ПРИКАЗ ОПЕРАТИВНО-АНАЛИТИЧЕСКОГО ЦЕНТРА ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ БЕЛАРУСЬ
30 августа 2013 г. № 62

О некоторых вопросах технической и криптографической защиты информации

Изменения и дополнения:

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 16 января 2015 г. № 3 (зарегистрировано в Национальном реестре - № 7/3030 от 19.01.2015 г.) <T61503030>;

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 11 октября 2017 г. № 64 (зарегистрировано в Национальном реестре - № 7/3911 от 11.10.2017 г.) <T61703911>

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. Утвердить прилагаемые:

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

Положение 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;

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

2. Настоящий приказ вступает в силу с 19 октября 2013 г.

Первый заместитель начальника **В.А.Рябоволов**

УТВЕРЖДЕНО

Приказ
Оперативно-аналитического
центра при Президенте
Республики Беларусь
30.08.2013 № 62
(в редакции приказа
Оперативно-аналитического
центра при Президенте
Республики Беларусь
11.10.2017 № 64)

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 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 о технической и криптографической защите информации в Республике Беларусь, техническими нормативными правовыми актами, а также следующий термин и его определение:

политика информационной безопасности организации – общие намерения и направления деятельности по обеспечению конфиденциальности, целостности, подлинности, доступности и сохранности информации, официально сформулированные собственником (владельцем) информационной системы.

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. Работы по технической защите информации у собственника (владельца) информационной системы могут выполняться:

подразделением технической защиты информации или иными подразделениями (должностными лицами), выполняющими функции по технической защите информации (далее – подразделение технической защиты информации);

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).

6. Комплекс мероприятий по технической 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

7. На этапе проектирования системы защиты информации осуществляются:

классификация информации, хранящейся и обрабатываемой в информационной системе, в соответствии с законодательством;

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

отнесение информационной системы к классу типовых информационных систем в порядке, установленном СТБ 34.101.30-2017 «Информационные технологии. Методы и средства безопасности. Информационные системы. Классификация» (далее – класс типовой информационной системы);

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

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

Частное техническое задание должно содержать:

цели создания системы защиты информации;

класс типовой информационной системы;

перечень требований, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации, включая требования согласно приложению 1;

сведения об организации взаимодействия с иными информационными системами (в случае предполагаемого взаимодействия) с учетом требований согласно приложению 2.

Разработка задания по безопасности осуществляется в случае, если информационная система имеет подключение к сетям электросвязи общего пользования (в том числе к глобальной компьютерной сети Интернет).

Задание по безопасности разрабатывается в соответствии с техническими нормативными правовыми актами и должно содержать перечень требований, направленных

на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации, включая требования согласно приложению 1.

Задание по безопасности подлежит оценке в аккредитованной испытательной лаборатории (центре).

Собственник (владелец) информационной системы не позднее 30 календарных дней со дня получения из аккредитованной испытательной лаборатории (центра) протокола оценки задания по безопасности, свидетельствующего о положительных результатах оценки, представляет копию этого задания в ОАЦ.

9. Для организации технической защиты информации в нескольких информационных системах, функционирующих в общей программно-технической среде и принадлежащих одному собственнику (владельцу), может создаваться единая система защиты информации взаимодействующих информационных систем.

ГЛАВА 3
СОЗДАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

10. На этапе создания системы защиты информации осуществляются:

разработка политики информационной безопасности организации;

разработка локальных нормативных правовых актов, направленных на реализацию политики информационной безопасности организации, в соответствии с требованиями, изложенными в задании по безопасности или частном техническом задании;

внедрение средств технической защиты информации, необходимых для реализации требований, изложенных в задании по безопасности или частном техническом задании, проверка работоспособности и совместимости этих средств;

реализация организационных мер по защите информации в соответствии с требованиями политики информационной безопасности организации;

опытная эксплуатация системы защиты информации.

11. Политика информационной безопасности организации должна содержать:

цели создания системы защиты информации;

права и обязанности субъектов информационной системы;

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

12. Локальные нормативные правовые акты, направленные на реализацию политики информационной безопасности организации, должны содержать:

перечень средств вычислительной техники, сетевого оборудования, системного и прикладного программного обеспечения, средств технической защиты информации (далее – объекты информационной системы) и субъектов информационной системы, сведения о месте их размещения и порядке информационного взаимодействия субъектов информационной системы с объектами этой системы и объектов между собой;

способы разграничения доступа субъектов к объектам информационной системы;

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;

порядок резервирования и уничтожения информации;

порядок защиты от вредоносного программного обеспечения;

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

порядок осуществления контроля (мониторинга) за функционированием информационной системы.

13. В ходе внедрения средств технической защиты информации осуществляется их монтаж и наладка в соответствии с эксплуатационной документацией, а также смена реквизитов доступа к функциям управления и настройкам, установленным по умолчанию, либо блокировка учетных записей, не предусматривающих смену указанных реквизитов.

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

14. Реализация организационных мер защиты информации осуществляется в целях выполнения требований, изложенных в локальных нормативных правовых актах собственника (владельца) информационной системы, которые доводятся до сведения субъектов информационной системы под роспись.

15. Опытная эксплуатация системы защиты информации осуществляется для проверки ее работоспособности в различных режимах функционирования информационной системы, в том числе при необходимости в условиях нештатной ситуации.

ГЛАВА 4
ОСОБЕННОСТИ ЭКСПЛУАТАЦИИ ИНФОРМАЦИОННОЙ СИСТЕМЫ С ПРИМЕНЕНИЕМ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

16. В процессе эксплуатации информационной системы с применением 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 собственника (владельца) информационной системы;

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.

17. Собственники (владельцы) информационных систем в соответствии с их 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 их выявления собственники (владельцы) информационных систем обязаны:

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

осуществить доработку системы защиты информации информационной системы и провести оценку на предмет необходимости ее повторной аттестации.

Собственники (владельцы) информационных систем в произвольной форме информируют ОАЦ о прекращении или нарушении функционирования информационной системы, нарушении конфиденциальности, целостности, подлинности, доступности либо сохранности информации в течение суток с момента выявления этих событий.

18. Наладочные работы и сервисное обслуживание информационной системы проводятся с участием подразделения технической защиты информации.

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

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

защите информации, содержавшейся 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.

Приложение 1
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 частное техническое задание или задание по безопасности на информационную систему

	Наименование требований	Условие об обязательности выполнения требований в соответствии с классом типовой информационной системы					
		4-фл	4-юл	4-дсп	3-фл	3-юл	3-дсп
1	Требования по обеспечению аудита безопасности						
1.1	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации (идентификация и аутентификация пользователей, нарушения прав доступа пользователей, выявленные нарушения информационной безопасности и др.)	+	+	+	+	+	+
1.2	Обеспечение сбора, записи и хранения информации о событиях безопасности в течение установленного срока хранения, но не менее шести месяцев	+	+	+	+	+	+
1.3	Осуществление мониторинга (просмотра, анализа) событий безопасности уполномоченными субъектами информационной системы	+	+	+	+	+	+
1.4	Обеспечение мониторинга (просмотра, анализа) информации о сбоях в механизмах сбора информации и о достижении предела объема (емкости) памяти устройств хранения уполномоченными пользователями	+	+	+	+	+	+
2	Требования по обеспечению защиты данных						
2.1	Обеспечение полномочного управления (создание, активация, блокировка и уничтожение) учетными записями субъектов информационной системы	+	+	+	+	+	+
2.2	Реализация правил разграничения доступа субъектов информационной системы к объектам информационной системы (средства вычислительной техники, сетевое оборудование, системное и прикладное программное обеспечение, средства защиты информации) (далее – объекты)	+	+	+	+	+	+
2.3	Обеспечение управления информационными потоками (маршрутизация) между информационными системами	+	+	+	+	+	+
2.4	Обеспечение ограничений входящего и исходящего трафика (фильтрация) только необходимыми соединениями	–	–	+	+	+	+
2.5	Обеспечение безопасного взаимодействия с иными информационными системами, контроль за таким взаимодействием и управление подключением	+	+	+	+	+	+
2.6	Обеспечение регламентации порядка использования в информационной системе мобильных технических средств и контроля за таким использованием	–	–	+	+	+	+
2.7	Исключение возможности отрицания пользователем факта отправки информации другому пользователю, а также получения информации от другого пользователя	–	–	+	–	–	+

2.8	Определение порядка использования съемных носителей информации	+	+	+	+	+	+
2.9	Обеспечение уничтожения (удаления) данных с машинных носителей информации при их передаче лицам, не являющимся субъектами информационной системы, в том числе для ремонта, технического обслуживания	+	+	+	+	+	+
2.10	Обеспечение защиты архивных файлов, параметров настройки средств защиты информации, программного обеспечения	+	+	+	+	+	+
2.11	Обеспечение криптографической защиты 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	–	–	–	+	+	+
3	Требования по обеспечению идентификации и аутентификации						
3.1	Обеспечение идентификации объектов и закрепления за ними субъектов информационной системы	+	+	+	+	+	+
3.2	Обеспечение идентификации и аутентификации субъектов информационной системы	+	+	+	+	+	+
3.3	Обеспечение управления средствами аутентификации, в том числе хранением, выдачей, инициализацией, блокированием средств аутентификации и принятием мер в случае утраты и (или) компрометации средств аутентификации	+	+	+	+	+	+
3.4	Обеспечение защиты обратной связи при вводе аутентификационной информации	+	+	+	+	+	+
3.5	Обеспечение определения прав и обязанностей субъектов информационной системы	+	+	+	+	+	+
3.6	Обеспечение контроля за соблюдением правил генерации и смены паролей субъектов информационной системы	+	+	+	+	+	+
3.7	Обеспечение защиты от подбора реквизитов доступа	+	+	+	+	+	+
3.8	Определение действий субъектов информационной системы, которые могут совершаться такими субъектами до их идентификации и аутентификации	+	+	+	+	+	+
3.9	Обеспечение блокировки доступа к информационной системе после истечения установленного времени бездействия (неактивности) субъекта информационной системы или по его запросу	+	+	+	+	+	+
4	Требования по обеспечению защиты системы защиты информации информационной системы						
4.1	Обеспечение изменения атрибутов безопасности, установленных по умолчанию в соответствии с политикой информационной безопасности организации	+	+	+	+	+	+
4.2	Обеспечение синхронизации временных меток и (или) системного времени в информационной системе и системе защиты информации	+	+	+	+	+	+
4.3	Обеспечение защиты информации о событиях безопасности	–	–	+	+	+	+
4.4	Обеспечение контроля за установкой обновлений программного обеспечения средств защиты информации	+	+	+	+	+	+
4.5	Обеспечение контроля за составом средств защиты информации	+	+	+	+	+	+
4.6	Обеспечение контроля и управления физическим доступом в помещения, в которых постоянно размещаются объекты информационной системы	+	+	+	+	+	+
4.7	Обеспечение защиты информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы	–	–	–	+	+	+

4.8	Регламентирование порядка доступа к настройкам средств защиты информации и контроль за таким доступом	+	+	+	+	+	+
4.9	Обеспечение разделения в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации	–	–	+	+	+	+
5	Требования по обеспечению защищенного канала передачи данных						
5.1	Обеспечение сетевых соединений от подмены сетевых устройств	–	–	–	+	+	+
5.2	Обеспечение защищенного канала между рабочими местами субъектов информационной системы и объектами, на которых данные уполномоченные субъекты осуществляют администрирование, мониторинг, а также иные определенные в соответствии с правами и обязанностями функции	+	+	+	+	+	+
6	Требования по обеспечению защиты информации в виртуальной инфраструктуре						
6.1	Обеспечение синхронизации временных меток и (или) системного времени виртуальной инфраструктуры и иных компонентов информационной системы	+	+	+	+	+	+
6.2	Обеспечение идентификации и аутентификации субъектов информационной системы и объектов в виртуальной инфраструктуре	+	+	+	+	+	+
6.3	Обеспечение регистрации событий безопасности в виртуальной инфраструктуре	+	+	+	+	+	+
6.4	Обеспечение защиты от агрессивного использования ресурсов виртуальной инфраструктуры потребителями услуг	–	–	+	+	+	+
6.5	Обеспечение защиты виртуальной инфраструктуры от несанкционированного доступа и сетевых атак из виртуальной и физической сети, а также виртуальных машин	–	–	+	+	–	+
6.6	Обеспечение безопасного перемещения виртуальных машин и обрабатываемых на них данных	–	–	+	+	–	+
6.7	Обеспечение защиты архивных файлов, параметров настройки средств защиты информации и программного обеспечения управления виртуальной инфраструктурой	–	–	+	+	–	+
6.8	Обеспечение резервного копирования данных, резервирования технических средств	–	–	+	+	–	+
6.9	Обеспечение защиты от вредоносного программного обеспечения в виртуальной инфраструктуре	+	+	+	+	+	+
6.10	Физическая изоляция сегмента виртуальной инфраструктуры (системы хранения и обработки данных), предназначенного для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам	–	+	+	–	+	+
7	Иные требования						
7.1	Наличие схемы информационной системы с указанием объектов, внешних подключений и информационных потоков	+	+	+	+	+	+
7.2	Наличие регламента для организации подключений к иным информационным системам	+	+	+	+	+	+
7.3	Определение перечня разрешенного программного обеспечения и регламентация порядка его установки и использования	–	–	–	+	+	+
7.4	Обеспечение защиты от вредоносного программного обеспечения	+	+	+	+	+	+
7.5	Обеспечение обновления базы данных признаков вредоносного программного обеспечения	+	+	+	+	+	+
7.6	Обеспечение функционирования подсистемы обнаружения вторжений	–	–	–	–	+	+

7.7	Обеспечение обновления базы сигнатур подсистемы обнаружения вторжений	–	–	–	–	+	+
7.8	Обеспечение контроля за установкой обновлений программного обеспечения	+	+	+	+	+	+
7.9	Обеспечение контроля за работоспособностью, параметрами настройки и правильностью функционирования средств защиты информации	+	+	+	+	+	+
7.10	Обеспечение контроля за составом технических средств информационной системы	+	+	+	+	+	+
7.11	Обеспечение резервирования информации и программного обеспечения	–	–	+	–	–	+

Примечания:

1. Обозначения «3-фл», «3-юл», «3-дсп», «4-фл», «4-юл», «4-дсп» соответствуют классам типовых информационных систем.

2. Требования, отмеченные знаком «+», являются обязательными, исключение которых из частного технического задания или задания по безопасности допустимо только в случаях отсутствия в информационной системе соответствующего объекта либо технологии.

3. Требования, отмеченные знаком «–», являются необязательными.

Приложение 2
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

Требования к организации взаимодействия информационных систем

	6-частн/6-гос	5-частн/5-гос	4-фл/4-юл/4-дсп	3-фл/3-юл /3-дсп
4-фл	х	не допускается	х	не допускается
4-юл	х	не допускается	х	не допускается
4-дсп	х	не допускается	х	не допускается
3-фл	не допускается	х/о	не допускается	х/о
3-юл	не допускается	х/о	не допускается	х/о
3-дсп	не допускается	х/о	не допускается	х/о

Примечания:

1. Обозначения «3-фл», «3-юл», «3-дсп», «4-фл», «4-юл», «4-дсп», «5-частн», «5-гос», «6-частн», «6-гос» соответствуют классам типовых информационных систем.

2. Под символом «х» понимается физически выделенный канал передачи данных.

3. Под символом «о» понимается наличие подключения к сетям электросвязи общего пользования (в том числе к глобальной компьютерной сети Интернет).

УТВЕРЖДЕНО

Приказ
Оперативно-аналитического
центра при Президенте
Республики Беларусь
30.08.2013 № 62
(в редакции приказа
Оперативно-аналитического
центра при Президенте
Республики Беларусь
11.10.2017 № 64)

ПОЛОЖЕНИЕ
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

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), пунктом 6 Положения об отнесении объектов информатизации к критически важным и обеспечении безопасности критически важных объектов информатизации, утвержденного 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), и пунктом 3 Указа Президента Республики Беларусь от 8 ноября 2011 г. № 515 «О некоторых вопросах развития информационного общества в Республике Беларусь» (Национальный реестр правовых актов Республики Беларусь, 2011 г., № 125, 1/13064), устанавливается порядок криптографической защиты информации:

в государственных информационных системах (далее – ГИС) в части обеспечения целостности и подлинности электронных документов;

в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам (далее – информационные системы);

на критически важных объектах информатизации (далее – КВОИ).

2. 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 о технической и криптографической защите информации в Республике Беларусь, Положением об отнесении объектов информатизации к критически важным и обеспечении безопасности критически важных объектов информатизации и техническими нормативными правовыми актами.

3. Решение об организации криптографической защиты информации принимается:

собственником (владельцем) информационной системы – при реализации комплекса мероприятий по созданию системы защиты информации информационной системы на этапе выполнения работ по проектированию системы защиты информации информационной системы;

собственником (владельцем) ГИС – при использовании в этих системах электронных документов;

владельцем КВОИ – при реализации комплекса мероприятий по созданию системы безопасности этих объектов на этапе разработки или корректировки требований к системе безопасности КВОИ.

4. Системы защиты информации информационных систем, системы безопасности КВОИ и ГИС (при использовании в этих системах электронных документов) должны включать в себя средства криптографической защиты информации (далее – СКЗИ), реализующие криптографические операции в зависимости от задач безопасности, управление криптографическими ключами данных СКЗИ, а также функциональные возможности безопасности.

5. СКЗИ должны выполнять криптографические операции в соответствии с заданными криптографическими алгоритмами и криптографическими ключами на основе требований согласно приложению.

6. Для каждой криптографической операции, реализованной в СКЗИ, собственником (владельцем) информационной системы, ГИС и владельцем КВОИ определяются требования по управлению криптографическими ключами, включая требования по их генерации, распределению, хранению, доступу к ним и их уничтожению. Средства управления криптографическими ключами должны реализовывать алгоритмы генерации криптографических ключей, методы распределения, доступа, хранения и уничтожения криптографических ключей на основе требований согласно приложению. На всех этапах жизненного цикла криптографических ключей должна быть обеспечена их защита от несанкционированного доступа.

Порядок управления криптографическими ключами СКЗИ определяется в задании по безопасности на информационную систему или в частном техническом задании на систему защиты информации информационной системы, в документах по системе безопасности КВОИ и ГИС.

7. Функциональные возможности безопасности СКЗИ должны обеспечивать:

защиту СКЗИ от несанкционированного воздействия или несанкционированного использования;

предотвращение несанкционированного раскрытия критических объектов;

предотвращение несанкционированной модификации СКЗИ, включая несанкционированные изменение, замену, добавление и уничтожение криптографических ключей, а также других критических объектов;

выявление ошибок в работе и нарушений целостности СКЗИ, предотвращение компрометации критических объектов в результате этих ошибок.

Требования к функциональным возможностям безопасности СКЗИ должны основываться на технических нормативных правовых актах согласно приложению.

8. В процессе эксплуатации СКЗИ должны быть реализованы организационные меры, включая обеспечение особого режима допуска на территорию (в помещения), на которой может быть осуществлен доступ к СКЗИ и криптографическим ключам (носителям), а также разграничение доступа к ним по кругу лиц. Данные организационные меры должны быть отражены в политике информационной безопасности или в локальных нормативных правовых актах организации.

9. СКЗИ, используемые в системах защиты информации информационных систем, системах безопасности КВОИ и ГИС, подлежат сертификации в Национальной системе подтверждения соответствия Республики Беларусь на соответствие требованиям технических нормативных правовых актов согласно приложению или государственной экспертизе.

Для совместимости СКЗИ данные обмена между ними и используемые криптографические ключи должны иметь одни и те же форматы. Различия могут иметь место:

при управлении криптографическими ключами СКЗИ одного класса, если не предполагается использование ключей одного СКЗИ на другом СКЗИ;

во внутренних служебных механизмах, реализующих функциональные возможности безопасности СКЗИ, за исключением обеспечения конфиденциальности и контроля целостности личных (секретных) ключей.

Управление криптографическими ключами и механизмы, реализующие функциональные возможности безопасности СКЗИ, должны соответствовать требованиям согласно приложению.

10. В случае принятия собственником (владельцем) информационной системы решения о применении СКЗИ для защиты служебной информации ограниченного распространения, определенной в соответствии с законодательством, реализуются следующие организационные и технические меры:

обеспечение криптографической защиты служебной информации ограниченного распространения на отдельно выделенном средстве вычислительной техники, не имеющем подключения к сетям электросвязи общего пользования (в том числе к глобальной компьютерной сети Интернет). В случае когда такое подключение требуется для обеспечения технологических процессов функционирования информационных систем, оно должно осуществляться с применением средств защиты информации, имеющих сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь, обеспечивающих исключение возможности несанкционированного доступа к служебной информации ограниченного распространения и к самой информационной системе;

применение в средствах криптографической защиты служебной информации ограниченного распространения технологических (конструктивных) решений, исключающих появление личных (долговременных секретных) криптографических ключей в открытом виде вне криптографической границы указанных средств;

управление криптографическими ключами средств криптографической защиты служебной информации ограниченного распространения должно быть организовано так, чтобы при компрометации ключей одного из пользователей не снижалась безопасность сети иных пользователей;

исключение физического доступа неуполномоченных лиц к средству вычислительной техники и средствам криптографической защиты служебной информации ограниченного распространения;

обеспечение защиты от вредоносного программного обеспечения и периодическое обновление базы данных его признаков;

использование программно-аппаратных или технических СКЗИ, удовлетворяющих требованиям согласно приложению, для обеспечения защищенного канала передачи служебной информации ограниченного распространения между несколькими контролируемыми зонами 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

ТРЕБОВАНИЯ
к средствам криптографической защиты информации

Таблица 1

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

Условные обозначения криптографических механизмов	Криптографические механизмы	Наименование технических нормативных правовых актов
Ш	шифрование	
Ш1		ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования» (раздел 3 или 4)*
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 34.101.47-2017 «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	
Х1		СТБ 34.101.31-2011 (подраздел 6.9 раздела 6)
Х2		СТБ 34.101.77-2016 «Информационные технологии и безопасность. Алгоритмы хэширования» (l = 128, или l = 192, или l = 256)
П	электронная цифровая подпись	
П1		СТБ 1176.1-99 «Информационная технология. Защита информации. Функция хэширования»
		СТБ 1176.2-99 «Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи» (разделы 5, 6)**
П2		СТБ 34.101.31-2011 (подраздел 6.9 раздела 6)
		СТБ 34.101.45-2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых» (подраздел 6.3 раздела 6, подраздел 7.1 раздела 7, таблица Б1 приложения Б, приложение Д)

П3		СТБ 34.101.77-2016 (l = 128, или l = 192, или l = 256) СТБ 34.101.45-2013 (подраздел 6.3 раздела 6, подраздел 7.1 раздела 7, таблица Б1, или Б2, или Б3 приложения Б, приложение Д)
К	управление криптографическими ключами	
К1	расширение ключа	СТБ 34.101.31-2011 (подраздел 7.1 раздела 7)
К2	преобразование 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	СТБ 34.101.45-2013 (подраздел 7.2 раздела 7, таблица Б1, или Б2, или Б3 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 (пункт 5.1 раздела 5, пункт 6.1 раздела 6)**
К72		СТБ 34.101.45-2013 (подраздел 6.2 раздела 6, таблица Б1, или Б2, или Б3 приложения Б)
К8	формирование общего ключа	
К81		СТБ 34.101.66-2014 «Информационные технологии и безопасность. Протоколы аутентификации и выработки общего ключа на основе эллиптических кривых» (подраздел 7.4 или 7.5 раздела 7 или приложение А) СТБ 34.101.45-2013 (таблица Б1, или Б2, или Б3 приложения Б, приложение Д)
К82		СТБ 34.101.66-2014 (подраздел 7.6 раздела 7) СТБ 34.101.45-2013 (таблица Б1, или Б2, или Б3 приложения Б, приложение Д)
К83		СТБ 34.101.65-2014 «Информационные технологии и безопасность. Протокол защиты транспортного уровня (TLS)» (подпункт В2.5.1, или В2.5.2, или В2.5.4 пункта В2.5 приложения В)
К84		СТБ 34.101.65-2014 (подпункт В2.5.3 пункта В2.5 приложения В)
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)
Г2	генерация псевдослучайных чисел	СТБ 34.101.47-2017 (подраздел 6.2 или 6.3 раздела 6)
Т	высокоуровневые механизмы	
Т1	защита канала связи	СТБ 34.101.65-2014
Б	требования безопасности	
Б1	программные СКЗИ	СТБ 34.101.27-2011
Б2	программно-аппаратные и технические СКЗИ	СТБ 34.101.1-2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель», СТБ 34.101.2-2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности», СТБ 34.101.3-2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности», где в качестве основы для оценки СКЗИ используется задание по безопасности с учетом функциональных и гарантийных требований безопасности согласно таблице 3 настоящего приложения
Ф	форматы данных	
Ф1	форматы зашифрованных данных	СТБ 34.101.23-2012 «Информационные технологии и безопасность. Синтаксис криптографических сообщений» (раздел 9 или 13)
Ф2	форматы подписанных данных	СТБ 34.101.23-2012 (раздел 8)

---

* Стандартный блок подстановки ГОСТ 28147-89

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$K_1[i]$	2	6	3	14	12	15	7	5	11	13	8	9	10	0	4	1
$K_2[i]$	8	12	9	6	10	7	13	1	3	11	14	15	2	4	0	5
$K_3[i]$	1	5	4	13	3	8	0	14	12	6	7	2	9	15	11	10
$K_4[i]$	4	0	5	10	2	11	1	9	15	3	6	7	14	12	8	13
$K_5[i]$	7	9	6	11	15	10	8	12	4	14	1	0	5	3	13	2
$K_6[i]$	14	8	15	2	6	3	9	13	5	7	0	1	4	10	12	11
$K_7[i]$	9	13	8	5	11	4	12	2	0	10	15	14	1	7	3	6
$K_8[i]$	11	15	10	8	1	14	3	6	9	0	4	5	13	2	7	12

** Стандартные долговременные параметры СТБ 1176.2-99

Уровень стойкости 3

l 1022

r 175

p 2846B979 F51D4156 B881C96F 3C61A5F3 B5A8F4B4 7B604657 8B92205C A7ADCB9A 77CF7780 023B7217 1BB3BED1 569ECA57 2C5E423B 885C70F5 D2CD3C17 0E31CE50 7DE12C9E 535D71DA 16530C9B E6D078C4 67CE4D24 E7C63181 7FB4BE8F 16EB1B4D E7152DB1 8B23E9B8 99CDAAAB CF7BEC42 CBA90DE4 747EA228 BC267048 0EB191E5

q 7A3D 48C80B17 84985341 4EE450CC 636C93F5 1D63F3C5

a 0CA7F481 B9D2ABE2 E1CBC58F AB8B1FC9 D05234B0 B72AA69B 9A522E1C 18EB73FC CF86CBED 32BD11D0 41AE0434 0D9F732E 7D6A88D0 52BC2CEE 1F8F64CB 0893D92F 365D162E 67B04EEA D6F8FE7F 51B74CF6 1C90C9F4 53F35E56 8E2225F4 5C62BDF0 1E96E131 67CE3338 33B93F65 96332013 2112AADB E4D93404 7AFFBB35 7D931983

H 0

Уровень стойкости 6

l 1534

r 208

p 2E4BC383 5A5B41E3 5D9DC735 157891FC 868064AD 80086810 CB68F580 3DD79608 20A2BAAF 7588969A B9BF5187 3B1E393D 6DABA057 C219EDC6 8183B7EF 07C4C3CE D5466C41 A598A28B D0812BB7 F8AB721D CA6D6D09 AFB97604 4CE6D36C 5F4C1C58 6179EB2F B8F77415 70E8B492 44FD8E02 4398EBED 9B3DD66C 591FD864 83B9FA62 D66F3AFF 7F98ED22 61B15F45 5DEAB8D4 DDC3855D 6EBA0C8A 706F48AC A209ACE2 87AF3A81 CD0AF711 F82A1C65 3C5E5AAA 6BC05AA9 2591AC22 5BEBC6E5 5E953453

q B7B5 417D8085 27DED8EA EC7CFCB9 742C871B DF45DA71 5F6A453D

a 017CA54B C1BD338D 2F760ACF 08D1124A 57FF866C 24F3DC85 19E03C44 210F4E08 D9950280 C0CC9FBD BA3916D4 18CF1999 B91E413C 402BC00D B8B6BA76 8C45257F 25E9F4D7 1CC78ED3 EF1201D0 12E6B9CE 24913F2F 57E38606 C84D8E18 1A420D54 F1B1E2A1 987BED42 2079E48E 88A03E73 0C36055B 9C9A15D4 2BA8DCCB F810E193 A7653A9C 175A8185 FD73BB1C 17139B31 160B42CA EDF01F01 F799A0B6 1AF8FF8B DE3E2AC1 7145A727 FD7AE027 1BF97092 BF730F08 16C8F376 450A350E B7C78044

H 0

Уровень стойкости 10

l 2462

r 257

p 2F01EACA 0363BB43 DA7CF0A2 14D2FC03 3A592B2F 2E3FB58D 61D7E42B AA17455B 38167684 BF8F418E 2DF4EFD3 E1D105E0 34A497CF C0FA4C02 39E755C1 3965D096 452B055A 5314C80F C7F63C81 014EEE3F A9C6FDFE 9A88A2E8 D1137ABE 01E6DD80 6D0A64A4 05B3F30D 909C84B6 008F9D06 D1102024 A7D2CF7F 5C041887 3BD222EF 2BE1BFAF 66CB3BBD 7E34AEDF 10C5A70E 1CAC0566 DBC96E05 8B5D0B9D 6875951B 0ADF8D09 BCE5CE60 FC1CBEC0 C49DE8A4 94568263 9E9CF549 93A62251 372DD0EE B3007644 5EFD9B15 5194FA32 54CF3DA6 D0EE8B0C 0F515DF1 949E8F8B 67E7DC1A 14433033 9BA0AEA1 E93C551A 3117CE98 AFD69473 2667E4CE 226779E3 4726E78E 13E916D8 916D2918 BDF5DD77 8C9938E2 F52E3425 714CA7C9 122330D9 2A2DF086 1516CCE3 51E6D76D 7537432A F1F2285F 6F9B1D95

q 01 C3CED546 6C41A582 9D099FA4 4491B119 3D1AB138 A1781046 73D152C1 4F804EEB

a 1E921804 B4E9624E 38CE41C7 79846D4D BB98D53D F634ED69 85FA42BF 079A7BD0 5AAC508F BFC47892 8F9EE2B2 2C2F1B97 D98F6147 7EDC2AAB 4AA32499 552FF72F F1B3AEF2 7F5231DA 1880A153 F1B283E2 2A386554 3B642C35 EFE211C5 046AAE39 6C2811B8 1DBED9C4 AFB1F39E D2F36799 1CC77980 51B99F0B 7FEE1AB4 E85CDBBD 853BCB1B A1902175 9E588CC7 0AF9888A 5C4EC7FF F330749C EA1890BC F722BAE9 37D2B366 3805DC67 F55A591B 6E288962 9D11CD03 C1555AC8 63827B88 A0451A47 26597359 E5902CAD 1EEAF794 EB600530 9988F333 95F42041 4BB0B218 75305E12 CCF177BE 765DF18E DDB7E9AA 37631867

94D3C446 38E1B11A B87C6957 F5C14787 D540959D 3ACB53D3 1BBB2482 3F5AC505 FAF5D86E
0EBA65AE CB14B4B0 0601CC24 26CC476D 8837CC6C 4FCE7B07 0E19ABEB 6DC34FEE

H 0

Примечание. Числа *p*, *q*, *a* записаны в шестнадцатиричной системе счисления – цифры читаются слева направо и сверху вниз, первая цифра старшая, последняя – младшая.

Таблица 2

ПРОФИЛИ ТРЕБОВАНИЙ
к средствам криптографической защиты информации

Класс средств криптографической защиты информации	Требования к криптографическим операциям	Требования к управлению ключами	Требования 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	Г1 или Г2, К2, или К5, или К82, или К84 Г1 или Г2, К5, или К81, или К83, С2, С3 или С4	Б1 или Б2	Ф1
Средства канального (линейного) шифрования, в том числе для использования в системах профессиональной радиосвязи Республики Беларусь	(Ш1, И1), или (Ш2, И2), или ШИ	Г1 или Г2, К2, или К5, или К82, или К84 Г1 или Г2, К5, или К81, или К83, С2, С3 или С4 Г1 или Г2, Т1 Г1 или Г2, Х1 или Х2	Б1 или Б2	
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, или П3		Б1 или Б2	Ф2 или С1
Средства проверки ЭЦП, в том числе в соответствии с Законом Республики Беларусь «Об электронном документе и электронной цифровой подписи»	П1, или П2, или П3	С2 или (С2, С5), С3 или С4	Б1 или Б2	Ф2
Средства генерации личных и открытых ключей средств ЭЦП, в том числе в соответствии с Законом Республики Беларусь «Об электронном документе и электронной цифровой подписи»		Г1 или Г2, К71 или К72	Б1 или Б2	
Средства контроля целостности	Х1 или Х2			

	И1, или И2, или И3 П1, или П2, или П3	Г1 или Г2, К2 Г1 или Г2, К71 или К72	Б1 или Б2 Б1 или Б2	

Примечания:

1. В таблице 2 указаны условные обозначения криптографических механизмов.

2. Криптографические механизмы, условные обозначения которых указаны 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 или П3, Г1 или Г2, К72, К5 или К81, или Т1, С1, С2 или (С2, С5), С3 или С4, Б1 или Б2, Ф1, Ф2.

Таблица 3

ТРЕБОВАНИЯ
к функциональным возможностям безопасности программно-аппаратных или технических средств криптографической защиты информации

Обозначение функционального компонента	Название функционального компонента (в соответствии с СТБ 34.101.2-2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности»)
FCS_CKM.2	Распределение криптографических ключей
FCS_CKM.3	Доступ к криптографическим ключам
FCS_CKM.4	Уничтожение криптографических ключей
FDP_ACC.1	Ограниченное управление доступом
FDP_ACF.1	Управление доступом на основе атрибутов безопасности
FDP_IFC.1	Ограниченное управление информационными потоками
FDP_IFF.1	Простые атрибуты безопасности
FIA_AFL.1	Обработка отказов аутентификации
FIA_ATD.1	Определение атрибутов пользователя
FIA_SOS.1	Верификация секретов
FIA_UAU.1	Выбор момента времени аутентификации
FIA_UAU.6	Повторная аутентификация
FIA_UAU.7	Аутентификация с защищенной обратной связью
FIA_UID.1	Выбор момента времени идентификации
FMT_MOF.1	Управление режимами работы функций безопасности функциональных возможностей безопасности СКЗИ
FMT_MSA.1	Управление атрибутами безопасности
FMT_MSA.2	Безопасные атрибуты безопасности
FMT_MSA.3	Инициализация атрибутов безопасности
FMT_MTD.1	Управление данными функциональных возможностей безопасности СКЗИ
FMT_MTD.3	Безопасные данные функциональных возможностей безопасности СКЗИ
FMT_SMF.1	Определение функций управления
FMT_SMR.1	Роли безопасности
FPT_FLS.1	Сбой с сохранением безопасного состояния
FPT_PHP.3	Противодействие физической атаке
FPT_RCV.1	Ручное восстановление
FPT_RCV.4	Восстановление функции
FPT_RPL.1	Обнаружение повторного использования
FPT_TST.1	Тестирование функциональных возможностей безопасности СКЗИ
FTP_TRP.1	Доверенный путь

Примечания:

1. При наличии в программно-аппаратных или технических средствах криптографической защиты информации ввода ключей дополнительно добавляется компонент FDP_ITC.1 «Прием данных пользователя без атрибутов безопасности», вывода ключей – компонент FDP_ETC.2 «Передача данных пользователя с атрибутами безопасности», генерации ключей – компонент FCS_CKM.1 «Генерация криптографических ключей».

2. Гарантийные требования безопасности для программно-аппаратных или технических средств криптографической защиты информации должны соответствовать УГО4 по СТБ 34.101.3-2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности».

УТВЕРЖДЕНО

Приказ
Оперативно-аналитического
центра при Президенте
Республики Беларусь
30.08.2013 № 62
(в редакции приказа
Оперативно-аналитического
центра при Президенте
Республики Беларусь
11.10.2017 № 64)

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 применяются термины и их определения в значениях, определенных 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 или иное уполномоченное им лицо, обратившееся с заявкой на проведение аттестации;

технология обработки защищаемой информации – упорядоченная совокупность возможностей объектов информационной системы, направленная на выполнение системой своих функций.

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 собственником (владельцем) информационной системы самостоятельно работы по аттестации выполняются аттестационной комиссией, назначенной решением (приказом, иным документом) руководителя собственника (владельца) информационной системы.

Аттестация специализированными организациями проводится на основании заявки на проведение аттестации системы защиты информации по форме согласно приложению 1 и исходных данных по аттестуемой системе защиты информации согласно приложению 2 (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 технологии обработки защищаемой информации и (или) совокупности технических и организационных мер, реализованных при создании системы защиты информации информационной системы.

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

7. Наличие аттестата соответствия является обязательным условием для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, в течение установленного в нем срока.

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

анализ исходных данных;

предварительное ознакомление с информационной системой и системой защиты информации;

разработку программы и методики аттестации;

проведение обследования информационной системы и системы защиты информации;

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

анализ 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 локальных нормативных правовых актов собственника (владельца) информационной системы на предмет их соответствия требованиям законодательства об информации, информатизации и защите информации, в том числе техническим нормативным правовым актам;

закрепление ответственности персонала за организацию и обеспечение выполнения требований по защите информации;

проведение испытаний системы защиты информации на предмет выполнения установленных требований безопасности и корректности функционирования данной системы;

проверку отсутствия либо невозможности использования нарушителем свойств программного обеспечения и (или) технических средств информационной системы (в том числе средств защиты информации), которые могут быть случайно инициированы (активированы) или умышленно использованы для нарушения информационной безопасности системы и сведения о которых подтверждены производителями (разработчиками) этого программного обеспечения и технических средств;

оформление технического отчета и протокола испытаний;

оформление аттестата соответствия.

При аттестации информационных систем, имеющих подключение к сетям электросвязи общего пользования (в том числе к глобальной компьютерной сети Интернет), проведение мероприятий, предусмотренных абзацами десятым и одиннадцатым части первой настоящего пункта, осуществляется с использованием средства контроля эффективности защищенности информации.

Допускается выполнение мероприятий, предусмотренных частью первой настоящего пункта, на выделенном наборе сегментов информационной системы, реализующих полную технологию обработки защищаемой информации.

9. Программа и методика аттестации разрабатываются на основании исходных данных и должны содержать перечень выполняемых работ, продолжительность их выполнения, перечень методов проверки требований безопасности, реализованных в системе защиты информации, а также перечень используемой контрольной аппаратуры и тестовых средств.

Программа и методика аттестации разрабатываются:

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

специализированной организацией – при проведении аттестации такой организацией. В данном случае специализированная организация согласовывает разработанные программу и методику аттестации с заявителем.

10. Срок проведения аттестации:

определяется руководителем 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 оформляется по форме согласно приложению 3 и подписывается:

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

руководителем специализированной организации – при проведении аттестации специализированной организацией.

Аттестат соответствия оформляется сроком на 5 лет.

12. Собственники (владельцы) информационных систем не позднее 10 календарных дней со дня оформления (получения) аттестата соответствия представляют в Оперативно-аналитический центр при Президенте Республики Беларусь копии этого аттестата, технического отчета и протоколов испытаний, а также иные сведения по форме согласно приложению 2 к Положению о порядке предоставления в Оперативно-аналитический центр при Президенте Республики Беларусь сведений о состоянии технической защиты информации, утвержденному 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; 28.08.2015, 7/3199).

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, место нахождения)

просит провести аттестацию системы защиты информации _____
(наименование

_____
информационной системы)

на соответствие требованиям по защите информации, предусмотренным приказом 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), и _____
(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) (фамилия, инициалы)

__ _____ 20__ г.

Главный бухгалтер _____ _____
(подпись) (фамилия, инициалы)

__ _____ 20__ г.

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 у собственника (владельца) информационной системы подразделения технической защиты информации или иного подразделения (должностного лица), выполняющего функции по технической и (или) криптографической защите информации.

3. Описание информационной системы, включающее общую функциональную схему, физические и логические границы, информационные потоки и протоколы обмена защищаемой информацией, а также места размещения элементов системы (аппаратных и программных) и средств защиты информации.

4. Документ, устанавливающий отнесение информационной системы к классу типовых информационных систем в порядке, установленном СТБ 34.101.30-2017 «Информационные технологии. Методы и средства безопасности. Информационные системы. Классификация».

5. Задание по безопасности или частное техническое задание на систему защиты информации.

6. Политика информационной безопасности организации.

7. Локальные нормативные правовые акты, направленные на реализацию политики информационной безопасности организации.

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

9. Основные характеристики инженерно-физических средств защиты, технических средств и систем охраны информационной системы, в том числе помещений, в которых обрабатывается защищаемая информация и хранятся носители 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 34.101.30-2017)
предусмотренным приказом 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), и _____
(наименование документов)
_____.

Аттестация выполнена в соответствии с программой, утвержденной __ _____ 20__ г., и методикой, 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 технологии обработки защищаемой информации и совокупности технических и организационных мер, реализованных при создании системы защиты информации информационной системы.

Руководитель организации

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

М.П.

__ _____ 20__ г.