УКАЗ ПРЕЗИДЕНТА РЕСПУБЛИКИ БЕЛАРУСЬ
9 декабря 2019 г. № 449

О совершенствовании государственного регулирования в области защиты информации

В целях совершенствования государственного регулирования в сфере технической и криптографической защиты информации, повышения уровня национальной безопасности в информационной сфере п о с т а н о в л я ю:

1. Государственные органы и иные организации, осуществляющие деятельность с использованием государственных секретов, представляют в Оперативно-аналитический центр при Президенте Республики Беларусь сведения о состоянии технической защиты государственных секретов, если иное не предусмотрено законодательными актами. Перечень таких сведений и порядок их представления определяются Оперативно-аналитическим центром при Президенте Республики Беларусь.

2. Объекты информатизации, включенные в Государственный реестр критически важных объектов информатизации до вступления в силу настоящего Указа, сохраняют этот статус до их исключения из данного реестра по основаниям, предусмотренным Положением о порядке отнесения объектов информатизации к критически важным объектам информатизации, утвержденным Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196.

3. Внести изменения в следующие указы Президента Республики Беларусь:

3.1. пункт 2 Указа Президента Республики Беларусь от 25 октября 2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации» исключить;

3.2. в Указе Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации»:

пункт 1 изложить в следующей редакции:

«1. Утвердить:

Положение о технической и криптографической защите информации (прилагается);

Положение о порядке отнесения объектов информатизации к критически важным объектам информатизации (прилагается).»;

Положение о технической и криптографической защите информации в Республике Беларусь, утвержденное Указом, изложить в новой редакции (прилагается);

дополнить Указ Положением о порядке отнесения объектов информатизации к критически важным объектам информатизации (прилагается).

4. Совету Министров Республики Беларусь и Оперативно-аналитическому центру при Президенте Республики Беларусь в трехмесячный срок обеспечить приведение актов законодательства в соответствие с настоящим Указом.

5. Оперативно-аналитическому центру при Президенте Республики Беларусь в трехмесячный срок:

утвердить по согласованию с заинтересованными государственными органами показатели уровня вероятного ущерба национальным интересам Республики Беларусь в политической, экономической, социальной, информационной, экологической и иных сферах в случае создания угроз информационной безопасности либо в результате возникновения рисков информационной безопасности в отношении объекта информатизации, не предназначенного для проведения работ с использованием государственных секретов (его составляющих элементов);

принять иные меры по реализации настоящего Указа.

6. Государственным органам, иным государственным организациям, подчиненным (подотчетным) Президенту Республики Беларусь, республиканским органам государственного управления, иным государственным организациям, подчиненным Правительству Республики Беларусь, облисполкомам и Минскому горисполкому на основании критериев отнесения объектов информатизации к критически важным

объектам информатизации и показателей уровня вероятного ущерба национальным интересам Республики Беларусь в политической, экономической, социальной, информационной, экологической и иных сферах в шестимесячный срок:

определить из числа организаций, указанных в части второй пункта 6 Положения о порядке отнесения объектов информатизации к критически важным объектам информатизации, организации, объекты информатизации которых могут быть отнесены к критически важным объектам информатизации;

обеспечить составление указанными организациями заключений о соответствии объектов информатизации, определенных согласно абзацу второму настоящего пункта, критериям отнесения объектов информатизации к критически важным объектам информатизации и показателям уровня вероятного ущерба национальным интересам Республики Беларусь в политической, экономической, социальной, информационной, экологической и иных сферах.

7. Настоящий Указ вступает в силу в следующем порядке:

пункты 1–3 – через три месяца после его официального опубликования;

иные положения данного Указа – после его официального опубликования.

Президент Республики Беларусь **А.Лукашенко**

УТВЕРЖДЕНО

Указ Президента
Республики Беларусь
16.04.2013 № 196
(в редакции Указа Президента
Республики Беларусь
09.12.2019 № 449)

ПОЛОЖЕНИЕ
о технической и криптографической защите информации

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

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

2. Требования настоящего Положения не распространяются на объекты информатизации и информационные системы, предназначенные для обработки информации, содержащей государственные секреты.

3. Требования настоящего Положения обязательны для применения:

владельцами критически важных объектов информатизации;

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

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

собственниками (владельцами) информационных систем, в которых обрабатываются электронные документы;

государственными органами и иными государственными организациями, а также хозяйственными обществами, в уставных фондах которых 50 и более процентов акций

(долей) находится в собственности Республики Беларусь и (или) ее административно-территориальных единиц, являющимися собственниками (владельцами) информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено;

организациями, оказывающими услуги по распространению открытых ключей проверки электронной цифровой подписи, аккредитованными в Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь.

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

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

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

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

6. ОАЦ:

6.1. определяет приоритетные направления технической и криптографической защиты информации;

6.2. координирует деятельность государственных органов и иных организаций (далее – организации) по применению мер технической и криптографической защиты информации;

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

6.4. определяет порядок:

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

аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено (далее – аттестация систем защиты информации);

технической и криптографической защиты информации, обрабатываемой на критически важных объектах информатизации, в том числе порядок проведения аудита систем информационной безопасности критически важных объектов информатизации;

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

6.6. осуществляет:

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

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

6.7. выносит письменные требования (предписания) об устранении организациями выявленных нарушений настоящего Положения и иных нормативных правовых актов в сфере технической и криптографической защиты информации и (или) приостановлении

(прекращении) обработки информации в информационной системе или функционирования критически важного объекта информатизации;

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

6.9. осуществляет международное сотрудничество в сфере технической и криптографической защиты информации, в том числе взаимодействует с организациями иностранных государств и международными организациями, заключает в пределах своей компетенции международные договоры межведомственного характера;

6.10. разрабатывает проекты актов законодательства, в том числе обязательных для соблюдения технических нормативных правовых актов, и принимает такие акты по вопросам технической и криптографической защиты информации;

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

ГЛАВА 3
ОСНОВНЫЕ ПОЛОЖЕНИЯ ПО ОРГАНИЗАЦИИ ТЕХНИЧЕСКОЙ И КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

7. Организации – собственники (владельцы) информационных систем, владельцы критически важных объектов информатизации, организации, оказывающие услуги по распространению открытых ключей проверки электронной цифровой подписи, указанные в части первой пункта 3 настоящего Положения, в целях обеспечения технической и криптографической защиты информации:

7.1. обеспечивают проведение мероприятий по проектированию и созданию систем защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, в порядке, предусмотренном законодательством об информации, информатизации и защите информации;

7.2. организуют и проводят комплекс организационно-технических мероприятий по аттестации систем защиты информации;

7.3. организуют и проводят комплекс мероприятий по проектированию, созданию и аудиту систем информационной безопасности критически важных объектов информатизации;

7.4. организуют и проводят комплекс мероприятий по криптографической защите информации в информационных системах, в которых обрабатываются электронные документы;

7.5. организуют и проводят комплекс мероприятий по выполнению условий, на соответствие которым осуществляется аккредитация поставщиков услуг в Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь в соответствии с законодательством об электронном документе и электронной цифровой подписи;

7.6. осуществляют методическое руководство проведением мероприятий по технической и криптографической защите информации организациями, находящимися в их подчинении (входящими в их состав, систему), а также хозяйственными обществами, акции (доли в уставных фондах) которых принадлежат Республике Беларусь либо административно-территориальной единице и переданы в управление указанных организаций;

7.7. осуществляют сбор, анализ, хранение не менее одного года и представление в ОАЦ сведений о событиях информационной безопасности, в том числе о фактах возникновения угроз информационной безопасности критически важного объекта информатизации, нарушения или прекращения функционирования информационной

системы, нарушения конфиденциальности, целостности, подлинности, доступности и сохранности информации, в порядке и объемах, определяемых ОАЦ;

7.8. представляют в ОАЦ сведения о состоянии технической и криптографической защиты информации в порядке и объемах, определяемых ОАЦ.

8. Мероприятия по технической и криптографической защите информации, осуществляемые организациями, должны предусматривать:

в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, – защиту информации от несанкционированного доступа к ней и несанкционированного воздействия на нее, обеспечение целостности и подлинности обрабатываемой информации в порядке, установленном законодательством об информации, информатизации и защите информации;

в информационных системах, в которых обрабатываются электронные документы, – обеспечение целостности и подлинности данных документов;

на критически важных объектах информатизации:

предотвращение неправомерного доступа, уничтожения, модификации, копирования, предоставления и распространения информации, обрабатываемой на критически важном объекте информатизации;

обнаружение и предупреждение угроз информационной безопасности критически важного объекта информатизации и принятие мер по предупреждению и уменьшению рисков информационной безопасности;

недопущение реализации угроз информационной безопасности в отношении активов критически важного объекта информатизации, а также восстановление функционирования критически важного объекта информатизации в случае такого воздействия;

безопасное информационное взаимодействие критически важного объекта информатизации с иными информационными системами.

9. Работы по технической и криптографической защите информации в организации проводятся подразделением защиты информации или иным подразделением (должностным лицом), ответственным за обеспечение защиты информации. Работники такого подразделения (должностное лицо) должны иметь высшее образование в области защиты информации либо высшее или профессионально-техническое образование и пройти переподготовку или повышение квалификации по вопросам технической и криптографической защиты информации в порядке, установленном законодательством.

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

11. Аттестация систем защиты информации проводится до ввода в эксплуатацию информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено.

12. При передаче служебной информации ограниченного распространения по сетям электросвязи общего пользования данная информация должна быть защищена с использованием средств криптографической защиты информации, обеспечивающих линейное и (или) предварительное шифрование передаваемой информации.

Криптографическая защита служебной информации ограниченного распространения осуществляется только с применением программно-аппаратных средств криптографической защиты информации. Дополнительные организационные и технические меры по криптографической защите указанной информации определяются ОАЦ.

13. При осуществлении технической и криптографической защиты информации используются средства технической и криптографической защиты информации, имеющие сертификат соответствия Национальной системы подтверждения соответствия

Республики Беларусь или положительное экспертное заключение по результатам государственной экспертизы, проводимой ОАЦ.

14. Особенности криптографической защиты информации в информационных системах, в которых обрабатываются электронные документы, могут устанавливаться законодательством об электронном документе и электронной цифровой подписи. Дополнительные организационные и технические меры по криптографической защите информации в названных информационных системах определяются ОАЦ.

15. Руководитель организации несет персональную ответственность за организацию работ по технической и криптографической защите информации в организации.

ГЛАВА 4
ОСОБЕННОСТИ ТЕХНИЧЕСКОЙ И КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ НА КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ

16. Техническая и криптографическая защита информации, обрабатываемой на критически важных объектах информатизации, обеспечивается путем реализации владельцами критически важных объектов информатизации комплекса организационно-технических мероприятий по проектированию, созданию и аудиту систем информационной безопасности этих объектов, мониторингу угроз информационной безопасности, фактов возникновения рисков информационной безопасности и реагированию на них.

17. При реализации комплекса организационно-технических мероприятий по проектированию и созданию системы информационной безопасности критически важного объекта информатизации должны учитываться установленные законодательством, в том числе обязательными для соблюдения техническими нормативными правовыми актами, требования по обеспечению промышленной, пожарной, экологической, радиационной и иной безопасности при эксплуатации соответствующих объектов и (или) осуществлении технологических процессов.

18. Для проведения работ по технической и криптографической защите информации, обрабатываемой на критически важных объектах информатизации, в организации создается подразделение защиты информации или назначается уполномоченное должностное лицо. Работники такого подразделения (должностное лицо) должны иметь высшее образование в области защиты информации либо высшее или профессионально-техническое образование и пройти переподготовку или повышение квалификации по вопросам технической и криптографической защиты информации в порядке, установленном законодательством.

19. В целях определения соответствия системы информационной безопасности требованиям законодательства, в том числе обязательных для соблюдения технических нормативных правовых актов в сфере технической и криптографической защиты информации, проводится ее аудит.

Аудит системы информационной безопасности критически важного объекта информатизации проводится владельцем данного объекта информатизации не позднее чем через год после завершения мероприятий по созданию системы информационной безопасности и далее ежегодно.

Результаты аудита системы информационной безопасности критически важного объекта информатизации оформляются актом.

ГЛАВА 5
КОНТРОЛЬ ЗА ТЕХНИЧЕСКОЙ И КРИПТОГРАФИЧЕСКОЙ ЗАЩИТОЙ ИНФОРМАЦИИ

20. Контроль за технической и криптографической защитой информации (далее – контроль) проводится в целях проверки выполнения требований нормативных правовых актов в области технической и криптографической защиты информации организациями, указанными в части первой пункта 3 настоящего Положения.

Особенности контроля в организациях, оказывающих услуги по распространению открытых ключей проверки электронной цифровой подписи, аккредитованных в Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь, определяются ОАЦ.

21. Контроль осуществляется ОАЦ в форме проверок, проводимых в соответствии с планом проверок технической и криптографической защиты информации, утверждаемым начальником ОАЦ и размещаемым на официальном сайте ОАЦ в глобальной компьютерной сети Интернет не позднее 30 декабря года, предшествующего году проведения проверки.

Без включения в план, указанный в части первой настоящего пункта, проверки организаций могут назначаться начальником ОАЦ или его уполномоченным заместителем при наличии сведений, в том числе полученных от организации или физического лица, свидетельствующих о совершаемом (совершенном) нарушении требований нормативных правовых актов в сфере технической и криптографической защиты информации, о фактах возникновения предпосылок к несанкционированному распространению информации, распространение и (или) предоставление которой ограничено, в случаях возникновения рисков информационной безопасности, а также чрезвычайной ситуации техногенного характера по месту расположения критически важного объекта информатизации.

22. Для проведения проверки решением начальника ОАЦ или его уполномоченного заместителя назначается комиссия.

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

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

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

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

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

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

26. Проверочные мероприятия проводятся в присутствии определенных руководителем организации или его уполномоченным заместителем представителей этой организации.

27. В ходе проверки оцениваются:

27.1. наличие подразделения защиты информации или иного подразделения (должностного лица), ответственного за обеспечение защиты информации, их задачи и функции в части обеспечения технической и криптографической защиты информации;

27.2. наличие и содержание:

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

документов, определяющих порядок и содержащих результаты проведения мероприятий по созданию систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, аттестации указанных систем защиты информации, созданию систем информационной безопасности критически важных объектов информатизации и их аудиту;

27.3. эффективность и достаточность технических и криптографических мер защиты информации в реальных условиях эксплуатации.

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

29. По результатам проверки составляется акт в количестве не менее двух экземпляров с отражением в нем экспертной оценки соответствия принятых мер

по технической и криптографической защите информации требованиям законодательства, выявленных нарушений, недостатков и предложений по их устранению.

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

В течение трех рабочих дней после его составления первый экземпляр акта направляется в проверяемую организацию, второй – остается в ОАЦ.

30. В случае обнаружения нарушений требований законодательства, в том числе обязательных для соблюдения технических нормативных правовых актов в сфере технической и криптографической защиты информации, начальник ОАЦ или его уполномоченный заместитель выносит письменное требование (предписание) об устранении выявленных нарушений и (или) приостановлении (прекращении) обработки информации в информационной системе или функционирования критически важного объекта информатизации.

Об устранении нарушений организация письменно сообщает в ОАЦ в пределах срока, установленного в письменном требовании (предписании), который не может превышать шести месяцев.

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

О выполнении письменного требования (предписания) об устранении нарушений организация в сроки, установленные в этом требовании (предписании), письменно сообщает в ОАЦ с приложением подтверждающих документов, а также предоставляет ОАЦ возможность удостовериться на месте в устранении нарушений.

Решение о возобновлении обработки информации в соответствующих информационных системах или на соответствующих критически важных объектах информатизации принимается начальником ОАЦ или его уполномоченным заместителем после устранения нарушений, послуживших основанием вынесения письменного требования (предписания).

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

Обоснованность доводов, изложенных в возражениях, рассматривается ОАЦ не позднее десяти рабочих дней со дня их поступления. При необходимости по решению начальника ОАЦ для рассмотрения их обоснованности может быть назначена специальная комиссия. Результаты рассмотрения отражаются в письменном заключении, которое направляется в организацию.

32. Вынесенные по результатам проверки решения по акту проверки, письменное требование (предписание) об устранении нарушений и (или) приостановлении (прекращении) обработки информации в информационной системе или функционирования критически важного объекта информатизации, а также действия (бездействие) членов комиссии могут быть обжалованы организацией в суд в порядке, установленном законодательными актами.

ГЛАВА 6
ПОНЯТИЙНЫЙ АППАРАТ

33. Для целей настоящего Положения используемые термины имеют следующие значения:

активы критически важного объекта информатизации – входящие в состав критически важного объекта информатизации технические, программные, программно-аппаратные средства (в том числе средства защиты информации), обрабатываемая

информация, системы управления информационными, производственными и (или) технологическими процессами;

аудит системы информационной безопасности критически важного объекта информатизации – систематический, независимый и документированный процесс получения информации о деятельности владельца критически важного объекта информатизации по обеспечению информационной безопасности этого объекта информатизации и установлению степени соответствия выполнения требований, установленных законодательством, в том числе обязательными для соблюдения техническими нормативными правовыми актами;

владелец критически важного объекта информатизации – организация, в собственности, хозяйственном ведении или оперативном управлении которой находится критически важный объект информатизации;

информационная безопасность критически важного объекта информатизации – состояние защищенности активов критически важного объекта информатизации от угроз и рисков информационной безопасности критически важного объекта информатизации;

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

критически важный объект информатизации – объект информатизации, который на основании критериев отнесения объектов информатизации к критически важным объектам информатизации и показателей уровня вероятного ущерба национальным интересам Республики Беларусь в политической, экономической, социальной, информационной, экологической и иных сферах включен в Государственный реестр критически важных объектов информатизации;

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

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

объект информатизации – средства электронной вычислительной техники вместе с программным обеспечением, в том числе системы управления различного уровня и назначения, информационные системы и сети, автономные стационарные и персональные электронные вычислительные машины, используемые в соответствии с заданной информационной технологией, системы управления информационными, производственными и (или) технологическими процессами;

риск информационной безопасности критически важного объекта информатизации – вероятность реализации угроз информационной безопасности активам критически важного объекта информатизации, которая может повлечь нарушение или прекращение их функционирования;

система защиты информации – совокупность мер по защите информации, реализованных в информационной системе;

система информационной безопасности критически важного объекта информатизации – совокупность правовых, организационных и технических мер, направленных на обеспечение информационной безопасности критически важного объекта информатизации;

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

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

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

угроза информационной безопасности критически важного объекта информатизации – потенциальная или реально существующая возможность нанесения ущерба активам критически важного объекта информатизации, которая может повлечь нарушение или прекращение их функционирования.

УТВЕРЖДЕНО

Указ Президента
Республики Беларусь
16.04.2013 № 196
(в редакции Указа Президента
Республики Беларусь
09.12.2019 № 449)

ПОЛОЖЕНИЕ
о порядке отнесения объектов информатизации
к критически важным объектам информатизации

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1. В настоящем Положении определяется порядок отнесения объектов информатизации к критически важным объектам информатизации и исключения их из числа критически важных объектов информатизации.

2. Отнесение объектов информатизации к критически важным объектам информатизации осуществляется в целях выполнения владельцами критически важных объектов информатизации требований по обеспечению технической и криптографической защиты информации на данных объектах.

ГЛАВА 2
ПОРЯДОК ОТНЕСЕНИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ К КРИТИЧЕСКИ ВАЖНЫМ ОБЪЕКТАМ ИНФОРМАТИЗАЦИИ

3. Объект информатизации подлежит отнесению к критически важным при условии его соответствия критериям, перечисленным в пункте 5 настоящего Положения, и показателям уровня вероятного ущерба национальным интересам Республики Беларусь в политической, экономической, социальной, информационной, экологической и иных сферах (далее – показатели уровня вероятного ущерба) в случае создания угроз информационной безопасности либо в результате возникновения рисков информационной безопасности в отношении объекта информатизации (его составляющих элементов), утверждаемым ОАЦ по согласованию с заинтересованными государственными органами.

4. В целях накопления и хранения систематизированной информации о критически важных объектах информатизации, расположенных на территории Республики Беларусь, координации деятельности организаций по технической и криптографической защите информации, обрабатываемой на таких объектах, ОАЦ осуществляет ведение Государственного реестра критически важных объектов информатизации (далее – реестр).

Порядок ведения реестра и предоставления сведений из него определяется ОАЦ.

5. Критериями отнесения объектов информатизации к критически важным являются:

критерий социальной значимости – в отношении объектов информатизации, обеспечивающих жизнедеятельность населения (жилищно-коммунальное хозяйство, здравоохранение, образование, труд, занятость и социальная защита);

критерий экономической значимости – в отношении объектов информатизации, обеспечивающих функционирование объектов (организаций) основных отраслей

экономики и (или) иные важные экономические потребности, в том числе обеспечивающих проведение безналичных (межбанковских) расчетов, осуществляющих процессинг;

критерий экологической значимости – в отношении объектов информатизации, нарушение или прекращение функционирования которых может причинить ущерб окружающей среде;

критерий информационной значимости – в отношении объектов информатизации в области связи и средств массовой информации.

6. Для принятия решения об отнесении объекта информатизации к критически важным объектам информатизации владелец объекта информатизации составляет заключение о соответствии этого объекта критериям, перечисленным в пункте 5 настоящего Положения, и показателям уровня вероятного ущерба (далее – заключение) в двух экземплярах.

Один экземпляр заключения направляется:

в государственный орган (за исключением облисполкомов и Минского горисполкома) – в отношении объектов информатизации, находящихся в собственности, хозяйственном ведении или оперативном управлении подчиненных этому государственному органу (входящих в его состав, систему) организаций, а также хозяйственных обществ, акции (доли в уставных фондах) которых переданы в управление этого государственного органа либо находятся в хозяйственном ведении или оперативном управлении подчиненных этому государственному органу (входящих в его состав, систему) организаций;

в облисполком или Минский горисполком – в отношении объектов информатизации, находящихся в собственности, хозяйственном ведении или оперативном управлении организаций, имущество, акции (доли в уставных фондах) которых находятся в собственности соответствующей области, г. Минска, административно-территориальных единиц, входящих в состав территории этой области, г. Минска, а также объектов информатизации, находящихся в собственности, хозяйственном ведении или оперативном управлении иных организаций, не указанных в абзаце втором настоящей части, с местом нахождения на территории соответствующей области, г. Минска.

Второй экземпляр заключения направляется в ОАЦ в целях контроля принятия решения об отнесении объекта информатизации к критически важным объектам информатизации.

Заключение направляется в государственные органы, указанные в частях второй и третьей настоящего пункта, в течение трех рабочих дней со дня его составления.

Форма заключения определяется ОАЦ.

7. Не позднее десяти рабочих дней со дня поступления заключения государственный орган принимает решение об отнесении объекта информатизации к критически важным объектам информатизации.

Решение об отнесении объекта информатизации к критически важным объектам информатизации принимается в виде приказа (распоряжения) руководителем государственного органа или его уполномоченным заместителем.

О принятом решении государственный орган информирует владельца объекта информатизации в течение пяти рабочих дней со дня его принятия.

8. В случае, если владельцем объекта информатизации выступает непосредственно государственный орган, решение об отнесении такого объекта информатизации к критически важным объектам информатизации принимается руководителем (уполномоченным заместителем руководителя) этого государственного органа самостоятельно.

9. Государственные органы вправе по собственной инициативе рассмотреть вопрос о соответствии (несоответствии) объектов информатизации, указанных в части второй пункта 6 настоящего Положения, критериям отнесения объектов информатизации к критически важным, показателям уровня вероятного ущерба и принять решение об отнесении таких объектов к критически важным объектам информатизации.

10. Копия решения об отнесении объекта информатизации к критически важным объектам информатизации в течение пяти рабочих дней со дня его принятия направляется государственным органом в ОАЦ для включения объекта информатизации в реестр.

ОАЦ в течение пяти рабочих дней со дня получения копии решения государственного органа об отнесении объекта информатизации к критически важным объектам информатизации включает этот объект информатизации в реестр.

11. Объект информатизации считается отнесенным к критически важным объектам информатизации со дня его включения в реестр.

12. На основании информации, содержащейся в открытом доступе, а также полученной от государственных органов, владельцев объектов информатизации, ОАЦ вправе вынести письменное требование (предписание) об отнесении соответствующего объекта информатизации к критически важным объектам информатизации.

Письменное требование (предписание) об отнесении соответствующего объекта информатизации к критически важным объектам информатизации направляется владельцу объекта информатизации.

Владелец объекта информатизации, получивший письменное требование (предписание) о необходимости отнесения соответствующего объекта информатизации к критически важным объектам информатизации, в месячный срок со дня получения этого требования (предписания) обязан совершить действия, определенные в пункте 6 или 8 настоящего Положения.

13. Владельцы критически важных объектов информатизации:

в течение шести месяцев со дня принятия решения об отнесении объекта информатизации к критически важным осуществляют проектирование и создание системы информационной безопасности;

в течение пяти рабочих дней со дня создания системы информационной безопасности информируют об этом ОАЦ.

14. В связи с проведением владельцем критически важных объектов информатизации мероприятий правового, организационного или технического характера два и более критически важных объекта информатизации могут быть объединены в один критически важный объект информатизации.

Об объединении двух и более критически важных объектов информатизации в один критически важный объект информатизации владелец этих объектов составляет заключение по форме, определяемой ОАЦ, и в течение трех рабочих дней со дня его составления направляет данное заключение в государственный орган, принявший решение об отнесении этих объектов к критически важным объектам информатизации.

Не позднее десяти рабочих дней со дня поступления заключения государственный орган принимает решение об объединении критически важных объектов информатизации.

Решение об объединении критически важных объектов информатизации принимается в виде приказа (распоряжения) руководителем государственного органа или его уполномоченным заместителем.

О принятом решении государственный орган информирует владельца критически важных объектов информатизации в течение пяти рабочих дней со дня его принятия.

Копия решения об объединении критически важных объектов информатизации в течение пяти рабочих дней со дня его принятия направляется государственным органом в ОАЦ для внесения соответствующих изменений в реестр.

ГЛАВА 3
ИСКЛЮЧЕНИЕ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ ИЗ ЧИСЛА КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

15. Исключение объектов информатизации из числа критически важных объектов информатизации осуществляется в порядке, предусмотренном для отнесения таких объектов к критически важным объектам информатизации, с учетом особенностей, установленных в настоящей главе.

16. Исключение объекта информатизации из числа критически важных объектов информатизации осуществляется по согласованию с ОАЦ в следующих случаях:

если критически важный объект информатизации в процессе его эксплуатации перестал удовлетворять критериям, перечисленным в пункте 5 настоящего Положения, и показателям уровня вероятного ущерба;

прекращения эксплуатации критически важного объекта информатизации.

Для согласования вопроса об исключении объекта информатизации из числа критически важных объектов информатизации государственный орган направляет в ОАЦ письмо с обоснованием необходимости принятия такого решения.

17. В решении государственного органа об исключении объекта информатизации из числа критически важных объектов информатизации должна быть указана причина принятия такого решения в соответствии с пунктом 16 настоящего Положения.

18. Объект информатизации считается исключенным из числа критически важных объектов информатизации со дня его исключения из реестра.

ГЛАВА 4
ПОНЯТИЙНЫЙ АППАРАТ

19. Для целей настоящего Положения используемые термины имеют следующие значения:

владелец объекта информатизации – организация, в собственности, хозяйственном ведении или оперативном управлении которой находится объект информатизации;

государственный орган – государственный орган, иная государственная организация, подчиненные (подотчетные) Президенту Республики Беларусь, республиканский орган государственного управления, иная государственная организация, подчиненные Правительству Республики Беларусь, облисполкомы и Минский горисполком.