ПРИКАЗ ОПЕРАТИВНО-АНАЛИТИЧЕСКОГО ЦЕНТРА ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ БЕЛАРУСЬ

30 августа 2013 г. № 62

О некоторых вопросах технической и криптографической защиты информации

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», 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

ПОЛОЖЕНИЕ
о порядке технической защиты информации в информационных системах, 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), 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 применяются 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 и техническими нормативными правовыми актами.

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

4. При создании систем защиты информации информационных систем применяются средства защиты информации, имеющие сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь, или положительное экспертное заключение по результатам государственной экспертизы (далее, если не определено иное, – сертифицированные или имеющие положительное экспертное заключение средства защиты информации).

5. Не допускается подключение информационных систем к информационным сетям, в том числе к глобальной компьютерной сети Интернет, без принятия мер по технической и (или) криптографической защите информации, предусмотренных настоящим Положением и иным законодательством в области технической и криптографической защиты информации.

6. Создание и эксплуатация системы защиты информации информационной системы осуществляются подразделением технической защиты информации или иным подразделением (должностным лицом), выполняющим функции по технической и (или) криптографической защите информации у собственника (владельца) информационной системы (далее – подразделение технической защиты информации).

В случае невозможности выполнения работ по созданию систем защиты информации информационных систем силами подразделения технической защиты информации собственниками (владельцами) информационных систем могут привлекаться организации, имеющие специальные разрешения (лицензии) на деятельность по технической и (или) криптографической защите информации в части соответствующих составляющих данный вид деятельности работ и услуг (далее – специализированные организации).

7. Комплекс мероприятий по созданию системы защиты информации информационной системы включает:

классификацию хранящихся и обрабатываемых в информационной системе сведений и разделение информации по категориям доступа;

анализ организационной структуры информационной системы, порядка организации вычислительных процессов и условий ее функционирования;

присвоение информационной системе класса типового объекта информатизации в соответствии с требованиями законодательства об информации, информатизации и защите информации;

разработку или корректировку политики информационной безопасности;

разработку или корректировку задания по безопасности на информационную систему в соответствии с требованиями законодательства об информации, информатизации и защите информации, в том числе технических нормативных правовых актов;

реализацию требований задания по безопасности на информационную систему.

Создание системы защиты информации информационной системы осуществляется до ввода информационной системы в эксплуатацию.

8. Политика информационной безопасности, представляющая собой совокупность действующих у собственника (владельца) информационной

системы документированных правил, процедур и требований в области защиты информации, должна содержать:

цели построения системы защиты информации информационной системы;

перечень защищаемых сведений;

определение ответственности субъектов информационных отношений за обеспечение защиты информации;

определение прав и порядка доступа к защищаемой информации (субъектам информационных отношений предоставляется объективно необходимый для них уровень доступа к защищаемым сведениям);

порядок работы с электронной почтой и другими системами обмена и передачи сообщений;

порядок применения средств технической и (или) криптографической защиты информации;

организационные мероприятия по разграничению доступа к средствам технической защиты и обработки информации;

порядок действий при возникновении угроз обеспечению целостности и конфиденциальности информационных ресурсов, в том числе чрезвычайных и непредотвратимых обстоятельств (непреодолимой силы), и при ликвидации их последствий;

инструкции для субъектов информационных отношений, регламентирующие порядок доступа к ресурсам информационной системы, установления подлинности субъектов, аудита безопасности, резервирования и уничтожения информации, контроля целостности защищаемых сведений, защиты от вредоносного программного обеспечения и вторжений.

9. Собственник (владелец) информационной системы организует разработку задания по безопасности на информационную систему, утверждает его и проводит оценку этого задания в организации, аккредитованной для проведения испытаний систем защиты информации информационных систем.

Задание по безопасности на информационную систему разрабатывается в соответствии с требованиями законодательства об информации, информатизации и защите информации, в том числе технических нормативных правовых актов, и учитывается в Оперативно-аналитическом центре при Президенте Республики Беларусь.

10. Ремонтные, наладочные и профилактические работы в информационных системах проводятся с участием представителя подразделения технической защиты информации.

В случае необходимости передачи технических средств для проведения ремонта из этих технических средств должны быть изъяты все носители информации, содержащие информацию, распространение и (или) предоставление которой ограничено, либо должно быть произведено

гарантированное уничтожение информации с использованием сертифицированных средств.

11. Для организации защиты информации нескольких взаимодействующих между собой информационных систем, функционирующих в общей программно-технической среде, может создаваться единая система защиты информации взаимодействующих информационных систем.

12. При внесении изменений, затрагивающих условия и технологию обработки защищаемой информации, собственником (владельцем) информационной системы проводятся мероприятия по доработке системы защиты информации информационной системы.

13. Текущий контроль за соблюдением требований по защите информации у собственника (владельца) информационной системы осуществляется подразделением технической защиты информации.

14. Нарушения требований по защите информации, предусмотренных заданием по безопасности на информационную систему и (или) политикой информационной безопасности, устанавливаются и фиксируются собственником (владельцем) информационной системы, который принимает меры по своевременному устранению выявленных нарушений.

О фактах нарушения требований по защите информации собственник (владелец) информационной системы в течение пяти рабочих дней с момента выявления этих нарушений письменно информирует Оперативно-аналитический центр при Президенте Республики Беларусь.

15. Запрещается обработка информации, распространение и (или) предоставление которой ограничено, в случае выявления нарушений требований по защите информации.

УТВЕРЖДЕНО
Приказ
Оперативно-аналитического
центра при Президенте
Республики Беларусь
30.08.2013 № 62

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 (далее – КЗИ):

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 термины и их определения применяются 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, Положением об отнесении объектов информатизации к критически важным и обеспечении безопасности критически важных объектов информатизации и техническими нормативными правовыми актами.

3. Решение об организации КЗИ принимается:

собственником (владельцем) информационных систем – при реализации комплекса мероприятий по созданию системы защиты информации на этапе разработки или корректировки политики информационной безопасности и задания по безопасности на данную систему;

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

владельцем КВОИ – при реализации комплекса мероприятий по созданию системы безопасности этих объектов.

К указанным работам собственники (владельцы) информационных систем могут привлекать организации, имеющие специальные разрешения (лицензии) на деятельность по технической и (или) криптографической защите информации в части составляющих данный вид деятельности работ по разработке средств КЗИ (далее – СКЗИ).

4. Системы защиты информации информационных систем, системы безопасности КВОИ и системы электронных документов ГИС должны включать в себя СКЗИ, реализующие криптографические операции в зависимости от задач безопасности, управление криптографическими ключами данных СКЗИ, а также комплекс средств обеспечения безопасности СКЗИ.

5. СКЗИ должны выполнять криптографические операции в соответствии с заданными криптографическими алгоритмами и криптографическими ключами, которые соответствуют техническим нормативным правовым актам и документам согласно приложению к настоящему Положению (далее – приложение), а при их отсутствии должны быть рекомендованы Оперативно-аналитическим центром при Президенте Республики Беларусь (далее – ОАЦ).

6. Для каждой криптографической операции, реализованной в СКЗИ, собственником (владельцем) информационной системы определяются требования по управлению криптографическими ключами, включающие 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 в соответствии с техническими

нормативными правовыми актами и документами согласно приложению, а при их отсутствии должны быть рекомендованы ОАЦ. 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, в документах по системе безопасности КВОИ и системе электронных документов ГИС.

7. Комплекс средств обеспечения безопасности СКЗИ должен обеспечивать:

защиту СКЗИ от несанкционированного воздействия или несанкционированного использования;

предотвращение несанкционированного раскрытия критических объектов СКЗИ;

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 средствам обеспечения безопасности СКЗИ должны основываться на технических нормативных правовых актах и документах согласно приложению, а при их отсутствии должны быть рекомендованы ОАЦ.

8. Организационные меры, которые необходимо соблюдать при эксплуатации СКЗИ, должны включать в себя меры по обеспечению особого режима допуска на территорию (в помещения), на которой может быть осуществлен доступ к СКЗИ и криптографическим ключам (носителям), а также меры по разграничению доступа к ним по кругу лиц. Данные организационные меры должны быть отражены в политике информационной безопасности.

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

Программные СКЗИ и программное обеспечение аппаратных СКЗИ должны соответствовать требованиям, установленным СТБ 34.101.27-2011 «Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации»,

а программно-аппаратные и технические СКЗИ – требованиям, установленным СТБ П 34.101.43-2009 «Информационные технологии. Методы и средства безопасности. Профиль защиты технических и программно-аппаратных средств криптографической защиты информации».

Для совместимости СКЗИ данные обмена между ними 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 безопасности СКЗИ. При этом механизмы управления криптографическими ключами и служебные механизмы должны соответствовать требованиям технических нормативных правовых актов и документов согласно таблице 1 приложения.

10. При принятии собственником (владельцем) информационной системы решения о применении СКЗИ для защиты служебной информации ограниченного распространения, определенной в соответствии с законодательством, должно обеспечиваться выполнение следующих организационных и технических мер:

криптографическая защита служебной информации ограниченного распространения должна осуществляться на отдельно выделенном средстве вычислительной техники, не подключенном к информационным сетям, 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;

использование в средствах криптографической защиты служебной информации ограниченного распространения криптографических алгоритмов, их долговременных параметров (в том числе длин ключей), рекомендованных ОАЦ;

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;

использование лицензионного антивирусного программного обеспечения и его периодическое обновление;

использование программно-аппаратных или технических СКЗИ, удовлетворяющих требованиям технических нормативных правовых актов или документов 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

ПЕРЕЧЕНЬ
технических нормативных правовых актов, на соответствие которым осуществляется сертификация средств криптографической защиты информации, и документов, на соответствие требованиям безопасности которых проводится государственная экспертиза средств 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
	Криптографические операции	
Ш	шифрование	

Условное обозначение	Криптографические механизмы	Наименование технических нормативных правовых актов и документов
Ш1		ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования» (раздел 3 или 4) 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 6.4 или 6.5 раздела 6)
И	имитозащита	
И1		ГОСТ 28147-89 (раздел 5)
И2		СТБ 34.101.31-2011 (подпункт 6.6 пункта 6)
ШИ	шифрование и имитозащита	СТБ 34.101.31-2011 (подпункт 6.7 пункта 6)
Х	хэширование	
Х1		СТБ 1176.1-99 «Информационная технология. Защита информации. Процедура хэширования»
Х2		СТБ 34.101.31-2011 (подпункт 6.9 пункта 6)
П	электронная цифровая подпись	
П1		СТБ 1176.1-99 СТБ 1176.2-99 «Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи» (разделы 5, 6) СТБ П 34.101.50-2012 (приложения Б, В)
П2		СТБ 34.101.31-2011 (подраздел 6.5 раздела 6) СТБ 34.101.45-2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых» (подпункт 7.1 пункта 7, приложение Б, таблица Б1, приложение Д)
К	управление криптографическими ключами	
К1	диверсификация ключа	СТБ 34.101.31-2011 (подпункт 7.2 пункта 7)
К2	обновление ключа	СТБ 34.101.31-2011 (подпункт 7.2 пункта 7)
К3	защита ключа на другом ключе	СТБ 34.101.31-2011 (подпункт 6.8 пункта 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)

Условное обозначение	Криптографические механизмы	Наименование технических нормативных правовых актов и документов
К52		СТБ 34.101.45-2013 (подпункт 7.2 пункта 7, приложение Б, таблица Б1)
К6	разделение ключа	СТБ 34.101.60-2013 «Информационные технологии и безопасность. Алгоритмы разделения секрета» (раздел 7, приложение А, таблица А1)
К7	генерация личного и открытого ключей	
К71		СТБ 1176.2-99 (разделы 5, 6, 7)
К72		СТБ 34.101.45-2013 (подпункт 6.2 пункта 6, приложение Б, таблица Б1)
К8	формирование общего ключа	
К81		Проект Руководящего документа Республики Беларусь «Банковские технологии. Протоколы формирования общего ключа»
К82		СТБ 34.101.66-2013 «Информационные технологии и безопасность. Протоколы аутентификации и выработки общего ключа на основе эллиптических кривых» (приложение А), СТБ 34.101.45-2013 (таблица Б1 (параметры))
С	управление сертификатами открытых ключей	
С1	запрос на выдачу сертификата	СТБ 34.101.17-2012 «Информационные технологии и безопасность. Синтаксис запроса на получение сертификата»
С2	распространение сертификата	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 (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)»
	служебные механизмы	
Г1	генерация случайных чисел	СТБ 34.101.27-2011 «Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации»
Г2	генерация псевдослучайных чисел	СТБ 34.101.47-2012 «Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел» (подпункт 6.2 пункта 6)

Таблица 2

Требования к средствам криптографической защиты информации

Класс средств криптографической защиты информации	Требования к криптографическим операциям	Требования к управлению ключами	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	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 рекомендованные Оперативно-аналитическим центром при Президенте Республики Беларусь	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, Г1 или Г2	СТБ 34.101.23-2012 (раздел 8)
Средства проверки ЭЦП, в том числе в соответствии	П1 или П2	С2, С3 или С4	СТБ 34.101.23-2012 (раздел 8)

Класс средств криптографической защиты информации	Требования к криптографическим операциям	Требования к управлению ключами	Требования к форматам зашифрованных или подписанных данных (в случае совместимости средств криптографической защиты информации)
с Законом Республики Беларусь «Об электронном документе и электронной цифровой подписи»			

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, С3 или С4, СТБ 34.101.23-2012.

УТВЕРЖДЕНО
Приказ
Оперативно-аналитического
центра при Президенте
Республики Беларусь
30.08.2013 № 62

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), 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 применяются 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 применяются следующие термины и их определения:

аттестат соответствия – документ установленной формы, подтверждающий выполнение требований законодательства об информации, информатизации и защите информации, в том числе технических нормативных правовых актов;

аттестация – комплекс организационно-технических мероприятий, в результате которых документально подтверждается соответствие системы защиты информации информационной системы требованиям законодательства об информации, информатизации и защите информации, в том числе технических нормативных правовых актов;

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

3. Аттестация систем защиты информации информационных систем (далее – система защиты информации) 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. Аттестация систем защиты информации проводится до ввода информационной системы в эксплуатацию.

5. Наличие аттестата соответствия является основанием для использования системы защиты информации на период, установленный в аттестате соответствия.

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

анализ исходных данных по аттестуемой системе защиты информации;

разработка программы аттестации;

предварительное ознакомление с информационной системой и системой защиты информации;

проведение обследования информационной системы и системы защиты информации;

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

проведение оценки системы защиты информации в реальных условиях эксплуатации информационной системы;

анализ документов, подтверждающих соответствие средств защиты информации требованиям, установленным для системы защиты информации, и принятие решения об оформлении аттестата соответствия;

оформление аттестата соответствия.

7. Расходы по проведению аттестации оплачиваются заявителем в соответствии с договором на проведение аттестации, заключенным между заявителем и специализированной организацией.

8. Затраты по аттестации вновь создаваемых или модернизируемых систем защиты информации включаются в общую смету расходов на их разработку (модернизацию).

9. Оперативно-аналитический центр при Президенте Республики Беларусь (далее – ОАЦ) ведет информационную базу аттестованных систем защиты информации.

10. Собственники (владельцы) информационных систем информируют ОАЦ об аттестованных в установленном порядке системах защиты информации.

11. Заявители:

осуществляют подготовку системы защиты информации для проведения аттестации путем реализации организационных и технических мер по защите информации;

привлекают на договорной основе специализированные организации для проведения аттестации системы защиты информации;

представляют документы и обеспечивают условия, необходимые для проведения аттестации системы защиты информации;

осуществляют эксплуатацию системы защиты информации;

извещают специализированные организации, которые провели аттестацию, обо всех изменениях в информационных технологиях, составе и размещении средств защиты информации, условиях их эксплуатации, которые могут повлиять на эффективность принятых мер по защите информации.

12. Аттестация проводится на основании заявки, подаваемой заявителем в специализированную организацию, по форме согласно приложению 1 и исходных данных согласно приложению 2.

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

13. Для проведения аттестации разрабатывается программа аттестации, которая должна содержать перечень выполняемых работ и их продолжительность, а также перечень используемой контрольной аппаратуры и тестовых средств.

14. Специализированная организация в течение 30 календарных дней с момента поступления заявки на проведение аттестации рассматривает ее и на основании анализа исходных данных разрабатывает программу аттестации, согласовывает ее с заявителем и принимает решение о проведении аттестации.

15. Специализированная организация представляет заявителю решение о проведении аттестации и после согласования программы аттестации высылает проект договора на аттестацию.

16. Оценка системы защиты информации включает:

анализ организационной структуры информационной системы, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения системы защиты информации, разработанной документации и ее соответствия требованиям нормативных правовых актов в области защиты информации, в том числе технических нормативных правовых актов;

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

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

оценку системы защиты информации в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации;

оформление протоколов испытаний (оценки) и заключения по результатам проверок.

17. При использовании в системах защиты информации средств криптографической защиты информации (далее – СКЗИ) должна проводиться оценка реализации криптографических операций, выполняемых СКЗИ, управления криптографическими ключами данных

СКЗИ, а также комплекса средств обеспечения безопасности СКЗИ в реальных условиях эксплуатации информационных систем (в том числе корректность их встраивания и применения). К проведению такой оценки привлекаются специализированные организации, область аккредитации которых включает соответствующие испытания.

18. По результатам аттестации оформляется аттестат соответствия.

19. Аттестация проводится до полного завершения всех проверок вне зависимости от промежуточных результатов испытаний. Если выявленные недостатки невозможно устранить в течение периода проведения аттестации, принимается решение об отказе в выдаче аттестата соответствия. Повторная аттестация специализированной организацией проводится после заключения отдельного договора на проведение работ по аттестации.

20. Аттестат соответствия подписывается руководителем организации – владельца государственной информационной системы либо руководителем специализированной организации, которая провела аттестацию, и заверяется печатью.

21. Аттестат соответствия на систему защиты информации, отвечающую требованиям по защите информации, выдается по форме согласно приложению 3.

22. Регистрация аттестатов соответствия осуществляется специализированной организацией в целях ведения информационной базы аттестованных систем защиты информации.

23. Сведения об аттестованных системах защиты информации представляются специализированной организацией (владельцем государственной информационной системы) в ОАЦ не позднее 30 дней со дня выдачи аттестата соответствия.

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

Владелец аттестованной системы защиты информации несет ответственность за функционирование системы защиты информации в соответствии с законодательством.

В случае изменения условий и технологии обработки защищаемой информации владельцы аттестованных систем защиты информации обязаны пройти повторную аттестацию системы защиты информации.

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, пункты)

Необходимые исходные данные по аттестуемой системе защиты информации прилагаются.

Заявитель готов предоставить необходимые документы и условия для проведения аттестации.

Заявитель согласен на договорной основе оплатить расходы по всем видам работ и услуг по аттестации.

Приложение:

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

Главный бухгалтер _____ _____
(подпись) (инициалы, фамилия)
_____ 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. Полное и точное наименование информационной системы, ее назначение.
2. Перечень информации, распространение и (или) предоставление которой ограничено.
3. Организационная структура информационной системы.
4. Правила разграничения доступа в информационной системе.
5. Модель нарушителя правил разграничения доступа в информационной системе.
6. Состав комплекса технических средств, на которых обрабатывается защищаемая информация.
7. Структура используемого программного обеспечения, предназначенного для обработки защищаемой информации, используемые протоколы обмена информацией.
8. Общая функциональная схема информационной системы, включая схему информационных потоков и режимы обработки защищаемой информации.
9. Сведения о наличии и характере взаимодействия с другими объектами.
10. Состав и структура системы защиты информации.
11. Сведения о разработчиках системы защиты информации.
12. Копии сертификатов соответствия либо экспертных заключений на средства защиты информации.
13. Основные характеристики средств физической защиты информационной системы (помещений, в которых обрабатывается защищаемая информация и хранятся информационные носители).
14. Документы, устанавливающие отнесение информационной системы к классу типовых объектов информатизации согласно СТБ 34.101.30-2007.
15. Задание по безопасности на информационную систему.

16. Проектная и эксплуатационная документация на систему защиты информации, другие данные, влияющие на обеспечение защиты информации.

17. Организационно-распорядительные документы, регламентирующие вопросы обеспечения защиты информации в информационной системе (выписки из документов), включая:

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

инструкцию по обеспечению защиты информации в информационной системе;

инструкцию о порядке применения средств защиты информации в информационной системе.

18. Программа проведения приемочных испытаний системы защиты информации.

19. Акт и протоколы приемочных испытаний системы защиты информации.

20. Протокол оценки задания по безопасности.

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
требованиям по защите информации
от __ _____ 20__ г. № _____

_____
(наименование информационной системы)
Действителен до __ _____ 20__ г.

Настоящим аттестатом удостоверяется, что система защиты информации _____
(наименование информационной системы)
класса _____
(по СТБ 34.101.30-2007)

соответствует следующим требованиям по защите информации:

_____

(наименование документов)

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

Результаты испытаний (оценки) приведены в протоколе от __ _____ 20__ г. № ____

С учетом результатов испытаний в информационной системе разрешается обработка следующей информации: _____

(перечень информации)

При эксплуатации информационной системы запрещается:

_____

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

Дополнительные сведения: _____

Руководитель организации

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

_____ 20___ г.