложенных в локальных нормативных правовых актах организации, которые доводятся до сведения субъектов информационной системы под подпись.

16. Опытная эксплуатация системы защиты информации осуществляется для проверки ее работоспособности в различных режимах функционирования информационной системы, в том числе при необходимости в условиях чрезвычайной ситуации. В случае выявления в процессе опытной эксплуатации системы защиты информации недостатков осуществляется их устранение с последующей повторной опытной эксплуатацией.

17. Приемочные испытания системы защиты информации проводятся в целях проверки выполнения требований к системе защиты информации, изложенных в задании по безопасности или в техническом задании.

## ГЛАВА 4
## ОСОБЕННОСТИ ЭКСПЛУАТАЦИИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

18. В процессе эксплуатации аттестованной в установленном порядке системы защиты информации осуществляются:

контроль за соблюдением требований, установленных в нормативных правовых актах, в том числе в технических нормативных правовых актах, локальных нормативных правовых актах организации;

контроль за порядком использования объектов информационной системы;

мониторинг функционирования системы защиты информации;

выявление угроз, которые могут привести к сбоям, нарушению функционирования информационной системы;

резервное копирование информации, содержащейся в информационной системе;

обучение (повышение квалификации) субъектов информационной системы.

19. Собственники (владельцы) информационных систем в соответствии с локальными нормативными правовыми актами выявляют и фиксируют нарушения требований по защите информации, принимают меры по своевременному устранению таких нарушений.

В случае невозможности устранения выявленных нарушений в течение пяти рабочих дней с момента выявления собственники (владельцы) информационных систем обязаны:

прекратить обработку информации, распространение и (или) предоставление которой ограничено, и письменно информировать ОАЦ о данных нарушениях;

провести оценку достаточности принятых мер по защите информации, обрабатываемой в информационной системе, на предмет необходимости доработки системы защиты информации информационной системы и ее повторной аттестации.

20. Ремонтные, наладочные и профилактические работы в информационной системе проводятся с участием представителя подразделения технической защиты информации.

21. В случае прекращения эксплуатации информационной системы собственник (владелец) информационной системы в соответствии с локальными нормативными правовыми актами организации принимает меры по:

защите информации, содержащейся в информационной системе;

резервному копированию информации (при необходимости), обеспечению ее конфиденциальности и целостности;

уничтожению (удалению) данных с машинных носителей информации и (или) уничтожению таких носителей информации.

Уничтожение (удаление) данных с машинных носителей информации производится при необходимости передачи машинного носителя информации лицам, не являющимся субъектами информационной системы, в том числе для ремонта, технического обслуживания.

22. Модернизация действующих систем защиты информации осуществляется в порядке, установленном настоящим Положением для создания этих систем.

Приложение
к Положению о порядке
технической защиты информации
в информационных системах,
предназначенных для обработки
информации, распространение
и (или) предоставление которой
ограничено, не отнесенной
к государственным секретам

**ПЕРЕЧЕНЬ**
**требований к системе защиты информации, подлежащих включению в задание по безопасности на информационную систему или в техническое задание на информационную систему**

| № п/п | Требования к системе защиты информации, подлежащие включению в задание по безопасности на информационную систему или в техническое задание на информационную систему | Класс объекта информатизации | | |
|---|---|---|---|---|
| | | А2 | Б2 | В2 |
| 1 | Идентификация объектов информационной системы (далее – объекты) и закрепление за ними субъектов информационной системы (далее – субъекты) | + | + | + |
| 2 | Идентификация и аутентификация субъектов | + | + | + |
| 3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение | + | + | + |
| 4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации | + | + | + |
| 5 | Исключение отображения аутентификационной информации (защита обратной связи при вводе аутентификационной информации) | + | + | + |
| 6 | Изменение атрибутов безопасности, установленных по умолчанию в соответствии с политикой информационной безопасности | + | + | + |
| 7 | Полномочное управление (создание, активация, блокировка и уничтожение) учетными записями субъектов | + | + | + |
| 8 | Определение прав и обязанностей субъектов | + | + | + |
| 9 | Реализация правил разграничения доступа субъектов к объектам | + | + | + |
| 10 | Контроль за соблюдением правил генерации и смены паролей субъектов | + | + | + |
| 11 | Ограничение неуспешных попыток аутентификации | + | + | + |
| 12 | Блокирование доступа к информационной системе после истечения установленного времени бездействия (неактивности) субъекта или по его запросу | + | + | + |
| 13 | Определение при необходимости действий субъектов, которые могут совершаться такими субъектами до их идентификации и аутентификации | + | + | + |
| 14 | Реализация защищенного удаленного доступа субъектов к объектам через внешние информационно-телекоммуникационные сети | – | – | + |
| 15 | Наличие актуальной схемы сети с указанием объектов, внешних подключений и информационных потоков | ± | + | + |
| 16 | Управление (фильтрация, маршрутизация, контроль соединений) информационными потоками между объектами, а также между информационными системами | ± | + | + |
| 17 | Ограничение входящего и исходящего трафика только необходимыми соединениями | – | + | + |
| 18 | Запрет на использование в информационной системе технологий беспроводного доступа | + | + | + |
| 19 | Регламентация порядка использования в информационной системе мобильных технических средств и контроля за таким использованием | + | + | + |
| 20 | Регламентация порядка взаимодействия с информационными системами третьих лиц (внешние информационные системы), контроля за таким взаимодействием и управления подключением | – | – | + |
| 21 | Определение перечня разрешенного программного обеспечения и регламентация порядка его установки и использования | + | + | + |
| 22 | Учет машинных носителей информации, использующихся для обработки и хранения информации | + | + | + |

| | | | | |
|---|---|---|---|---|
| 23 | Регламентация доступа к учтенным машинным носителям информации | + | + | + |
| 24 | Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на учтенных машинных носителях информации | + | + | + |
| 25 | Исключение возможности использования учтенных машинных носителей информации в информационных системах третьих лиц | ±[1] | ±[1] | ±[1] |
| 26 | Контроль за использованием интерфейсов ввода (вывода) информации на машинные носители информации | ±[1] | ±[1] | ±[1] |
| 27 | Контроль за вводом (выводом) информации на машинные носители информации | ±[1] | ±[1] | ±[1] |
| 28 | Уничтожение (удаление) данных с машинных носителей информации при их передаче лицам, не являющимся субъектами информационной системы, в том числе для ремонта, технического обслуживания | + | + | + |
| 29 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации | + | + | + |
| 30 | Сбор, запись и хранение информации о событиях безопасности в течение установленного срока хранения | + | + | + |
| 31 | Мониторинг (просмотр, анализ) событий безопасности уполномоченными субъектами | + | + | + |
| 32 | Сбор, запись и хранение, а также мониторинг (просмотр, анализ) информации о сбоях в механизмах сбора информации и достижении предела объема (емкости) памяти устройств хранения уполномоченными пользователями | + | + | + |
| 33 | Синхронизация временных меток и (или) системного времени в информационной системе | ± | + | + |
| 34 | Защита информации о событиях безопасности | + | + | + |
| 35 | Сбор, запись и хранение информации о действиях отдельных субъектов в течение установленного времени хранения, а также регламентирование прав и обязанностей уполномоченных пользователей, осуществляющих просмотр и анализ такой информации | ±[1] | ±[1] | ±[1] |
| 36 | Реализация антивирусной защиты | + | + | + |
| 37 | Регламентация обновления базы данных признаков вредоносного программного обеспечения | + | + | + |
| 38 | Регламентация проведения проверок операционных систем на предмет обнаружения аномалий, вызванных присутствием в системе вредоносного программного обеспечения | + | + | + |
| 39 | Реализация подсистемы обнаружения вторжений | – | ±[1] | + |
| 40 | Обновление базы сигнатур подсистемы обнаружения вторжений | – | ±[1] | + |
| 41 | Выявление уязвимостей информационной системы и оперативное их устранение | + | + | + |
| 42 | Контроль за установкой обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации | + | + | + |
| 43 | Контроль за работоспособностью, параметрами настройки и правильностью функционирования программного обеспечения и средств защиты информации | + | + | + |
| 44 | Контроль за неизменностью состава технических средств, программного обеспечения и средств защиты информации | + | + | + |
| 45 | Регламентирование порядка резервирования информации и программного обеспечения, включая программное обеспечение средств защиты информации | + | + | + |
| 46 | Контроль за содержанием информации, передаваемой из информационной системы (основанный на свойствах объекта доступа и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, шаблонов и иных методов) | – | ±[1] | + |
| 47 | Идентификация и аутентификация субъектов и объектов в виртуальной инфраструктуре, в том числе уполномоченных пользователей по управлению средствами виртуализации | + | + | + |
| 48 | Управление доступом субъектов к объектам в виртуальной инфраструктуре, в том числе внутри виртуальных машин | + | + | + |
| 49 | Регистрация событий безопасности в виртуальной инфраструктуре | + | + | + |
| 50 | Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных | + | + | + |
| 51 | Контроль за обеспечением целостности виртуальной инфраструктуры и ее конфигураций | + | + | + |
| 52 | Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры | + | + | + |

| | | | | |
|---|---|---|---|---|
| 53 | Реализация и управление антивирусной защитой в виртуальной инфраструктуре | + | + | + |
| 54 | Деление виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки в них информации отдельным пользователем и (или) группой пользователей | + | + | + |
| 55 | Установление контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации | + | + | + |
| 56 | Контроль и управление физическим доступом внутри контролируемой зоны к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они размещены (установлены), исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, а также в помещения и сооружения, в которых они установлены | + | + | + |
| 57 | Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации | + | + | + |
| 58 | Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе по беспроводным каналам связи | – | + | + |
| 59 | Обеспечение доверенного канала между рабочими местами уполномоченных пользователей и объектами, на которых данные уполномоченные пользователи осуществляют администрирование, мониторинг, а также иные определенные (в соответствии с правами и обязанностями) функции | + | + | + |
| 60 | Контроль за обеспечением санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи | ± | + | + |
| 61 | Контроль за обеспечением санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации | ± | + | + |
| 62 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов | ±[1] | ±[1] | ±[1] |
| 63 | Исключение возможности отрицания пользователем факта отправки информации другому пользователю, а также получения информации от другого пользователя | ±[1] | ±[1] | ±[1] |
| 64 | Защита архивных файлов, параметров настройки средств защиты информации, программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации | + | + | + |
| 65 | Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов | + | + | + |
| 66 | Деление информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы | ±[1] | + | + |
| 67 | Запрет на использование незащищенного подключения к другим информационным системам | ± | + | + |
| 68 | Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы | ±[1] | ±[1] | ±[1] |
| 69 | Защита периметра информационной системы при ее взаимодействии с иными информационными системами и при использовании сетей электросвязи общего пользования, в том числе глобальной компьютерной сети Интернет | – | + | + |
| 70 | Прекращение сетевых соединений по их завершении или по истечении заданного временного интервала неактивности сетевого соединения | ± | + | + |
| 71 | Использование в информационной системе или в ее сегментах различных типов общесистемного программного обеспечения | ±[1] | ±[1] | + |
| 72 | Воспроизведение ложных и (или) сокрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик информационной системы или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных информационных технологиях и (или) структурно- | – | ±[1] | ±[1] |

| | | | | |
|---|---|---|---|---|
| | функциональных характеристиках информационной системы | | | |
| 73 | Регламентирование порядка доступа к настройкам средств защиты и контроль за таким доступом | + | + | + |
| 74 | Реализация комплекса мер по криптографической защите информации, обрабатываемой в информационной системе и (или) передаваемой за пределы такой системы в соответствии с требованиями, изложенными в Положении о порядке криптографической защиты информации в государственных информационных системах, информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, и на критически важных объектах информатизации | + | + | + |

Примечание. Обозначения, используемые в настоящем приложении, означают:

«+» – обязательные требования;

«–» – необязательные требования;

«±» – обязательные требования к системе защиты информации информационной системы, организованной посредством локально-вычислительной сети;

«±[1]» – требования, обязательность использования которых определяется руководителем собственника (владельца) информационной системы.

Приложение
к Положению о порядке
криптографической защиты
информации в государственных
информационных системах,
информационных системах,
предназначенных для обработки
информации, распространение
и (или) предоставление которой
ограничено, не отнесенной
к государственным секретам,
и на критически важных
объектах информатизации
(в редакции приказа
Оперативно-аналитического
центра при Президенте
Республики Беларусь
16.01.2015 № 3)

## ПЕРЕЧЕНЬ
## технических нормативных правовых актов и документов, в которых определены требования к средствам криптографической защиты информации

Таблица 1

## ПЕРЕЧЕНЬ
## технических нормативных правовых актов и документов, в которых определены требования к криптографическим механизмам

| Условное обозначение | Криптографические механизмы | Наименование технических нормативных правовых актов и документов |
|---|---|---|
| Ш | шифрование | |
| Ш1 | | ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования» (раздел 3 или 4)<br>СТБ П 34.101.50-2012 «Информационные технологии и безопасность. Правила регистрации объектов информационных технологий» (приложение Г) |

| | | |
|---|---|---|
| Ш2 | | СТБ 34.101.31-2011 «Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности» (подраздел 6.3, или 6.4, или 6.5 раздела 6) |
| И | имитозащита | |
| И1 | | ГОСТ 28147-89 (раздел 5) |
| И2 | | СТБ 34.101.31-2011 (подраздел 6.6 раздела 6) |
| И3 | | СТБ 34.101.47-2012 «Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел» (подраздел 6.1 раздела 6) |
| ШИ | шифрование и имитозащита | СТБ 34.101.31-2011 (подраздел 6.7 раздела 6) |
| Х | хэширование | СТБ 34.101.31-2011 (подраздел 6.9 раздела 6) |
| П | электронная цифровая подпись | |
| П1 | | СТБ 1176.1-99<br>СТБ 1176.2-99 «Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи» (разделы 5, 6)<br>СТБ П 34.101.50-2012 (приложения Б, В) |
| П2 | | СТБ 34.101.31-2011 (подраздел 6.9 раздела 6)<br>СТБ 34.101.45-2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых» (подраздел 7.1 раздела 7, таблица Б1 приложения Б, приложение Д) |
| К | управление криптографическими ключами | |
| К1 | диверсификация ключа | СТБ 34.101.31-2011 (подраздел 7.2 раздела 7) |
| К2 | обновление ключа | СТБ 34.101.31-2011 (подраздел 7.2 раздела 7) |
| К3 | защита ключа на другом ключе | СТБ 34.101.31-2011 (подраздел 6.8 раздела 6) |
| К4 | парольная защита ключа | |
| К41 | | СТБ 34.101.18-2009 «Информационные технологии. Синтаксис обмена персональной информацией» (приложение В с учетом использования СТБ 34.101.31-2011) |
| К42 | | СТБ 34.101.45-2013 (приложение Е) |
| К5 | транспорт ключа | |
| К51 | | СТБ П 34.101.50-2012 (приложение В, протокол bdh-keytransport) |
| К52 | | СТБ 34.101.45-2013 (подраздел 7.2 раздела 7, таблица Б1 приложения Б) |
| К6 | разделение ключа | СТБ 34.101.60-2014 «Информационные технологии и безопасность. Алгоритмы разделения секрета» (раздел 7, таблица А1 приложения А) |
| К7 | генерация личного и открытого ключей | |
| К71 | | СТБ 1176.2-99 (разделы 5, 6, 7) |
| К72 | | СТБ 34.101.45-2013 (подраздел 6.2 раздела 6, таблица Б1 приложения Б) |
| К8 | формирование | |

| | | |
|---|---|---|
| | общего ключа | |
| К81 | | проект Руководящего документа Республики Беларусь «Банковские технологии. Протоколы формирования общего ключа» |
| К82 | | СТБ 34.101.66-2014 «Информационные технологии и безопасность. Протоколы аутентификации и выработки общего ключа на основе эллиптических кривых» (приложение А)<br>СТБ 34.101.45-2013 (таблица Б1 (долговременные параметры) приложения Б, приложение Д (форматы данных)) |
| С | управление сертификатами | |
| С1 | запрос на выдачу сертификата открытого ключа | СТБ 34.101.17-2012 «Информационные технологии и безопасность. Синтаксис запроса на получение сертификата» |
| С2 | распространение сертификата открытого ключа | СТБ 34.101.19-2012 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей» (разделы 6, 8) |
| С3 | проверка статуса сертификата открытого ключа (списки отозванных сертификатов) | СТБ 34.101.19-2012 (раздел 7) |
| С4 | проверка статуса сертификата (онлайн) | СТБ 34.101.26-2012 «Информационные технологии и безопасность. Онлайновый протокол проверки статуса сертификата (OCSP)» |
| С5 | распространение атрибутного сертификата | СТБ 34.101.67-2014 «Информационные технологии и безопасность. Инфраструктура атрибутных сертификатов» |
| Г | служебные механизмы | |
| Г1 | генерация случайных чисел | СТБ 34.101.27-2011 «Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации» (подраздел 5.6 раздела 5) или СТБ П 34.101.43-2009 «Информационные технологии. Методы и средства безопасности. Профиль защиты технических и программно-аппаратных средств криптографической защиты информации» (подраздел А.3 приложения А) |
| Г2 | генерация псевдослучайных чисел | СТБ 34.101.47-2012 (подразделы 6.2, 6.3 раздела 6) |
| Т | высокоуровневые механизмы | |
| Т1 | защита канала связи | СТБ 34.101.65-2011 «Информационные технологии и безопасность. Протокол защиты транспортного уровня (TLS)» |
| Б | требования безопасности | |
| Б1 | программные СКЗИ и программное обеспечение программно-аппаратных и технических СКЗИ | СТБ 34.101.27-2011 «Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации» |
| Б2 | программно-аппаратные и технические СКЗИ | СТБ П 34.101.43-2009 |

Таблица 2

**ТРЕБОВАНИЯ**
**к средствам криптографической защиты информации**

| Класс средств криптографической защиты информации | Требования к криптографическим операциям | Требования к управлению ключами | Требования по безопасности | Требования к форматам зашифрованных или подписанных данных (в случае совместимости средств криптографической защиты информации) |
|---|---|---|---|---|
| Средства предварительного шифрования | (Ш1, И1), или (Ш2, И2), или ШИ | ((К51 или К52, С2, С3 или С4), или (К41 или К42), (Г1 или Г2)), или рекомендованные Оперативно-аналитическим центром при Президенте Республики Беларусь | Б1 или Б2 | СТБ 34.101.23-2012 «Информационные технологии и безопасность. Синтаксис криптографических сообщений» (раздел 9 или 13) |
| Средства канального (линейного) шифрования, в том числе для использования в системах профессиональной радиосвязи Республики Беларусь | (Ш1, И1), или (Ш2, И2), или ШИ | (К2, (((К51 или К52), или (К81 или К82)), С2, С3 или С4), или (К3, К6), Г1 или Г2), или Т1, или рекомендованные Оперативно-аналитическим центром при Президенте Республики Беларусь | Б1 или Б2 | В зависимости от системы связи могут быть рекомендованы Оперативно-аналитическим центром при Президенте Республики Беларусь |
| Средства выработки электронной цифровой подписи (далее – ЭЦП), в том числе в соответствии с Законом Республики Беларусь от 28 декабря 2009 года «Об электронном документе и электронной цифровой подписи» (Национальный реестр правовых актов Республики Беларусь, 2010 г., № 15, 2/1665) | П1 или П2 | (К71 или К72, (С1, С2), или С2, или (С2, С5), Г1 или Г2), или рекомендованные Оперативно-аналитическим центром при Президенте Республики Беларусь | Б1 или Б2 | СТБ 34.101.23-2012 (раздел 8) |
| Средства проверки ЭЦП, в том числе в соответствии с Законом Республики Беларусь «Об электронном документе и электронной цифровой подписи» | П1 или П2 | (С2 или (С2, С5), С3 или С4) или рекомендованные Оперативно-аналитическим центром при Президенте Республики Беларусь | Б1 или Б2 | СТБ 34.101.23-2012 (раздел 8) |
| Средства контроля целостности | Х<br>или И1, или И2, или И3<br>или П1, или П2 | <br>К41 или К42, Г1 или Г2<br>К71 или К72, Г1 или Г2 | нет<br>Б1 или Б2<br>Б1 или Б2 | |

Примечания:

1. В таблице 2 указаны условные обозначения криптографических механизмов из таблицы 1 настоящего приложения.

2. Криптографические механизмы, указанные в таблице 2 в скобках, реализуются совместно.

3. При межведомственном информационном взаимодействии информационных систем для обеспечения совместимости средств криптографической защиты информации и в зависимости от задач безопасности используются следующие криптографические механизмы: (Ш2, И2) или ШИ, П2, К52, или К82, К72, С1, С2 или (С2, С5), С3 или С4, Б1 или Б2, СТБ 34.101.23-2012.

УТВЕРЖДЕНО

Приказ
Оперативно-аналитического
центра при Президенте
Республики Беларусь
30.08.2013 № 62
(в редакции приказа
Оперативно-аналитического
центра при Президенте
Республики Беларусь
16.01.2015 № 3)

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

1. В настоящем Положении, разработанном в соответствии с подпунктом 9.4 пункта 9 Положения о технической и криптографической защите информации в Республике Беларусь, утвержденного Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации» (Национальный правовой Интернет-портал Республики Беларусь, 18.04.2013, 1/14225), и частью четвертой статьи 28 Закона Республики Беларусь от 10 ноября 2008 года «Об информации, информатизации и защите информации» (Национальный реестр правовых актов Республики Беларусь, 2008 г., № 279, 2/1552), устанавливается порядок аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам (далее – информационные системы).

2. Для целей настоящего Положения термины и их определения используются в значениях, установленных Законом Республики Беларусь «Об информации, информатизации и защите информации», Положением о технической и криптографической защите информации в Республике Беларусь, техническими нормативными правовыми актами, а также следующие термины и их определения:

аттестат соответствия системы защиты информации информационной системы требованиям по защите информации (далее – аттестат соответствия) – документ установленной формы, подтверждающий выполнение требований законодательства об информации, информатизации и защите информации, в том числе технических нормативных правовых актов;

аттестация системы защиты информации информационной системы (далее – аттестация) – комплекс организационно-технических мероприятий, в результате которых документально подтверждается соответствие системы защиты информации информационной системы требованиям законодательства об информации, информатизации и защите информации;

заявитель – собственник (владелец) информационной системы, обратившийся с заявкой на проведение аттестации.

3. Аттестация проводится организациями, имеющими специальные разрешения (лицензии) на деятельность по технической и (или) криптографической защите информации в части соответствующих составляющих данный вид деятельности работ и услуг (далее – специализированные организации).

Собственники (владельцы) информационных систем, имеющие в своем составе подразделения технической защиты информации или иные подразделения (должностных лиц), выполняющие функции по технической и (или) криптографической защите информации, вправе самостоятельно проводить аттестацию систем защиты информации этих информационных систем.

4. При проведении аттестации системы защиты информации собственником (владельцем) информационной системы самостоятельно работы по аттестации выполняются аттестационной комиссией, назначенной приказом (решением) руководителя организации – собственника (владельца) информационной системы.

Аттестация специализированными организациями проводится на основании заявки на проведение аттестации системы защиты информации по форме согласно приложению 1 к настоящему Положению (далее – заявка) и исходных данных по аттестуемой системе защиты информации согласно приложению 2 к настоящему Положению (далее – исходные данные). При этом расходы по проведению аттестации оплачиваются заявителем в соответствии с договором на проведение аттестации, заключенным между заявителем и специализированной организацией.

5. Аттестация проводится в случаях:

создания системы защиты информации информационной системы;

истечения срока действия аттестата соответствия;

изменения условий и технологии обработки защищаемой информации;

выявления собственником (владельцем) информационной системы либо Оперативно-аналитическим центром при Президенте Республики Беларусь (далее – ОАЦ) фактов недостаточности принятых мер по защите информации, обрабатываемой в информационной системе.

6. Аттестация вновь создаваемой системы защиты информации осуществляется до ввода информационной системы в эксплуатацию.

7. Наличие аттестата соответствия является основанием для ввода информационной системы в эксплуатацию и использования ее в течение срока, установленного в аттестате соответствия.

8. Для проведения аттестации на основании исходных данных разрабатывается программа аттестации, которая должна содержать перечень выполняемых работ и их продолжительность, а также перечень используемой контрольной аппаратуры и тестовых средств.

Программа аттестации разрабатывается:

аттестационной комиссией, назначенной приказом (решением) руководителя организации – собственника (владельца) информационной системы, при проведении аттестации собственником (владельцем) информационной системы самостоятельно;

специализированной организацией в течение 30 календарных дней с даты поступления заявки на проведение аттестации при проведении аттестации такой организацией. В течение данного срока разработанная специализированной организацией программа аттестации согласовывается с заявителем.

9. Аттестация предусматривает комплексную оценку системы защиты информации в реальных условиях эксплуатации информационной системы и включает проведение следующих мероприятий:

анализ исходных данных;

разработку программы аттестации;

предварительное ознакомление с информационной системой и системой защиты информации;

проведение обследования информационной системы и системы защиты информации;

проверку правильности отнесения информационной системы к классу типовых объектов информатизации, выбора и применения средств защиты информации;

анализ организационной структуры, состава и структуры комплекса технических средств и программного обеспечения информационной системы, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения системы защиты информации;

анализ разработанной документации и ее соответствие требованиям законодательства об информации, информатизации и защите информации, в том числе технических нормативных правовых актов;

проверку подготовки кадров и распределения ответственности персонала за организацию и обеспечение выполнения требований по защите информации;

проведение испытаний системы защиты информации на предмет выполнения установленных требований безопасности на различных этапах технологического процесса обработки информации и корректности функционирования данной системы;

оформление протоколов испытаний и заключения по результатам проверок;

оформление аттестата соответствия.

10. Срок проведения аттестации:

определяется руководителем организации – собственника (владельца) информационной системы при проведении аттестации собственником (владельцем) информационной системы самостоятельно;

не может превышать 90 календарных дней при проведении аттестации специализированной организацией. В случае выявления в процессе проведения аттестации недостатков специализированная организация не позднее чем за 35 календарных дней до истечения срока проведения аттестации направляет заявителю соответствующее уведомление. Заявителем должны быть устранены недостатки, выявленные указанной организацией, в течение 30 календарных дней со дня получения уведомления. При невозможности устранения заявителем выявленных недостатков в указанный срок специализированная организация отказывает в выдаче аттестата соответствия. После устранения недостатков заявитель вправе повторно обратиться за проведением аттестации в порядке, установленном настоящим Положением.

11. Аттестат соответствия выдается по форме согласно приложению 3 к настоящему Положению.

Аттестат соответствия подписывается руководителем организации – собственника (владельца) информационной системы либо руководителем специализированной организации, которая провела аттестацию, и заверяется печатью.

Аттестат соответствия выдается на срок, в течение которого должна обеспечиваться неизменность условий функционирования информационной системы и технологии обработки информации, но не более чем на 5 лет.

12. Собственники (владельцы) информационных систем не позднее 10 календарных дней со дня получения аттестата соответствия представляют в ОАЦ копию этого аттестата и иные сведения, предусмотренные в подпункте 4.2 пункта 4 Положения о порядке предоставления в Оперативно-аналитический центр при Президенте Республики Беларусь сведений о состоянии технической защиты информации, утвержденного приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 29 июля 2013 г. № 49 (Национальный правовой Интернет-портал Республики Беларусь, 02.08.2013, 7/2488).

Приложение 1
к Положению о порядке аттестации
систем защиты информации
информационных систем,
предназначенных для обработки
информации, распространение
и (или) предоставление которой
ограничено, не отнесенной
к государственным секретам

Форма

**ЗАЯВКА**
**на проведение аттестации системы защиты информации**

_____
(наименование заявителя, местонахождение)
просит провести аттестацию системы защиты информации _____
(наименование
_____
информационной системы)
на соответствие требованиям по защите информации: _____
(наименование
_____.
документов)

Необходимые исходные данные по аттестуемой системе защиты информации прилагаются.

Согласны на договорной основе оплатить расходы по аттестации.

Приложение: на ___ л.

Руководитель организации _____ _____
(подпись) (инициалы, фамилия)
___._____.20__ М.П.

Главный бухгалтер _____ _____
(подпись) (инициалы, фамилия)
___._____.20__

Приложение 2
к Положению о порядке аттестации
систем защиты информации
информационных систем,
предназначенных для обработки
информации, распространение
и (или) предоставление которой
ограничено, не отнесенной
к государственным секретам

**ПЕРЕЧЕНЬ**
**исходных данных, представляемых заявителем по аттестуемой системе защиты информации**

1. Наименование информационной системы, ее назначение.

2. Документ, подтверждающий наличие в организации подразделения технической защиты информации или иного подразделения (должностного лица), выполняющего функции по технической и (или) криптографической защите информации.

3. Общая функциональная схема информационной системы с указанием ее физических и логических границ, мест размещения элементов системы (аппаратных и программных), средств защиты информации, информационных потоков и протоколов обмена защищаемой информацией.

4. Документ, устанавливающий отнесение информационной системы к классу типовых объектов информатизации согласно СТБ 34.101.30-2007 «Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация».

5. Задание по безопасности или техническое задание на информационную систему.

6. Политика информационной безопасности.

7. Локальные нормативные правовые акты организации, регламентирующие порядок:

использования объектов информационной системы и их управления (администрирования);

резервирования и уничтожения информации;

защиты от вредоносного программного обеспечения;

выявления угроз, которые могут привести к сбоям, нарушению функционирования информационной системы;

реагирования на инциденты информационной безопасности;

контроля (мониторинга) за функционированием информационной системы.

8. Копии сертификатов соответствия либо экспертных заключений на средства защиты информации.

9. Основные характеристики средств физической защиты информационной системы, в том числе помещений, в которых обрабатывается защищаемая информация и хранятся машинные носители информации.

10. Акт и протокол приемочных испытаний системы защиты информации.

Приложение 3
к Положению о порядке аттестации
систем защиты информации
информационных систем,
предназначенных для обработки
информации, распространение
и (или) предоставление которой
ограничено, не отнесенной
к государственным секретам

Форма

**АТТЕСТАТ СООТВЕТСТВИЯ**
**системы защиты информации информационной системы**
**требованиям по защите информации**

№ _____ от __ _____ 20__ г.

_____
(наименование информационной системы)

Действителен до __ _____ 20__ г.

Настоящим аттестатом соответствия удостоверяется, что система защиты информации _____
(наименование информационной системы)
класса _____ соответствует требованиям по защите информации:
(по СТБ 34.101.30-2007)
_____.
(наименование документов)

Аттестация выполнена в соответствии с программой, утвержденной __ _____ 20__ г. № _____.

Результаты испытаний (оценки) приведены в протоколе от __ _____ 20__ г. № ____, утвержденном _____
(наименование организации,
_____.
проводившей испытания)

В информационной системе разрешается обработка информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам.

При эксплуатации информационной системы запрещается:
_____.

Аттестат соответствия действителен при обеспечении неизменности условий функционирования системы защиты информации и технологии обработки защищаемой информации.

Руководитель организации

| _____ | _____ | _____ |
|---|---|---|
| (должность с указанием наименования организации) | (подпись) | (инициалы, фамилия) |

___._____.20__ М.П.